

CTR 教室 Windows システムについて

浜 正 樹

要 旨

2004年度夏季に、情報リテラシー教育やデザイン教育など外国語学部・経営学部・短期大学のカリキュラムを実現するために、Windows 端末および Macintosh 端末から構成される CTR 教室システムを構築した。要件としては、Windows と Macintosh 双方に対し、クライアント/サーバシステムによる統合認証・ファイル共有・個人別デスクトップ環境を実現した。また、運用面では、教育面で利便性の高い教材提示フォルダや課題提出フォルダなどの従来からのサービスを継続し、更に授業支援ツールや印刷枚数制限システムなどの導入を行っている。特に、Windows 教室では、初期環境設定の自動化や安全なセキュリティ設定の提供を行って、初心者でもストレスなく利用が可能なシステムを構築している。本稿では、Windows 教室システムを中心に、その仕様および運用について報告する。

はじめに

2004年度夏季に、本郷キャンパスでは、ネットワークおよび教育用コンピュータシステムのリプレースを行った。2005年度の紀要では、リプレース後の本郷キャンパスネットワークについて、その設計理念や仕様について報告した。

CTR 教室システムの構築にあたっては、情報処理教育カリキュラム実現や学生の創造力を伸ばせる柔軟な環境の提供を主目的にした。特に、パソコン初心者の多い本学の学生に対し、ストレスなくシステム利用を可能にするために、綿密な設計と構築を行っている。本稿の構成は、以下の通りである。

I 章では、CTR 教室を構成するクライアントとサーバについて、そのハードウェア構成や配置などの概要を述べる。

II 章では、本学の認証システムに採用している Active Directory についての概略と実環境での構成について述べる。

III 章では、Windows クライアントの運用について、ログオンスクリプト、グループポリシーといった運用技術の概要にふれ、本学のユーザーに合わせて CTR 教室システムで設定されている項目について説明する。また、インターネットセキュリティの確保において、「セキュ

「クライアント」の概念についてもふれる。

I 章. システム構成概要

1 節. サーバ構成

本学の CTR 教室では、クライアント/サーバシステムを採用し、Active Directory サービス、認証サービス、ファイル共有サービス、プリントサービス、移動プロファイルサービス、Hotfix 配布サービス、ウイルス対策サービス、印刷枚数制限サービス、WebDAV サービス、時刻同期サービス、tftp サービスなどを提供している。

上記のサービスを提供しているサーバ群は、次の表 1 に示す構成になっている。

ホスト名	ハードウェア	用途
mdc	HP ProLiant DL360G3	CTR 教室システム認証サーバ
		Hotfix 配信サーバ
		印刷枚数ログ管理サーバ
		TFTP サーバ (CTR2/3/4向け)
dc1	HP ProLiant DL360G3	CTR 教室システム認証サーバ
		TFTP サーバ (CTR1/5向け)
dc2	HP ProLiant DL360G3	CTR 教室システム認証サーバ
fs1	HP StorageWorks NAS4000s	ファイルサーバ
		プリントサーバ
fs3	HP ProLiant DL360G3	プロファイルサーバ
adml	HP ProLiant DL360G3	アンチウイルスサーバ
		印刷枚数ログ取得サーバ
		TFTP サーバ (S-CTR 向け)
hoffer	HP ProLiant DL360G3	バックアップサーバ
sma	HP StorageWorks Management Appliance III	ストレージマネジメントサーバ

(2006/10/08現在)

表 1 サーバ構成

上記のサーバ群は、すべて B 館 2F サーバ室に設置され、集中管理されている。特に、後述する SAN Boot と呼ばれる特殊な方法で、すべてのサーバのシステムドライブを、1 台のストレージサーバに集約し、メンテナンスコスト削減に大きく寄与している。

2 節. クライアント端末の配置

クライアント端末は、Windows 端末と Macintosh 端末の 2 種類であり、次の表 2 に示す配置となっている。

教室名	場所	OS	台数	ハードウェア
CTR1	B 館 1F	Windows XP SP2	32	hp Compaq d530 SFF
CTR2	B 館 2F	Windows XP SP2	41	hp Compaq d530 SFF
CTR3	B 館 3F	Windows XP SP2	24	hp Compaq d530 SFF
CTR4	B 館 3F	Windows XP SP2	24	hp Compaq d530 SFF
CTR5	B 館 3F	Windows XP SP2	57	hp Compaq d530 SFF
CTR6	B 館 3F	Mac OS X 10.3	44	Power Mac G5
自習室	S 館 7F	Windows XP SP2	24	Fujitsu FMV7000FL

(2006/10/08現在)

表 2 クライアント端末のハードウェア仕様と配置

なお、上記の他に、2005年度秋季より外国語学研究科の大学院生室(B 館 5 F) にも、Windows 端末 (Epson Endeavor MR2000) を 5 台提供しており、後述する CTR 教室の Active Directory に参加させ、本稿で述べる Windows 教室システムと同様のユーザー環境を提供している。

