<u>E-Post Mail Server (x64)</u> <u>E-Post SMTP Server (x64)</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.1.7 (2022.3.30)





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 (x64)インストールマシンの用意	14 -
5	Windows Server へ導入前の注意と E-Post Mail Server (x64) インストー	・ル - 15 -
6	E-Post Mail Server (x64) 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	20 -
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	E-Post Account Manager から確認する	23 -
10	「複雑さの要件を満たす必要があるパスワード」設定に影響されることに注	意 27 -
(1)	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	30 -
4.	参考情報と応用	31 -
Activ	/e Directory 連携時の認証パスワードについて	31 -
同一+	ナーバに Active Directory ドメインとメールサーバを設定する場合	32 -
E-Po	st Mail Server (x64)のドメイン名と AD のドメインの関係	32 -
Activ	re 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	家照される
しくみ	みについて	32 -
Activ	e Directory 連携時のアカウント情報インポートの挙動について	34 -
Activ	re Directory への問い合わせリトライ間隔と時間を調整するには	35 -
Activ	re 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	Eするとき
		36 -
Activ	re 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	치 38 -
Activ	re 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	39 -
5.	トラブルシューティング	40 -
6.	索引	41 -



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 (x64)・E-Post SMTP Server (x64)シリーズは、メールユーザー管理 について、Windows Server 2008 R2 / 2012 / 2012 R2 / 2016 / 2019 / 2022 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 (x64)・E-Post SMTP Server (x64)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ー」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 (x64)・E-Post SMTP Server (x64)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 (x64)シリーズ・E-Post SMTP Server (x64)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 2008 R2/2012/2012 R2/2016/2019/2022 の Active Directory 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 ピューター」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。

📔 Active Directory ユーザー	とコンピュータ			
ファイル(F) 操作(A) 表示(V)	ヘルプ(H)			
🗢 🔿 🖄 📅 📋 🗔 .	a 🕞 🛛 📅 🐍 💩 🖆	i 🔻 🗾 🕱		
Active Directory ユーザーとコ	ンピュ 名前	種類	【説明	
🗉 🧾 保存されたクエリ	Builtin	builtinDomain		
E Builtin	Computers	דדעב	Default containe	r for upgr r for dom
E Computers	ወንሀለታና		Y X taine	r for sec
⊞ Domain Controllers	全般 管理者		taine	r for upgr
H E ForeignbecurityPrin				
	Endermannen	NET.		
	ドメイン名 (Windows 2000 以	(前)(N):		
	EPPORS TO MARKS			
	見8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			
			·····································	
•	•			

▲ Windows Server 2008 で作成済みドメイン名を確認する



	EPOSTHVD2 MHRのプロパティ ? ×	×
ファイル(F) 操作(A) ◆ ● ② 匠 ① ○ Active Directory ユー ▷ 保存されたクリ ○ Builtin ▷ ○ Computers ▷ ○ Domain Con ▷ ○ Domain Con ▷ ○ PoreignSecu ▷ ○ Users	 全般 管理者 ■ EPOSTINACE Instit F×イン名 (Windows 2000 より前)(N): ■ EPOSTINACE ジジボリ(D): [F×インの機能レベル(M): Windows Server 2012 フォレストの機能レベル(F): Windows Server 2012 	月 fault container for fault container for fault container for fault container for fault container for
<	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	コンピューター	_ — — X
ファイル(F) 操作(A) 表示(EPOSTHVD6.localのプロパティ ? ×	
🗢 🄿 🖄 🖬 📋 🖾	全般 管理者	5.
 Active Directory ユーザーと ○ 保存されたクエリ > ○ 保存されたクエリ 	EPOSTHVD6.local	
Builtin Computers Domain Controller	ドメイン名 (Windows 2000 より前)(N):	
 ForeignSecurityPri Managed Security 	EPOSTINUSS	
> Contraction of the service of the	說明(D):	
	ドメインの機能レベル(M): Windows Server 2016	
	フォレストの機能レベル(F):	
	Windows Server 2016	
	OK キャンセル 適用(A)	

▲ Windows Server 2022 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ー」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。



② -2 IMSUsers グループの確認

「Active Directory ユーザーとコンピューター」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。

