

電子メールサーバ (mbox) の紹介

– 新しくなった mbox はこんなに便利！ –

赤坂 浩一 * 平野 彰雄 *

1 はじめに

前回の解説記事「大型計算機システムのインターネットサービス」で、京都大学学術情報メディアセンター・大型計算機システム (以下、本センター) の電子メールサービスについて簡単に解説しましたが、スケジュール等の都合で執筆を断念した電子メールサーバ (以下、mbox) について紹介します。

mbox での電子メールサービスは、平成 9 年 10 月よりパソコン通信システム (愛称: クラリネット) で SMTP/POP3,IMAP4 プロトコル対応の電子メールサービスとして運用していましたが、古いシステムであるため新しい機能への対応が困難になっていました。

平成 14 年 11 月 24 日にシステムのリプレースを行ない、mbox での電子メールサービスを一新しましたので、あらためてサービスの概要や利用方法について簡単に紹介します。

2 サービスの概要と機能改善

mbox は、SMTP/POP3,IMAP4 プロトコルに対応した電子メールサーバで、利用するためには別途登録が必要となりますが、登録時に任意のユーザ名を選択することができ、そのユーザ名をメールアドレスとして利用できることが大きな特徴です。

今回、次のような機能改善を行ない、より使いやすい電子メールサービスを目指しました。

- Web からの利用者管理機能

mbox への利用登録や取消、転送設定等の利用者管理を専用の Web ページからオンラインで行なえます。

- TLS や SSL による暗号化通信

どのようなネットワーク環境からでも安全にお使いいただくために、TLS(Transport Layer Security) や SSL(Secure Socket Layer) による暗号化通信が行なえます。

- POP before SMTP によるメール送信

mbox の送信 (SMTP) サーバは、送信前に POP3 や IMAP4 で受信操作を行なうことにより、一定時間、その IP アドレスからの送信を無条件に受け付けます。つまり、mbox に利用登録した方は、どこから接続していても、送信者として、どのようなメールアドレスを記述していても送信が可能になります。

- SMTP AUTH 認証によるメール送信

送信 (SMTP) サーバに対して、使用時に利用者認証を行なうことができます。この機能を利用するためには、TLS や SSL による暗号化通信をサポートしているメールクライアントが必要となります。なお、SMTP AUTH 認証は、mbox に利用登録せずとも本センターの利用者であれば利用可能です。

また、mbox も sakura と同様に電子メールを使ったウイルスによる被害を最小限に食い止めることを目的に、メールサーバに対してネットワークアソシエイツ社製 Virus Scan Server を導入し、全てのメールをウイルスに汚染されていないかチェックを行なっています。

なお、ウイルスに汚染されている場合、可能な限り駆除あるいは削除を行ないますが、ウイルス攻撃を完全に防御できるものではありません。

それでは、次に具体的な利用方法を説明します。

*あかさか ひろかず , ひらの あきお (京都大学 学術情報メディアセンター)

3 利用登録

利用登録を行なうためには、本センターのトップページ¹の「[mbox サービス](#)」のリンクからアクセスすると図 1のように mbox の専用 Web ページに移動します。



図 1. mbox の専用 Web ページ (トップページ)

なお、mbox の専用 Web ページは、本センターの利用番号とパスワードによる利用者認証が必要となりますので、安全性を考慮して暗号化通信を行ないます。但し、現在、自署証明書で運用しているために、図 2のようなサイトの信頼性に関する警告が表示されますが、「はい(Y)」をクリックし続行すると、図 1のページに移動します。

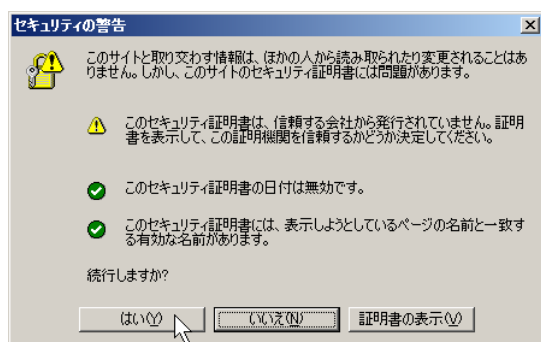


図 2. サイトの信頼性に関する警告 (IE の場合)

図 1の「Login Name」と「Password」の欄に利用番号とパスワードを記入し、「LOGON」をクリックすると、利用者認証を行ないます。

これまでに、mbox の利用登録 (メールアカウント取得) を行なっていない場合は、図 3のページが表示されます。



図 3. 利用登録 (メールアカウント取得)

初めてアクセスされた方は、まず「ヘルプ」のリンクをアクセスし、利用方法や注意事項を必ずお読みください。特にメールアカウントの命名規則は十分理解しておいてください。

では、図 3のように、取得したいメールアカウントを入力し、「APPLY」をクリックします。

取得したいメールアカウントが既に他の利用者に取得されている場合は、その旨のメッセージが表示されますので、別のメールアカウントをお選びください。取得したいメールアカウントが取得できる場合は、確認のページが表示されますので、「OK」をクリックすると利用登録が完了します。「CANCEL」をクリックすると再び図 3のメールアカウント取得のページに戻ります。

利用登録 (メールアカウント取得) が完了すると、図 4のページが表示されます。このページは、mbox の利用登録が完了している方の「現在の設定」です。



図 4. 現在の設定

メールアカウントを取得した直後は、図 4のように「IMAP4,POP3 を利用する」「転送先アドレ

¹URL は、<http://www.kudpc.kyoto-u.ac.jp/> です。

スは、設定されてません」の設定になっています。
現在の設定を変更するには、「[設定の変更](#)」をクリックし、図 5 のページで行ないます。利用方法は「[ヘルプ](#)」をご覧ください。



図 5. 設定の変更

取得したメールアカウントを削除するには、「[アカウントの削除](#)」から行ないます。アカウントの削除を行なうと取得したメールアカウントと共にスプール (メールボックス) も削除します。また、取得していたメールアカウントは一定期間再利用できません。

「[終了](#)」をクリックすると、この専用 Web ページから本センターのトップページに移動します。

4 mbox での電子メールサービス

mbox でのメールアドレスは、利用登録で取得したメールアカウントがユーザ名となり、次のようになります。

ユーザ名 @mbox.kudpc.kyoto-u.ac.jp

メールクライアントで指定する送信 (SMTP) サーバ・受信 (POP3,IMAP4) サーバは、次のようになります。

送信 (SMTP) サーバ	
ホスト名	mbox.kudpc.kyoto-u.ac.jp
受信 (POP3,IMAP4) サーバ	
ホスト名	mbox.kudpc.kyoto-u.ac.jp

なお、受信サーバの私書箱 (メールボックス) のアクセスや送信サーバの SMTP AUTH 認証時のアカウントとパスワードには、本センターの利用番号とパスワードを使用しますので、ご注意ください。

mbox で電子メールサービスを利用するためには、お使いのパソコンやワークステーションに SMTP/POP3 または IMAP4 プロトコルに対応したメールクライアントを用意してください。

メールクライアントは数多くが存在しますが、メールクライアントによって利用できる機能 (例えば、IMAP4 プロトコルのサポートの有無や TLS や SSL による暗号化通信・SMTP AUTH 認証のサポートの有無) に違いがありますので、各自で判断してください。

4.1 POP3 と IMAP4、どちらが良い？

mbox では、POP3 プロトコルの他に IMAP4 プロトコルが利用できます。POP3 と IMAP4 の違いは簡単に言えば、受信サーバ上の私書箱 (メールボックス) にあるメールをクライアントに取り込んでから読むか、受信サーバ上に置いたまま読むかの違いです。

例えば、研究室と自宅で別々のパソコンでメールを読みたい場合、POP3 では、一方のパソコンで読み込んだメールは、もう一方のパソコンで読めなくなりますので、意識的に「サーバにメールを残す (削除しない)」ような設定が必要です。但し、このような設定を行なうと同じメールを二度読むことになったりします。

IMAP4 では、受信サーバ上の私書箱に置いたままクライアントでメールを読むことができ、未読・既読の管理も行なわれていますので、複数台のパソコンで同じメールを読まなくて済みます。

また、POP3 で「サーバにメールを残す (削除しない)」設定を行ない、いつまでも受信サーバにメールを溜めておくと徐々にメールを受信する時間がかかるようになります。

IMAP4 では、受信サーバ上の私書箱にフォルダを作成し、メールを振り分けて利用すれば、短時間で新着メールを読むことができます。

IMAP4 プロトコルに対応したメールクライアントも数年前と比較して増えてきていますので、お使いのメールクライアントで IMAP4 プロトコルが利用できる場合は、この機会に POP3 から IMAP4 に

移行することもご検討ください。

なお、IMAP4 での利用を強いるわけではありませんので、最終的には各自の判断にお任せします。

4.2 より安全に利用するためには

電子メールサービスを利用する場合、メールの受信時に必ず利用者認証が行なわれます。この認証に必要なアカウントやパスワードは、決して他人に知られてはならない重要な情報ですが、ネットワーク上を平文 (暗号化されない文字列) のままで流れていきますので、悪意のある人に盗聴される危険があります。

より安全に利用するためには、TLS や SSL による暗号化通信がもっとも効果的なのですが、暗号化通信をサポートしているメールクライアントは、まだまだ数が少ないようです。

そこで、暗号化通信をサポートしていないメールクライアントで SSL による暗号化通信を実現させる便利なフリーソフト「wstone」を紹介します。

wstone は、Windows パソコンで動作するソフトウェアで、以下の URL からダウンロードすることができます。この原稿を執筆中の現時点ではバージョン 1.2 が最新バージョンのようです。

<http://www.orangesoft.co.jp/wstone/>

インストールはダウンロードしたファイルを実行するとセットアップが始まりますので、指示に従ってインストールしてください。

次に使い方ですが、wstone を起動すると図 6 のウィンドウが表示されます。このウィンドウで、SSL による暗号化通信を行ないたいプロトコルを

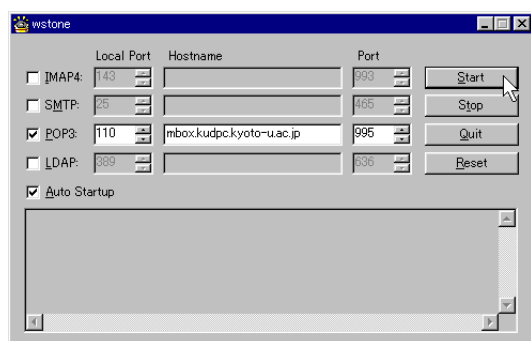


図 6. wstone の設定

チェックし、右側の「Hostname」の欄に、接続するホスト `mbox.kudpc.kyoto-u.ac.jp` を記述し、`Start` をクリックすると SSL による暗号化通信の準備が完了します。

この他のプロトコル (IMAP4,SMTP) も SSL による暗号化通信を行ないたい場合は、同様にチェックし、接続するホストを指定します。

「Local Port」や「Port」のポート番号は変更する必要はありません。また、「Auto Startup」をチェックしておくで、wstone を起動時に設定したプロトコルの SSL による暗号化通信の準備が完了します。

お使いのメールクライアントで、POP3/IMAP4 プロトコルを SSL による暗号化通信を行なうためには、受信 (POP3 または IMAP4) サーバ名に、「`mbox.kudpc.kyoto-u.ac.jp`」を記述するのではなく、「`localhost`」としてください。

また、同様に SMTP プロトコルも SSL による暗号化通信を行なう場合は、送信 (SMTP) サーバ名に、「`localhost`」を記述してください。

このように、wstone を中継することで、暗号化通信をサポートしていないメールクライアントでも安全にメールの送受信が可能となります。

なお、mbox では APOP 対応を行なう予定がありませんので、安全に利用するためには、TLS や SSL による暗号化通信をご利用ください。

4.3 どこからでもメールを送りたい

メールの配信を行なう送信 (SMTP) サーバは、近年、迷惑メールの送信などの不正使用を防ぐために、制限を設けるのが常識となっています。

sakura では、送信者の接続 IP アドレスやメールアドレスにより、使用を制限しています。具体的には、民間プロバイダなどに接続している場合やメールクライアントの送信者 (From:) のメールアドレスに本センターのメールアドレスを記述していない場合は、使用できないように設定されています。

mbox では、POP before SMTP をサポートしており、送信前に mbox の受信サーバに対して受信操作を行なうことで、その接続 IP アドレスを登録

し、一定時間(5分間)、無条件にそのIPアドレスからの送信が可能となります。

つまり、mboxのメールアカウントを持っていれば、学内・学外どこからでも、送信者のメールアドレスに何を書いても、メールの送信ができるようになります。

また、mboxは、送信サーバの使用時に利用者認証を行なう、SMTP AUTH認証もサポートしています。このSMTP AUTH認証には、TLSやSSLによる暗号化通信を行なえるメールクライアントが必要となりますが、利用者認証を行なうことでPOP before SMTPと同じように、学内・学外どこからでも、送信者のメールアドレスに何を書いても、メールの送信ができるようになります。

SMTP AUTH認証は、本センターのアカウントをお持ちの利用者であれば、どなたでも利用できる機能です。

4.4 メールクライアントの設定例

先にも述べましたが、TLSやSSLによる暗号化通信をサポートしているメールクライアントは、まだまだ数少ないようです。

この原稿を執筆中の現時点で、Windows系はMicrosoft社のOutlook Express、Netscape社のNetscape6.2、オレンジソフト社のWinbiffなどがあります。UNIX系だとsylpheedやWanderlustなどがあります。Macintoshについては、近くに環境がないもので...申し訳ありません。

今回、メールクライアントとして、Microsoft社のOutlook Express(以下、OE)を例に紹介します。OEは、近年のウィルスメール騒動でもっともウィルスに感染しやすいメールクライアントとして有名になり、敬遠される方も多いと思いますが、少なくともパソコンの初心者には、馴染みやすい²メールクライアントだと思います。

ここでは、OEをメールクライアントとして利用する上で、注意すべき設定と合わせて、mboxをメールサーバとするための設定を紹介します。

²すぐ使える。標準でインストールされているという理由で...

なお、WindowsパソコンはOSやアプリケーション(特にIE:Internet Explorer)のセキュリティパッチなどが頻繁(!?)に公開されていますので、定期的に「Windows Update」を実施するようにしてください。

4.4.1 OEで注意すべき設定

近年、メールに添付されたファイルを開くことで感染するタイプの他に、プレビューするだけで感染してしまうタイプのウィルスが登場しています。

OEの初期設定では、「プレビューウィンドウを表示する」設定となっていますので、まず始めに、このプレビューウィンドウの表示を行なわないようにウィンドウのレイアウトを変更します。

図7のように、OEのメニューバーの「表示」をクリックし、プルダウンメニューの中から「レイアウト」を選択します。

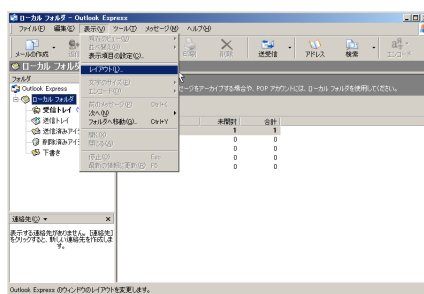


図7. ウィンドウのレイアウトの変更1

図8のように、ウィンドウのレイアウトのプロパティが表示されますので、「プレビューウィンドウを表示する」のチェックを外して、**OK**をクリックしてください。

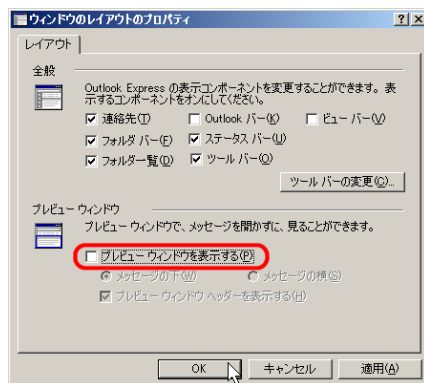


図8. ウィンドウのレイアウトの変更2

つづいて、オプションの構成を行ないます。オプションの構成は、OEの基本的な動作を制御するもので、今回は、「全般」と「メッセージの読み取り」と「送信」のオプションの構成を行ないます。

それでは、図9のように、OEのメニューバーの「ツール」をクリックし、プルダウンメニューの中から「オプション」を選択すると、オプションのウィンドウが表示されます。

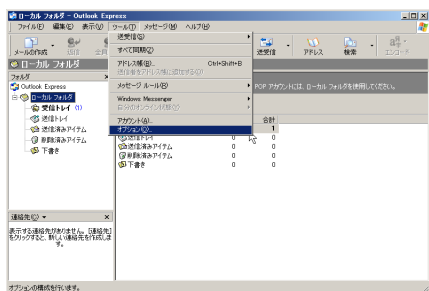


図 9. オプションの構成 1

まず、図10のように、「全般」で「自動的に未開封メッセージがあるフォルダを表示する」のチェックを外し、**適用** をクリックします。

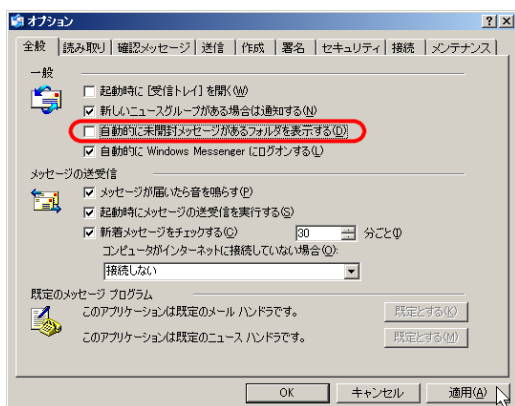


図 10. オプションの構成 2

次に、「読み取り」をクリックすると、図11のように、読み取りのオプションのウィンドウに切替わりますので、「プレビューウィンドウで表示するメッセージを自動的にダウンロードする」のチェックを外し、**適用** をクリックします。

最後に、「送信」のオプションの構成です。OEだけではありませんが、近頃のメールクライアントには、メールの本文をHTML形式に変換し、添付ファイルとして送信するものがありますが、このよ

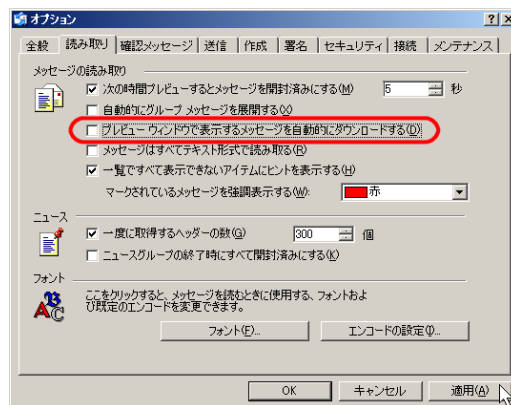


図 11. オプションの構成 3

うなメールは、一般的に歓迎されていません。

同じ内容のものが、テキスト形式とHTML形式で送られてくるので、一通のメールのサイズが大きくなります。そもそも、メールを受け取る人が、HTML形式のファイルを読むためのツールを必ず持っているとは限りませんので、普段は、テキスト形式のみで送信するのが、良いでしょう。

「送信」をクリックすると、図12のように、送信のオプションのウィンドウに切替わります。初期設定では、メール送信の形式は「HTML形式」が選択されていますので、これを「テキスト形式」に変更し、**OK** をクリックしてください。

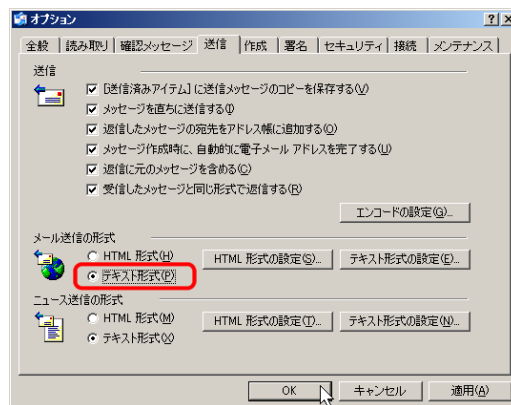


図 12. オプションの構成 4

以上で、OEで注意すべき設定は終了です。

4.4.2 mbox をメールサーバとする設定

初めてOEを起動すると、図13のように、インターネット接続ウィザードが表示されますので、このウィザードを使ってインターネットアカウント

(メール) の作成を行ないましょう。先に紹介した「OE で注意すべき設定」は、ここでの設定が完了してから行なってください。

このウィザードは、「名前」「インターネット電子メールアドレス」「電子メールサーバ名」「インターネットメールログオン」「設定完了」のステップがあります。

図 13の「表示名」の欄には、ご自分の名前を記述します。漢字を使って書くことも可能です。

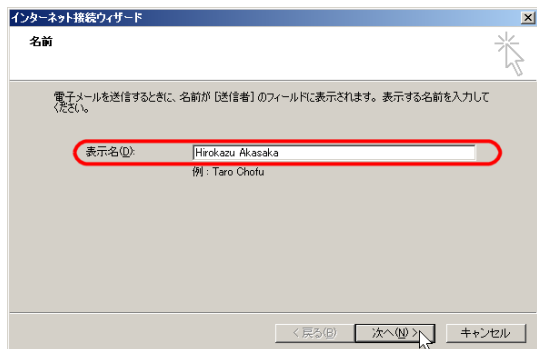


図 13. インターネット接続ウィザード 1

「次へ」をクリックすると、図 14の「インターネット電子メールアドレス」のステップへ移ります。

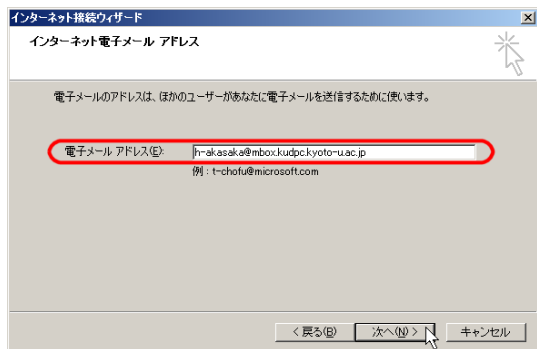


図 14. インターネット接続ウィザード 2

「電子メールアドレス」の欄には、ご自分のメールアドレスを記述します。普段、お使いのメールアドレスでも結構です。

「次へ」をクリックすると、図 15の「電子メールサーバ名」のステップへ移ります。

「受信メールサーバの種類」は、メニューからPOP3,IMAP,HTTP の三種類が選択できますが、mbox では、POP3 もしくは IMAP のどちらかを選択します。

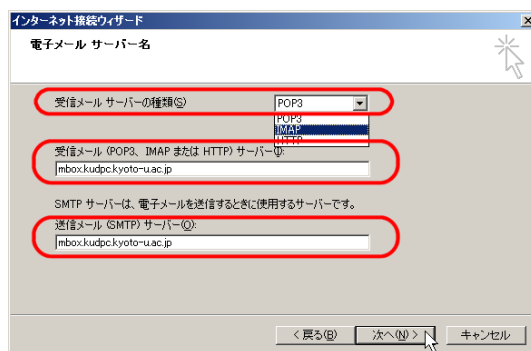


図 15. インターネット接続ウィザード 3

「受信メールサーバ」と「送信メールサーバ」の欄には、それぞれ `mbox.kudpc.kyoto-u.ac.jp` と記述します。

「次へ」をクリックすると、図 16の「インターネットメールログオン」のステップへ移ります。

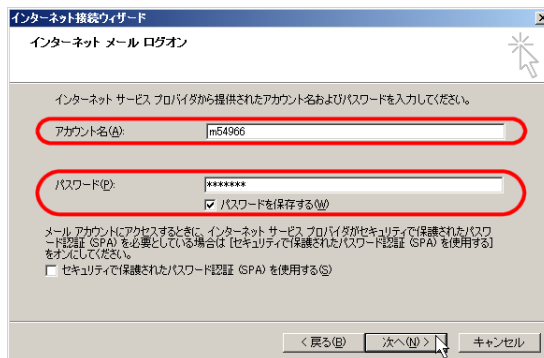


図 16. インターネット接続ウィザード 4

「アカウント名」の欄には、本センターの利用番号を記述します。mbox で取得したメールアカウントではありませんので、注意してください。

「パスワード」の欄には、本センターのパスワードを記述し、「パスワードを保存する」をチェックします。このチェックを外すと、送受信の際に、必要に応じてパスワードの入力要求が行なわれますので、正しいパスワードをタイプしてください。

なお、「セキュリティで保護されたパスワード認証 (SPA) を使用する」のチェックボックスは、mbox や sakura をメールサーバとして利用する場合は、絶対にチェックしないでください。

「次へ」をクリックすると、「設定完了」のステップへ移りますので、「完了」をクリックしてウィザードを終了します。

これで、「mbox をメールサーバとする設定」は完了ですが、最後に、より安全に利用するために OE で暗号化通信を行なう設定を紹介します。

4.4.3 OE で暗号化通信を行なう設定

先ほどウィザードで作成したインターネットアカウント(メール)のプロパティで設定します。インターネットアカウント(メール)のプロパティは、アカウントの構成で表示することができます。

図 17 のように、メニューバーの「ツール」をクリックし、プルダウンメニューの中から「アカウント」を選択すると、インターネットアカウント(メール)のウィンドウが表示されますので、作成したアカウントをマウスで選択し、「プロパティ」をクリックします。

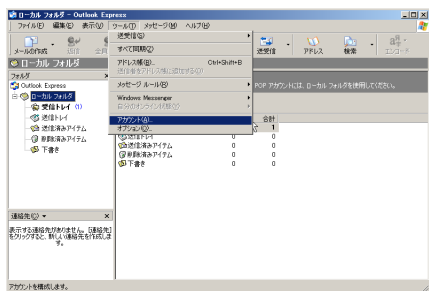


図 17. アカウントのプロパティ 1

暗号化通信に関する設定は図 18 のように、「詳細設定」で行ないます。暗号化通信を行ないたいサーバ(送信メール・受信メール)の下にある「このサーバはセキュリティで保護された接続(SSL)が必要」をチェックボックスをチェックします。

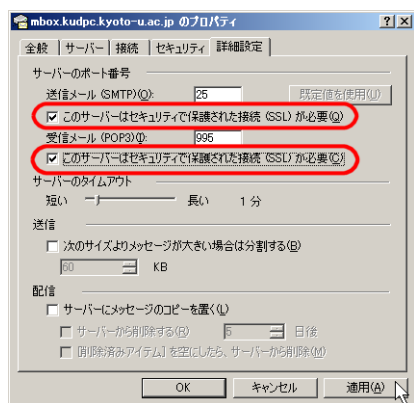


図 18. アカウントのプロパティ 3

今回は、両方ともチェックしてみました。

なお、送信メールで暗号化通信を行なうためには、利用者認証が必要となりますので、「サーバー」を開き、図 19 のように、「このサーバは認証が必要」のチェックボックスを忘れずにチェックしてください。

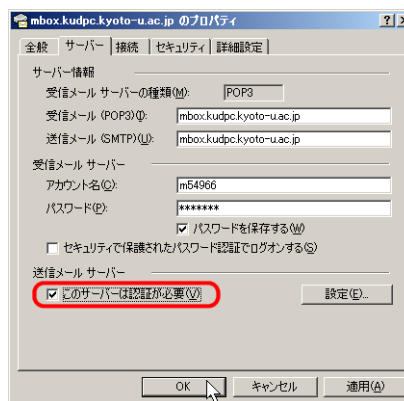


図 19. アカウントのプロパティ 4

最後に、「OK」をクリックし、アカウントのプロパティを閉じ、インターネットアカウントのウィンドウも「閉じる」をクリックして終了します。

以上で、OE の設定は全て完了です。

なお、ここで紹介した暗号化通信のための設定では、初めて mbox に対して「送受信」を行なうと、図 20 のような警告が表示されます。

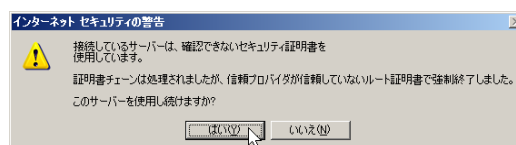


図 20. セキュリティの警告

これは、自署証明書で運用しているために表示されます。「はい」をクリックすると、暗号化通信による送受信を行ないますので、ご安心ください。

5 おわりに

今回は、新しくなった mbox での電子メールサービスについて、紹介しました。

現在、sakura での電子メールサービスをお使いになっておられる方は、是非、一度 mbox での電子メールサービスをお試しください。