II 章. 認証システム

1 節. 認証システムの概要

CTR 教室の端末では、利用時にログオン認証を行い、共有ファイルや個人所有データへのアクセスをコントロールしている。その認証を行うスキームとしては、Active Directory⁽¹⁾を採用している。

Active Directory とは、Microsoft が提供するディレクトリサービスである。ディレクトリとは、ユーザー、グループ、コンピュータ、ドメイン、組織単位、およびセキュリティポリシーなど、コンピュータシステム全体を管理する上で必要なオブジェクトについての情報を登録するデータ領域である。ディレクトリサービスは、これらディレクトリの持つ情報をネットワーク上に公開し、ユーザーおよびシステム管理者の利用を可能にするサービスである。Active Directory は、主に Windows 2000 Server 以降のサーバ OS で採用されている。更に、次節で述べるように Windows 以外の OS からのディレクトリ参照にも答えることが可能であるため、本学のように Windows, Macintosh, UNIX など様々な OS から構成されたシステムの認証基盤としては適していると言える。

2 節. Active Directory の概要

ディレクトリサービスとして、著名なものに LDAP と呼ばれる仕様がある。LDAP は、1988年に国際標準化機構 (ISO) および国際電気通信連合 (ITU) によって発表された X.500 仕様が基になっている。X.500では、ユーザーおよびアプリケーションが参照・検索するディレクトリを、階層的な構造を持つオブジェクトとして定義し、それぞれのオブジェクトには、各種属性が定義されている。この X.500は、不要な機能とクライアント側の処理の複雑さがネックとなり、普及しなかったという問題があった。その後、1993年にミシガン大学で、X.500 クライアントのゲイトウェイサービスとして LDAP が開発された。更に、1994年には、X.500 の仕様から離れて、簡略化されたディレクトリサービスとして仕様の修正が行われた。

その後、LDAP は、TCP/IP による通信方法を採用し、様々な修正を加えて、1997年にインターネット技術標準化委員会 (IETF) から LDAP v3⁽²⁾ として発表された。現在は、ディレクトリサービスのデファクトスタンダードとして定着している。

Active Directory は、LDAP に準拠して Microsoft が独自に実装したディレクトリサービスである。DNS や Microsoft Network を統合した点にも特長があり、Windows NT で構成されたレガシーネットワークからの移行も可能である。更に、ディレクトリサービスの提供のみならず、グループポリシーなど Windows 端末の集中管理機能も有するため、大学における教室システムの運用にも非常に有益なサービスである。

3 節. Active Directory の構成

Active Directory を提供するためには、ドメインと呼ばれる DNS のグループを構成する必要がある。本学の CTR 教室では、mdc, dc1, dc2の3台のサーバ機で、Windows Server 2003をドメインコントローラとして稼働させて、Active Directory を提供している。

また、Active Directory のディレクトリとして、以下の表3に示す構成を採用している。なお、OU (Organizational Unit) は、Active Directory を構成する最小の組織単位であり、セキュリティや管理ポリシーのための最小の範囲として機能する。

また、2 節で述べたように、Active Directory は、認証の標準プロトコルである LDAP に準拠しているため、Mac OS X からの認証サービスにも利用している。

Active Directory (LDAP) を利用して、クライアントが参照するディレクトリの構造と内容の規則を記述したファイルをスキーマと呼ぶ。スキーマには、ホームディレクトリのパスやユーザーのメールアドレスなど運用に必要な情報の構造が定義される。従来、Mac OS X から Active Directory の認証機能を利用する際には、このスキーマの拡張が必要であった。Mac OS X 10.3からは、スキーマの拡張は不要になったにも拘らず、Mac OS X 10.4では、クライアントのシェルの情報を別途与える必要があり、スキーマや端末側の属性のマッピングに工夫が必要となっている。

このように、異種 OS 間でのクライアント/サーバシステムの構成には、精密なチューニン

ad.u-bunkyo.ac.jp (Active Directory を提供するドメイン)
BGU(OU)
BA(OU)：経営学部
ELL(OU)：短期大学
FS(OU)：外国語学部
Teachers(OU)：教職員
Builtin
Computers：メンバサーバ/クライアントマスター
CTRs(OU)
CTR1(OU)：B館 CTR1 のコンピュータアカウント
CTR2(OU)：B館 CTR2 のコンピュータアカウント
CTR3(OU)：B館 CTR3 のコンピュータアカウント
CTR4(OU)：B館 CTR4 のコンピュータアカウント
CTR5(OU)：B館 CTR5 のコンピュータアカウント
S-CTR(OU)：S館自習室のコンピュータアカウント
Domain Controllers(OU)：ドメインコントローラ
ForeignSecurityPrincipals
nfsshareformac：B館 CTR6 Macintosh 用 NFS サービス
Users：administrator 等のポリシーを適用しないユーザやグループ