📔 Active Directory ユーザーとコン	ピュータ		_ 🗆 ×
ファイル(E) 操作(A) 表示(V) へ	ルプ(出)		
🗢 🔿 🙍 🔂 🔀 🖸] 🖸 📑 🛛 🖬 🐍 😣	1 7 2 8	
Active Directory ユーザーとコンピュ 保存されたクロリ 日 Builtin Computers 日 Domain Controllers 日 ForeignSecurityPrincipals Users	Administrator Administrator Administrator Cert Publishers Denied RODC Password Dras Admins Donain Ocmputers Domain Computers Domain Controllers Domain Controllers Domain Controllers Domain Controllers Domain Guests Domain Guests Domain Guests Enterprise Read-only Do Guest IMSUsers Read-only Domain Contr Read-only Domain Contr Schema Admins	福田 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 - 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 - 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 - エンパーサル 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 - エンパーサル セキュリティ グループ - エンパーサル	
	1		

▲Windows Server 2008 で IMSUsers を確認する

	Active Directory 1-	ザーとコンピューター	_ D X					
ファイル(F) 操作(A) 表示(V)	√レプ(H)							
🗢 🔿 📶 🤞 🖬 🔀 🖬 🔀 📷 🗏 🕸 🗑 🖉 🚨								
 Active Directory ユーザーとコンと 原子なれたクエリ 第日の日本 ○ Builtin ○ Computers ○ Domain Controllers ○ ForeignSecurityPrincip ○ Managed Service Acco ○ Users 	名前 Administrator Administrator Cert Publishers Coneable Domain Controll Coneable Domain Controll Donaid RODC Password Re Donaid RODC Password Re Donain Admins Donain Admins Domain Controllers Domain Controllers Domain Controllers Domain Users Domain Users Enterprise Read-only Dom Group Policy Creator Owners Guest MISUSers RAS and IAS Servers RAS and IAS Servers RAS and IAS Servers RAS and IAS Servers RAS and IAS Servers 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 - ゲロー/Ch セキュリティ グループ - グロー/Ch セキュリティ グループ - グロー/Ch セキュリティ グループ - グロー/Ch セキュリティ グループ - ヴロー/Ch セキュリティ グループ - ヴロー/Ch セキュリティ グループ - ロー/Ch セキュリティ グループ - エニ/(ーサル 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 - ドメイン ローカル	説明 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、ドメインコ このガルーブの、ドメインコ DNS 管理者方ルーブ DHCP サーバーなどのほか ドメインの管理者 ドメインの管理者 ドメインの管理者 このガルーブのメンバーは、 ンターブライズの管理者 このガルーブのメンバーは、 このガルーブのメンバーは、 コンピューター/ドメインへの 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、 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、 このガルーブのメンバーは、 このガルーブのオンパーは、 このガルーブのオンパーは、 このガルーブのメンバーは、 このガルーブのメンバーは、 このガルーブのメンバーは、 このガルーブのメンバーは、 このガルーブのオンパーは、 このガルーブのメンバーは、 このガルーブのメンバーは、 このガルーブのメンバーは、 このガルーブのメンバーは、 このガルーブのオンパーは、 このガルーブのメンバーは、					
< III >	<		>					
Land Andrea and Andrea	(

▲Windows Server 2012 で IMSUsers を確認する



ファイル(F) 操作(A) 表示	(V) ヘルプ(H)	🍬 ûn 📟 📼 🕼		
Active Directory ユーザ 承存されたクエリ 孫存されたクエリ 愛 Builtin Computers る Domain Contre ご Domain Contre ご ForeignSecurit 込 Managed Servi Users		Se S	×	^
¢	/ル / 1 (Windows 2000 な / Hy)/ IMSUsers グループのスユープ ④ ドメイン ローカル(O) ○ グローパル(G) ○ ユニパーサル(U)	グルーブの種類 ● セキュリティ(S) ○ 配布(D)	キャンセル	v

