<u>E-Post Mail Server</u> <u>E-Post SMTP Server</u>

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-

Rev.1.5





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

1.	メールサーバの Active Directory 連携とは	5 -
2.	Active Directory 連携のメリット・デメリット	- 6 -
1	ユーザー管理の一本化	- 6 -
2	バーチャルドメインによる使用時の注意	- 6 -
З.	Active Directory 連携とメールサーバ設定方法の手順	7 -
3	Active Directory ドメインコントローラの用意	7-
4	E-Post Mail Server インストールマシンの用意	14 -
5	E-Post Mail Server インストール	16 -
6	ウィザード(簡単セットアップ)の起動	16 -
\bigcirc	Active Directory 連携を確認する	21 -
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	22 -
9	アカウントマネージャのドメイン名を選択	24 -
(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	27 -
(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	29 -
4.	参考情報と応用	- 30 -
Act	ive Directory 連携時のユーザー認証について	- 30 -
<u> </u>	・サーバに Active Directory ドメインとメールサーバを設定する場合	31 -
E-P	Post Mail Server のドメイン名と AD のドメインの関係	31 -
Win	dows XP Pro でのインストール・設定作業の注意	31 -
Act	ive Directory への問い合わせリトライ間隔と時間を調整するには	32 -
Act	ive 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	プが参照さ
れる	しくみについて	34 -
5.	トラブルシューティング	36 -
6.	索引	37 -



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。

🗳 Active Directory ユーザーとコンピ	1-9	
- ≪ ファイル(E) 操作(A) 表示(公 !	rンドウW ヘルプ(H)	
	😫 💷 🦉 🦉 💩 🖓 🍕 🙍	
Active Directory ユーザーとコンピュー	epost.test 5個のオブジェクト	
E EP	名前 🔺	説明
- Builtin - Computers - 20 Domain Controllers	posttestのプリパティ 全般 管理者 グループ ポリシー	ault container for upgr ault container for dom ault container for sec
Users	请	ault container for upgr
	ドメイン名 (Windows 2000 以前)(小) 現明(小): ドメインの機能レベル(小): Windows 2000 混在 フォレストの機能レベル(上): Windows 2000	- 一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一
		🐜 🜒 🖞 舟役 🕺 🍘 🕜 CAPS 🗧

▲Windows Server 2003 で作成済みドメイン名を確認する



I Active Directory ユーザーと	コンピュータ			- D ×
ファイル(F) 操作(A) 表示(V)	ヘルプ(H)			
🧢 🔿 🖄 📅 📋 🗔 🖉	ù 🕞 🛛 🖬 🗏 🐭 🛅 🦷	7 🧕 🖗		
 □ Active Directory ユーザーとコン Ⅲ □ 保存されたクエリ 	ピュ 名前 Builtin	種類 builtinDomain	【説明	I
E Britis Twitte sault	Computers	コンテナ	Default co	ntainer for upgr
E Computers	のプロパティ		? ×	tainer for sec
I I I Domain Controllers I I I I Domain Controllers I I I I Domain Controllers I I I I Domain Controllers	主版 管理者		1	tainer for upgr
🛅 Users	EPOSTMAD/well			
		NI)-		
	ERCE TWALE			
	【見日月(D):			
	I			
	ドメインの機能レベル(M): Windows Server 2008			
	フォレストの機能レベル(F):			
	Windows Server 2008			
		OK キャンセル	適用(A)	
	>			-

▲ Windows Server 2008 で作成済みドメイン名を確認する

	EPOSTHVD2 hellのプロパティ ? ×	×
ファイル(F) 操作(A) ● ● ② 匠 ① ● Active Directory ユー ▶ ● 保存されたクエリ ■ © Computers ▶ ◎ Domain Cont ▶ ◎ Domain Cont ▶ ◎ Domain Cont ▶ ◎ Domain Cont ▶ ◎ Users	 全般	月 fault container for fault container for fault container for fault container for fault container for
< 111	OK キャンセル 適用(A)	

