E-Post Mail Server

E-Post SMTP Server

Active Directory 連携 メールサーバ 構築ガイド

ーメールアカウントを AD のユーザー管理と
連携させるメールサーバ構築入門ー

Rev.1.6 〔2015.12.15〕

32bit版
64bit版
対 応

e-POST

株式会社イー・ポスト

Active Directory 連携メールサーバ構築ガイド

目　　次

E-Post およびイー・ポストは、株式会社イー・ポストの日本における登録商標です。
Microsoft、Windows および Windows Server は、米国およびその他の国の Microsoft 社の登録商標または商標です。
その他の社名および製品名は、それぞれの会社の登録商標または商標です。
本マニュアルの無断複製および引用を禁じます。 ©イー・ポスト

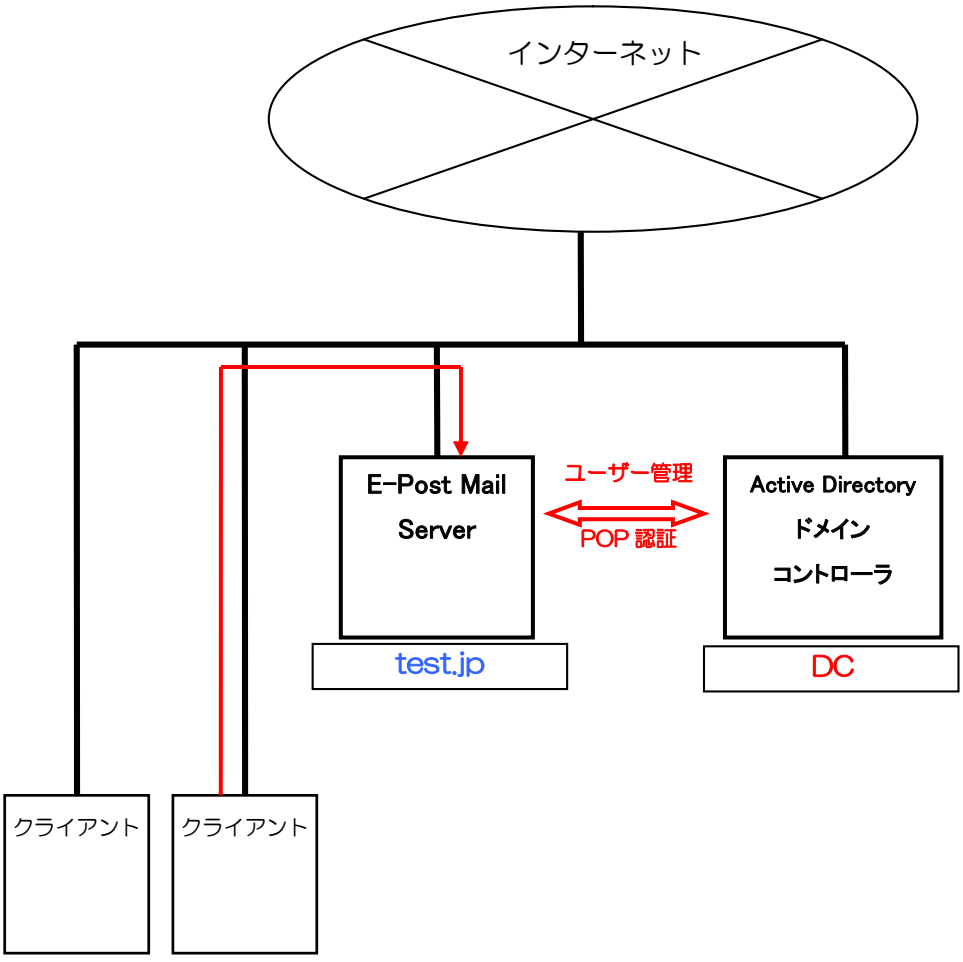
1．　メールサーバの Active Directory 連携とは

Active Directory 連携の機能

E-Post Mail Server・E-Post SMTP Server シリーズは、メールユーザー管理について、Windows Server 2012、Windows Server 2008、Windows Server 2003、Windows 2000 Server の Active Directory ユーザーとの連携機能があります。

構成の基本的考え方

E-Post Mail Server・E-Post SMTP Server シリーズのメールサーバが Active Directory 連携を行うシステムを構築するには、Active Directory のサーバであるドメインコントローラが別に必要になります。メールサーバをインストールするマシンは、Windows ドメインのメンバーマシンとしてあらかじめ設定されていることが必要です。



2. Active Directory 連携のメリット・デメリット

Active Directory連携のメールサーバを構築することによるメリットとデメリットを考えてみましょう。

① ユーザー管理の一本化

Active Directory 連携のメールサーバを構築することによる最大のメリットは、ユーザー管理の一本化があげられるでしょう。「Active Directory ユーザーとコンピュータ」で作成・管理するユーザーをそのままメールユーザーとして登録すれば、一元管理ができるようになり、管理しやすくなります。
なお、Active Directory にログインするユーザー名として、「A001」のように、社員番号のような氏名を含まない文字列で登録しているときは、メールアカウントとして使うには無理があります。そのような場合は、「suzuki」のような氏名を意味するエイリアスを作り、そのエイリアスと実アドレスを関連づけて運用するようにすれば、「suzuki@domain名」を対外的なメールアドレスにしつつ、なおかつユーザー管理は Active Directory で行うことができます。
ただし、エイリアスを最大限に利用するときは、E-Post Mail Server・E-Post SMTP Server 購入時に、作成するエイリアスの分だけライセンス数をプラスして計画しておく必要があります。仮に、ユーザー数が 100 人でも、全員にエイリアスを用意しようとすれば、ライセンス数にプラス 100 して、合わせて 200 人分が必要になるという利用形態になっていますので、気をつけましょう。
なお、ライセンス数については、メールをしないユーザーを含む Active Directory ユーザー全員分が必要になることはありません。デフォルトで”IMSUsers”という”MailGroup”に入ったユーザーだけが連携され、登録アカウントとしてカウントされるようになっています。

② バーチャルドメインによる使用時の注意

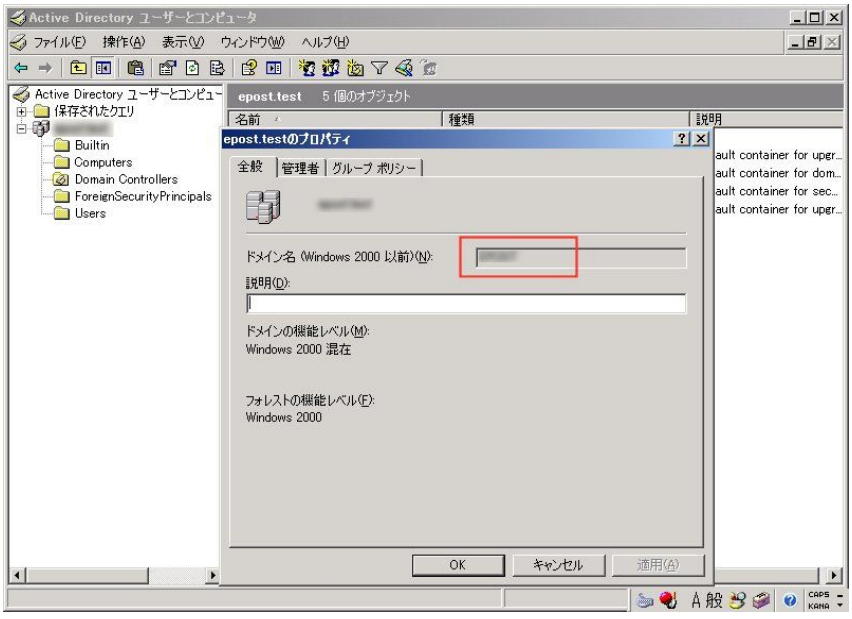
E-Post Mail Server シリーズ・E-Post SMTP Server シリーズ製品は、独自アカウント管理方法を使っているときは、完全なマルチドメインでの運用が可能になっています。
それに対して、Active Directory 連携を行ったときは、完全なマルチドメインでの運用はできなくなり、バーチャルドメインでの運用形態となります。
具体的には、Active Directory 連携時でも、「a_domain」と「b_domain」というように複数のドメインを作成することもできますが、それぞれのドメインに同じアカウントが存在できない状態になります。つまり、「suzuki@a_domain」と「suzuki@b_domain」とは、区別できなくなります。
Active Directory 連携時に複数のドメインを運用するときは、その点に十分注意を払ってユーザーアカウントが重複しないように管理する必要があります。

3. Active Directory 連携とメールサーバ設定方法の手順

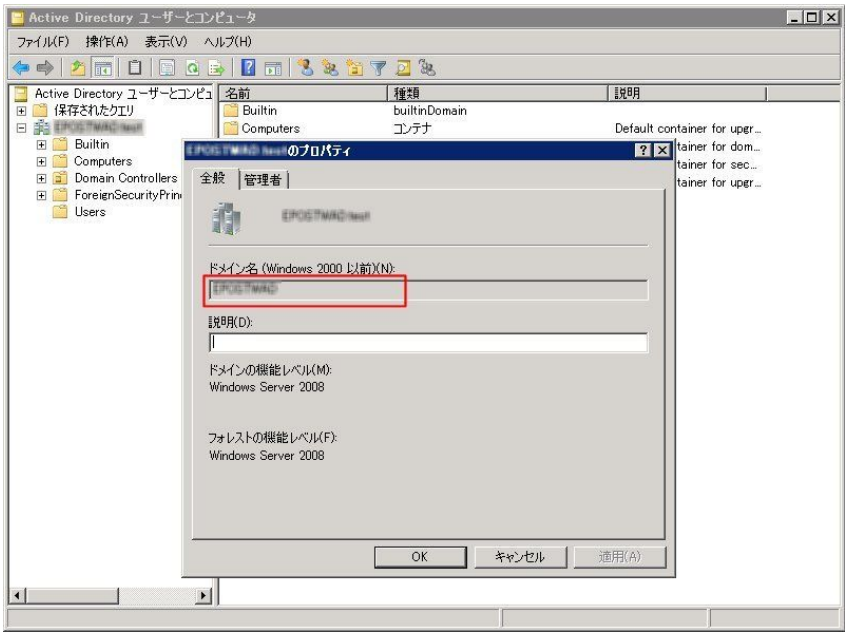
③ Active Directory ドメインコントローラの用意

③-1 Active Directory のモードとドメイン名の確認

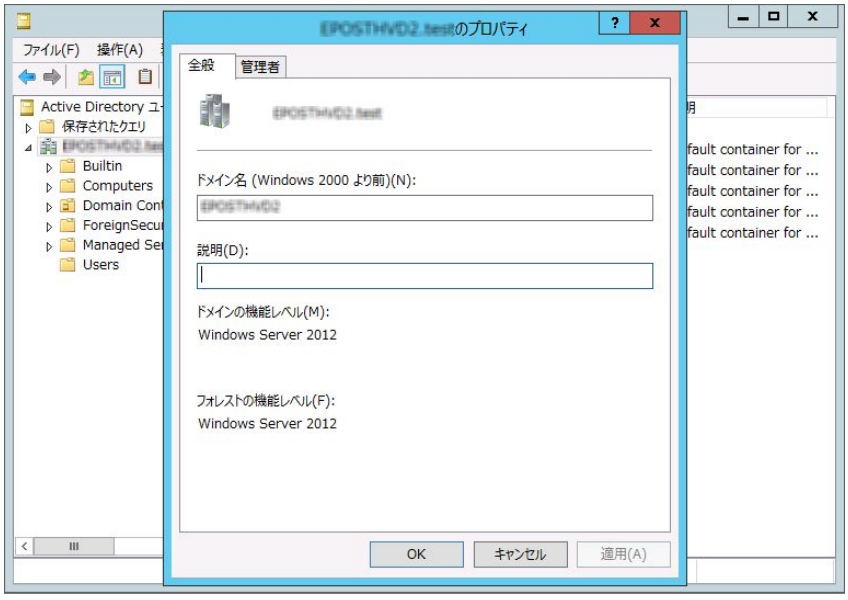
メールサーバのユーザー管理を Active Directory 連携させるためには、当然のことですが、ドメインコントローラ（Active Directory サーバ）が必要です。同一ネットワーク内に Windows Server 2012 か、Windows Server 2008、Windows Server 2003 マシンを用意し、Active Directory のドメインコントローラを用意してください。実際のハードウェアを何台も用意することがむずかしいときは、Hyper-V や Microsoft Virtual Server などの仮想マシンソフトウェアを使って試してもかまいません。複数の仮想マシンをそれぞれドメインコントローラ、メンバーサーバにして動作を確認してください。
なお、作成するドメインの機能レベルは、ネイティブモードでも混在モードでもどちらでもかまいません。
その後、ドメインコントローラを設定したマシンから「Active Directory ユーザーとコンピュータ」を開き、作成したドメインを確認します。
メールサーバと連携する Active Directory ドメイン名は、作成済みのドメイン名のうち、「ドメイン名（Windows 2000 以前）」項目を確認してください。ちなみに Windows Server 2008 の「Active Directory ドメイン サービス インストール ウィザード（dcpromo.exe）」の画面では、ウィザード内に出てくる「ドメイン NetBIOS 名」項目がこの項目に該当します。