▲Windows Server 2022 で IMSUsers を追加する

🗢 🔿 📩 🔏 📋 🗙 🛙	a 🗟 🛛 🗖	1 % 🛰 🖆 🔻 🖻 🐍		
Active Directory ユーザーとコンビュ ティオテクエリ シ の 保存されたクエリ シ の Builtin ・ Computers シ ひ Domain Controllers シ ご ForeignSecurityPrincipal: シ ご Managed Service Accour じ Users	名前 總 Cert Publish 總 Concable D 總 Densied ROD 總 Densied ROD 總 DensubdateR 總 Domain dens 總 Domain dens 總 Domain Gon 總 Domain Gon 總 Domain Gue 總 Enterprise R 總 Foroup Polic 總 Guest 總 MSUsers 總 Protected Us 總 RAS and IAS	律類 世キュリティグループ - ドメイン ローカル ゼキュリティグループ - ゲメイン ローカル ゼキュリティグループ - ゲメイン ローカル ゼキュリティグループ - ドメイン ローカル ゼキュリティグループ - ゲローパル ゼキュリティグループ - グローパル ゼキュリティグループ - グローパル ゼキュリティグループ - グローパル ゼキュリティグループ - クローパル ゼキュリティグループ - クローパル ゼキュリティグループ - クローパル ゼキュリティグループ - コニパーサル ゼキュリティグループ - ユニパーサル ゼキュリティグループ - コニパーサル ゼキュリティグループ - コニパーサル ゼキュリティグループ - ゲメークローカル ゼキュリティグループ - ドメイン ローカル ゼキュリティグループ - ゲローパル ゼキュリティグループ - ゲメークローカル	説明 このグルーブのメンバーはディ このグルーブのメンバーはディ このグルーブのメンバーは、ド DNS 管理者グルーブ DHCP サーバーなどのおかの ドメインのすべてのドクイク コ ドメインのすべてのドメイン コ ドメインのすべてのドメイン コ ドメインのすってのチンパーは、ア このグルーブのメンバーは、ア このグルーブのメンバーは、ド このグルーブのメンバーは、ド このグルーブのメンバーは、 このグルーブのメンバーには、 このグルーブのメンバーには、 このグルーブのサンバーには、 このグルーブのサンバーには、	
< >>	Schema Ad	ヤキュリティグループ - ユニバーサル	スキーマの指定された管理者	

▲Windows Server 2022 で追加した 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・グループポリシーの確認

ユーザーグループ"IMSUsers"を追加・登録したときは、「グループポリシー管理エディタ」 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。







📓 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)	- 8 ×			
♦ ♦ 2 0 4 0 ×	Q 🛛 🖬				
グルーブポリシーの管理	Default Domain Controllers Policy				
 ✓ ▲ JAUAN ✓ ▲ FX12 	スコープ 詳細 設定 委任 状態				
✓ ∯ EPOETHNDEAN AI	リンク まニオ		나는 것은 것이 같은 것이다.		
Default Domain			- 🗆 X		
✓ 📑 グループ ポリシー オ	次00 ファイル(F) 操作(A) 表示(V) ヘルプ(H)				
Default Dom	場所 💠 🔿 📶 🗙 🗒 🗟 🖬				
> 🔐 Derault Dom > 🎇 WMI フィルター	Default Domain Controllers Policy [HV4EPST: A	ポリシー	ポリシー設定 ^		
> 🛅 スターター GPO	 ・ ・ ・	副コンピューターとユーザーアカウントに委任時の信頼を付与	Administrators		
> 🏥 サイト 🔊 グループ ポリシーのエデルが	→ □ ソフトウェアの設定	図 サービスとしてのロクオンを担合 図 サービスとしてのグオン	未定義		
🔀 グループ ポリシーの結果	- Windows の設定 この GR 、 10 名前録法式USL	📓 システム パフォーマンスのプロファイル	Administrators,NT SERVI		
	名前 スクリプト (スタートアップ/シャットダ	◎ システムのシャットダウン	Administrators, Backup (
	総A > La セキュリティの設定	回 システム時刻の変更 回 シンボリック リンクの作成	LOCAL SERVICE, Adminis 夫定差		
	> 画 アカワント ホリシー マ 語 ローカル ポリシー		Administrators, Window		
	> 画 監査ポリシー	い セキュリティ 監査の 生成	LOCAL SERVICE, NETWO		
		図 タイム ソーンの変更 ◎ ディレクトリ サービス データの同期化	未定義		
	WMI > 3 4X250	副 デバイス ドライバーのロードとアンロード	Administrators, Print Op		
< >	> 0 制限されたグループ	🔤 トークン オブジェクトの作成	未定義		
	> 4 9X74 9-EX > 12 192XFU	協計・ツキンクステーションからコンピューターを削除 除じょイン(ニロークステーションを追加)	Administrators Authenticated Licens		
	> 强 ファイル システム		Everyone, Administrators		
	> ju/ ワイヤード(有線)ネットワーク」	製 ネットワーク経由のアクセスを拒否	未定義		
	📫 ネットワーク リスト マネージャー	○ パッチ ジョブとしてログオンを担当 パッチ ジョブとしてログオン	木定義 Administrators Backup (
	> 100 ワイヤレスネットワーク (IEEE 8)	副 ファームウェア環境値の修正			
	> 🧾 公園1 のホッシー	図ファイルとその他のオブジェクトの所有権の取得 の ファイルとその他のオブジェクトの所有権の取得 の ファイルとその他のオブジェクトの の ボックアップ	バッチ ジョフとしてロクオンのフロバティ		? ×
	< · · · · · · · · · · · · · · · · · · ·	<	ヤキュリティポリシーの設定 詳明		
			are 73		
			パッチ ジョブとしてロク	オン	
A 14	lindows Comer 2022	の坦人			
	indows server 2022	の場合	「オマカにのポリシーの設定を定美	+ 3(D)-	
				5 0(0).	
			Administrators		
			EPOSTHVD6¥IMSUsers		
			IIS_IUSRS		
			IMSUsers Derformance Leo Lloors		
			Performance Log Osers		
			ユーザーまたはグループの追加(し	リ 削除(R)	
				OK ++1/4	·濟田(A)
				TYPEIV	A) (T) (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ー」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> 名前 Domain Lisers	(): Active Directory フォルダ enotwartiset // Levre
MSUsers	epostvad.test/Users epostvad.test/Users
追加(<u>D</u>)	肖·顺朱(2)
<u>追加(D)</u> イマリ ガループ:	- 削除(R) Domain Users