(2006/10/08現在)

表 3 Active Directory の OU 構成

グが必要となることが多い。

4 節. 問題点

Active Directory は、登場以来 6 年が経ち、クライアント/サーバシステムの認証サービスとして、OS のログイン認証やメールソフトからのディレクトリ参照など、典型的な応用は定着してきている。しかし、一部のサービスやアプリケーションの利用に障害を起こすこともある。本学の CTR 教育システムでも、以下の表 4 に挙げる障害が発生している。この問題につ

OS	アプリケーション	障害
Mac OS X 10.3/10.4	Flash	Publish 機能が使えない
Mac OS X 10.4	Illustrator	作成ファイルの保存時に仮想ドライブが不可視
Mac OS X 10.4	Photoshop	作成ファイルの保存時に仮想ドライブが不可視

表 4 Macintosh アプリケーション障害一覧

いては、システム全体の仕様変更も視野に入れて、来年度に向けた改善策を検討している。

III章. Windows クライアントの運用

1 節. 基本方針

CTR 教室システム構築の主目的は、外国語学部・経営学部・短期大学の情報リテラシー教育環境や課外活動での柔軟な利用環境を提供することである。そのため、Windows 端末には単なるアプリケーションのインストールだけではなく、システム全体で以下の要件を実現している。

- 1) 初回ログオン時から、ユーザー個人別の初期設定が完了している
- 2) ユーザー自身が柔軟に設定できるデスクトップ環境の提供
- 3) セキュアなインターネット環境の提供

本学の学生の場合、パソコン初心者も多いため、アプリケーションの初期設定などで躓くケースが多い。実際に、筆者が着任した2000年当時の Windows システムでは、Internet Explorer やメールソフトが未設定であり、学生にその設定方法を指導していた。ところが、この設定作業に失敗し、1年間経っても肝心のアプリケーションの利用自体ができないケースも散見された。そこで、要件 1) を、次節で述べるログオンスクリプトなどの技術を用いて実現した。

また、学生数の多い大規模な大学では、教育システムのメンテナンス性を重視して、固定されたデスクトップ環境を提供し、学生自身の行う設定変更を許可しないケースも多い。しかし、これでは、授業時間外の学生の自由な創造力の育成を妨げることになるとも考えられるため、本学では、要件 2) を実現して個人別のデスクトップ環境を提供している。その実現には、「移動ユーザープロファイル」と呼ばれる仕組みを用いている。移動ユーザープロファイルは、Windows 95から原型が実装されている。ユーザーは、認証成功後、プロファイルサーバ(fs3)から、プロファイルと呼ばれる個人環境の設定情報を記述したファイルおよび個人データフォルダを取得し、ログオンした端末に自動的にコピーすることで個人環境の復元を可能にする。プロファイルは、端末からのログオフ時にプロファイルサーバにコピーされ、次のログオン時に再利用される。

最近では、ウイルス対策も定着し珍しくなくなったが、筆者は、大学で提供するシステムは、要件 3) を満たして家庭でのパソコン環境よりも安全性が高くならなければならないと考えている。特に、本学のユーザーのように、インターネット利用のほとんどが Web 閲覧や電子メール利用である場合には、Web ブラウザやメールソフトの安全性についても注意を払う必要がある。この要件 3) については、グループポリシーなどの技術を用いて実現する。

2 節. ログオンスクリプト

ログオンスクリプトとは、認証の成功したユーザーのログオン時に、バックグラウンドで実

施される環境設定処理を記述したスクリプトである。ユーザー別に異なる処理を行うことも可能である。本学で設定しているログオンスクリプトでは、ユーザーがCTR教室のWindowsクライアントにログオンした場合、初回利用であるかどうかを判定した上で、以下の処理を行う。

1) 初回ログオン時のみの処理

- i) Outlook Express アカウント情報の設定
- ii) IME 辞書ファイルの設定
- iii) Office の作成者の設定
- iv) 各アプリケーションの初期設定および保存先設定

2) ログオン時に常に実行される処理

- i) ネットワークドライブをマウント
- ii) プリンタの登録
- iii) ネットワークドライブ表示名の変更
- iv) シャットダウン操作の指定 ([ログオフ]/[シャットダウン] の選択)
- v) アドレス帳の復元
- vi) IME 辞書の復元
- vii) 各アプリケーション設定ファイルの復元

上記1) の処理により、ユーザーは初回ログオン時から、アプリケーションの初期設定が完了しており、ファイルの保存先も自動的にユーザーのマイドキュメントに指定される。即ち、初心者でも、まるで自分専用のパソコンのように環境設定がなされ、快適にアプリケーションを利用できるのである。

各アプリケーションの初期設定や保存先の設定には、ログオンスクリプトの実行やプロファイルの編集を行うが、その過程でレジストリと呼ばれる特殊なファイルの書換えを行う。レジストリとは、Windows OS 独自の中央階層型データベースであり、Windows 端末の詳細なシステム設定情報が含まれている。レジストリの編集作業には、高度な知識と非常に精密な調査が必要であり、情報教育研究センターで半期毎に行う教室システムの更新作業の中でも最もタイムコストの掛かる仕事の一つである。