▲Windows Server 2003 で作成済みドメイン名を確認する



▲ Windows Server 2008 で作成済みドメイン名を確認する

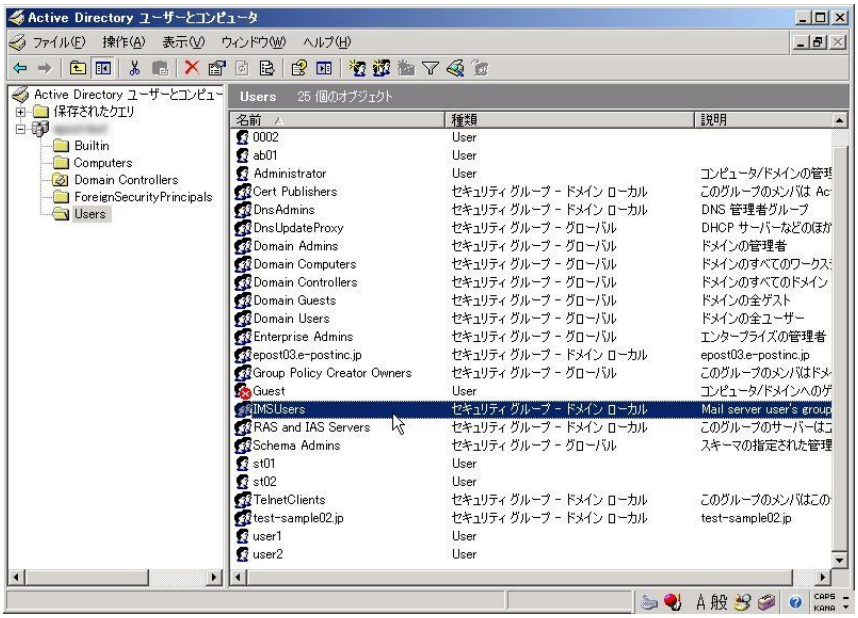


▲ Windows Server 2012 で作成済みドメイン名を確認する

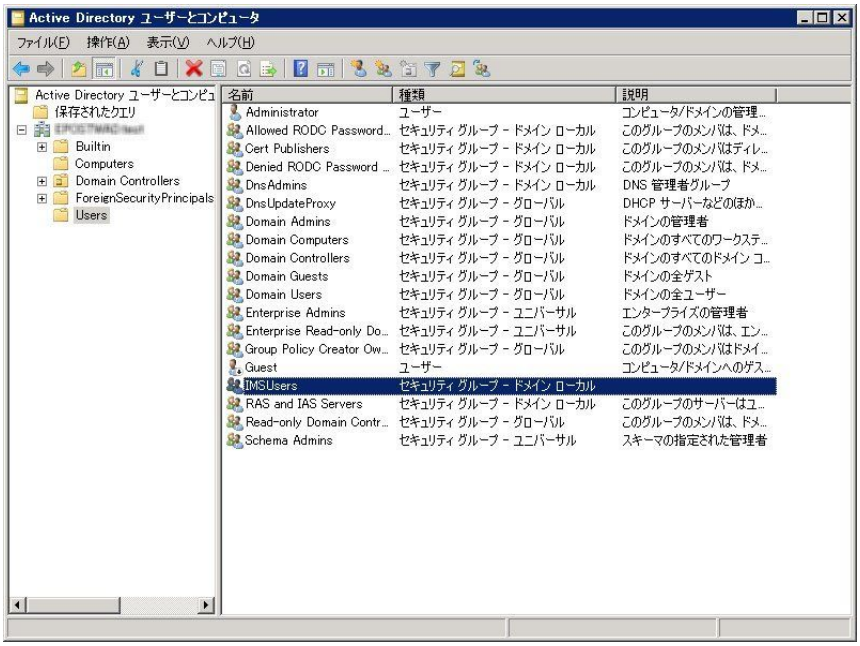
「Active Directory ユーザーとコンピュータ」を開いて確認した後、引き続き、ドメインに参加するコンピュータの１つに、メンバーサーバとなるメールサーバのインストールマシンを登録しておきます。ここでは、Computers の中にメールサーバのコンピュータ名をあらかじめ登録しておきましょう。

③-2 IMSUsers グループの確認

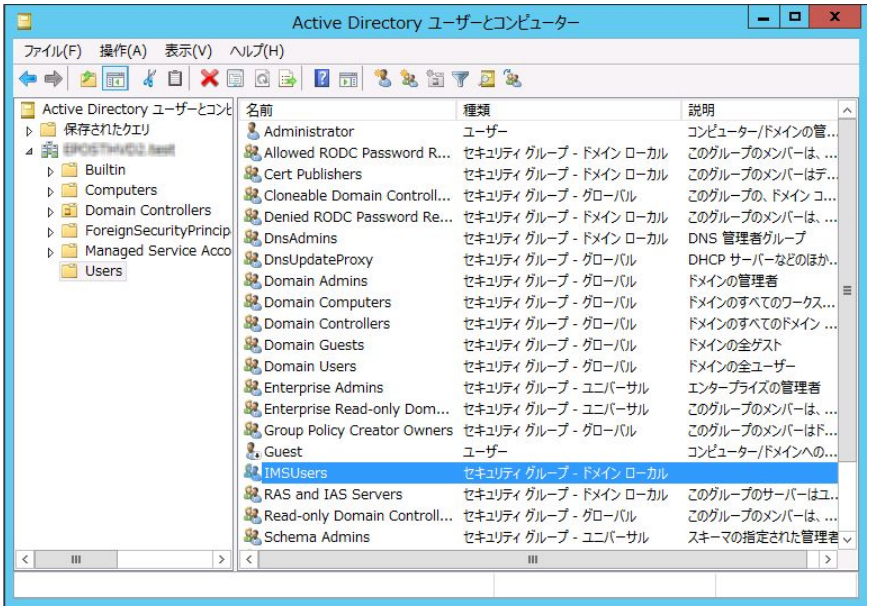
「Active Directory ユーザーとコンピュータ」から、グループ「IMSUsers」が登録済みかどうかを確認します。IMSUsers は、メールサーバのユーザーグループであり、「ドメインローカル セキュリティグループ」です。ユーザーグループ「IMSUsers」が存在していなければ、新たにドメインローカル セキュリティグループとして追加・登録してください。



▲Windows Server 2003 で IMSUsers を確認する



▲Windows Server 2008 で IMSUsers を確認する



▲Windows Server 2012 で IMSUsers を確認する

IMSUsers 以外の手動で作成したメールグループ名を設定するときの注意

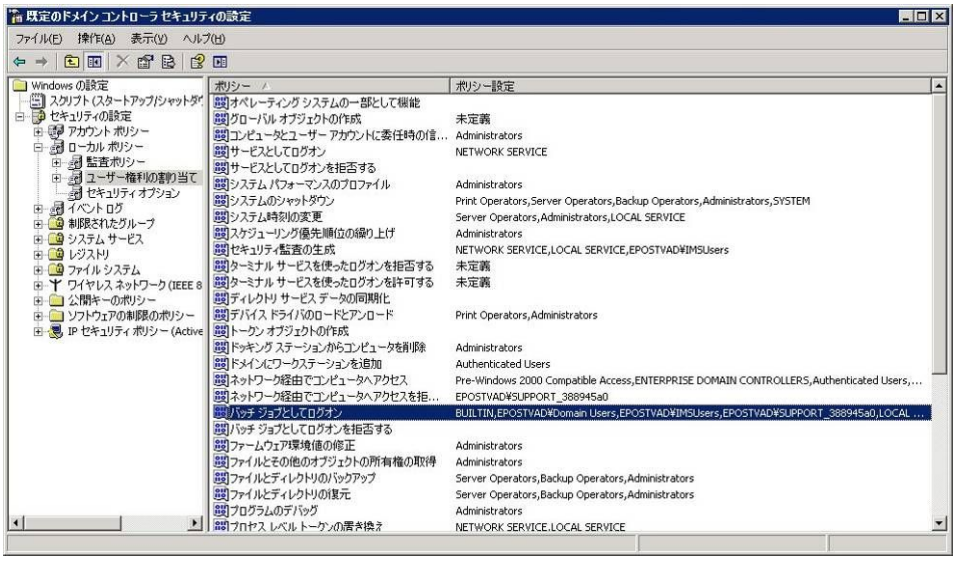
IMSUsers は、初回起動するウィザード（簡易セットアップ）でデフォルトで用意されているメールグループ名です。
IMSUsers 以外に、手動で作成したメールグループ名を設定するときの注意点としては、セキュリティの設定などが煩雑です。IMSUsers を選択しておけば、設定が簡単に完了しますが、任意のメールグループ名を作成したときは、「バッチジョブとしてのログオン」を許可するなど、Windows Server 側での設定がいくつか必要です。

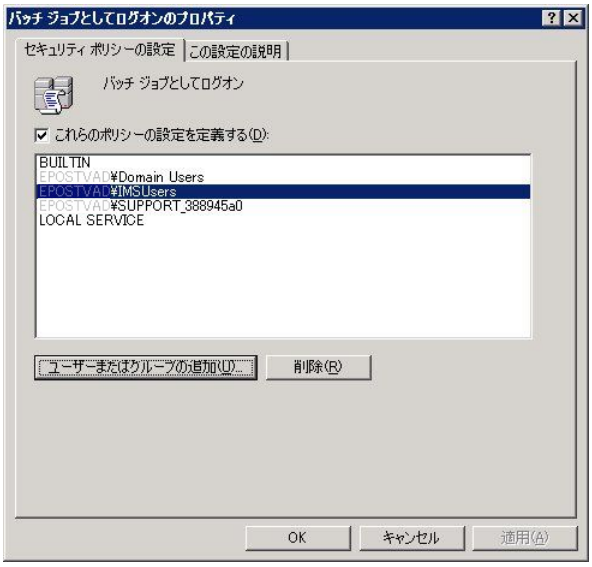
③-3 ドメインコントローラ・セキュリティポリシーの確認

ユーザーグループ"IMSUsers"を追加・登録したときは、「ドメインコントローラ・セキュリティポリシー」を開き「バッチジョブとしてのログオン」が可能になるよう設定します。
（Windows Server 2008 の場合は「グループポリシー管理エディタ」を利用）

●Windows Server 2003 の場合

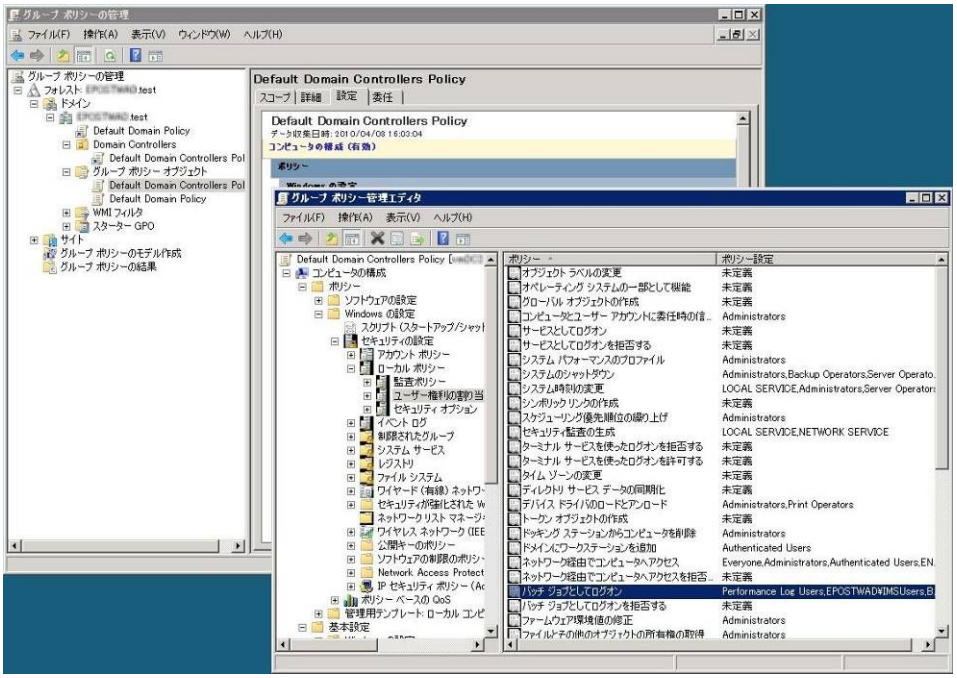
［ドメインコントローラ・セキュリティ・ポリシー］を起動
→［セキュリティの設定］
→［ローカルポリシー］
→［ユーザー権利の割り当て］
→［バッチジョブとしてのログオン］
メール用グループとして利用するドメインローカルグループを追加
（例・IMSUsers）

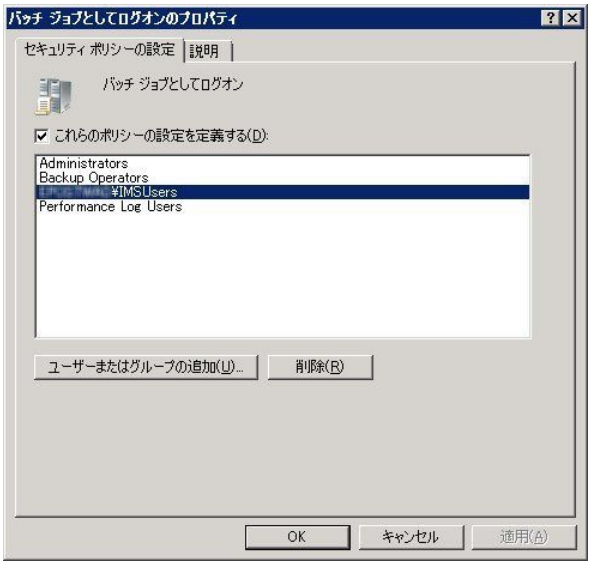




●Windows Server 2008 / 2012 の場合

「グループポリシーの管理」を起動
→［フォレスト ○○○］
→［ドメイン］
→「ドメイン名 △△△」
→［グループポリシーオブジェクト］
→［Default Domain Controllers Policy］
右クリックから「編集」を選択するとグループポリシー管理エディタが起動
「グループ ポリシー管理エディタ」
→［コンピュータの構成］
→［ポリシー］
→［Windows の設定］
→［セキュリティの設定］
→［ローカルポリシー］
→［ユーザー権利の割り当て］
→［バッチジョブとしてのログオン］
メール用グループとして利用するドメインローカルグループを追加
（例・IMSUsers）


グループ ポリシーの管理
ファイル(F) 操作(A) 表示(V) ウィンドウ(W) ヘルプ(H)
Default Domain Controllers Policy
スコープ | 詳細 | 設定 | 委任
Default Domain Controllers Policy
グループ ポリシー管理エディタ
ファイル(F) 操作(A) 表示(V) ヘルプ(H)
ポリシー
ポリシー設定
バッチ ジョブとしてログオン
Performance Log Users,EPOSTWAD¥IMSUsers,B


バッチ ジョブとしてログオンのプロパティ
セキュリティ ポリシーの設定
説明
バッチ ジョブとしてログオン
これらのポリシーの設定を定義する(D):
Administrators
Backup Operators
¥IMSUsers
Performance Log Users
ユーザーまたはグループの追加(U)...
削除(R)
OK
キャンセル
適用(A)

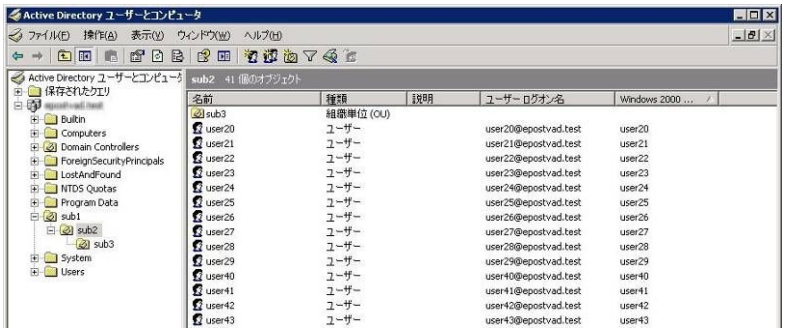
③-4 必要に応じてメールを行うアカウントの所属グループ追加

メール送受信を行いたいアカウントが、既にユーザーとして Active Directory に登録済みのときは、「Active Directory ユーザーとコンピュータ」から、メール送受信を行う個々のユーザーについて、"IMSUsers"を「所属するグループ」として追加します。

なお、メール送受信を行うアカウントが、ユーザーとしてまだ Active Directory に登録されていないときは、E-Post Mail Server の Account Manager からアカウントを登録した後、「Active Directory ユーザーとコンピュータ」で表示させると、"Domain Users"と"IMSUsers"が「所属するグループ」として登録されていることが確認できます。

③-5 必要に応じて OU（組織単位）別に登録する

ユーザーを OU（組織単位）別に登録する場合は、「Active Directory ユーザーとコンピュータ」で、必要に応じて行ってください。OU のどの階層内でもかまいませんが、前項目でも述べたように、メールを行う予定のユーザーは、"IMSUsers"グループに入っていることが必須条件です。



OU（組織単位）に分かれていないときは、特別に作る必要はありません。ドメイン名直下にそのままユーザーを作成してください。

④ E-Post Mail Server インストールマシンの用意

④-1 ドメインに参加させメンバーサーバにする

メールサーバをインストールするマシンについて、Active Directory ドメインに参加させておき、あらかじめメンバーサーバに設定してください。

④-2 再ログイン

通常はドメインに参加させた後、再起動、ログインの手順になります。Windows Server 2003 や Windows Server 2008 / 2012 では、そのまま Administrator 権限でドメインにログインして設定を続行してください。一方、Windows XP や Windows Vista などのクライアント系 OS で設定するときには、再起動後に再ログイン時のユーザー名とログイン先として、それぞれ「Administrator」「このコンピュータ」でログインしてください。

④-3 メンバーサーバ側のセキュリティポリシー設定を確認

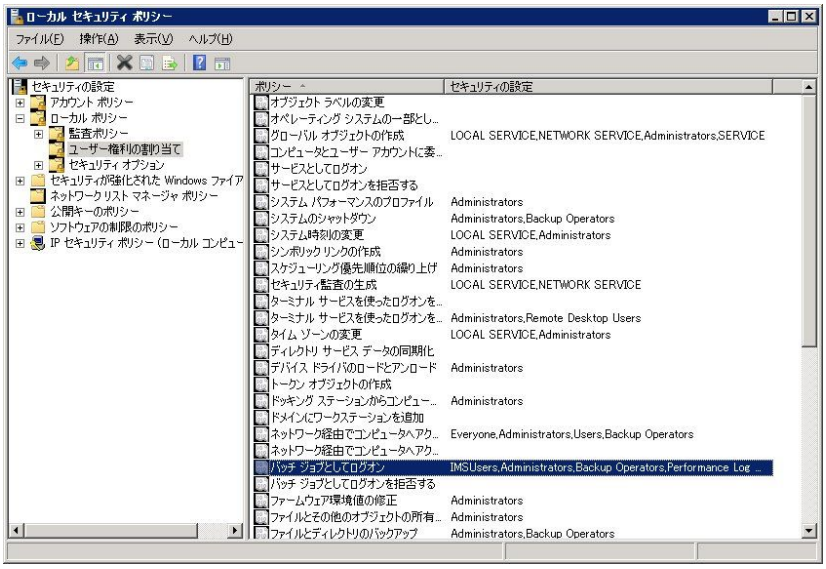
メンバーサーバ側のセキュリティポリシーの設定についても、メール用グループ"IMSUsers"について、確認しておく必要があります。

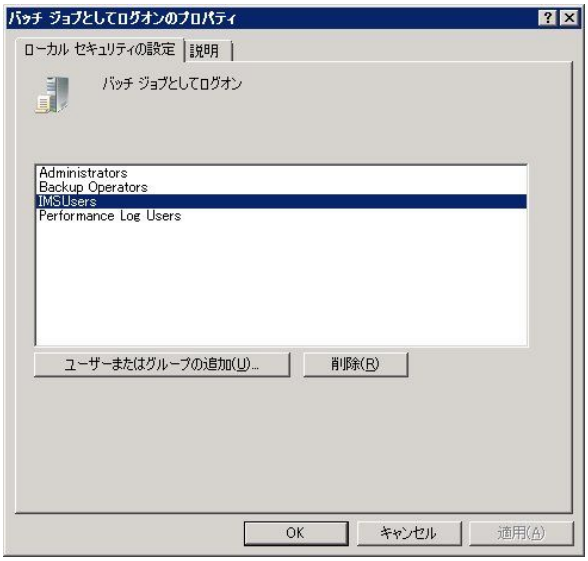
●Windows Server 2003 の場合

［ローカル・セキュリティ・ポリシー］
→［セキュリティの設定］
→［ローカルポリシー］
→［ユーザー権利の割り当て］
→［バッチジョブとしてのログオン］
Active Directory 側のドメインローカルグループ名を追加

●Windows Server 2008 / 2012 の場合

［ローカル・セキュリティ・ポリシー］
→［セキュリティの設定］
→［ローカルポリシー］
→［ユーザー権利の割り当て］
→［バッチジョブとしてのログオン］
Active Directory 側のドメインローカルグループ名を追加





⑤ E-Post Mail Server インストール

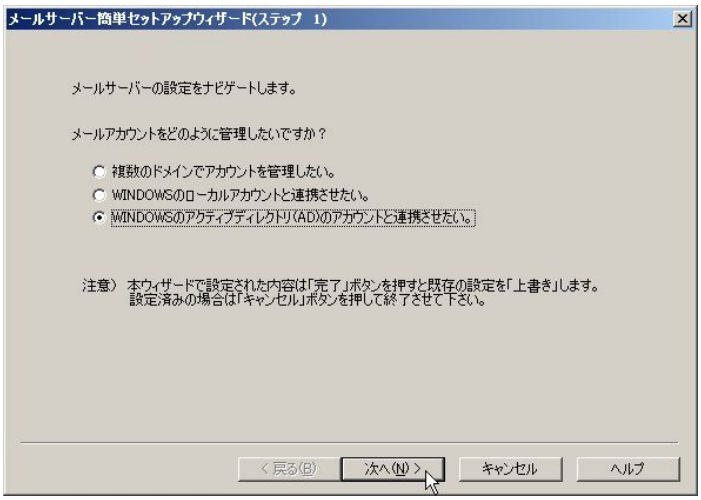
メンバーサーバとして、「Administrator」で Windows ドメインへログイン後、E-Post Mail Server シリーズをインストールします。すでにインストールしてあるときは、次の操作に進んでください。

⑥ ウィザード（簡単セットアップ）の起動

⑤でインストールした直後のときは、E-Post Mail Server のアイコンを初めてダブルクリックすると、自動的にウィザードが起動します。
すでにウィザードを実行したことがあるときは、ウィザードは自動的に起動しませんので、［スタート］メニューから、「E-Post Mail Server for JP」－「簡単セットアップ」を選択します。
Active Directory 連携させる設定を行うとき、手動でも設定できないことはありませんが、ウィザード（簡単セットアップ）を使った方が、設定がよりスムーズに行われ、設定ミスを防ぐことができます。

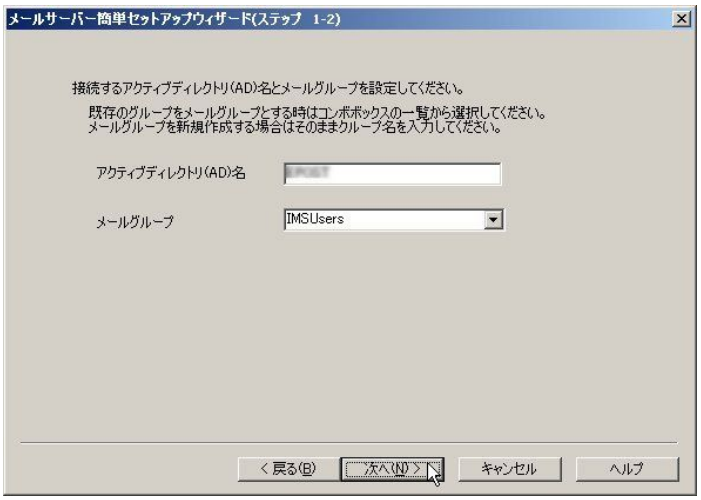
⑥-1 Active Directory アカウントとの連携を選択

ウィザードの（ステップ 1）では、三番目の「Windows の Active Directory アカウントと連携させたい」を選択します。
ドメインコントローラとメンバーサーバが同一マシンとして設定するとき、つまり同居させるときは、二番目の「Windows のローカルアカウントと連携させたい」を選択します。



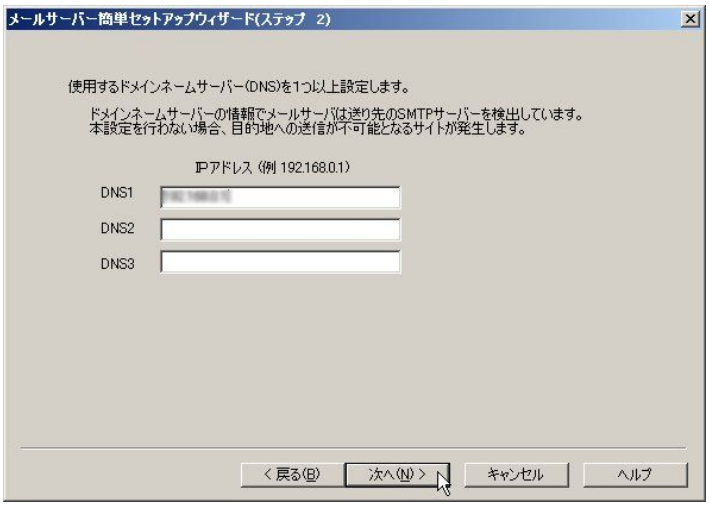
⑥-2 ドメイン名を入力、メールグループには IMSUsers を指定

（ステップ 1-2）では、Active Directory のドメイン名を入力し、メールグループ名として▼ボタンから「IMSUsers」を選択します。Active Directory のドメイン名は、③-1 で確認した「ドメイン名（Windows 2000 以前）」（「ドメイン NetBIOS 名」）を入力します。



⑥-3　DNS サーバには Active Directory のドメインコントローラを入力

（ステップ 2）では、E-Post Mail Server・E-Post SMTP Server が利用する DNS サーバを指定します。
ここで指定する DNS サーバには、Active Directory のドメインコントローラを指定してください。この DNS サーバは、同時にメールサーバが参照する DNS になり、合わせてユーザーアカウント情報を参照する Active Directory のサーバともなります。



なお、ここで指定する DNS サーバは、SMTP 配送部サービスプログラムがメールを送信するときに名前解決のために参照されます。
万が一、Active Directory のドメインコントローラ内に設定される DNS サーバが、外部

の DNS に対してフォワードしていないときは、２番目か３番目の DNS サーバに、外部を参照できる DNS サーバか、DNS 中継機能のあるルータの IP アドレスをさらに指定してください。

メールサーバにおける DNS サーバ情報設定の重要性

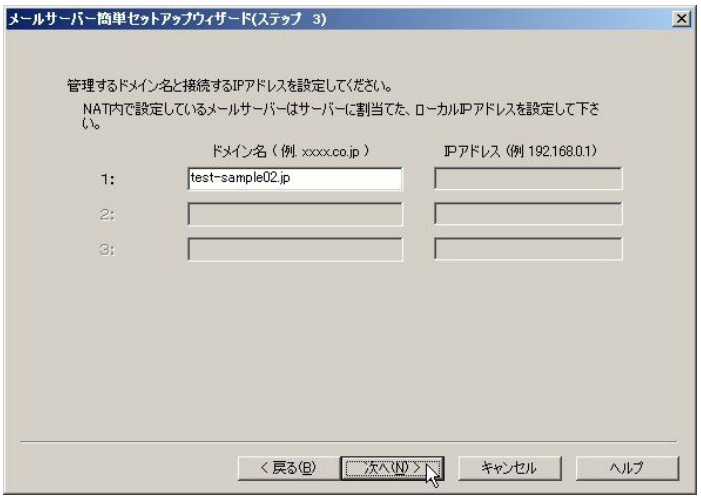
DNS サーバの情報を間違ったり、問い合わせできない DNS サーバの設定を行ったりすると、外部のドメインへメールが送れるところと、送れないところが発生します。
E-Post Mail Server／E-Post SMTP Server シリーズでは、メール送信時、まず最初にウィザード画面及び Mail Control 画面内にある DNS サーバ設定項目を MX レコード参照に用います。MX レコード参照がうまくいかないとき、２回目以降に Windows のネットワーク設定にある DNS サーバ設定値を A レコード参照するために用いる仕様になっています。

つまり、MX レコードの参照がまったくできないときでも、メールがたまたま送れた前者のケースは、ドメイン名が DNS の A レコードでアドレス解決できたために送れてしまうためであり、メールが送れなかった後者のケースは、DNS の A レコードで参照した名前ではうまく接続できなかったためです。
外部に問い合わせが可能な DNS サーバが設定されていないと、送り先のドメインの名前解決ができないことになりますので、実際に運用可能なサーバを構築する際は、十分な注意が必要です。

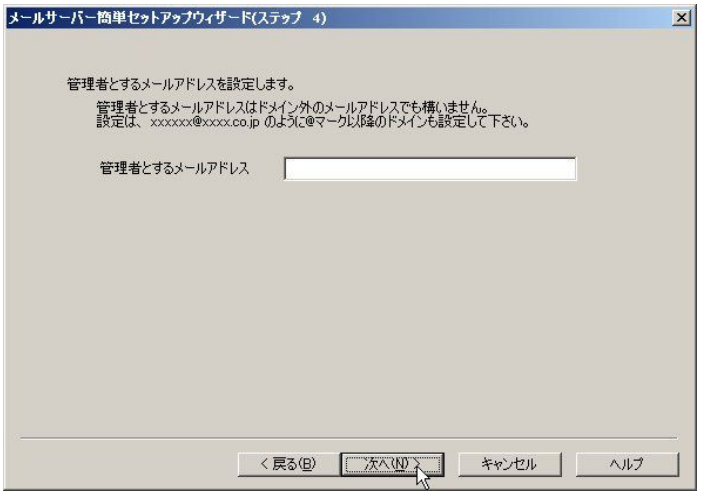
Active Directory 連携のメールサーバを練習用に構築するとき、外部のドメインに配送する必要がなく、動作を確認できればよいというレベルで十分ということでしたら、Active Directory のドメインコントローラに設定する DNS サーバは、外部を参照しない“閉じたサーバ”であってもかまいません。

⑥-4　ドメイン名やメール作業フォルダを設定

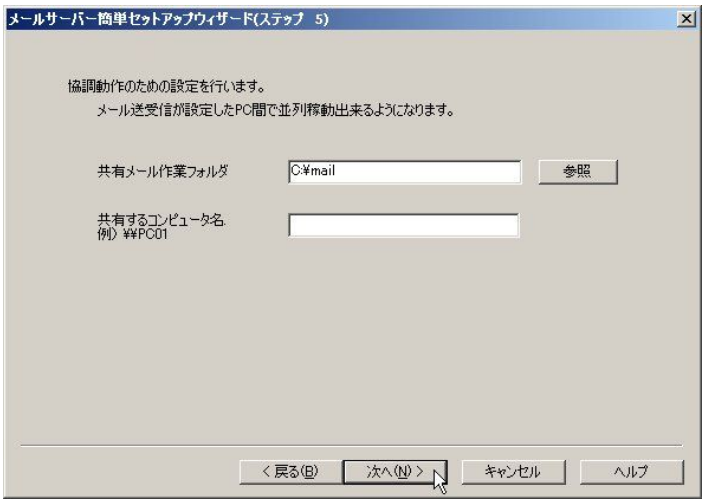
（ステップ 3）では、管理するドメイン名を設定します。



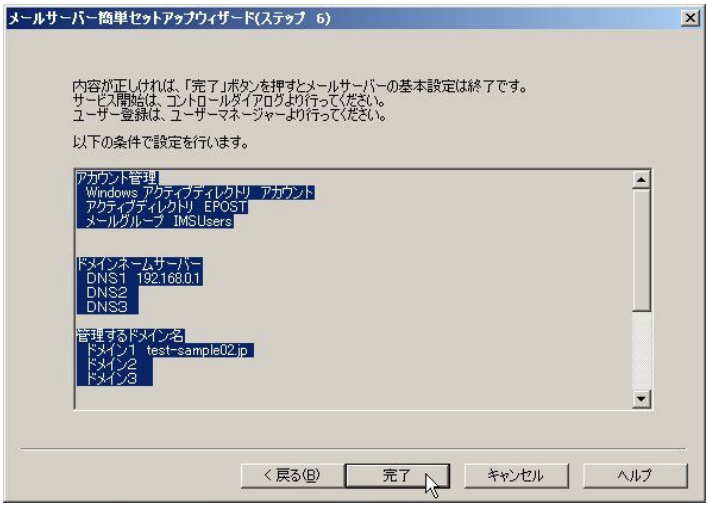
（ステップ 4）は、管理者メールアドレスを設定しますが、決まっていないときは、未入力のまま進めてかまいません。



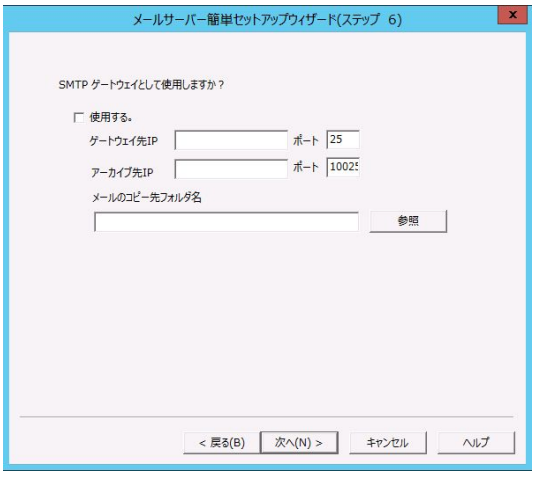
（ステップ 5）は、メール作業フォルダを設定します。シングルサーバにする通常の場合は「C:¥mail」「D:¥mail」などのローカルドライブを設定してください。



最後の（ステップ 6）は、設定情報を確認して［完了］してください。

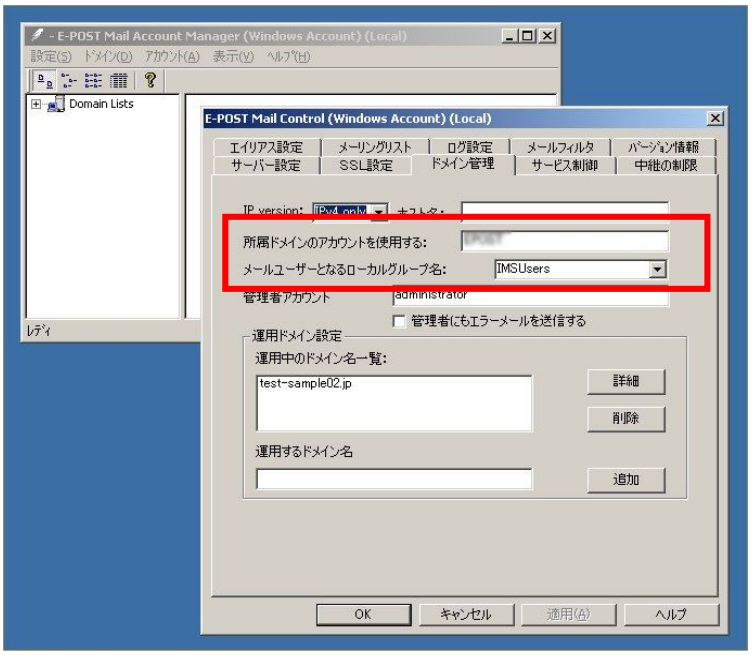


なお、64bit 版では、上の画面の前に下のような画面が表示されますが、特に何も設定しないで次へ進んでください。

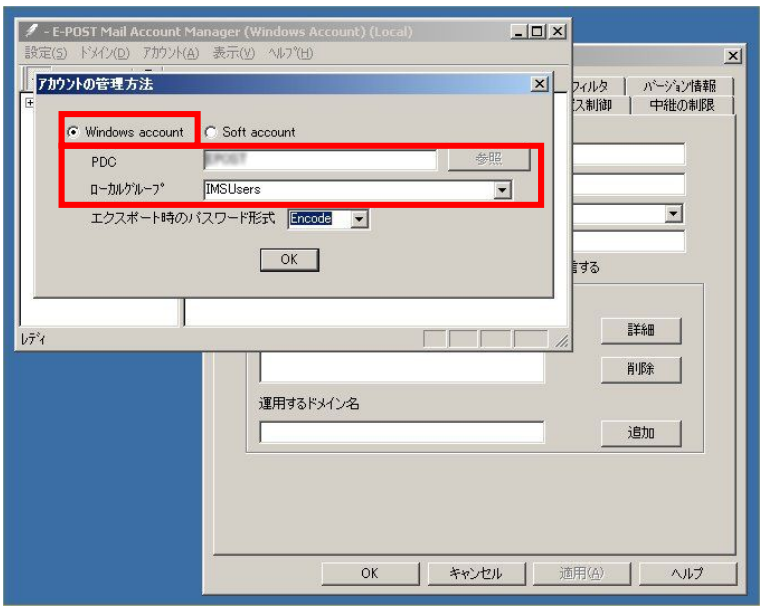


⑦ Active Directory 連携を確認する

自動的に Mail Control が起動したら、「ドメイン管理」タブを選択します。
「ドメイン管理」タブ画面では、ドメイン名が設定されていること、メールユーザーとなるローカルグループ名として、IMSUsers が設定されていることをそれぞれ確認します。
「ドメイン管理」タブ画面で、(Active Directory 連携をしない) 独自アカウント管理のときは「アカウントフォルダ」と表示されていましたが、Active Directory 連携をしているときは、「所属ドメインのアカウントを使用する」表示に変わっています。



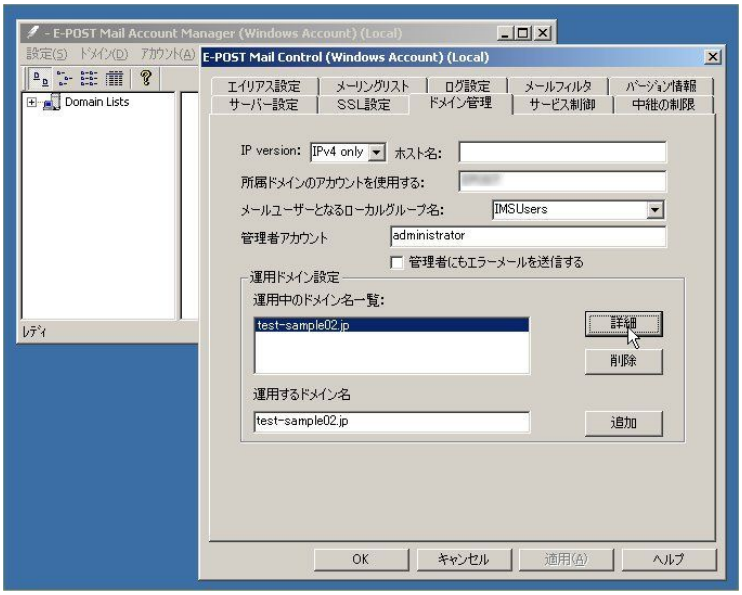
次に、Account Manager に切り替え、「設定」－「アカウント管理」を選択します。
表示される「アカウントの管理方法」ダイアログボックスでは、「Windows account」が選択され、「PDC」にはドメイン名、「ローカルグループ」には「IMSUsers」の MailGroup がそれぞれ設定されているのを確認します。



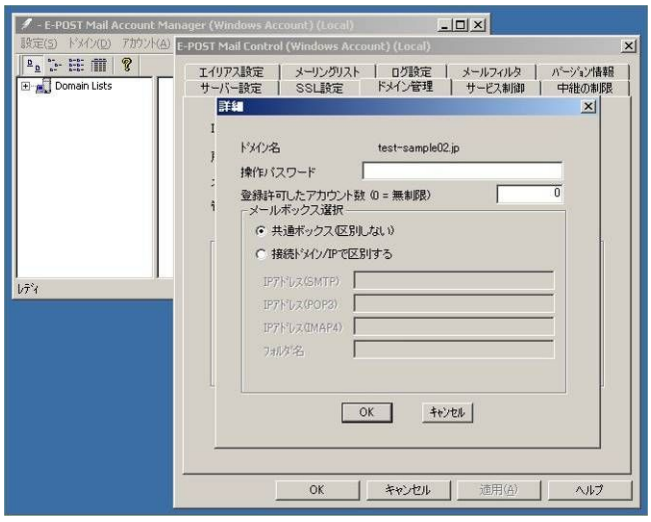
最後に「OK」ボタンをクリックして閉じてください。
ちなみに、ドメインが正常に読めないときや、うまく見つからないときは、「PDC が見つかりません」というエラーメッセージが表示されます。エラーメッセージが表示されたときは、改めて一から設定を見直して確認してください。

⑧ 運用ドメインを詳細で選び、共通メールボックスで運用する設定

続いて「ドメイン管理」タブに表示されている運用中のドメイン一覧からドメイン名を選択し、「詳細」ボタンをクリックします。

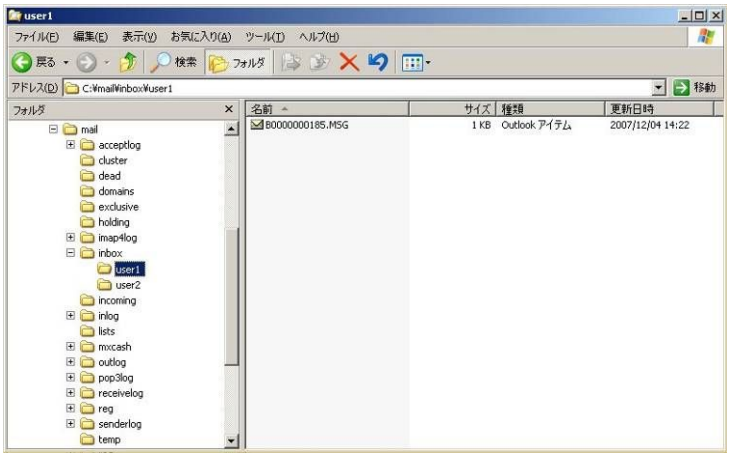


表示される「詳細」ダイアログボックスでは、**「共通ボックス（区別しない）」設定**になっていることを確認してください。「IP/ドメイン別に区別する方式」で運用しているときは、「共通ボックス方式」に切り替える必要があります。Active Directory 連携時のユーザー認証は、@から左のアカウント部分のみであるため、万が一、「区別する方式」のままのメールボックスフォルダの位置では、来ているメールを POP 受信できないことになってしまいます。

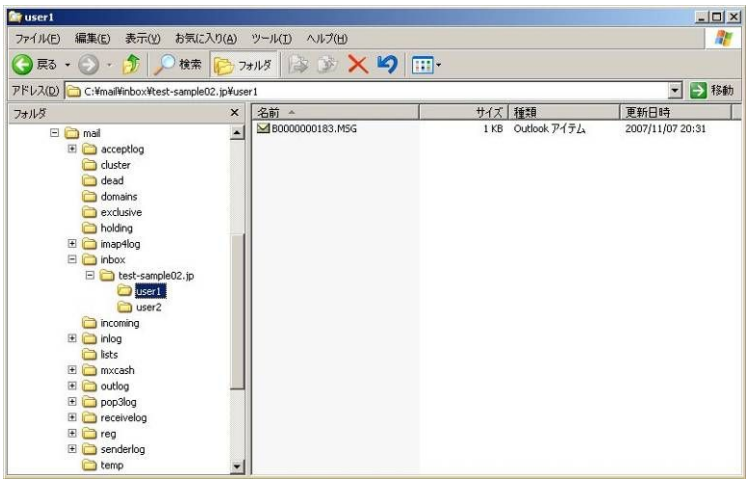


ちなみに、Active Directory 連携時には、マルチドメイン設定は可能ですが、バーチャルドメインでの対応になります。ただし、アカウント名が同一で異なるドメインを作り分けることができないので、完全なマルチドメイン運用はできません。言い換えると、同じアカウント名がなければ、複数のドメインを運用することは可能です。

「共通ボックス」設定で運用したときのメールボックスフォルダ構成は下図のようになり、［メール作業フォルダ］－inbox フォルダの下にアカウント名のメールボックスフォルダが作成されます。
なお、メールクライアントからのログインユーザー名は、アカウント名のみ（例・user1 ）です。



一方、接続ドメイン／IP で区別する設定で運用したときのメールボックスフォルダ構成は下図の通りで、［メール作業フォルダ］－inbox フォルダードメイン名フォルダの下にアカウント名のメールボックスフォルダが作成されています。Active Directory 連携設定の前に、接続ドメイン／IP で区別する設定で運用していたときは、「共通ボックス」設定に切り替える際、メールデータや設定ファイルの手動での移動作業が必要になります。

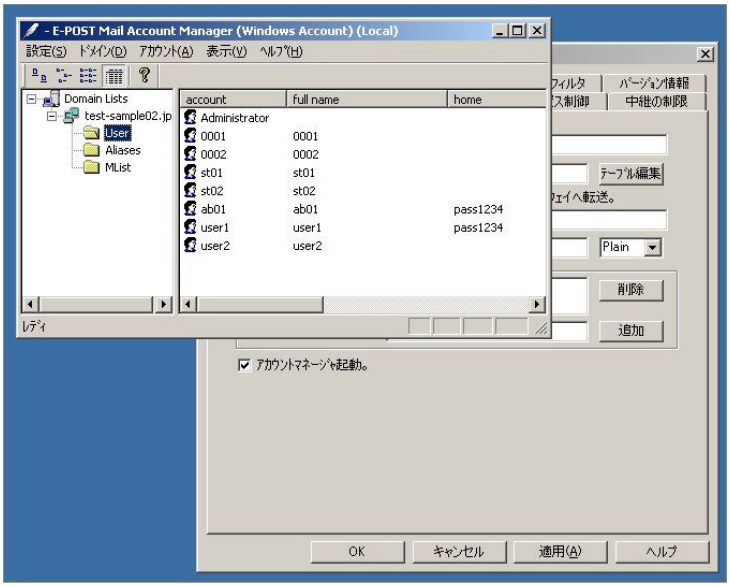


⑨ アカウントマネージャのドメイン名を選択

⑨-1 アカウントマネージャからドメインが選択されているか確認

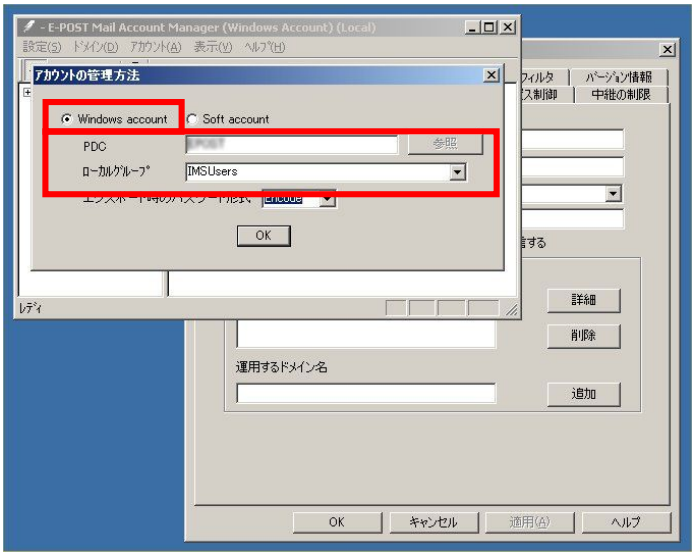
アカウントマネージャに切り替え、Active Directory で管理されているユーザーが読み込めるかどうかを確認します。

左側のツリーから、「Domain List」－「ドメイン名」－「User」を選択します。ドメインを認識しているときでも、MailGroup である IMSUsers に属するユーザーを作成しないときは、ユーザーは表示されません。すでにユーザーを作成しているときには、ユーザーが表示されます。



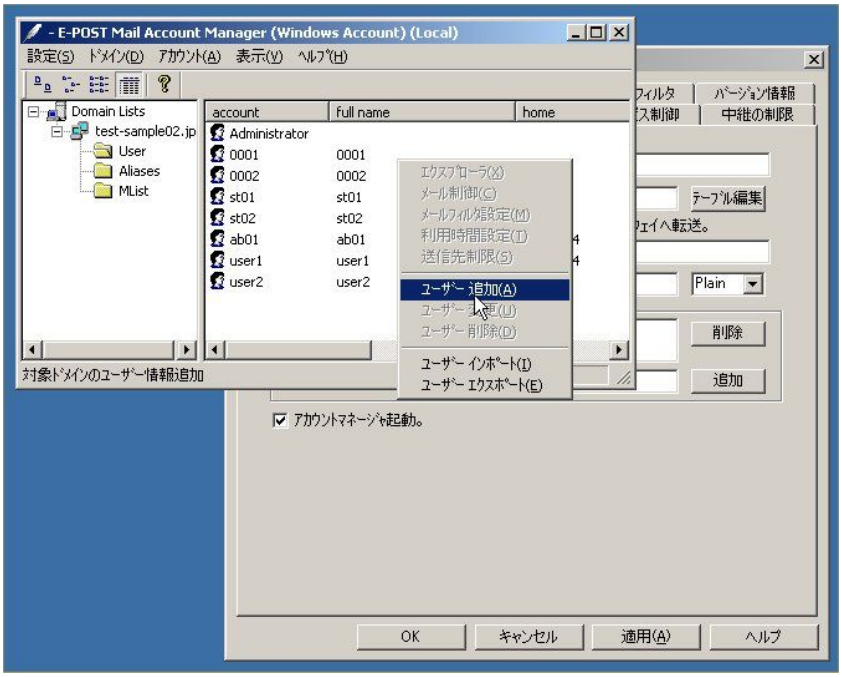
ドメインコントローラをうまく読み込めないときや、「PDC が見つかりません」と表示されたときは、アカウントマネージャの「設定」－「アカウント管理」を選択します。

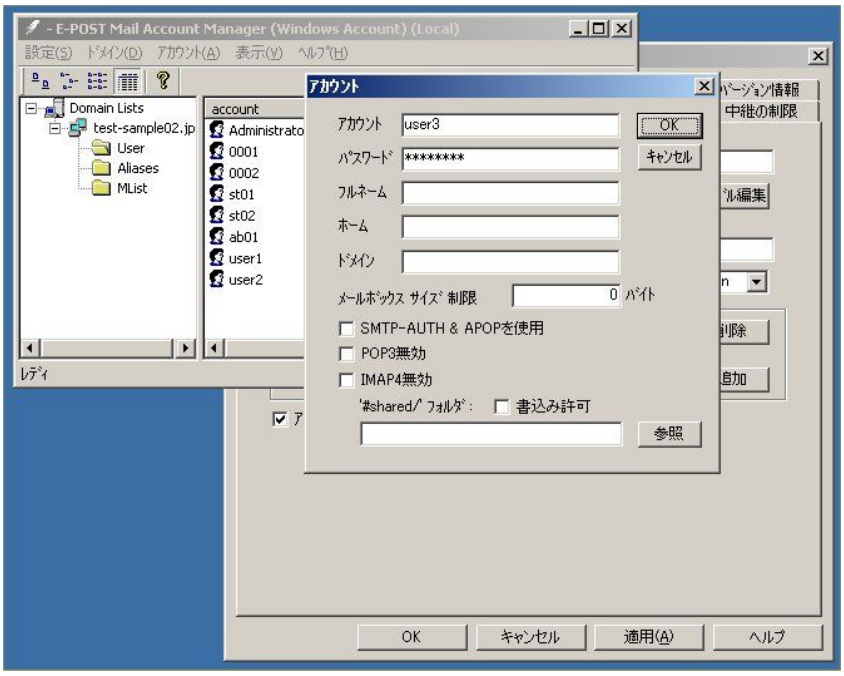
「アカウントの管理方法」ダイアログボックスで「Windows account」が選択されており、「PDC」にドメイン名が入っていなければ再度入力し、「ローカルグループ」に「IMSUsers」が入っていなければ再び入力、最後に「OK」ボタンをクリックします。



⑨-2 User リストを選択しユーザーを追加

アカウントマネージャの左側ツリーから「User」リストを選択し、ユーザーを追加します。右クリックメニューでユーザーを追加し、アカウント、パスワードを入力します。

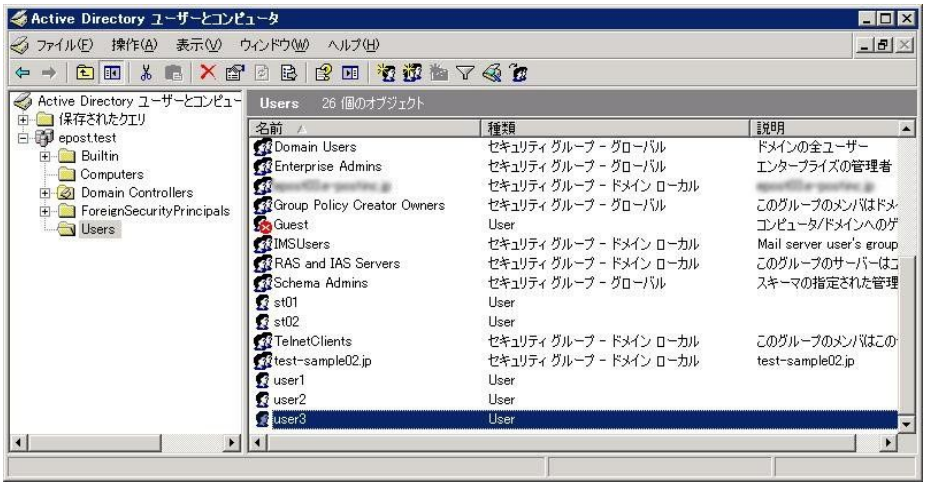




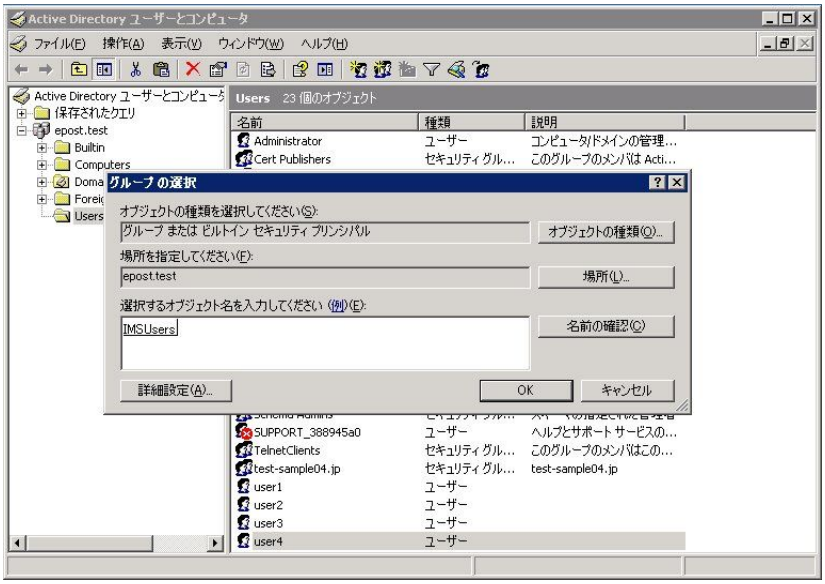
⑨-3 「Active Directory ユーザーとコンピュータ」で追加したユーザーを確認

メールサーバ側のアカウントマネージャから追加したユーザーが、ドメインコントローラ側の「Active Directory ユーザーとコンピュータ」に正常に表示されているかどうかを確認します。
ドメインコントローラの「管理ツール」－「コンピュータの管理」－「Active Directory ユーザーとコンピュータ」を起動します。

「Active Directory ユーザーとコンピュータ」のユーザーとして正式に追加されていることを確認します。



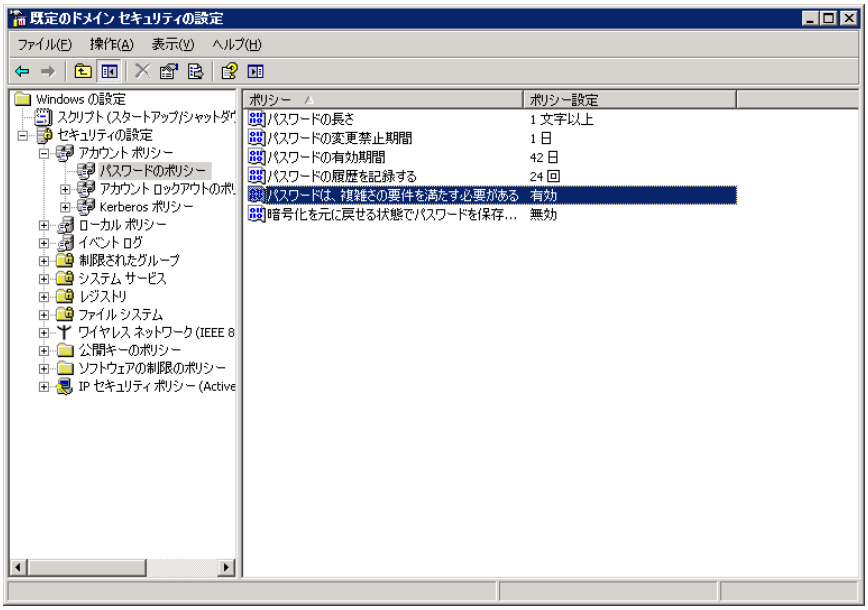
また一方で、ドメインコントローラ側の「Active Directory ユーザーとコンピュータ」からユーザーを追加し、追加したユーザーを IMSUsers に所属させれば、アカウントマネージャ側のユーザー一覧にも追加したユーザーが表示されます。
結果的には、両者が連動していることを確認することができます。

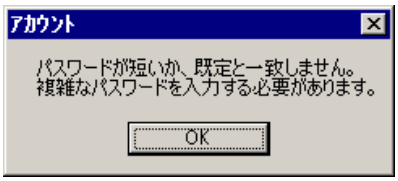


⑩　「パスワードは複雑さの要件を満たす…」設定に影響されることに注意

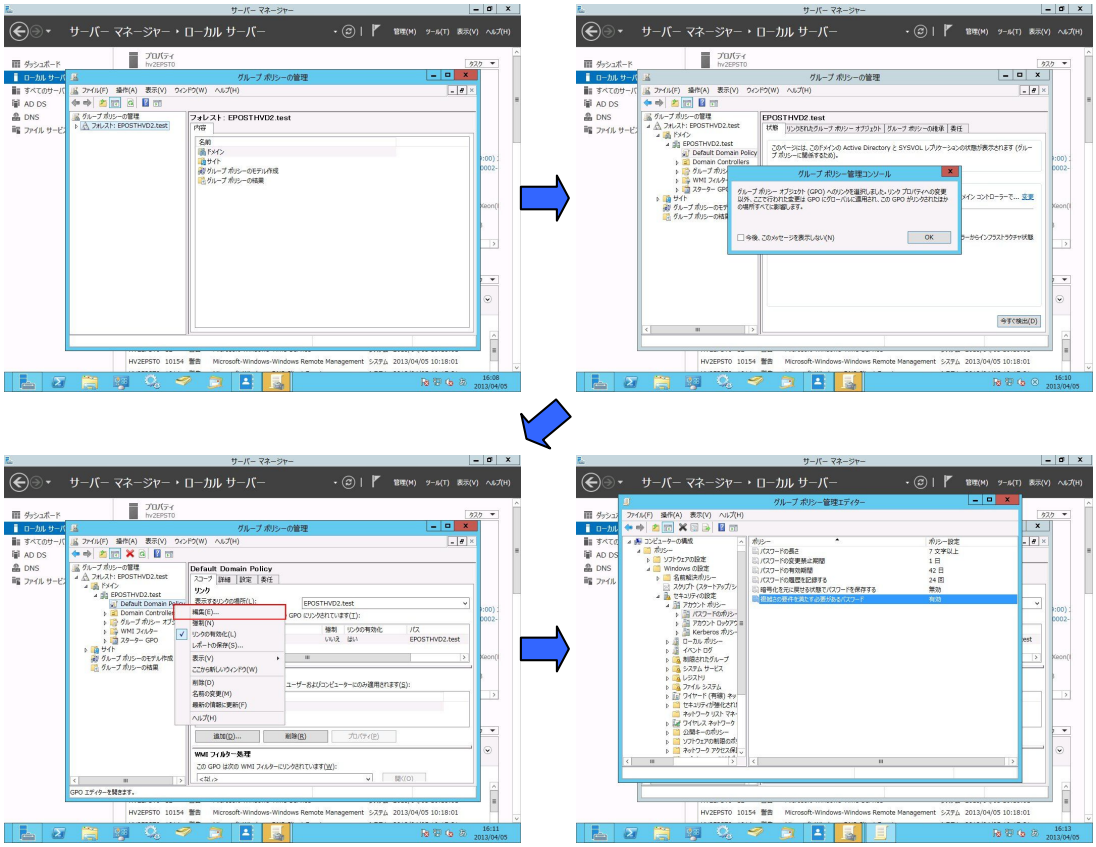
「Active Directory」で管理するアカウント認証パスワードの複雑さ度合いは、ドメインコントローラ側の「管理ツール」－「ドメイン セキュリティ ポリシー」を開くと表示される「パスワードは複雑さの要件を満たす必要がある」設定が「有効」か「無効」かによって影響されます。「ドメイン セキュリティ ポリシー」では、[セキュリティの設定]－[アカウントポリシー]－[パスワードのポリシー]で設定します。
なお、ドメインに参加したマシン全体に適用される「ドメイン セキュリティ ポリシー」の設定内容が、ドメインコントローラマシンだけに適用される「ドメイン コントローラ セキュリティ ポリシー」の設定よりも適用範囲が広いので、間違えないようにしましょう。

「パスワードは複雑さの要件を満たす必要がある」設定が「有効」の場合、ルールに則っていないパスワード、たとえば「12345678」のような数字だけ、「pass1234」のような英小文字＋数字だけのパスワードで、アカウント登録しようとした場合、下図のような警告メッセージが返されるようになり、結果としてアカウント登録はできません。





Windows Server 2012 では「ドメイン セキュリティ ポリシー」ではなく、サーバーマネージャから「グループポリシーの管理」を呼び出して設定します。



1.ドメインコントローラーで[サーバーマネージャー]を起動。
2.[ツール]－[グループポリシーの管理]を選択、[グループポリシーの管理]を起動。
3.デフォルトで「Default Domain Policy」というグループポリシーがドメインに関連付けられており、デフォルト値の確認も兼ねてこれを編集。
4.編集対象のグループポリシーを右クリックし、[編集]を選択。
5.[グループポリシー管理エディター]が起動し、グループポリシーが編集可能な状態になるので、[コンピュータの構成]－[ポリシー]－[Windows の設定]－[セキュリティの設定]－[アカウントポリシー]の順に展開。
6.「パスワードは複雑さの要件を満たす・・・」設定を行ったら、ウインドウの右上にある閉じるボタンをクリックし、グループポリシー管理エディターを閉じる。

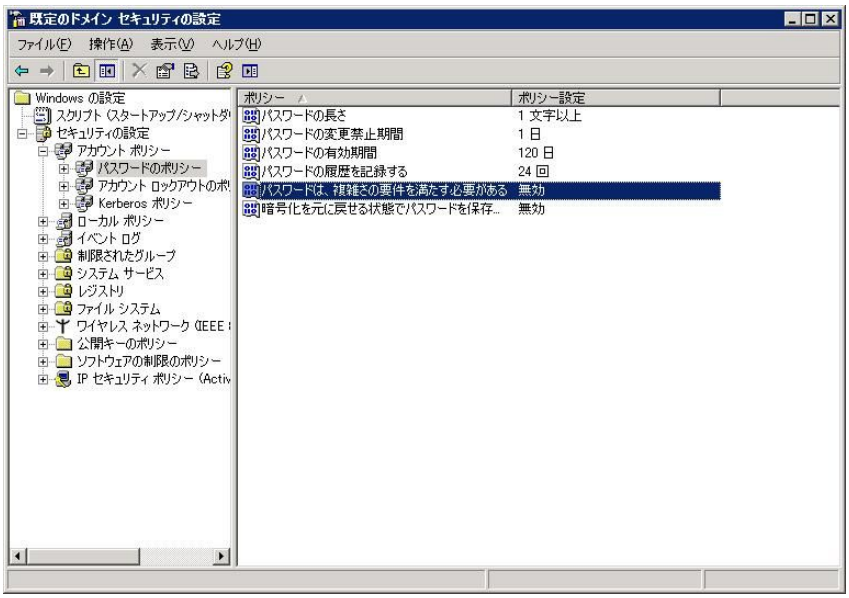
上記の設定がわかりにくければ、他社サイトで恐縮ですが、以下に手順がくわしく書かれていますので参照してください。

http://www.edifist.co.jp/onepoint/Password%20policy.pdf

パスワードが複雑さの要件を満たす条件

1．ユーザーのアカウント名の全部または一部を使用しない。
2．長さは 6 文字以上にする。
3．次の 4 カテゴリのうち 3 つから文字を使う。
英大文字（A ～ Z）
英小文字（a ～ z）
10 進数の数字（0 ～ 9）
アルファベット以外の文字（!、$、#、% など）

もし、上記の条件を満たすことができないパスワードを設定したいときには、「パスワードは複雑さの要件を満たす必要がある」設定を「無効」にします。さらに、状況によっては、「パスワードの長さ」を任意の数字に下げるなどの必要があります。
自明のことですが、こうした状況下では、セキュリティを下げる結果につながることも留意してください。



⑪ メールクライアントに設定情報を登録し、メールの送受信テスト

ユーザー管理情報が Active Directory 連携できていることを確認した後は、実際にメールクライアントに設定情報を登録し、メールの送受信テストをしっかり行いましょう。認証パスワードが使われるのは、POP3 受信のときですので、パスワードが通るかどうかの確認は、メールクライアントから POP3 受信できるかを試せば確認することができます。
メールの送受信テストが問題なく完了すれば、Active Directory 連携のメールサーバ構築の基本設定が完了です。
あとは、通常の独自アカウント管理でおこなうメールサーバ設定と同様、各種設定をおこなってください。

4. 参考情報と応用

Active Directory 連携時の認証パスワードについて

Active Directory 連携時において、認証パスワードが使われるのは、POP3 認証と IMAP4 認証の場合です。SMTP 認証パスワードは AD 側のパスワードとは連動していません。SMTP 認証パスワードの情報は、「認証ファイル」として E-Post 側のアカウント単位で管理され認証時に照合されます。
ただし、ユーザー名については、SMTP 受信時と SMTP 送信リクエスト時のアカウントについて AD のユーザー名がそのままマッチングに利用されます。

Active Directory 連携時の連動項目

アカウント関連の操作内容	連携	Active Directory ユーザーとコンピュータ	連動	E-Post Account Manager
アカウント新規作成	あり	・Window2000 以前のユーザーログオン名(※1) ・表示名	←→ ←→	・アカウント ・フルネーム
アカウント名前変更	あり	・Window2000 以前のユーザーログオン名 ・表示名	←→ ←→	・アカウント ・フルネーム
POP3 パスワード変更	あり	・パスワード	←→	・パスワード
IMAP4 パスワード変更	あり	・パスワード	◄ ►	・パスワード
SMTP 認証パスワード変更	なし	ーー		・SMTP 認証パスワード(※2)
フルネーム	あり	・表示名	←→	・フルネーム
ホームディレクトリ	あり	・ホームフォルダ（ローカルパス）	←→	・ホーム
ドメイン名	あり	・所属するグループ	←→	・ドメイン

※1) 「Active Directory ユーザーとコンピュータ」にある 2003 以降の「ユーザーログオン名」は対象外となり連動項目とはなりません。電子メール、姓や名の項目も対象外です。
※2) 「SMTP-AUTH & APOP を利用する」チェックボックスをオンにし、表示されるダイアログボックス内に SMTP 認証パスワードを入力すると、暗号化された SMTP 認証ファイル "apop.dat"がメールボックスフォルダに作成・保存されます。この SMTP 認証パスワードは「Active Directory ユーザーとコンピュータ」で管理するパスワードとは連動しません。

同一サーバに Active Directory ドメインとメールサーバを設定する場合

Active Directory ドメインを設定したマシン自体にメールサーバをインストールするときは、Active Directory ドメインを使ったユーザー管理ではなく、Windows ローカルアカウントを使ったユーザー管理になります。「簡単セットアップ」（設定ウィザード）のステップ 1 の画面で、「Windows のローカルアカウントと連携させたい」を選択して、設定するようにします。

E-Post Mail Server のドメイン名と AD のドメインの関係

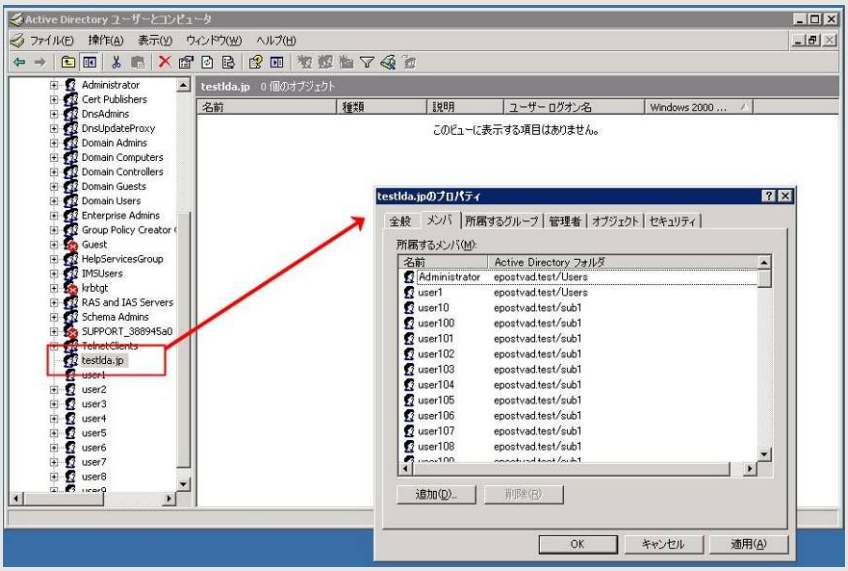
E-Post Mail Server のドメイン名は、Active Directory のドメイン名とは無関係に設定できます。気をつけたいのは、Active Directory に対してはアカウント情報およびそのパスワード情報しか参照していないということです。
また、Active Directory のアカウント情報を参照しているため、アカウントとパスワードの組み合わせは 1 対しか作成はできません。1 つのアカウントに複数のパスワードを設定したりすることは、できませんので注意してください。
なお、Active Directory のドメイン名は、2000 以前の NT ドメイン名として参照します。

Active Directory 連携時にマルチドメイン設定を行うと セキュリティグループが参照されるしくみについて

ActiveDirectry 連携時のメールサーバを移行するため、アカウント情報のエクスポート・インポート作業を行うとき、インポートされたデータ内にはドメイン名があるにもかかわらず、インポート後のアカウント情報を見ても、ドメイン名が空欄のままになっていることがあります。そのようなときは、「ActiveDirectry ユーザーとコンピュータ」の Users の中にドメイン名のセキュリティグループができているはずですので、セキュリティグループのプロパティを開き、「メンバ」タブにユーザーを追加すると、ドメイン名が表示されるようになります。
これは、AD 連携時にマルチドメイン設定を行うと、ドメイン名項目として Active Directory 側のセキュリティグループが参照されるしくみになっていることが理由です。

（解説）
・AD 連携時にも仮想的とはいえ、マルチドメイン対応が取れるようになっています。た

だし、AD 連携時には、アカウント（ユーザー名）が一意のものとして管理されますので、アカウントが重複しなければマルチドメインの設定が可能です。
・単一ドメイン名での管理のときは、ドメイン名が空欄のままで特に問題はありませんが、AD 連携時にマルチドメイン設定を行う場合、所属ドメイン名の区別をつけるため、Account Manager 内でのドメイン名項目は、AD で管理されているセキュリティグループ名を参照するようにしていますので、必ずセキュリティグループ内に加えてください。



・たとえば、次の設定のとき、AD で管理されているセキュリティグループ内それぞれにユーザーが所属されていることになります。

（メールサーバ側の Account Manager）

アカウント	ドメイン名（domain）
user1	abc.jp
user2	abc.jp
user3	def.jp
user4	def.jp
user5	ghi.jp
user6	ghi.jp

（Active Directory 側）

セキュリティグループ	所属ユーザー
abc.jp	user1,user2
def.jp	user3,user4
ghi.jp	user5,user6

・つまり、AD 連携時に、メールサーバ側の Account Manager で表示したときに、ドメイン名項目（domain）が空欄になっているものは、セキュリティグループに所属していないことになります。
・アカウントデータをエクスポートする際は、Account Manager で表示されている状態をそのまま出力します。つまり、ドメイン名項目（domain）が空欄になっているものは、そのまま空欄として出力します。

Active Directory 連携時のアカウント情報インポートの挙動について

１．Active Directory 連携時のインポート動作について

Active Directory 連携時に、Account Manager にてインポートを行った場合の動作についてパターン別にまとめると下記のようになります。

パターン A. Active Directory 上に存在せず かつ E-Post に存在しない Account の場合
インポートすると次の結果になります。
・アカウント（＝AD のメンバー）を作成
・IMSUser グループへのメンバー追加
・メールボックスフォルダの作成可能状態
・各種フラグの設定可能状態

パターン B. Active Directory 上に存在し かつ E-Post に存在しない Account の場合
インポートすると次の結果になります。
・IMSUser グループへのメンバー追加
・それ以外はなにもしない

パターン C. Active Directory 上に存在し かつ E-Post に存在する Account の場合
この場合、インポートしても、何も変更しません。

２．Active Directory 連携時のインポートで「ドメイン」がインポートされない制約事項

Active Directory 連携時、マルチドメイン設定のために[Domain]名項目にドメイン名を指定してインポートを行った場合、「ドメイン」は下記の環境で正しくインポートできない制約があります。なお、このとき AD 側に該当ドメイン名の「セキュリティグループ」が自動作成されますが、そのグループ内にメンバーは自動的には入りません。