ー方、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 (x64)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ー」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 ーター」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	ピュータ					_ 🗆 X
	ウィンドウ(※) ヘルプ(と	0				_8×
⇔ → 🗈 🗷 🖻 🙆	B 2 0 7 0	0746				
Active Directory ユーザーとコンピュ		フェクト				-
🐵 🧰 保存されたクエリ	名前	種類	[说8月	ユーザーログオン名	Windows 2000 /	
	Sub3	組織単位 (OL	J)			
E G Complete	🖸 user20	ユーザー		user20@epostvad.test	user20	
The Compared Providers	g user21	ユーザー		user21@epostvad.test	user21	
E P ForeignSecurityPrincipals	g user22	ユーザー		user22@epostvad.test	user22	
F O LostAndFound	🖸 user23	ユーザー		user23@epostvad.test	user23	
MTDS Quotas	🖸 user24	ユーザー		user24@epostvad.test	user24	
🕀 🤐 Program Data	g user25	ユーザー		user25@epostvad.test	user25	
🖃 🐼 sub1	🖸 user26	ユーザー		user26@epostvad.test	user26	
sub2	g 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	
🕀 🦲 Users	🖸 user40	ユーザー		user40@epostvad.test	user40	
	g user41	ユーザー		user41@epostvad.test	user41	
1	🖸 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 (x64)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 2008/2012/2016/2019/2022 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。

④-3 メンバーサーバ側のローカルセキュリティポリシー設定を確認

メンバーサーバ側のローカル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"が「バッチジョブとしてのログオン」許可されているのか確認しておきます。 メール用グループ"IMSUsers"が入っていなければ追加してください。

[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

🔓 ローカル セキュリティ ポリシー					
ファイル(E) 操作(A) 表示(V) ヘルブ(H)					
🗢 🤿 🖄 📷 🗙 🗊 💿 🚺 🖬					
セキュリティの設定	ポリシー ~	セキュリティの設定			
		LOCAL SERVICE,NETWORK SERVIC Administrators Administrators.Backup Operators LOCAL SERVICE,Administrators Administrators LOCAL SERVICE,NETWORK SERV Administrators.Remote Desktop Us LOCAL SERVICE,NETWORK SERV Administrators Administrators Everyone,Administrators,Users,Bac INSUSera,Administrators,Users,Bac INSUSera,Administrators, Backup O Administrators Administrators Administrators Administrators Administrators	E.Administrators.SERVICE Sッチ ジョブとしてログオンのプロパジ ローカル セキュリティの設定 [現明 パッチ ジョブとしてログ パッチ ジョブとしてログ パッチ ジョブとしてログ パッチ ジョブとしてログ パッチ ジョブとしてログ ローカル セキュリティの設定 [100] パッチ ジョブとしてログ ユーザーまた(40ループの)ま	ディ オン カ <u>ロ(U) 商</u> 明除(E)	
	CI 2000 / 2012	♥ / 物口			
				OK ¥	rンセル 適用(A)