3 節. グループポリシーの概要

グループポリシーとは、Microsoft から提供されている Windows 端末の集中管理機能である。Windows NT Server 4.0で実装された「システムポリシー」の後継機能であり、Windows 2000 Server から登場した。その実装は、Windows 端末のレジストリを、サーバ側から

一括して書き換える機能などを提供するものである。グループポリシーの適用のためには、Windows 端末は Active Directory への参加が必須となる。

グループポリシーで適用できる設定事項は、以下の通りである。

- 1) セキュリティ設定
- 2) ソフトウェアの配布
- 3) スタートアップ/シャットダウンスクリプト
 - ※端末の起動/停止時に実行されるスクリプト処理の指定
- 4) Internet Explorer の設定
- 5) フォルダのファイルサーバへのリダイレクト
 - ※プロファイルや端末ローカルに保存されるフォルダを、ホームフォルダへリダイレクトさせる機能

グループポリシーの設定項目は、「コンピュータの構成」と「ユーザーの構成」の2種類に分かれており、それぞれ以下に示すレジストリキーに設定が保存される。

設定項目	レジストリキー
コンピュータの構成	HKEY_LOCAL_MACHINE¥Microsoft¥Windows¥CurrentVersion¥Policies
ユーザーの構成	HKEY_CURRENT_USER¥Software¥Policies

表 5 グループポリシーのレジストリキー

ユーザーには、これらのキーの読み取りだけが可能で、勝手に編集することはできない。適用のタイミングは、以下の通りである。

ポリシー	適用のタイミング
コンピュータの構成	コンピュータの起動時
ユーザーの構成	ユーザーのログオン時

表 6 ポリシーの適用タイミング

また、グループポリシーの設定項目に含まれていないものも、対応するレジストリキーを把握すれば、カスタムポリシーとして独自に設定可能である。

4 節. グループポリシーの構成

教室システムを設計する上で、2 節で記述したログオンスクリプトと 3 節で述べたグループポリシーを併用して、ユーザーにどのような環境を提供するかという点は、教育システムの根

幹をなす問題である。その意味で、グループポリシーの設定項目は非常に重要な検討事項である。特に、セキュリティ面での設定やアプリケーションの初期設定等、初学者には敷居の高い項目を最適な設定値にして提供しなければならない。

本稿では、グループポリシーの設定全体については割愛するが、特に重要な設定項目については、以下の表7および表8に示し、その概要を述べる。

1) コンピュータの構成

ポリシー項目	デフォルト	設定
1. アカウントロックアウトポリシー		
a) アカウントロックアウトのしきい値 ⁱ⁾	0回	15回
b) ロックアカウントのリセット	未構成	30分
2. ローカルポリシー セキュリティオプション		
a) シャットダウン：仮想メモリのページファイルをクリアする ⁱⁱ⁾	未構成	有効
b) 対話型ログオン：最後のユーザー名を表示しない	未構成	有効
3. Windows Messenger		
a) Windows Messenger の実行を許可しない	未構成	有効
4. システム		
a) ログオンスクリプトを同期的に実行する ⁱⁱⁱ⁾	未構成	有効

表7 グループポリシー設定項目1

- i) ログオン失敗回数の上限を決める項目である。デフォルトでは、無制限(0回)になっているが、これでは短時間に何度もログオン試行が可能となってしまい、セキュリティ上の問題がある。一方で、4月に新入生を迎えるとログオンの失敗も増えるため、ある程度余裕を持った上限値に設定している。
- ii) メモリが不足した場合、ハードディスク上にデータをページファイルとして退避する場合がある。このページファイルを読み取られると、場合によっては、プライバシー情報が漏れることもある。したがって、シャットダウン時に、そのデータを削除することが妥当である。
- iii) この設定を有効にすることで、ログオンスクリプトの処理が終了してから、エクスプローラの起動が可能となる。本学のログオンスクリプトでは、ドライブのマウントや初期設定が多く含まれるため、この設定を有効にしてユーザーの環境の安定性を確保している。但し、デスクトップの利用開始が遅くなるという欠点もある。