下記の OS を Active Directory のドメインコントローラにしている場合、AD 連携時のインポートで[Home]および[Domain]項目がインポートできません。

・Windows Server 2008 R2(64bit) / 2008 SP1 (64bit) / 2008 SP1 (32bit)

また、下記の OS を Active Directory のドメインコントローラにしている場合、[Domain]項目がインポートできません。一方で[Home]項目はインポートされます。

・Windows Server 2003 SP2(32bit)

上記の環境では、インポート作業後に、AD 側の「Active Directory ユーザーとコンピュータ」から、該当ドメイン名の「セキュリティグループ」にメンバーを追加しておくことが必要です。「セキュリティグループ」を選び、メンバーを追加、加入させてください。これは、E-Post Mail Server 側で、「Domain」項目が入っていないと、マルチドメイン構成時に区別がつかなくなってしまうためです。シングルドメイン構成時には、この作業は必須ではありませんが、念のため、自動作成された「セキュリティグループ」に、メンバーを追加、加入させておくことを推奨します。

Active Directory への問い合わせリトライ間隔と時間を調整するには

Active Directory 連携時に、メールサーバから AD への問い合わせが大量に発生するケースで、認証に時間がかかる現象のときには、2009 年 12 月以降にリリースされたモジュールで追加されたレジストリ項目によって、AD への問い合わせリトライ待ち時間を短く調整できるようになりました。さらに、従来から用意されているレジストリ項目を組み合わせることで、AD への問い合わせリトライ総時間の調整が可能です。
もともと、E-Post Mail Server が AD 連携環境にてパスワード認証をする際、メールサーバから AD に向けて、ユーザー検索のリクエストを数回行う仕様になっています。このとき、AD への問い合わせリトライ間隔は、従来バージョンではプログラム内部で 1 秒固定ですが、新しいバージョンでは、このリトライ間隔を調整できるようになっています。

2009 年 12 月以降に公開されている最新差分を適用後、レジストリのキー"ADRetryMSec"を DWORD で作成、数値を設定することによって、リトライ間隔を調整できるようになります。このキーが有効なサービスプログラムのバージョンは以下の通りです。

・EPSTRS　　4.63 以降
・EPSTDS　　4.47 以降
・EPSTPOP3S　4.26 以降
・EPSTIMAP4S　4.30 以降

[AD 連携時のユーザー情報問い合わせリトライ間隔（リトライ待ち時間）設定レジストリ]

HKEY_LOCAL_MACHINE
　→SYSTEM
　　→CurrentControlSet
　　　→Services
　　　　→EPSTRS
　　　　　→ADRetryMSec (DWORD) デフォルト 1000（ミリ秒）
　　　　→EPSTDS
　　　　　→ADRetryMSec (DWORD) デフォルト 1000（ミリ秒）
　　　　→EPSTPOP3S
　　　　　→ADRetryMSec (DWORD) デフォルト 1000（ミリ秒）
　　　　→EPSTIMAP4S
　　　　　→ADRetryMSec (DWORD) デフォルト 1000（ミリ秒）

（例）デフォルト 1000（ミリ秒）＝1 秒　→　300（ミリ秒）＝0.3 秒

レジストリ設定値を変更したときは、各サービスの再起動が必要です。

ちなみに、上記バージョンからは、AD 連携設定時に、メールボックスの設定が環境変数 %USERNAME% を含む設定のときに限り、AD への問い合わせ２回目以降にホームフォルダの検索をしないようにしました。その結果、AD 連携時の処理速度の高速化がはかられています。環境変数 %HOME% を含む設定のときは変わりません。

なお、リトライ回数を設定するための"ADRetryTime"キーについては、従来バージョンから有効であり、最新版でも利用可能です。

[AD 連携時のユーザー情報問い合わせリトライ回数設定レジストリ]

HKEY_LOCAL_MACHINE
　→SYSTEM
　　→CurrentControlSet
　　　→Services
　　　　→EPSTRS
　　　　　→ADRetryTime (DWORD) デフォルト 10（回）
　　　　→EPSTDS
　　　　　→ADRetryTime (DWORD) デフォルト 10（回）
　　　　→EPSTPOP3S
　　　　　→ADRetryTime (DWORD) デフォルト 10（回）
　　　　→EPSTIMAP4S
　　　　　→ADRetryTime (DWORD) デフォルト 10（回）

レジストリ設定値を変更したときは、各サービスの再起動が必要です。
この新しい"ADRetryMSec"値と、従来バージョンから設けられている"ADRetryTime"値との掛け算によって、AD への問い合わせリトライ総時間が決まります。言い換えると、AD リトライ待ち時間×AD リトライ回数の調整で AD 問い合わせリトライ時間を調整します。

ADRetryMSec 値（ミリ秒）×ADRetryTime 値（回）＝
AD ユーザー情報問合せリトライ総時間

例）1000 ミリ秒（1 秒）×10 回＝10 秒
　　300 ミリ秒（0.3 秒）×30 回＝9 秒
　　300 ミリ秒（0.3 秒）×20 回＝6 秒

調整のしかたによっては、AD への問い合わせが大量に発生するケースで、リトライ待ち総時間が増えたり、認証できず接続エラーが増える状況も考えられます。設定値を変更するときは、速度を上げることだけを目的としないで、より安全かつ確実に認証が通ることを確認した上で変更作業を行ってください。

Active Directory 連携時にまれに送信エラーになったり、POP 受信エラーが発生するとき

アカウントの Active Directory 連携（AD 連携）をしているとき、E-Post Mail Server と AD（ドメインコントローラ）との間で通信に時間がかかることが原因となり、ふだんは正常に送ることができる社内メールで、まれに送信エラーになったり、POP 受信エラーになることが発生することがあります。そのような事象が発生する場合、メールサーバと AD（ドメインコントローラ）との間の通信で少し時間がかかることにより、ユーザーのマッチングが完ぺきにできていないおそれがあります。AD（ドメインコントローラ）との間で、通信タイムアウトの設定を見直してください。

AD との通信については、下記のレジストリ項目によって、リトライ回数を上げて試すことができるようになっています。 "ADRetryTime"のキーはデフォルトで作成されていませんので、DWORD 値 10 進でキーを新規作成し、値を 10 より上の任意の数、たとえば 20 や 30 などの数値を入れて試してください。変更後は、該当する各サービスの再起動が必要です。この"ADRetryTime"キーは、EPSTRS、EPSTDS、EPSTPOP3S、EPSTIMAP4S それぞれに作成、設定します。

[AD 連携時のユーザー情報問い合わせリトライ回数設定レジストリ]
[EPSTRS] (E-POST SMTP Receiver)
HKEY_LOCAL_MACHINE
→SYSTEM
　→CurrentControlSet
　　→Services
　　　→EPSTRS
　　　　→ADRetryTime
　　　　(DWORD Default 10) AD へのユーザー情報問合せリトライ回数

[EPSTDS] (E-POST SMTP Delivry Agent)
HKEY_LOCAL_MACHINE
→SYSTEM
　→CurrentControlSet
　　→Services
　　　→EPSTDS
　　　　→ADRetryTime
　　　　(DWORD Default 10) AD へのユーザー情報問合せリトライ回数

[EPSTPOP3S] (E-POST POP3 Server)
HKEY_LOCAL_MACHINE

→SYSTEM
　→CurrentControlSet
　　→Services
　　　→EPSTPOP3S
　　　　→ADRetryTime
　　　　(DWORD Default 10) AD へのユーザー情報問合せリトライ回数

[EPSTIMAP4S] (E-POST IMAP4rev1 Server)
HKEY_LOCAL_MACHINE
→SYSTEM
　→CurrentControlSet
　　→Services
　　　→EPSTIMAP4S
　　　　→ADRetryTime
　　　　(DWORD Default 10) AD へのユーザー情報問合せリトライ回数

Active Directory 連携時、AD 側から ユーザーログオン名を変更したときの注意点

Active Directory 連携時、AD のドメインコントローラ側からユーザーログオン名を変更するときは、注意してください。E-Post が AD 連携設定された状態のとき、AD のドメインコントローラ側から、IMSUsers グループ内のユーザーログオン名を変更したときは、Account Manager のユーザー表示のうち、アカウントは AD 側のユーザーログオン名と連動して変わります。ただし、メールボックスフォルダの扱いに関して、注意する必要があります。

それは、連動してメールボックスフォルダはリネームされないということです。AD のドメインコントローラ側のユーザーログオン名を変更した場合、それに連動して Account Manager のユーザー表示のアカウントが変更されますが、それに合わせてプロトコル発生時にメールボックスフォルダが自動的に新しく生成されます。
しかし、以前の古いアカウント名からのメールボックスフォルダは引き継がれません。これは仕組み的にフォルダのリネームではなく、新規作成になってしまうからです。古いメールボックスフォルダに保管されていたメールデータや、自動転送・自動応答などの設定ファイルなどは新しいメールボックスフォルダに移行されず、残ったままになります。

アカウント名を変更する場合は、ドメインコントローラ側の「Active Directory ユーザーとコンピュータ」からではなく、E-Post Account Manager から変更すれば、そのような

問題は発生しません。

もし、AD のドメインコントローラ側からしか、変更する段取りができないのであれば、古いメールボックスフォルダに入っているメールデータ（拡張子.MSG）や各種設定ファイル（拡張子.dat や拡張子.CTL など）をまるごと新しいメールボックスフォルダへコピーする必要があります。

Active Directory 連携時でのログインパスワードにダブルクォーテーション（″）や円マーク（¥）を使用しているときの問題と対応について

Active Directory 連携時でのログインパスワードにダブルクォーテーション（"）や円マーク（¥）の文字を使用しているとき、POP3/IMAP4 サービス利用時に該当するログインユーザーは、パスワードを正しく返すことができず、結果として認証エラーとなります。この問題の原因として、POP3 サービス時の USER 命令、IMAP4 サービス時の LOGIN 命令を受ける際、ダブルクォーテーションが含まれているパスワードの場合に、ダブルクォーテーション（"）以降の文字列をいわゆる囲み文字として、削る処理を行うことが原因です。円マーク（¥）が含まれているパスワードも同様です。そのため、正常にパスワード取得ができないために認証が失敗する結果になります。

現行バージョンでの運用にあたっては、Active Directory 連携時でのログインパスワードにダブルクォーテーション（"）や円マーク（¥）を禁則文字として扱っていただくようお願いします。
2016 年以降の次期最新差分アップデートで公開する予定である EPSTPOP3S v4.35～および EPSTIMAP4S v4.50～のバージョンでは、Active Directory 連携時でのログインパスワードにダブルクォーテーション（"）および円マーク（¥）を使用しているときでも、パスワードとして有効に通すことができるように対策が取られる予定です。

5. トラブルシューティング

サービス開始・サービス終了ができない

E-Post Mail Server インストール・セットアップ時には、Administrator 権限が必要なので、Administrator そのものか、Administrators グループに入っているユーザーでログインしてセットアップを行います。
ウィザードでドメインコントローラ名を指定して、設定を完了した後、Administrator で再ログインし直して確認しましょう。
なお、Active Directory 連携を行うときの、サービス登録時の権限は、Local System 権限で行っても、Administrator 権限で行っても、どちらでもかまいません。
また、デバッグモードでプログラムが正常に動作するものかどうか調べる必要があることもあります。万が一、プログラムファイルが破損してしまっているかどうかを調べることができます。デバッグモードの使い方は下記の通りです。

Active Directory ユーザーが Account Manager に表示されないとき

E-Post Mail Server 側でユーザーグループの指定を IMSUsers にしておきましょう。
うまくいかないときは、簡単セットアップをもう一度起動し、指定します。
また、Windows サーバ側の「Active Directory ユーザーとコンピュータ」でユーザーを追加する際は、ユーザーグループ IMSUsers 内に追加するのを忘れないようにします。

デバッグモードの使い方

1．各サービスを停止する。
2．コマンドプロンプトを開く。
3．カレントフォルダについてプログラムインストールしたフォルダに移動。

```
cd "C:¥Program files¥EPOST¥MS" 《Enter》
```

4．EPSTDS サービスのデバッグモードを起動するには、epstds　–debug と入力。

```
epstds  -debug 《Enter》
```

ステータスやメッセージがたくさん表示されれば、プログラムファイルの破損はなく、基本的に正しいプログラムファイルといえます。
このデバッグモードの最中にクライアントからメールの送受信テストを行うことができ、表示される画面で基本的な動作を確認することができます。
デバッグモードは《Ctrl》＋[C]キーを押して停止します。
他のサービスのデバッグモードも同様にオプションをつけて起動します。

6. 索引