■ ローカル セキュリティ ボリシー ファイル(F) 操作(A) 表示(V) ヘルプ(H)		- 🗆 X		
🗢 🔿 🙍 📰 🗙 🗐 📑 🚺 🗊				
	ボリシー 、システムパフォーマンスのプロファイル 、システムのシャットダウン システム時刻の変更 シンボリックリンクの作成 、オケジューリング優先順位の練り上げ し、セキュリティ監査の生成 、オケジューリング優先順位の練り上げ し、セキュリティ監査の生成 、ディレクトリサービスデータの同期化 、ディレクトリサービスデータの同期化 、ディレクトリサービスデータの同期化 、ディンパンフの変更 、ディントリサービスデータの同期化 、ディンパンフクステーションを追加 、ディンパンテークステーションを追加 、ドッチングステーションから追加 、シンデジョンとしてログオンを拒否 、パッヂ ジョブとしてログオンを拒否 、アイルとその他のオブジェクトの所有権の取得 、フィイルとディレクトリの(ホックアップ 、フィールンディレクトリの(ホックアップ 、フィールンディレクトリの復元 、プロセスローキャッグ セットの一参加	セキュリティの設定 Administrators,NT SERVI Administrators,Backup ヘ パッチ ジョブとしてログオンのプロパティ ローカル セキュリティの設定 説明 通 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 MSUsers IIS_USRS Performance Log Users ユーザーまたはグループの追加(U) 剤除(R)	?	×
		ОК <i>キャンセル</i>	適用((A)

▲Windows Server 2022 の場合

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 (x64)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。

⑤ Windows Server へ導入前の注意と E-Post Mail Server (x64)インストール

Windows Server への導入時の注意の概要は下記の通りです。詳細は導入後の製品 FAQ に掲載されている「Windows Server への導入時の注意」をご覧ください。

- (1) [UAC の無効化] (ユーザーアカウント制御設定の変更)
- (2) [ローカル管理者としての完全な Administrator 権限]
- (3) [Windows ファイアウォールの許可設定]
- (4) 必要に応じて機能や役割の追加
- (5) Windows Defender ウイルス対策のリアルタイムスキャン除外設定



⑥ E-Post Mail Server (x64) ウィザード(簡単セットアップ)の起動

E-Post Mail Server (x64) をインストールした直後のときは、E-Post Mail Server (x64) 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、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。	
◎ MINDOWS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。	
(戻る(別) 法へ(2)> キャンセル ヘルブ	

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。



ールサーバー簡単セットアップウィザード()	くテップ 1-2)		2
接続するアクティブディレクトリ(AD)。 既存のグループをメールグループ	るとメールグループを設定してく とする時はコンボボックスの一覧	ださい。 「から選択してください。	
メールジルーフを新規『Fbbx9@Ji アクティブディレクトリ(AD)名	が合いておりルーフ名をハフ	1001/2010	
メールグループ	IMSUsers	×	
	(戻る(B) (次へ(M)))	*+>>tu	ヘルプ

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 (x64)・E-Post SMTP Server (x64)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ッ	トアップウィザード(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。	
ドメインネー本設定を行	ムサーバーの情報でメールサーバは迷り先のSMTPサーバーを検出しています。 おない場合、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	PRE-MALE N	
DNS2		
DNS3		
	〈 良る(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 (x64)/E-Post SMTP Server (x64)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、作成し運用するメールドメイン名を設定します。

	ドメイン名(例.xxxx.co.jp)	
1:	test-sample02.jp	
2:		J
з:		



(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「次へ」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ません。 設定は、xxxxxxxのbxxxx.co.jp のように@マークルJ&金のドメインも設定して下さい。	
管理者とするメールアドレス	
< 戻る(B) 次へ(W) 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。メール作業フォルダ項目は必須で 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PC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	
< 戻る(B) 次へ(M) > N キャンセル ヘルブ	

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。



内容が正しければ、「デ	E了」ボタンを押すとメールサーバ コールガイアログナ的行ってください	ーの基本設定は終了です	t.
ユーザー登録は、ユーサ 以下の条件で設定を	ナーマネージャーより行ってください 元います。	•	
アカウント管理			<u> </u>
Windows アクティフラ アクティブディレクトリ メールグループ IMSI	EPOST Jsers		
DNS1 19216801 DNS2			
で理するドメイン名			
ドメイン1 test-sam ドメイン2 ドメイン2	iple02.jp		
1,21,30			-1

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。

א-א-א-א-א-א-א-א-א-א-א-א-א-א-א-א-א-א-א-	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用 「 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ォノ	1しますか? ポート 25 ポート 1002: レダ名	参照
		§ 291
	< 戻る(B) 次へ(N) >	±12/2/1 \\\7

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」項目が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」項目表示に変わります。