2) ユーザーの構成

ポリシー項目	デフォルト	設定
1. パスワードポリシー		
a) パスワードの変更禁止期間 ⁱ⁾	1日	0日
2. Internet Explorer		
a) インターネット一時ファイルの設定変更を許可しない	未構成	有効
b) プロキシ設定の変更を許可しない ⁱⁱ⁾	未構成	有効
c) ブラウザの表示メニューの全画面表示コマンドを許可しない	未構成	有効
d) ブラウザのツールバーの変更を許可しない	未構成	有効
3. エクスプローラ		
a) 移動プロファイル使用中にシェルのショートカットを追跡しない ⁱⁱⁱ⁾	未構成	有効
b) 縮小表示の画像のキャッシュをオフにする	未構成	有効
4. タスクバーと「スタート」メニュー		
a) タスクバーと「スタート」メニューの設定を変更できないようにする	未構成	有効
5. デスクトップ		
a) 「ゴミ箱」のコンテキストメニューから「プロパティ」を削除する ^{iv)}	未構成	有効
6. コントロールパネル		
a) 指定されたコントロールパネルの項目のみを表示する ^{v)}	未構成	有効
b) 画面の「設定」タブを非表示にする ^{vi)}	未構成	有効

表 8 グループポリシー設定項目 2

- i) デフォルトでは、ユーザーのパスワードは設定後、1日間の変更が禁止されている。この設定により、「ユーザーがパスワード変更時に古いパスワードに戻す」というセキュリティ上問題のある使い方を回避するという想定である。しかし、本学の運用上、登録したばかりの新入生ユーザーにパスワードの変更を行わせる場合もあるため、変更禁止期間を0日にしている。
- ii) 本学では、ネットワーク負荷の軽減と不正アクセス防止法などのコンプライアンスを想定して、CTR 教室からの Web 閲覧は、すべてプロキシを経由することになっている。プロキシの経由措置は、ユーザー全員に徹底しなければ意義がないため、プロキシ設定の変更を許可しないようにしている。
- iii) 教育機関では、ソフトウェア仕様の同じ端末を大量に設置する必要がある。そのため、雛形となるパソコンを作成して、その複製イメージをすべての端末に展開することが常套手段となっている。このような方法で教室システムを構築した場合、シェルのショートカット追跡を許可すると、雛形となったパソコンのシェルを起動しようとして、非常に大きな混乱を来す。

- iv) ゴミ箱のコンテキストメニューでは、ゴミ箱の容量を調節できる。しかし、ゴミ箱の容量は、ユーザーが自由に変更するべきではない。システム提供側で適切な容量を決定し、ハードディスク消費に無駄のない運用を行うことが肝要である。
- v) コントロールパネルは、端末の様々な設定を変更するためのインターフェースである。パソコンの設定を保持し、常に安定した状態におくためには、コントロールパネルの利用を禁止することが、一番確実な方法である。しかし、就職試験などで、操作経験を問われるなど、コントロールパネルそのものは常識として定着しつつある。そこで、一般ユーザーでは変更できない項目のみ不可視にするという措置を行っている。
- vi) 背景画像などの画面の変更は、ユーザーにとって創造力を刺激するカスタマイズである。しかし「画面の設定」には、解像度や色数など変更されては他のユーザーにも影響のある設定項目が並んでいる。そこで、「設定」タブ自体を非表示にしている。

システムを構築する上で重要な設計思想として「FoolProof」と呼ばれる概念がある。FoolProofとは、コンピュータなどのシステムについて、人間が誤って操作した際にも致命的な障害が起こらないようにする設計とその実装のことを指す。本節で示したセキュリティ設定やインターフェースの制限は、グループポリシーを通して、FoolProofを実現したとも考えられる。

また、本学では、上記の安全性を考慮した設定を提供する他に、SUSと呼ばれる Hotfix 配布システムを用いて脆弱性の修正を迅速に行っている。この SUS は、グループポリシーとの併用によって、定期的な配布作業を自動化している。

5 節. インターネットセキュリティの確保

1 節の基本方針で述べたように、Web ブラウザやメールソフトのセキュリティについても安全性の考慮が必要である。一般に Windows のデフォルト設定では、Internet Explorer や Outlook Express にセキュリティ面で問題のあることが多い。筆者は、ユーザーのインターネットセキュリティの確保のため、本学として適切なセキュリティ設定を施した環境を提供することが、大学におけるシステム構築の重要な点の一つと位置づけている。

CTR 教室では、以下の設定を独自にカスタムポリシーとして実装し、グループポリシーを利用して、すべてのユーザーに適用している。

1) Internet Explorer 詳細設定

ポリシー項目	デフォルト	設定
1. HTTP1.1設定		
a) HTTP1.1を使用する ⁱ⁾	—	有効

b) プロキシ接続で HTTP1.1 を接続する	—	有効
2. セキュリティ		
a) SSL/TLS プロトコルの構成	—	有効
b) サーバ証明書の取り消しを確認する ii)	—	有効
c) ダウンロードしたプログラムの署名を確認する iii)	—	有効
d) ブラウザを閉じたとき、[Temporary Internet Files] フォルダを空にする iv)	—	有効

表9 Internet Explorer 詳細設定項目

- i) 従来普及していた HTTP1.0 よりも、永続的な接続や分散処理といった機能を追加した HTTP1.1 の使用を推奨している。
- ii) SSL や TLS の信頼性を支えるサーバ証明書も、その取り消しがなされると意味を失う。取り消し手続きは、サーバ証明書の有効期限切れや秘密鍵の漏洩などにより発生する。Web を安全に利用するためには、非常に重要な確認事項であるため、本設定を有効にしている。
- iii) インターネットに公開されているプログラムをダウンロードする際に、作者の署名があるかを確認する。署名自体が、プログラムの安全性を保証するものではないが、作者が不明なものよりは危険性を減少できると思われる。
- iv) Temporary Internet Files には、Web 閲覧したコンテンツが一時的に保存されている。これにより、同じコンテンツを 2 度目に閲覧した場合、効率の良いキャッシュアクセスが実現できる。しかし、本学のシステム構成では、プロキシサーバがそのキャッシュの役割を果たしているため、Temporary Internet Files 内のデータを残しておくことは、ハードディスクの無駄な消費と考えられる。また、Web 閲覧に関するプライバシー保護の観点からも、Web ブラウザを閉じると同時に、一時ファイルを削除することが望ましい。

2) Outlook Express オプション設定

ポリシー項目	デフォルト	設定
1. 読み取り		
a) メッセージはすべてテキスト形式で読み取る i)	—	有効
2. セキュリティ		
a) 使用する Internet Explorer セキュリティゾーン	—	有効
b) 他のアプリケーションが私の名前でメールを送信しようとしたら警告する ii)	—	有効
c) ウイルスの可能性のある添付ファイルを保存したり開いたりしない iii)	—	無効

表10 Outlook Express オプション設定項目

- i) 最近では、HTML メールも市民権を得て、ビジュアルに訴えるメールを作成・受信することが可能となっている。しかし、一方でこの HTML メールに JavaScript や VBScript などによって作成されたウイルスやワームを仕込んで、メールを開封した瞬間に感染や悪操作を行うことも可能になってきた。そこで、利便性は失うものの、メール本文は必ずテキストとして読み取り処理することになっている。
- ii) メールの送信プロトコルは、かなり単純な仕様であり、悪意のあるプログラムで簡単に偽装送信が可能である。この設定項目を有効にすることで、ユーザーが気付かずにメールを勝手に送信されることを防止することが可能である。
- iii) メールの添付ファイルにウイルスやワームを仕込む手法は、昔から非常に良く利用されている。この設定項目は、その防止を目的にしたものと思われるが、実際に有効にすると、すべての添付ファイルを閲覧不可能にしてしまい、利便性を著しく損なう。そのため、本設定項目は敢えて無効化している。

以上のように、インターネット利用の利便性と安全性のトレードオフのバランスを考慮しながら、Windows 端末の環境構築を行っている。筆者は、これらインターネット利用環境の安全な設定と適切な Hotfix を適用した端末を、「セキュアクライアント」と呼んで重要視している。

6 節. 授業支援ツール

CTR 教室には、授業の円滑な進行を支援するため、様々な機能を持つ「授業支援ツール」を、教卓の専用機に導入している。この授業支援ツールは、日本電子計算が開発を行っているが、レイアウトや機能選定は、情報教育研究センターで行った。

授業支援ツールは、以下に列挙する機能を有す。

- 1) ログオン状態の取得
- 2) 学生機の画面キャプチャ
- 3) キーボード・マウス操作ロック機能
- 4) アナライザ機能
- 5) メッセージ送信機能
- 6) リモート電源管理機能
- 7) 出欠管理機能
- 8) ログオン状況の CSV 形式エクスポート
- 9) ユーザー利用アプリケーションの情報取得

授業支援ツールを起動した画面のキャプチャを図 1 に示す。

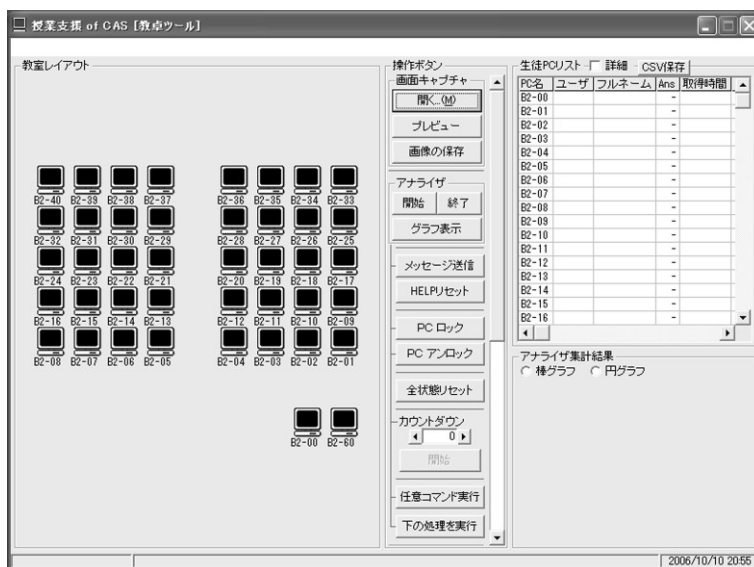


図 1 授業支援ツール画面図

導入時には、それほど需要のないツールであろうと考えていたが、予想に反し教員からは非常に好評である。

特に、出欠管理機能は、利用頻度が非常に高い。図 2 にキャプチャ画面を示す。成功した要因は、CTR 教室での実際のログオン状態を、CSV データに保存する機能を実装して利便性を高めたことにあると思われる。