▲ 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。

う ファイル(E) 操作(<u>A</u>) 表示(⊻) ウィ	ンドウ(型) ヘルプ(団)		_B_>
- → 🖻 🔢 👗 💼 🗡 😭 [d 🖻 😫 🖬 🎽 🖉 🔤 7	7 🍕 ն	
Active Directory ユーザーとコンピュー	Users 25 個のオブジェクト		
	名前 🛆	種類	[
Builtin	0002	User	
Gomputers	🛿 ab01	User	
- Domain Controllers	🛿 Administrator	User	コンピュータ/ドメインの管理
- ForeignSecurityPrincipals	Cert Publishers	セキュリティ グループ - ドメイン ローカル	このグループのメンバは Ac
- 🔄 Users	💯 Dns Admins	セキュリティ グループ - ドメイン ローカル	DNS 管理者グループ
	22 DnsUpdateProxy	セキュリティ グループ - グローバル	DHCP サーバーなどのほか
9	🚰 Domain Admins	セキュリティ グループ - グローバル	ドメインの管理者
9	Domain Computers	セキュリティ グループ - グローバル	ドメインのすべてのワークス
9	🙀 Domain Controllers	セキュリティ グループ - グローバル	ドメインのすべてのドメイン
9	💯 Domain Guests	セキュリティ グループ - グローバル	ドメインの全ゲスト
9	🙀 Domain Users	セキュリティ グループ - グローバル	ドメインの全ユーザー
1	🔂 Enterprise Admins	セキュリティ グループ - グローバル	エンタープライズの管理者
	🖸 epost03.e-postinc.jp	セキュリティ グループ - ドメイン ローカル	epost03.e-postinc.jp
1	Group Policy Creator Owners	セキュリティ グループ - グローバル	このグループのメンバはドメ
1	🗞 Guest	User	コンピュータ/ドメインへのゲ
1	MIMSUsers	セキュリティ グループ - ドメイン ローカル	Mail server user's group
9	RAS and IAS Servers	セキュリティ グループ - ドメイン ローカル	このグループのサーバーはコ
9	🐼 Schema Admins	セキュリティ グループ - グローバル	スキーマの指定された管理
9	🛿 st01	User	
1	🛿 st02	User	
1	37 TelnetClients	セキュリティ グループ - ドメイン ローカル	このグループのメンバはこの
1	🔐 test-sample02.jp	セキュリティ グループ - ドメイン ローカル	test-sample02.jp
9	🔮 user1	User	
	🛿 user2	User	1
	d		

▲Windows Server 2003 で IMSUsers を確認する

ive Directory ユーザーとコンピュ	名前	種類	[[〕 〕 〕 〕 〕 〕 〕 〕 〕 〕 〕 〕 〕 〕 〕 〕 〕 〕
Itre Directory 2-J-23/23 (#7474/2-DJ) Builtin Computers Domain Controllers Forein/SecurityPrincipals Users	Administrator Administrator Administrator Administrator Cert Publishers Denied RODC Password Domain CODC Password Domain Admins Domain Computers Domain Controllers Domain Guests Domain Guests Domain Guests Domain Guests Enterprise Read-only Do Guest Acup Policy Creator Ow Guest Read-only Domain Contr Read-only Domain Contr Schema Admins	$\begin{array}{c} \frac{14}{12} \\ 2-\Psi^-\\ 2-\Psi^-\\ 2+J^-\\ 2+J^$	認明

▲Windows Server 2008 で IMSUsers を確認する



	Active Directory ユー	ザーとコンピューター	_ 🗆 X
ファイル(F) 操作(A) 表示(V) /	√レプ(H)		
🗢 🔿 🖄 🗊 🔏 🖬 🗙 🛙	1 @ 🗟 🛛 🖬 🗏 🐮 🕯	7 🧕 🐍	
 Active Directory ユーザーとコンと 除存されたクエリ 第一時間 第二時間 第二時間<th>名前 Administrator Administrator Administrator Cert Publishers Coneable Domain Controll Denied RODC Password Re Domain Controllers Domain Computers Domain Computers Domain Computers Domain Controllers Domain Guests Domain Guests Domain Guests Domain Guests Domain Guests Domain Guests Domain Guests Domain Users Enterprise Admins Enterprise Read-only Dom Group Policy Creator Owners Guest MSUsers Read-only Domain Controll Read-only Domain Controll</th><th>種類 ユーザー セキュリティ グループ・ドメイン ローカル セキュリティ グループ・ドメイン ローカル セキュリティ グループ・ゲーハン セキュリティ グループ・ゲーハン セキュリティ グループ・ドメイン ローカル セキュリティ グループ・ゲイン ローカル セキュリティ グループ・ゲローバル セキュリティ グループ・グローバル セキュリティ グループ・ブローバル セキュリティ グループ・グローバル セキュリティ グループ・ゲローバル セキュリティ グループ・ゲローバル セキュリティ グループ・ゲローバル セキュリティ グループ・ゲローバル セキュリティ グループ・ゲローバル</th><th>説明 へ コンピューター/ドメインの管 このガルーブのメンバーは、 このガルーブのメンバーは、 このガルーブのメンバーはボ このガルーブのメンバーはボ このガルーブのメンバーは、 DNS 管理者グルーブ DHCP サーバーなどのほか ドメインの雪々てのドメイン ドメインのすべてのドメイン ドメインのすべてのドメイン ドメインのなくてのドメイン ドメインのなくてのドメイン ドメインのなくてのドメイン ドメインのなくてのドメイン ドメインのなくてのドメイン ドメインのなくてのドメイン ドメインのなくていドメイン ドメインのなくていドメイン ドメインのなくていドメイン ドメインのなくていドメイン ドメインのなくていドメート このガルーブのオンバーは、 このガルーブのサーバーはユ このガルーブのオンバーには、 スキーマの指定された管理者</th>	名前 Administrator Administrator Administrator Cert Publishers Coneable Domain Controll Denied RODC Password Re Domain Controllers Domain Computers Domain Computers Domain Computers Domain Controllers Domain Guests Domain Guests Domain Guests Domain Guests Domain Guests Domain Guests Domain Guests Domain Users Enterprise Admins Enterprise Read-only Dom Group Policy Creator Owners Guest MSUsers Read-only Domain Controll Read-only Domain Controll	種類 ユーザー セキュリティ グループ・ドメイン ローカル セキュリティ グループ・ドメイン ローカル セキュリティ グループ・ゲーハン セキュリティ グループ・ゲーハン セキュリティ グループ・ドメイン ローカル セキュリティ グループ・ゲイン ローカル セキュリティ グループ・ゲローバル セキュリティ グループ・グローバル セキュリティ グループ・ブローバル セキュリティ グループ・グローバル セキュリティ グループ・ゲローバル セキュリティ グループ・ゲローバル セキュリティ グループ・ゲローバル セキュリティ グループ・ゲローバル セキュリティ グループ・ゲローバル	説明 へ コンピューター/ドメインの管 このガルーブのメンバーは、 このガルーブのメンバーは、 このガルーブのメンバーはボ このガルーブのメンバーはボ このガルーブのメンバーは、 DNS 管理者グルーブ DHCP サーバーなどのほか ドメインの雪々てのドメイン ドメインのすべてのドメイン ドメインのすべてのドメイン ドメインのなくてのドメイン ドメインのなくてのドメイン ドメインのなくてのドメイン ドメインのなくてのドメイン ドメインのなくてのドメイン ドメインのなくてのドメイン ドメインのなくていドメイン ドメインのなくていドメイン ドメインのなくていドメイン ドメインのなくていドメイン ドメインのなくていドメート このガルーブのオンバーは、 このガルーブのサーバーはユ このガルーブのオンバーには、 スキーマの指定された管理者
< III >	<	ш	>

