

能開総合大におけるネットワーク環境について

事務処理効率化のためのイントラネットシステム

職業能力開発総合大学校 電子計算機室 富山 泰佑

1. イントラネットについて

1.1 概要

イントラネットとは、インターネットの技術を積極的に取り入れた企業内（組織内）の情報システムである。企業内の情報システムは、その導入の目的などによって千差万別であり、インターネットの技術だけでは不十分な場合も多くある。

本大学校においては、すでに図書館の蔵書管理システムや教務の成績管理や受講管理を行うシステムなどが稼働している。研究センターにおいても職業能力開発に関わる情報を提供するシステムが完成し運用を開始している。

電子計算機室では、電子計算機システムを用いて、本大学校の教育訓練を支援する事務的な業務の省力化・効率化を目指すイントラネット環境を構築し、2000年9月より稼働している。

従来からこれらの事務的な業務は、通常、紙媒体を用いた文書によって進められている。近年、事務文書はパソコンなどのコンピュータでワープロや表計算ソフトなどを用いて電子ファイル化され、これを紙に印書することで紙媒体の文書が作成されている。しかし、事務文書の配布・回覧やその承認などは、文書の電子ファイル化がなされる以前とほとんど変わっていないのが現状である。

本大学校においては、事務連絡などが電子メールやWebなどのインターネット技術だけでは、文書を中心にした業務のワークフローを実現するには無理



図1 イントラネットトップ画面

がある。

なお、当該環境は原則として本大学校の教職員のみ（学生は必要に応じて参照できる）を対象とする。

1.2 基本機能

(1) 文書管理（文書共有）

Documentum*1を使用して各部署・委員会等で必要となる文書の保管を行っている。運用方法としては、各部署用のキャビネットとフォルダを作成し、同時にユーザを各部署のグループに登録する。作成したグループごとにアクセス権を与えて、作成した文書にそのアクセス権を付与すると、グループ（部署）の関係者のみが作成した文書を見ることが出来る。また共有キャビネットの中には、すべての教職員・学生が閲覧できるフォルダが用意されている。アクセス権が与えられていないキャビネットやフォルダは表示されないため、すっきりした画面となっている。

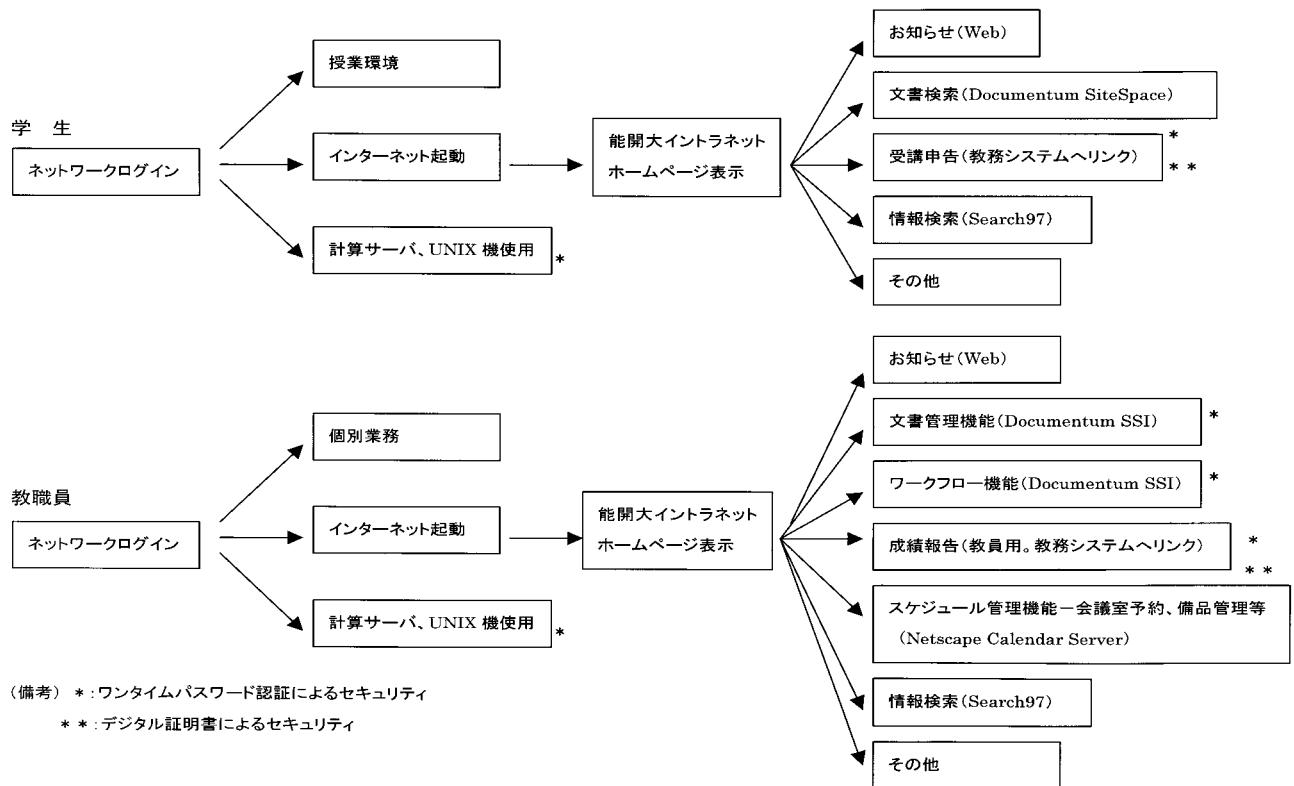


図2 イン트라ネット環境利用の流れ

(2) ワークフロー機能

Documentumを使用して、起案・決裁、稟議書、委員会や会議で必要となる文書を配布・照査する担当者を選択し、回覧する機能を提供している。ワークフローが配信された担当者にはインターネットメールにてワークフローが配信されたことが通知され、文書が担当者に配信されたことがわかる。

(3) スケジュール管理

Netscape Calendar Serverを使用して、各個人のスケジュール管理、会議等イベントの参加依頼、会議室・教室等のリソースのスケジュール管理機能を提供している。

(4) 情報システム(他システムとのリンク)

教職員については教務システムの成績報告機能、学生については受講申告機能へリンクできる機能を提供している。

(5) 情報検索

Search97を使用して各分野、キーワードを入力す

ることにより、全文検索処理を行い、ヒットしたもののについて表示する機能を提供している。

(6) ご利用にあたって

当システムの機能が有効かつ効果的に活用されるための情報欄であり、ユーザが必要に応じて適宜参照できる。

1.3 現状と可能性

(1) 各都道府県研修担当者への情報提供

各都道府県の研修担当者が文書管理を使用して、研修部で保管している文書をインターネット経由で参照を可能にする。

1.4 実際の運用上の問題点

(1) ユーザへの教育

ユーザにより、コンピュータに対するスキルが異なる。提供している機能を使用させるためのスキルアップが必要である。

(2) ユーザからの質問対応

システム自体のトラブル，コンピュータ搭載ソフトウェアの使用方法に関する質問，コンピュータ自体のトラブル等，すべてのトラブルに対して細かく対応ができていない。

(3) Documentumのレスポンス

Webブラウザ（一部にJAVAソフト使用）で文書管理，ワークフロー機能を提供するDocumentumの応答レスポンスが遅い（JAVAの起動に時間がかかるため）。

(4) MacOSに未対応

イントラネット環境を利用するためのクライアントには，以下の環境が必要である。

・OS：Windows系（マイクロソフト社）

・アプリケーションソフト：

Netscape Communicator 4.6以上（Calendar付き）

Adobe Acrobat 4.0（文書共有・ワークフロー，会議室の予約等）

パソコン決裁3.0（電子印鑑）

1.5 その他

Adobe Acrobatライターを使用することによって，各種アプリケーションで作成した文書やイメージ図は，PDFファイルに変換することができる。PDFファイルにすることでAdobe社が無償提供しているAcrobatリーダーを使用して，作成したツールに依存することなく，ユーザはそのファイルを参照することができる。一般にPDFファイルのファイルサイズは，テキスト文書は小さくなるが，イメージ図は大きくなってしまいう欠点がある。

2．電子決済（電子印鑑）

文書（書類）に印鑑を必要とするとき，今までの印鑑が電子印鑑で認められるようになると，大変便利でセキュリティ面においても向上するであろう。「一度に全員に配信」の場合と，原義書のように印

鑑を押す順番がある場合にも，「受取人の順番に配信」が可能である。

「パソコン決済PDF対応版」は，Acrobat に組み込まれるプラグインプログラムで，あたかもAcrobatの中の機能のように利用できる。

各ユーザ個人の電子印鑑は前もって作成しておく。

「パソ決管理ツール」と「パソ決捺印ツール」をセットアップし，Acrobat の「ツール」「パソコン決裁」でユーザ名とパスワードを入力することにより，自分の印鑑が表示され，「一太郎」「Word」「PDF」等の文書に捺印して送信することができる。一度捺印された文書は変更不可となり，セキュリティ面での確保ができる。



図3 「パソ決捺印ツール」より印鑑表示画面

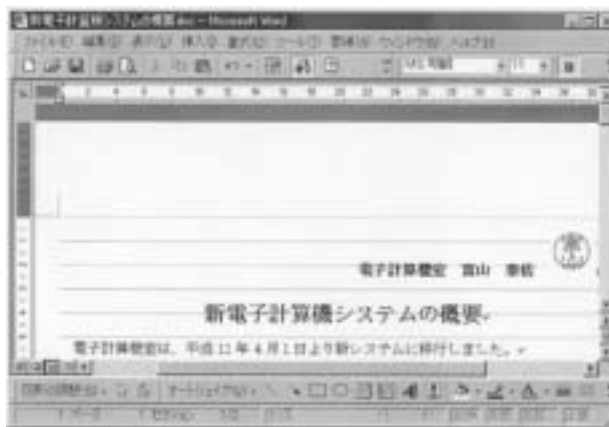


図4 「Word」文書に電子印鑑を設定した画面

前述のパスワードは、ユーザが設定あるいは再設定することができるのでセキュリティ面でも安全と思われる。

電子決済については、現在試行の段階である。

3. 能開総合大における取り組み等

昨年の2月に官公庁のホームページに連続不正アクセスが発生した。当大学においても、ハッキングの対象にならないようなシステム構成をし、アタックに対して防衛しなければならない。インターネット、イントラネット、メールなどが普通に利用できるのが当たり前になっているが、各種サーバやクライアントが常に正常に稼働するためには、セキュリティやコンピュータウイルスについての対策を講じなければならない。

(1) ネットワークセキュリティ

サイバーガード (Cyber Guard)^{*2}により、各サーバに対して不必要なプロトコルを通過させないようにして、セキュリティを確保している。

(2) セキュリティ対策

本人確認のための「デジタル証明書」^{*3}の認証と「ワンタイムパスワードカード(RSA SecurID)」^{*4}は、「本人なりすまし」に対して防御できる。

(3) コンピュータウイルス

Webサーバ、メールサーバ等にアンチウイルス・ソフトである「インタースキャン」を導入し、週1回ウイルスパターンを更新しチェックしている。ウイルスが入ってくると自動的に発見し、取り除くことができる。

以下のデータは多くのウイルスが侵入しようとしていることがわかる。

「Outlook Express」や「Microsoft Outlook」などのWindowsのMAPI^{*5}を使用している場合、特に添付ファイルを開くときには注意が必要である。

【参考】ウイルスデータ

2000/6/1から現在まで、Webサーバに入ったウ

イルスは34件である。

以下にそのウイルス名を一部表示した。

TROJ_SKA, TROJ_BACKDOOR.NB, W97M_MELISSA.A, TROJ_BO2K, TROJ_NETBUS.160A, W97M_THUS。

2000/6/1から現在まで、メールサーバに入ったウイルスは6件である。

以下にそのウイルス名を一部表示した。

TROJ_NAVIDAD.A, W97M_VERLOR.A, W97M_THUS。

以上から、約半年間で多くのウイルスがチェックされ、排除されたことになる。

4. ま と め

能開総合大のイントラネットシステムは、まだ始まったばかりで試行錯誤している。

電子メールが利用され始めた頃、連絡するには、「電話やFAXで十分であると...」。

しかし、今やメールなくしては、仕事ができなくなっている。このシステムが有効利用され、紙媒体による伝達事項が一日でも早くなるよう望みたい。

注

*1 Documentum : 文書管理をするソフトウェアの名称 (または文書管理をする会社名)

*2 サイバーガード (Cyber Guard) : セキュアOSを含んだファイアウォールソフトウェア

*3 デジタル証明書 : セキュリティ対策の1つで電子認証や暗号化電子メールが可能

*4 ワンタイムパスワードカード : セキュリティ対策の1つで1分間に一度変わる数字6桁のパスワード (紛失や、盗難によって他人に不正使用されないように、この6桁の数字の前に、さらに各ユーザ固有の4桁の数字が付加される)

*5 MAPI : Microsoft社のAPIでパソコン間におけるメッセージ交換用プログラムの集まり (Messaging API)