また、メッセージ送信機能やキーボード・マウスのロック機能も実技試験などで活用がなされている。

授業支援ツールの導入時に、本学側で検討した追加仕様・機能要件を以下の表11に列挙する。

I. 学生用 PC リスト要件	
1. 項目を追加	
a)	フルネーム：Active Directory から取得
b)	アナライザ回答番号：アナライザの結果を数字で表示
c)	アプリケーション：アクティブウィンドウ、タスクバー上に表示されるアプリケーション名を取得
2. 項目の表示選択	
a)	TeacherTool の設定画面で、表示項目を選択可能にする
b)	「PC 名」「ユーザ」は常に表示したいので、選択対象から除外
c)	デフォルトはすべて選択
3. 項目の分類	

a) 「簡易表示」「詳細表示」に分類し、デフォルトは「簡易表示」
b) 「表示切替」ボタンの追加 <ul style="list-style-type: none"> ・簡易表示：PC名、ユーザ、フルネーム、アナライザ回答番号、状態取得 ・詳細表示：PC名、ユーザ、フルネーム、アナライザ回答番号、状態、状態取得、IPアドレス、アプリケーション
4. CSV形式でリストをダウンロード
a) 現在表示している項目をCSV形式でダウンロード
b) ダウンロードするファイルの先頭行は、「教室名,日付」を記載
c) 「リスト保存」ボタンの追加
II. 教室レイアウト要件
1. Call状態のアイコンを変更
a) アイコン自体を点滅させる
2. PCアイコンの下にフルネームを表示する
a) フルネームは頭の3文字を表示する（バイト取得ではない。文字数取得）
b) フルネームがない場合にはアカウント名を表示する
3. アナライザ利用時に、回答番号をPCアイコンの下に表示する
a) 回答番号の表示は、グラフに対応した色で、文字の背景を色づけする
III. 機能要件
1. カウントダウン機能の追加
a) 「カウントダウン」ボタンの追加
b) 秒数設定項目の追加（デフォルト0）
c) カウントダウンウィンドウを「常に前面に表示」するかどうかTeacherToolの設定画面で選択できるようにする
2. キャプチャした画像の保存機能
a) 「画面保存」ボタンの追加
b) プレビュー状態・別ウインドウ表示状態のどちらでも保存できるようにする
c) 別ウインドウ表示状態の場合は、そのウインドウのメニューにも保存項目を追加
3. 状態クリア機能の追加
a) ロック機能やCall等の複数の状態を一度に解除する機能
b) 「状態クリア」ボタンの追加
4. アナライザダイアログの設定機能
a) TeacherToolの設定画面で、アナライザダイアログの「HELP」ボタンの表示選択を可能にする（デフォルトは表示する）
5. グラフ表示の機能追加
a) 棒グラフ
縦目盛りに単位（件）を表示

目盛りは整数のみ
凡例に、回答数も表示
b) 円グラフ
凡例に、割合 (%) も表示
IV. 操作ボタン要件
1. 操作ボタングループの背景色（ボタンの色ではない）を色分けする
a) 機能別に色分けすることで、関連ボタンを分かりやすくする
2. 「表示切替」ボタンの追加
a) 「I-2」を参照
3. 「リスト保存」ボタンの追加
a) 「I-4」を参照
4. 「カウントダウン」ボタンと秒数設定項目の追加
a) 「III-1」を参照
5. 「画面保存」ボタンの追加
a) 「III-2」を参照
6. 「状態クリア」ボタンの追加
a) 「III-3」を参照
7. 利用できないボタンは無効にする

表11 授業支援ツール追加仕様・機能要件一覧

7 節. その他

Windows 端末を設置している CTR1～5 教室では、各プリンタでの印刷枚数について、ユーザー別のログを収集・管理し、年間の印刷枚数に上限を設けている。学生にもコスト意識を持って利用してもらうことを目的に、年間3000枚を上限としている。印刷枚数が過度に多いユーザーについては、情報教育委員会で事情を聞き、紙やインクの使用に無駄のない運用に協力を要請している。

また、本稿では CTR 教室を中心に述べたが、ファイル共有サービスは、教員の研究室からも利用が必要なサービスである。そこで、本学のファイルサーバでは、CTR 教室内でのみ提供している Windows ファイル共有サービスのみならず、WebDAV⁽³⁾サービスを提供している。WebDAV サービスは、HTTP プロトコルを拡張し、クライアントで作成された文書をサーバに送信して公開したり、サーバ上のファイルやフォルダの一覧を取得したり、ファイル・フォルダの複製・移動・削除が行えるようになっている。本サービスにより、教員が研究室から CTR 教室のファイルサーバの個人領域に接続して、ファイル操作を行うことも可能である。

また、1 節でふれたが、CTR 教室のサーバ群 (mdc, dc1, dc2, fs1, fs3, adm1) は、

【教室名 :CTR 4】	現在: 2006/05/09 14:52				
PC名	ユーザ	フルネーム	Ans	取得時間	アプリケーション
B4-00			-		
B4-01	学籍番号1	学生名1	-	14:52:06	Microsoft PowerPoint - [宇宙]
B4-02	学籍番号2	学生名2	-	14:52:09	Microsoft PowerPoint - [宇宙]
B4-03			-		
B4-04	学籍番号3	学生名3	-	14:52:07	Microsoft PowerPoint - [宇宙]
B4-05	学籍番号4	学生名4	-	14:52:07	ワードアートの書式設定
B4-06	学籍番号5	学生名5	-	14:52:11	
B4-07	学籍番号6	学生名6	-	14:52:05	Microsoft PowerPoint - [筋]
B4-08	学籍番号7	学生名7	-	14:52:03	Microsoft PowerPoint - [宇宙]
B4-09	学籍番号8	学生名8	-	14:52:11	Microsoft PowerPoint - [宇宙]
B4-10	学籍番号9	学生名9	-	14:52:08	Microsoft PowerPoint - [宇宙]
B4-11	学籍番号10	学生名10	-	14:52:08	Microsoft PowerPoint - [宇宙]
B4-12	学籍番号11	学生名11	-	14:52:04	Microsoft PowerPoint - [宇宙]
B4-13			-		
B4-14	学籍番号12	学生名12	-	14:52:11	Microsoft PowerPoint - [宇宙]
B4-15			-		
B4-16			-		
B4-17			-		
B4-18			-		
B4-19	学籍番号13	学生名13	-	14:52:02	
B4-20	学籍番号14	学生名14	-	14:52:05	魔法のiらんど - Microsoft Inte
B4-21	学籍番号15	学生名15	-	14:52:09	ソーシャル・ネットワーキングサ
B4-22			-		
B4-60			-		

図2 ログオン状態表示機能

SAN Boot⁽⁴⁾ と呼ばれる特殊な起動システムを採用している。通常、コンピュータは、ローカルに所有するハードディスクにインストールされた OS から起動する。しかし、SAN Boot の場合は、Storage Area Network と呼ばれる外部記憶装置とコンピュータの間を結ぶ高速なネットワークを利用して、共有ハードディスクにインストールされた OS を起動する。この手法により、サーバの統合、集中管理、サーバ障害からの復旧作業の単純化といった長所を甘受できる。SAN Boot 構成は、ハードウェアシステムが複雑な構成になるが、バックアップ、Hotfix のインストールおよびハードディスクのオンライン拡張など日々のメンテナンスには、非常に大きな利便性を提供できている。

本稿ではふれることができなかったが、Macintosh 環境でも、教材提示フォルダ、課題回収スクリプトや学生用端末の画面キャプチャといった機能を、情報教育研究センターのスタッフが開発し、実際に運用している。

おわりに

本稿で述べたシステムは、外国語学部・経営学部・短期大学の基本的な教育要求やユーザーの利便性要求を、ある一定の水準で満たしており完成度は高いと考えている。

しかし、教育現場での様々な要求に応えるためには、それぞれのケースに対応してシステムや端末の仕様修正を行う必要が発生する。2005年度の実績では、教室端末仕様の変更は、一時的なものも含めると16回を数えた。現在はこういった柔軟な運用を維持しながら、作業時間などの運用コストの軽減を図るため、仮想環境やネットワークブート環境を応用した運用の試みも行っている。更なる検証を続けて、次期システム仕様へ織り込んでいく予定である。

謝辞

本稿に述べたシステムの構築には、鈴木智広氏をはじめとする株式会社日本電子計算のメンバーに大変なご尽力を頂いた。また、本システムがトラブルも少なく運用されているのは、学習支援センター（情報教育研究センター）のスタッフの日々の献身的な努力によるところが大きい。スタッフには、本稿の資料作成にもご助力を頂いた。この場を借りて御礼を申し上げる。

参考文献

- (1) Active Directory 技術概要
<http://www.microsoft.com/japan/technet/prodtechnol/windows2000serv/plan/actdirts.msp>
- (2) Lightweight Directory Access Protocol (v3).
<http://www.ietf.org/rfc/rfc2251.txt>
- (3) HTTP Extensions for Distributed Authoring — WEBDAV.
<http://www.ietf.org/rfc/rfc2518.txt>
- (4) Boot from SAN in Windows Server 2003 and Windows 2000 Server
<http://www.microsoft.com/windowsserversystem/wss2003/techinfo/plandeploy/bootfromsaninwindows.msp>