P₂: :- :::: :::: ?	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 メーノ サーバー設定 SSL設定 ドメイン管理 サー	- レフィルタ バージョン情報 ビス制御 中継の制限
	IP version: IPv4 only ホスト名: 所属ドメインのアカウントを使用する: メールユーザーとなるローカルグループ名: [IMSUsers	
	管理者アカウント administrator	
ν 7 °1	「運用ドメイン設定」	1890
	連用中のドメイン名一覧: test-sample02.ip	≣¥糸田 ┃
		 肖· 贤 余
	運用するドメイン名	
		追加

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。

アカウントの管理方	法				×	フィルタ	バージョン情報
Windows	account C	Soft account				【人制印	中推の制度
PDC	1.0	067		参照			
ローカルゲ	μ−7° [IM:	GUsers]		
エクスオ	パート時のバスワ	7ード形式 <mark>Encode</mark>	•				-
		ОК				-+	
						590	
						1	≣¥ém (
*i					1	_	5740
							削除
		運用するドメイ	ン名				
							追加
		L					

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) トゲイン(D) アカウント(A)	E-POST Mail Control (Windows Account) (Local)	×
E Domain Lists ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	エイリアス設定 メーリングリスト ログ設定 メールフイレタ パーツン付け 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 マ ホスト名: 所属ドメインのアカウントを使用する: メールユーザーとなるローカルグループ名: IMSUsers マ 管理者アカウント administrator 「管理者にちエラーメールを送信する 運用ドメイン設定 運用するドメイン名 運用するドメイン名 前原除 運用するドメイン名	

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。

P b b b b b b b b b b	エイリアス酸定 メーリングリスト ログ酸定 メールフィルタ ハーウルパ情報 サーバー酸定 SSL酸定 ドメイン管理 サービス制御 中継の制限 王44 王4 王4 王4 王4 王4 王
	1 ・ ドメ()名 test-sample02.jp 操作p1スワード
	● 金綱キ可したアカウント数 (0 = 無制限) 0 メールボックス選択
	 ・ 共通ホッシスにありしない ・ 接続ドメリンIPで区別する
τ [°] i	IP7NUZ(SMTP)
	1971-U.2.(MAP4)
	OK ++yth

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、複数のメール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 フォルダのすぐ下の位置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、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(例・user1)です。



ちなみに Active Directory 連携設定では次のようにはなりませんが、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る形となります。万が一、Active Directory 連携設定の前に、メ ールドメインを接続ドメイン/IP で区別する設定で運用していたときは、「共通ボック ス」設定に切り替える必要が出てきますが、この際、メールデータや設定ファイルなどを 手動で移動する作業が必要になります。

😂 user1			
ファイル(E) 編集(E) 表示(Y) お気に入り(A) ツール(D) ヘルプ(H)		
🔇 戻る • 🚫 · 🎓 🔎 検索 🝞	7オルダ 🕼 🔅 🗙 🍤 [•	
アドレス(D) 🛅 C:¥mail¥inbox¥test-sample02.jp	fuser1		• 🛃 移動
フォルダ	× 名前 ▲	サイズ 種類	更新日時
□ mal ∅ □ ∅ □ □ duster □ maytlog □ maytlog □ imbox □ imbox	▲ 28000000183.M55	1K8 Outlook747£	2007/11/07 20:31

⑨ E-Post Account Manager から確認する

(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

Account Manager 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。

IMSUsers グループに属するユーザーがいないときは、何も表示されません。そのときは 後述するように Account Manager からアカウントを作成できるか確認します。

ドメインを認識しているときでも、MailGroup である IMSUsers グループに属するユー 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 IMSUsers に属するユー ザーを作成しているときには、Account Manager 内にユーザーが表示されます。



B V				フィルター バージョン情報
🛃 Domain Lists	account	full name	home	ス制御 中継の制限
E st-sample02.jp	🖸 Administrati	or		
	🖸 0001	0001		
Aliases	1 0002	0002		
MLISC	🖸 st01	st01		テーフル編集
	🖸 st02	st02		江へ転送。
	🖸 ab01	ab01	pass1234	
	🖸 user1	user1	pass1234	
	🖸 user2	user2		Plain 💌
				削除
•	1			
1				isto l
	V 1	アカウントマネージャ起動。		

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。

/ - E-POST Mail Account M 設定(5) トソイン(D) 7カウント(A	anager (Windows Account) (Local)) 表示(Y) ヘルプ(出)	<u>-0×</u>	<u>></u>
7カウントの管理方法 E で Windows account	C Soft account	×	フィルタ / バージョン情報 ス制御 中継の制限
PDC ローカルグルーフ*	IMSUsers	参照 一	
エンスホードッチのフ			
			Į¥&m
<i>V</i> 74			 肖IB余
	運用するドメイン名		追加

(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。入 力するパスワードは、「ActiveDirectory ユーザーとコンピューター」側で管理されている 「複雑さの要件を満たす必要があるパスワード」設定を満たしているかどうかが判定され ますので注意してください。



 - E-POST Mail Account Manager (Win 設定(S) トメイン(D) アカウント(A) 表示(V) く 	dows Account) ህርጋ የዘነ		V
	107 (117		
Domain Lists	full name	Pイルタ パーツョン間 home 2割節 中継の制	F¥IX IBR
🗄 🚅 test-sample02.jp 🖸 Administrato	r	Statistics 1 areas in	
User 🔮 0001	0001	Th739-5/9	
MList 2 cto1	0002 ct01	レバス/ ローバム) メール制御(C)	
sto2	st02	メールフィルク設定(1)	
🖸 ab01	ab01	利用時間設定(I) 4 (II / 東広志。	
🖸 user1	user1	送信先制限(5) 4 4	
S user2	user2	ユーザー 注意加(A)	
			1
	1		
対象トメインのユーザー情報追加		ユーザーインボート(I) コーザー エカスポート(E) 道加	
	カウントマネージャ起	b.	
	1		· · · ·
		ストレージャンセル 週月(四) ヘル	
🖋 - E-POST Mail Account Manager (Win	dows Account)	(Local)	
✓ - E-POST Mail Account Manager (Win 設定(S) トジイン(D) 7カウント(A) 表示(Y) ^	dows Account) ル7°(円)	(Local)	×
 ✓ - E-POST Mail Account Manager (Win 設定(S) ドメイソ(D) アカウン(A) 表示(Y) ^ ▲ ひ 詳 前 ? 	dows Account) ゆ? ⁽ 出) アカウント	(Local)	<u>×</u> 報
 ✓ - E-POST Mail Account Manager (Win 設定(S) ドメイソ(D) アカウン(A) 表示(Y) A Pa ご 証 面 ? □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	dows Account) ルプ(田) <mark>アカウント</mark> マカウント	(Local)	× 漏 限
	dows Account) ポアで出 <mark>アカウント</mark> アカウント	(tocal) メージン メージン まer3 のK	× 編 限
	dows Account) ルプ(出) <mark>アカウント</mark> アカウント [パマワート [*]]	(Local) メージン メージン メージン メージン レー 本 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	× 報 限
	dows Account) ルフで出 アカウント アカウント 「 ハ*スワート*「 フルネーム 「	(Local) エロメ メページョン情 メページョン情 中能の制 キャンセル 162年	× 報 限
	dows Account) ルク ⁽ 出) アカウント アカウント 「 ハ*スワード' 「 フルネーム 「 キーム」	(Local) エロメ メージョンパ メージョンパ ロメ ロメ ロメ ロメ ロメ ロメ ロメ ロ マン マン マン マン マン マン マン マン マン マン	× 限
	dows Account) ポフ [*] (土) アカウント パスワート [*] フルネーム 「 ホーム 「	(Local) ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	× 限
	dows Account) ポフ ^ッ (土) アカウント アガウント 「 パマスワード」 フルネーム 「 ホーム 「 ドジイン 「	(Local) ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	× 限
 ✓ - E-POST Mail Account Manager (Win 該定(5) ドダン(0) 万方ント(A) 表示(y) へ ▲ ① Domain Lists ● ② test-sample02.jp ④ User ▲ Muist ④ Muist ○ Muinistrato ○ Stol2 ○ stol2	dows Account) ルフで出) アカウント アカウント 「 フルネーム 「 ホーム 「 ドメイン 「 メールボックス	(Local) ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	× 報 限
 ✓ - E-POST Mail Account Manager (Win 設定(S) ドメイン(D) 7カウント(A) 表示(Y) へ ● 1000000000000000000000000000000000000	dows Account) 小フ(土) アカウント アカウント 「 ハウスワード」 フルネーム 「 ホーム 「 ドメイン 「 メールボッウス	(Local) ■ I X iser3 F******* サイズ* 制限 0 ハ ² イト N編集	潮。
▲ - E-POST Mail Account Manager (Win 該定意) ド杉/(四) 7/77/(A) 表示(Y) へ ● a · · · 证 前 ? Domain Lists User Aliases Muist Store Aliases Muist Store Aliases Store Alias	lows Account) 小フ(土) アカウント アカウント アカウント アルウント 「 パスワード」 フルネーム 「 ドメイン 「 メールボックス 「 SMTP- 「 POP2町	(Local) Iser3 メーション相 ローン サイズ・制限 の ハ ² ハ イーション相 中能の制 「 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	報
	dows Account) ルフで出) 7カウント アカウント 「 ハ*スワード" 「 フルネーム 「 ホーム 「 ドメイン 「 メールボックス SMTP- 「 POP3編 「 POP3編	(Local) メートン・ションド メートン・ションド メートン・ションド ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	報
	dows Account) ルフで仕) アカウント アカウント パンスワード アルネーム 「 ホーム 「 メールボックス SMTP- 「 POP3無 「 IMAP44 ' IMAP44	(Local) Iser3	× 限
- E-POST Mail Account Manager (Win 該定(5) ドメイン(0) アカウント(A) 表示(y) へ 一 (1) 日本 一 (1) 日本	dows Account) ルフ(土) アカウント アカウント アルネーム ボーム ドメイン SMTP- POP3無 IMAP44 *share-	(Local) ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	×
	dows Account) ルフ(土) アカウント アカウント アカウント 「 フルネーム 「 ホーム 「 ドメイン 「 メール木ッウス SMTP- 「 POP3無 「 IMAP44 *#sharea	(Local) ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	× 限
	dows Account) ルフ(土) アカウント アカウント アルネーム 「 ホーム 「 ドメイン 「 メールホックス SMTP- 「 POP3無 「 IMAP44 '#share	(Local) LINE	× 程
	dows Account) ルフ(ビ) アカウント アカウント 「 ハペスワード 「 フルネーム 「 ホーム 「 ドメイン 「 メールホックス SMTP- 「 POP3編 「 IMAP44 *sharee	(Local) LIER3 メートンシャン語 AUTH & APOPを使用 対力、和原 0 パイト AUTH & APOPを使用 対力 加 量込み許可 参照	× 程限
	dows Account) ルフ(日) アカウント アカウント 「 ハ*スワード" 「 フルネーム 「 ドメイン 「 メールボ*ウカス 「 SMTP- 「 POP3無 「 IMAP44 ***********************************	(Local) メート・ションド メート・ションド メート・ションド メート・ションド メート・ションド メート・ションド メート・ションド メート・ションド ション ション ション ション ション ション ション ション	×
	dows Account) パノウ(土) アカウント アカウント パンスワード [®] フルネーム ドメイン メールボッウス SMTP- POP3舞 「IMAP44 '#sharee	(Local) ■■× Iser3 ******** サイズ* 制限 0 パイト AUTH & APOPを使用 致か 数が ** ****** ● 一 ● 一 ● 一 ● 一 ● 一 ● 一 ● 一 ● 一	× 種種 限
	dows Account) パフウビ) アカウント アカウント パンマード 「 フルネーム 「 メールホックス 「 SMTP- 「 POP3無 「 IMAP43 '#sharee	(Local) Iser3 Iser3 サインマルター サインマルター サインマルター サインマルター サインマルター サインマルター サインマルター サインマルター (Local) レーン・シート ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	× [] [] [] [] [] [] [] [] [] [] [] [] []
	dows Account) ポノプ(土) アカウント アカウント アルネーム 「 ホーム 「 ドメイン 「 メールボックス 「 SMTP- 「 POP3無 「 IMAP44 *sharee	(Local) ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	× 限
	dows Account) ルフ(土) アカウント アカウント アカウント 「 フルネーム 「 ホーム 「 ドメイン 「 メール木ックス 「 SMTP- 「 POP3無 「 IMAP44 *#sharea	(Local) - 二 × ******** ******** ******** ********	× 一 月 日 日 日 日 日 日 日 日 日 日

(3) 「Active Directory ユーザーとコンピューター」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ー」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「Active Directory ユーザーとコンピューター」を起動し、 「Active Directory ユーザーとコンピューター」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。



 	≪ Active Directory ユーザーとコンピ			
	<) /////// 採用(A) 表示(型) '			<u>=101</u> 2
 Active Directory ユーザーとコンピュー ● Active Directory ユーザーとコンピュー ● Active Directory ユーザーとコンピュー ● Active Directory ユーザーとコンピュー ● Active Directory ユーザーとコンピュー ● Builtin ● