

LDAP による情報管理機能を有する ウェブメールソフトウェアの開発 Web-based Mail System Managing Personal Data by LDAP

松原義継¹, 只木進一

Yoshitsugu MATSUBARA, Shin-ichi TADAKI

佐賀大学学術情報処理センター

Computer and Network Center, Saga University

840-8502 佐賀市本庄町 1

1 Honjo, Saga 840-8502

Web ブラウザさへあればどこからでもメールの読み書きができる Web 対応のメールシステムの需要が増大している。一方で、メールの読み書きの際に必要な認証やアドレス帳などの個人情報の管理が問題となっている。本稿では Web 対応メールシステムが必要とする認証だけでなく、アドレス帳などの個人情報を、LDAP を介して認証システムに統合する手法について提案する。また佐賀大学での実装について報告する。

キーワード：ウェブメール, 個人情報, LDAP

1 序論

インターネットは情報伝達の基盤として不可欠な要素となっている。なかでも電子メールは電話と同様に遠隔地間の基本的な情報交換手段となっている。電子メールの利用には、POP や IMAP などの電子メール読み書きの protocols を利用する専用の電子メールブラウザを活用するのが一般的である。一方で、専用の電子メールブラウザを使わず、Web ブラウザさへあればどこからでも電子メールの読み書きができる Web 対応のメールシステムも利用されている。

電子メールの読み書きの際には、個人特定のための認証のほかにも様々な個人情報を必要とする。例えば、電子メール本文の末尾につける署名やアドレス帳などである。専用の電子メールブラウザを利用する際には、こうした情報はそのソフトウェアが管理する設定ファイルに保存されている。しかし Web 対応メールシステムの場合には、そうした個人情報は Web サーバに置くことになる。

近年の情報システムの拡大に対応して、それらの情報システムに分散する個人情報の管理手法が重要となっている。つまり、組織内の情報システムに分散する個人情報を集中管理すると同時に、多様な認証サービスを提供するシステ

ムが必要とされている。複数の OS に対応した認証を行うとともに、図書館などの情報サービスでの利用者管理を行うものである。LDAP はそのような統合された利用者認証を支える基礎技術として期待されているものの一つである。

本稿では、竹田の開発した「ウェブメーカー」[1] [2] [3] のアイデアを基礎にして、個人情報を LDAP を介して管理するシステムを提案する。また、佐賀大学で運用している統合認証システムの下でのシステム構築及び運用状況について報告する。

2 基本設計

2.1 従来のシステムとその問題点

ウェブメーカーは、Web を介してメールの読み書きを行うためのシステムである。その基本構成を図 1(a) に示す。利用者は HTTP や HTTPS を介してシステムに接続する。メールを読む場合、システムは POP または IMAP を使って、指定されたメールサーバからメールの一覧または本文を受け取り表示する。メール送信の際には、システムは指定されたメールサーバへ SMTP を介してリクエストを送信する。

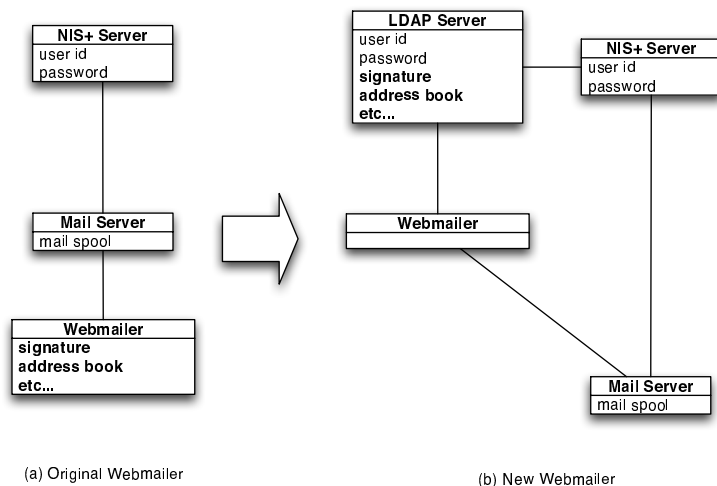


図 1: システムの基本構成

メール本文を作成したり送信する際には、いくつかの個人情報が必要である。メール本文末尾につける署名やアドレス帳である。ウェブメールでは、これらの情報は暗号化されたテキストファイルという形でウェブメールが稼動している Web サーバ内の保存されている。しかし通常は、当該 Web サーバには利用者の ID は存在しない。また、Web サーバからのファイル操作は、通常、Web サーバプロセスのユーザ ID で行われる。従って、上記の個人情報を保持するファイルの所有者は Web サーバプロセスのユーザ ID である。

大学の情報システムでは、毎年 1000 人規模で利用者の登録削除が行われる。年度途中での利用者登録削除も必要である。利用者情報が分散していると、このような情報システムではそうした情報の管理コストが大きくなるばかりでなく、情報の操作誤りや漏洩の原因となる。従ってウェブメールが利用する個人情報についても、利用者 ID 管理と連動した適切な集中管理手法が必要である。

2.2 統合認証と LDAP

上述のように、大学の情報システムでは、毎年 1000 人規模で利用者の登録削除が行われる。

また、認証を提供しなければならない OS が複数ある場合が多いだけでなく、図書館利用者管理など他の情報システムでも共通の利用者管理が必要となる場合が多い。

そのような需要に応じて、利用者情報をデータベース化するとともに、多様な情報システムに多様な認証機構を提供する統合認証システムが提案されてきた [4] [5] [6] [7]。佐賀大学では、Windows 系 OS と UNIX 系 OS に認証を提供するとともに、情報処理センターと図書館の利用者管理を共通化するシステムが 2001 年から稼動してきた [4] [5]。2003 年からは LDAP の活用を開始している。

ドメインコントロールを使う Windows 系 OS と NIS または NIS+ を使う UNIX 系 OS のパスワード同期は一般に困難であり、同期のための様々な工夫が行われてきた。近年、LDAP (Lightweight Directory Access Protocol) が提案され、Windows 系 OS の Active Directory を使った認証と UNIX 系 OS の認証を統合するものとして期待されている [LDAP]。

更に LDAP では、保持する情報を柔軟に定義することができる。この機能を使って、認証情報以外の様々な情報をネットワークを介して提供することで、情報システムの統合に寄与することが可能である。

2.3 LDAP を使ったウェブメールの構築

LDAP を使った認証や個人情報の統合管理システムが構築されているのを受けて、ウェブメールにおける個人情報を LDAP で管理することが可能となる。新しいウェブメールの構成を図 1(b) に示す。LDAP は、通常の認証で使われるユーザ ID やパスワードなどのほかの情報を、柔軟に保持させることが可能である。ウェブメールが必要とする情報を保持するための属性を表 1 に示す。

竹田のウェブメールは、Perl 及び Servlet で実装されてきた。今回の開発にあたって、より Web ページを容易に開発することが可能であり、かつ LDAP をはじめとして POP や IMAP などの開発に必要なモジュールが揃っている PHP への全面的な書き換えを行った。

また、増大するアジアからの留学生の利用に対応するために、多言語対応を図った。基本文字コードを UTF-8 にするとともに、利用者の言語プリファレンスを個人情報として保持することとした。メール本文が UTF-8 に対応したために、日本語や英語だけでなく、中国語や韓国語などのメールの操作を行うことができる。

また、プログラム本体と各種メッセージを完全に分離したため、様々な言語でのメッセージを表示できる。ただし、現在実装されているのは、日本語と英語のメッセージのみである。メッセージは LDAP に登録された利用者の言語プリファレンスに応じて表示される。

2.4 実装と運用

開発に際し、既存のウェブメールを使い慣れている利用者がこの新しいウェブメールを違和感なく利用できるように、インターフェースは既存のものとは大差ないように心がけて開発した。

図 2 に、メールの購読画面を示す。ウェブメールの画面を構成する要素は 4 つある。上部には、メールの新規作成、アドレス帳、そして環境設定等の機能を実現するボタンを集めている。

中央部左には、今回新しく作成されたメールボックス選択が表示される。これは、利用者が IMAP を用いてメールを複数のメールボックスに分けている場合に対応するためである。

中央部には、1 つのメールボックスに格納されているメールの一覧が表示される。1 行につき 1 つのメールに関する情報 (サブジェクト、送信者、受信日時) が表示される。同時に、各メールにチェックボタンを用意し、チェックされたメールに対して削除及び他のメールボックスへの移動ができる。各メールのサブジェクトにはメールの内容を表示するためのリンクが張られており、そのリンクをクリックすることで画面下部にそのメールの内容が表示される。

下部には、メールの内容と同時に、その内容に対して返信もしくは転送するためのボタンが表示される。添付ファイルがある場合は、その添付ファイルを保存するためのボタンが表示される。返信もしくは転送ボタンをクリックすると、メールを作成するウィンドウが表示される。

今回の開発では、新たに携帯電話対応版も開発した。ウェブブラウザ版との機能の違いを表 2 に示す。携帯電話版は、ウェブブラウザ版が持っているメールボックスに対する各種機能は排除し、メールサーバのスプールディレクトリに保存されているメールのみを読み書きするだけである (図 3)。

3 まとめと議論

Web ブラウザさへあればどこからでもメールの読み書きができる Web 対応のメールシステムの需要が増大している。情報システムに分散している個人情報の統合に対応するため、Web 対応のメールシステムの一つであるウェブメールを LDAP 対応とした。佐賀大学では独自の OID を取得し、ウェブメール用の属性を LDAP に定義した。

LDAP 対応とすることで、ウェブメールがローカルに管理していた個人情報を LDAP サーバへ一元化することが可能となった。同時に、言語プリファレンスなど新しい情報を付加し、

属性名	用途	型
webmailer-order	メールの表示順位	Binary
webmailer-quotation-mark	引用符	Binary
webmailer-signature	署名	Binary
webmailer-addressbook	アドレス帳	Binary
webmailer-show-mailboxes	メールボックスの表示	Boolean
webmailer-mailboxes-root	メールボックスのルートディレクトリ名	Binary
webmailer-display-language	表示言語	Binary
webmailer-mobile-display-language	携帯電話版の表示言語	Binary

表 1: ウェブメーラー用 LDAP 属性

多言語対応とした。LDAP へ個人情報統合することで、利用者管理が容易になるとともに、情報漏洩のリスクを減少することができる。

LDAP は多様な OS に認証情報を提供できるだけでなく、保持する情報を柔軟に定義することができる。そのため、通常の認証より詳しい情報に応じた利用者サービスの展開が可能となる。また、ウェブメーラーの署名のような個人設定を、個々の情報システムではなく、統合認証システムに保存することが可能となる。

参考文献

- [1] 渡辺健次, 竹田暁彦, 只木進一「IMAP4 に対応した Web ベース電子メールクライアント WebMailer の開発」*学術情報処理研究*, No. 4, pp. 35-43, (2000)
 - [2] Kenzi Watanabe, Akihiko Takeda, Shin-ichi Tadaki *A Universal E-mail Environment - WebMailer: Web Based E-mail Client Software Supporting IMAP4 Protocol* Proc. Of International ICSC Symposium on INTERACTIVE AND COLLABORATIVE COMPUTING (ICC'2000), Vol. 2, pp. 600-609, (2000)
 - [3] 木下秀怜「お手軽メールシステムを作ろう」*月刊 UNIX MAGAZINE*, pp. 145-153, (2004)
 - [4] 江藤博文, 渡辺健次, 只木進一, 渡辺義明「全学的な共通情報アクセス環境のための統合認証システム」*分散システム/インターネット運用技術*, No. 27, (2002)
 - [5] 江藤博文, 渡辺健次, 只木進一, 渡辺義明「大学における情報基板整備の中核となる統合認証システム」*情報処理学会シンポジウムシリーズ*, Vol. 2003, No. 6, pp. 43-48, (2003)
 - [6] 奈古屋広昭, 松村芳樹, 入来院ひさ子, 鈴木令子, 鷹野三千代「オープンソースによる統合認証系の構築と運用」*分散システム/インターネット運用技術シンポジウム 2004*, pp. 43-48, (2004)
 - [7] 広島大学全学電子認証システム, <http://auth.hiroshima-u.ac.jp/>
- [LDAP] Lightweight Directory Access Protocol(V3), M. Wahl et al., RFC2251, (1997)

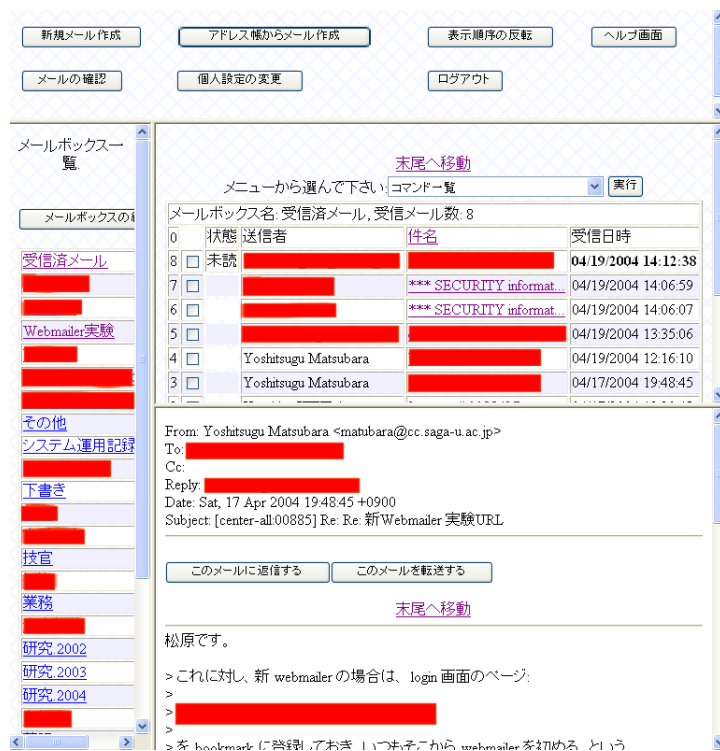


図 2: Web ブラウザ版のスクリーンショット

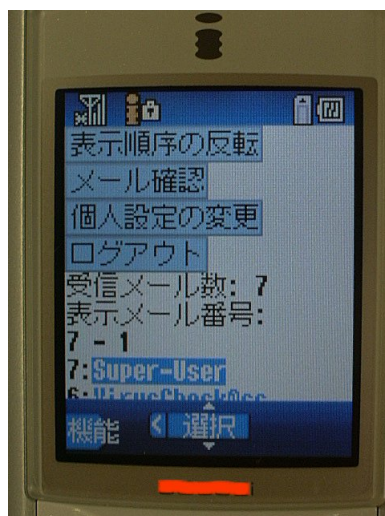


図 3: 携帯電話版でメールを見る

機能	ウェブブラウザ版	携帯電話版
受信メール読み		
新規メール作成		
メール返信		
メール転送		
メール削除		
複数メール一括削除		×
引用符編集		
メール作成時の引用符添付		
表示言語選択		(制限あり)
署名編集		×
メール作成時における署名添付		×
アドレス帳編集		×
アドレス帳からのメール作成		×
HTML メール表示		×
添付ファイル保存		×
メールボックス設定		×
メールボックス表示		×
メールボックス編集		×
複数メール一括移動		×
ヘルプ画面表示		×

表 2: ウェブブラウザ版と携帯電話版における機能の違い