▲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)



🌇 既定のドメイン コントローラ セキュリティの設定		
ファイル(E) 操作(A) 表示(Y) ヘルプ(H)		
Windows の設定 「「」 「」 「	ポリシー ステムの一部として戦能 入ウトの作成、 テントの作成、 テントの作成、 テントの作成、 テントの作成、 ケークカウンドに委任時の信… Adminic シン NETWC シンを相互する ノスのブロファイル Adminic ウンの「酸」と「 Bill立の酸り上げ Adminic デンのブリンを指否する 大地をコンセオータを利用能 ロードとアンロード アレインを追加 シンドコンビュータを利用能 クリンとは自転する クリンとレニータへアクセスを担応 アンシンピュータへアクセスを担応 アンシンとコータのアクセスを担応 グジンを相互する クリンを指否する の停正 クリンを相互する クリンを相互する の管正 合の部正 クリンを相互する クリンを相互する 白い市 クリンを相互する クリントロン クリン クリン クリン クリン クリン クリン クリン クリン <	教室 林市ない RK 5ERVICE trators RK 5ERVICE trators Service Service Se
100 プライルとディレクト 100 プライルとディレクト	の初の の 復元 Server	Operators, Backup Operators, Administrators Operators, Backup Operators, Administrators
) Admini: ウンの書き換え NETWO	trators RK SERVICE.LOCAL SERVICE

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しの設定の説明
パッチ ジョブとしてログオン
ア これらのポリシーの設定を定義する(D):
BUILTIN EPOSTVAD¥Domain Users EPOSTVAD¥IMSI Isers
EPOSTVAL¥SUPPORT_388945a0 LOCAL SERVICE
「ユーザーまたはクループの追加"(U)」 肖明徐(R)
のペーキャンセルション回用法

●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 000] → [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)



■ ヴルーフ ポリシーの管理			
3 ファイル(F) 操作(A) 表示(V) ウィンドウ(W) ∧	ルプ(H)		_1 <u>8</u> ×
🗢 🧆 🖄 📅 💁 🖬			
■ グループ ポリシーの管理 ■ 入 フォレスト・ Lest □ 論 ドメイン	Default Domain Controllers Policy スコープ 詳細 一説定 委任		
 ■ Portune test ■ Default Domain Policy ■ Domain Controllers ■ Default Domain Controllers Pol ■ Default Domain Controllers Pol ■ Default Domain Controllers Pol 	Default Domain Controllers Policy デージ収集目時:2010/04/08 15:03:04 コンピュータの構成(宿路) #99/- Windows:の歌文		
Default Domain Policy	夏 グループ ポリシー管理エディタ		
田 3 スターター GPO	ファイル(F) 操作(A) 表示(V) ヘルプ(H)		
		-	
☆ クルーフ ボワシーの45 M TEA 2 グルーフ ボワシーの48系 4 ま	Default Doman Controllers Policy [sendice] Default Doman Controllers Policy [sendice] Default Doman Controllers Default Doman Controlers Default Doman Controllers Default Doman Controllers	 ポジラン - オブランカ ラベルの変更 オブシンカ ラベルの変更 オベレーライング システムの一部として場論 ジロージル オブシレトの作法 ジロージル オブシレトの作法 ジロージル オブシレトの作法 ジストンシンク ジンク ジンシン ジンシン ジンシン ジンシン ジンシン ジンシン ジン ジン ジンシン ジンシン ジンシン ジン ジンシン ジンシン ジン ジン ジン ジン ジン ジンシン ジン ジン	地ジー想理 ・ ・ 大変 Administrators Frint CoAL SERVICE NETWORK SERVICE ・ 大変 Administrators Administrators Frint Frint Frint Frint F

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	
マ これらのポリシーの設定を定義する(D)	
Administrators Backup Operators	
Performance Log Users	
_ ユーザーまたはグループの追加(U)	
OK キャンセル 道用	(<u>A</u>)



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。

属するグループ(<u>№</u> 3前	(): Active Directory フォルダ
omain Users ISUsers	epostvad.test/Users epostvad.test/Users
注意为如(<u>D</u>)	
<u>追加(D)</u> イマリ グループ:	 削除(R) Domain Users

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。

≪Active Directory ユーザーとコンピ	1-9					_ 🗆 X
	ウィンドウ(型) ヘルプ(出	0				_8×
⇔ → 🗈 🖬 🛍 🗗 🖬	8 🗉 🗑 🗊	0746				
Active Directory ユーザーとコンピュー	sub2 41 個のオブジ	リェクト				
・ 一 ・ に ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	名前	種類	說明	ユーザーログオン名	Windows 2000 /	
E G Bultin	🖉 sub3	組織単位 (OL	I)			
E Completers	🖸 user20	ユーザー		user20@epostvad.test	user20	
Compare P Controllers	🖸 user21	ユーザー		user21@epostvad.test	user21	
F ForeignSecurityPrincipals	g user22	ユーザー		user22@epostvad.test	user22	
E OstAndFound	🖸 user23	ユーザー		user23@epostvad.test	user23	
Image: Imag	🖸 user24	ユーザー		user24@epostvad.test	user24	
🕀 🦲 Program Data	🖸 user25	ユーザー		user25@epostvad.test	user25	
🖻 🙆 sub1	🖸 user26	ユーザー		user26@epostvad.test	user26	
😑 🥝 sub2	🖸 user27	ユーザー		user27@epostvad.test	user27	
- 🙆 sub3	🖸 user28	ユーザー		user28@epostvad.test	user28	
🗄 🦲 System	🖸 user29	ユーザー		user29@epostvad.test	user29	
E Users	🖸 user40	ユーザー		user40@epostvad.test	user40	
	🖸 user41	ユーザー		user41@epostvad.test	user41	
	🖸 user42	ユーザー		user42@epostvad.test	user42	
	🖸 user43	ユーザー		user43@epostvad.test	user43	

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-_ → [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 🎦 ローカル セキュリティの設定 - 🗆 × ファイル(E) 操作(A) 表示(V) ヘルプ(H) + → **1 1** × **2 2 2**
 ポリシー・
 セキュリティの設定

 週ブロージル オブジュウトの作成
 Administrators,SERVICE

 週ブレビュータンユーザーアカワントに蒸
 RETWORK SERVICE

 週サービスとしてログオン
 NETWORK SERVICE

 週サービスとしてログオンを指答する
 301システムパシャージック、OVISTENA Administrators, Power Users, Big システムパシャージックのプロファイル

 週システムルのシャージが少、
 SYSTENA Administrators, Power Users, Big シンステムが別の変更

 ロンスインジョーンング優先順位の線の上げ
 Administrators

 週ウトミナル リーンスを使んのこグナッを
 CoAL SERVICE NETWORK SERVICE

 週ウトミナル リーンスを使んのこグナッを
 Nork
 セキュリティの設定 SYSTEM, Administrators, Power Users, Backup Operators LOCAL SERVICE, Administrators, Power Users 聞せキリナイ語室の生成 LOCAL SERVICE NETWORK SERVICE 聞かーさカリナーと2を使ったフカンを。 コントントリーンと2を使ったログカンを。Administrators.Remote Desktop Users 買デルレクトリ サービス テーシの同時化 買デルストントリ パリのコードとアンロード Administrators 聞トインク オブムシルの作成 聞ドキング ステーションからコンピュー。Administrators.Power Users 副ドキング ステーションからコンピュー。Administrators.Power Users 副ドキング ステーションからコンピュー。 Administrators.Power Users 調えットワーク経由でコンピュータへアク。 Everyone Administrators Users Power Users Backup Operators 調ネットワーク経由でコンピュータへアク。 SUPPORT 388945a0 題、ネットンーン経由とコンヒュータヘルシー 一 「ハッチ ジョンとしてロジオン 超」バッチ ジョンとしてロジオンを拒否する 超ファームウェア環境値の修正 LOCAL SERVICE, SUPPORT_ Administrators 関ファイルとその他のオブジェクトの所有_ Administrators Administrators, Backup Operators 週ファイルとディレクトリのバックアップ 週ファイルとディレクトリの復元 Administrators.Backup Operators (夏)アイルにしイレジアの後た
 (夏)ブログラムのデバッグ
 (夏)ブログスレベルトークンの置き換え
 (夏)ブロセスレベルトークシの置き換え
 (夏)ブロセスのメモリクォータの増加
 (夏)ボージ ファイルの作成 Administrators LOCAL SERVICE, NETWORK SERVICE LOCAL SERVICE, NETWORK SERVICE, Administrators Administrators



●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] → [パ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



ーカル セキュリティの設定 説明 パッチ ジョブとしてログオン Administrators Backup Operators	
パッチ ジョブとしてログオン Administrators Backup Operators MSUBare	
Administrators Backup Operators MSUBars	
IMSUsers	_
Performance Log Users	
ユーザーまたはグループの追加(U) 削除余(R)	
OF twitter	適用(か)



⑤ E-Post Mail Server インストール

メンバーサーバとして、「Administrator」で Windows ドメインヘログイン後、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。

メールサーバー簡単セットアップウィザード(ステップ 1)	×
メールサーバーの設定をナビゲートします。	
メールアカウントをどのように管理したいですか?	
○ 複数のドメインでアカウントを管理したい。	
○ WINDOWSのローカルアカウントと連携させたい。	
◎ WINDOWSのアクティブディレクトリ(AD)のアカウントと連携させたい。	
注意) 本ウィザードで設定された内容は「完了」ボタンを押すと既存の設定を「上書き」します。 設定済みの場合は「キャンセル」ボタンを押して終了させて下さい。	
	,



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。

リーハー簡単ゼットアップワイサード(ノ	、テップ 1-2)		
培结オスアカティブディレカトリ(AD)イ	ストマールガルニづち設守して	-/ 光文()	
既存のグループをメールグループ	ーマス時はコンボボックスの一	いっこい。 暫から選択してください。	
メールグループを新規作成する場	1合はそのままクループ名を入	、方しててたさい。	
アカティブディレクトリ(AD)名	EPOST.		
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	Part of the second		
メールグループ	IMSUsers	•	
		1 Instants	

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。

メールサーバー簡単セミ	ትアップウィザード(ステップ 2)	×
使用するドメイ	ンネームサーバー(DNS)を1つ以上設定します。	
ドメインネ・ 本設定を行	ームサーバーの情報でメールサーバは送り先のSMTPサーバーを検出しています。 テわない場合、目的地への送信が不可能となるサイトが発生します。	
	IPアドレス(例 192.168.0.1)	
DNS1	PRIME C	
DNS2		
DNS3		
	〈 戻ろ(B) 〉 次へ(N) 〉 ト キャンセル へルブ	

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。

ールサーバー簡単セット	アップウィザード(ステップ 3)		2
管理するドメイン	名と接続するIPアドレスを設定してください。		
NAT内で設定	目しているメールサーバーはサーバーに割当てた	、ローカルIPアドレスを設定して下さ	
ι, io			
	ドメイン名(例, xxxx.co.jp)	IPアドレス(例 192.168.0.1)	
1:	test-sample02.jp	J	
2;			
o.			
0,	J	1	
	< 良る(B) (二次へ)N		,
	- 260 (D)		

(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。

メールサーバー簡単セットアップウィザード(ステップ 4)	×
管理者とするメールアドレスを設定します。 管理者とするメールアドレスはドメイン外のメールアドレスでも構い 設定は、xxxxxx0mのxxxx.co.jpのように@マークレパ峰のドメインも副	ません。 安定して下さい。
管理者とするメールアドレス	
< 戻る(B) 次へ(M) 入	キャンセル ヘルプ



(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。

メールサーバー簡単セットアップウィザード	(ステップ 5)	×
協調動作のための設定を行います メール送受信が設定したPCI	。 間で並列稼動出来るようになります。	
共有メール作業フォルダ	C¥mail	参照
共有するコンピュータ名. 例〉¥¥PC01	[
	ノ戸ス(四) 「 ンヤム (5) \ 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、	

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。

ルサーバー簡単セットアップウィ	ザード(ステ ッ プ 6)		
内容が正しければ、「完了 サービス開始は、コントロー コーザーを発け、コードー	」ボタンを押すとメールサー/ ルダイアログより行ってくださ(マネージットートり行ってくださ)	、一の基本設定は終了です。 、	,
以下の条件で設定を行い	ます。	, 'o	
アカウント管理 Windows アクティブディし アクティブディレクトリ EP メールグループ IMSUse	クトリーアカウント OST rs		-
ドメインネームサーバー DNS1 192168.0.1 DNS2 DNS3			
管理するドメイン名 ドメイン1 test-sample ドメイン2 ドメイン3	02.jp		-1
1			<u> </u>
	〈戻る(風)	完了 キャン	セル ヘルプ

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。

メールサ	ーバー簡単セットアップウィザード(ステ	ップ 6)
SMTP ゲートウェイとして使 「使用する。 ゲートウェイ先IP アーカイブ先IP メールのコピー先ファ	用しますか? ポート 25 ポート 1002: ルダ名	参照



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。

B Image: Second se	E-POST Mail Control (Windows Account) (Local)	
	エイリアス設定 メーリングリスト ログ設定 メールフィ サーバー設定 SSL設定 ドメイン管理 サービス:	・ ルタ パージョン情報 制御 中継の制限
	IP version: IP ver	
	が構成でメインのアポリントを定用する: メールユーザーとなるローカルグループ名: IMSUsers	
<i>1</i> 7 [°] 1	管理者/パリンド journamotica 「管理者にもエラーメールを送信す	3
	運用中のドメイン名一覧:	E¥6m
	test-sampleU2.jp	<u></u> 首北6余
	運用するドメイン名	
		追加
	 OK キャンセル 適用	(a) ~1/7

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。

			ン フィルタ ス制徒	バージョン情 中継の制
Windows acc	count C Soft account			
PDC	1º ITMSI Jacova			
エクスポー	・時のパスワード形式 Encod			•
	ОК		する	
	1			
	1			目羊糸田
				削除
	, 運用するドン	イン名	-	
				追加



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。

🖋 - E-POST Mail Account Ma	nager (Windows Account) (Local)
設定(5) ドメイン(D) アカウント(A)	E-POST Mail Control (Windows Account) (Local)
P₂ :- ::: : III ? E _ Domain Lists	エイリアス設定 メーリングリスト ログ設定 メールフィルタ ハージルウ情報 サーバー設定 SSL設定 ドメイン管理 サービス制御 中継の制限
	IP version: IPv4 only I ホスト名:
	「加速ビントラのアガラフ」を定用する。 メールコーザーとわるローカルグループ名・ 「MSIlsers ↓
	S-ML-S-Calin - MPS/M- 小品。 Intosets ・
	管理者アガリント journal docs
	運用ドメイン設定
	運用中のドメイン名一覧:
ν 7 [×] ł	test-sample02.jp
	肖耶余
	運用するドメイン名
	test-sample02.jp 追加
	OK キャンセル 道用(鱼) ヘルプ

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。

E Domain Lists	_ エイリアス設定 メージングリスト ログ設定 メールアイルタ パージング構築 サーバー設定 SSL設定 ドメイン管理 サービス制御 中社の利取 「手種 ×
	1 メイン名 test-sample02.jp
	● 2時4年旬したアカリシア鉄 0 = 無利取り 0 で 1 マン・レボックス選択
	で共通ボックス区別しない)
	C 接続ドメイン/IPで区別する
7°1	IP7h'U.2.(SMTP)
	IP7FU2(POP3)
	IP7FU2@MAP4)
	7#07名
	OK ŦŧŻteli



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。

	(A) 表示(Y)	^/l/プ(⊞)		
°				フィルター バージョン情報
🛛 📶 Domain Lists	account	full name	home	ス制御 中維の制限
🖻 🚰 test-sample02.jp	🖸 Administrat	or		
- 🔂 User	1 0001	0001		
Aliases	1 0002	0002		
MList	🖸 st01	st01		テーフル編集
	🖸 st02	st02		
	🖸 ab01	ab01	pass1234	111/1#4/20
	🕵 user1	user1	pass1234	
	🖸 user2	user2		Plain V
				2011 10 10 10 10 10 10 10 10 10 10 10 10
	. 1	アカウントマネージャ起動。		
	: 7	アカウントマネージャ起動。		
	: 1	アカウントマネージャ起動。		
	: ସ	アカウントマネージャを起動。		

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。

771064774			<u> メ</u> - フィル (ス制	タ バージョン情 御 中継の制
Windows account	C Soft account			
PDC	EPOST			
ローカルクジルーフ*	IMSUsers		-	Ŧ
		1		
	OK		まする	\$
				III 新田
				肖耶余
	· 運用するドメイン:	名		
				追加
	L.			



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。

	Manager (Windo	ws Account)	(Local)	- 0 ×	1	
設定(S) ドメイン(D) アカウント	(A) 表示(Y) ヘル	7°(出)				×
₽ <u>0</u> 5- 555 mm 8					7/11/2	パーンシングまま品 】
🖃 🚛 Domain Lists	account	full name	hon	ie	ス制御	中維の制限
🗄 🛃 test-sample02.jp	🖸 Administrator				[1
User	1 0001	0001	- h			
Mist	0002	0002	エリスナローフ(法)			V. mal
	S st01	st01	メールコンルな話定(か)		7-	27ル編集
	C ab01	ab01	利用時間設定(T)	4	江イへ転送。	
	g user1	user1	送信先制限(5)	4		
	🖸 user2	user2	フーサキー i自力の(A)		Pla	ain 👻
	-		ユーザー 2010(円)	-		
			ユーザー 削卵余(D)			削除
•	<u> </u>	·		-		
対象トジインのユーザー情報追加	1		ユーザー エクスホペート(E)			追加
		(DK¥₩ンt2	ル 道	明(<u>A</u>)	
 E-POST Mail Account 設定(5) ドメイン(D) 7カウンド	Manager (Windo (A) 表示(Y) へル account	ws Account) 7℃ 1) カウント) (Local)		×	
📄 🚰 test-sample02.jp	🖸 Administrato	アカウント	user3		OK	T THE CONTRACT
User	1 0001	パスワード	****		キャンセル	
Aliases	2 0002	, ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,				au camel
- Theorem	1 9 2 StU1	2.0.645 - 25				ル編集
	C et02	200-1 A J				
	🔓 st02 😰 ab01	л-д				
	🖸 st02 🖸 ab01 🖸 user1	ホーム トジイン				
	9 st02 9 ab01 9 user1 9 user2	ホーム トジイン	++./->> 4ulRB		546	n 🗸
	S st02 S ab01 S user1 S user2	ホーム トドメイン メールボックス	サイズ、制限	<i>0 r</i>	ነዣኑ	n 💌
	Image: Stop	ホーム ト・メイン メールボックス	サイス [*] 制限 AUTH & APOPを使用	ı	የላጉ	n .▼
()	^Ω st02 ^Ω ab01 ^Ω user1 ^Ω user2 [⊥]	ホーム トドメイン メールボックス 「 SMTP- 「 POP3舞	サイズ [*] 制限 AUTH & APOPを使用 ^{株効}	r	የብኑ	n <u>▼</u> 削除
<mark>ر الم</mark>	1 st02 1 ab01 1 user1 1 user2	ホーム トジイン メールボックス 「 SMTP- 「 POP3舞 「 IMAP4	サイス [*] 制限 AUTH & APOPを使用 戦功 無効	 	Υŀ	n _ 」
↓ <i>i</i> 7 ² 4	st02 ab01 user1 user2 user2 vser2 vs	ホーム トッメイン メールボックス 「 SMTP- 「 POP3舞 「 IMAP4 **share	サイズ [*] 制限 AUTH & APOPを使用 R効 d/ [*] フォルダ [*] : 「「書込		i*/}	n <u>▼</u> 創版余 直力D
۱ کړ کې	¹ st02 ¹ ab01 ¹ user1 ¹ user2	ホーム トジイン メールボックス 「 SMTP- 「 POP3舞 「 IMAP4! *share	サイズ [*] 制限 AUTH & APOPを使用 取効 d ^{/*} フォルダ [*] : 「「書込	 0 / み許可	i 小 参照	n 💌
۱] ارته ا	¹ st02 ¹ ab01 ¹ user1 ¹ user2	ホーム トジイン メールボックス 「 SMTP- 「 POP3舞 「 IMAP4! #share	サイズ [*] 制限 AUTH & APOPを使用 既効 d ^{/*} フォルダ [*] : 「「書込	 0 / み許可	iY仆 	n v
<u>↓</u> <u>↓</u> <u>↓</u> 〕 〕 〕 〕 〕 〕 〕 〕	¹ / ₂ st02 ¹ / ₂ ab01 ¹ / ₂ user1 ¹ / ₂ user2 ¹ / ₂	ホーム ドメイン メールボックス 「 SMTP- 「 POP3舞 「 IMAP4 '#share	サイズ [*] 制限 AUTH & APOPを使用 戦功 d [/] フォルダ [*] : 「「書込	0 ; み許可	☆↓	n v
<u>↓</u> <u>↓</u> <u>7</u> ² 4	Image: storage	ホーム ドメイン メールボックス 「 SMTP- 「 POP3舞 「 IMAP4 '#share	サイズ [*] 制限 AUTH & APOPを使用 戦功 d [/] フォルダ [*] : 「「書込	0 ; み許可	小? 一	n v
↓ ↓ 7 ³ 4	1 st02 1 1 1 1 1 1	ホーム ドメイン メールボックス 「 SMTP- 「 POP3舞 「 IMAP4 '#share	サイズ [*] 制限 AUTH & APOPを使用 戦功 d [/] フォルダ [*] : 「「書込		小 ³ 一 <u>課零</u>	
↓ <u>↓</u> <u>↓</u> ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	1 st02 1 ab01 1 user1 1 user2	ホーム ドメイン メールボックス 「 SMTP- 「 POP3舞 「 IMAP4 '#share	サイズ [*] 制限 AUTH & APOPを使用 時効 低 ⁴ フォルズ [*] : 「 書込		└仆 	
<u>↓</u> <u>↓</u> 7 ² 4	Image: storage	ホーム ドメイン メールボックス 「 SMTP- 「 POP3舞 「 IMAP4 '#share	サイズ [*] 制限 AUTH & APOPを使用 時効 低 d [*] フォルズ [*] : 「 書込		於仆 	
↓ <i>↓</i> 7 ² 4	Image: storage	ホーム ドメイン メールボックス 「 SMTP- 「 POP3舞 「 IMAP4 '#share	サイズ [*] 制限 AUTH & APOPを使用 較功 低 ¹ フォルズ [*] : 「書込 OK キャンオ		於仆 	



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。



e-POST

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。

🐕 既定のドメイン セキュリティの設定			
ファイル(E) 操作(A) 表示(V) ヘルフ	?(H)		
	Þ		
 Windows の設定 スクリプト (スタートアップ/シャットダ) マセンティの設定 マナント ポリシー マサント ポリシー アカント ポリシー アカント ロップアウトのポ アカント ロップアウトのポ マリント ロップアウトのポ マリント ロップアウトの マリント ロップアウトの マリント ロップアウトの マリント ロップアウトの マリント ロップアウト マリント マリント マリント マノトレンスト マノトレント マノーン マノーン	ポリシー / 聞/スワードの長さ 酸パスワードの支更禁止期間 聞/スワードの周囲を記録する 酸パスワードは、複雑をの要件を満たす必要がある 酸 時号化を元に戻せる状態でパスワードを保存	ポリシー設定 1文字以上 1日 42日 24回 福助 無効	
	·		

7カウント 🗙
パスワードが短いか、既定と一致しません。 複雑なパスワードを入力する必要があります。
<u>OK</u>



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。

🌇 既定のドメイン セキュリティの設定			
ファイル(E) 操作(A) 表示(V) ヘル	プ(H)		
 Windows の設定 ※ スクリブト (スタートアップ/シャットダ) ※ セキュリティの設定 ● ジャンシト ポリシー ● ジャンシト ポリシー ● ジャンシト ロックアウトのボリシー ● ジャンシト ロックアウトのボリシー ● ジョー ーカル ポリシー ● ゴーカル ポリシー ● ゴーカル ポリシー ● ゴーカル ポリシー ● ゴーカル ポリシー ● ゴーシー オリシー ● ジャズト リーブ ● ビク キャンス キャレー ク 位EEE : ● ご シブトウェアの 本服の ポリシー ● ゴー シブトウェアの 本服の ポリシー ● ジャスリディ ポリシー (Activ 	ポリシー・/ 取りパスワードの長さ 取りパスワードの東京東赤上期間 取りパスワードの市効期間 取りパスワードの周辺歴を記录する ですべり用した様式の更佳を満たすどの更加ある 認識時号化を元に戻せる状態でパスワードを保存。	<u>州沙-殿定</u> 1 文字以上 1日 120日 24回 無効 無効	
]			

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 連携時のユーザー認証について

Active Directory 連携時において、ユーザー認証が使われるのは、POP3 認証のみです。 SMTP 認証を使うようにするには、SMTP 認証を後から有効にする必要がありますが、 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。ただし、SMTP 送 信リクエスト時のアカウント名は、AD のユーザー名とマッチングが行われます。SMTP 認証パスワードの情報は、「認証ファイル」としてメールサーバ側で管理され、認証時に 照合されます。

参考までに、SMTP 認証を有効にする手順を紹介します。詳細は『E-Post Mail Server 完全ガイド』や関連ドキュメントを参考にしてください。

●「サービス制御」タブから EPSTRS サービスを停止

●Mail Control 画面の「サービス制御」タブの「SMTP 認証方法」を選択、「セキュリティレベル」を「認証ファイル」、「適用」ボタンをクリック

●Account Manager のユーザーのアカウント詳細画面から「SMTP-AUTH & APOP を使 用」チェックボックスオンを確認するか、オフのときはオンに設定する。表示されるダイ アログボックスで SMTP 認証パスワードを入力する

●最後に「サービス制御」タブから EPSTRS サービスを開始する

アカウント関連の 操作内容	連携の 有無	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	+	・アカウント
		▶ 表示名	+ - >	・ノルネーム
アカウント	あり	・Window2000 以前の ューザーログオンタ		・アカウント
名前変更		・表示名	~~~	・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
SMTP 認証 パスワード変更	なし			・SMTP 認証パスワード
フルネーム	あり	·表示名	\leftrightarrow	・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

Active Directory 連携時の連動項目



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。

Windows XP Pro でのインストール・設定作業の注意

Active Directory に参加している Windows XP Professional マシンへ E-Post Mail Server をインストールする場合、インストール時には、ドメインにログインしない状態、つまり 「このコンピュータ」(ローカル) へ Administrator またはその権限ユーザーにてログイ ンを行って、インストール・設定作業を行う必要があります。Windows XP マシンでは、 ドメインにログインした状態でインストール・設定作業を行うと、うまく Active Directory 連携が行えないことが判明しています。設定が終わると、運用時にはドメインにログイン してメールサーバを利用できます。

くわしい原因は不明ですが、設定ウィザードが IMSUsers グループをドメインコントロ ーラに自動作成するときに生じている問題と考えられます。

なお、Windows Server 2003 や 2008 など、サーバ OS ではこの問題は起きません。ドメ インに参加した状態でインストール・設定作業を行うことができます。



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 でも有効です。 **[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 総時間が増えてしまったり、認証できず接続エラーが増える状況も考えられますので、設 定値を変更するときは、いたずらに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ながら行ってください。



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) abc.jp user1 user2 abc.jp def.jp user3 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 user3,user4 def.jp 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。



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:A	Program	files¥EP	OST¥MS"	<pre>《Enter》</pre>				
4. EPS	TDS サート	ビスのデバッ	ッグモード	を起動する	こは、	epstds	-debug	と入力。
epstds	-debug	<pre>《Enter》</pre>						

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

簡単セットアップ	16 -
サービス開始	36 -
デバッグモード	36 -
独自アカウント管理	21 -
ドメイン セキュリティ設定	27 -
ドメインコントローラ	5 -, - 7 -
ドメインローカルグループ	- 9 -
バーチャルドメイン	- 6 -
パスワード	
の長さ	- 29 -
の複雑さ	- 29 -
バッチジョブとしてのログオン	10 -
メール作業フォルダ	- 20 -
メールボックスフォルダ	23 -
メンバーマシン	5 -
ライヤンフ数	- 6 -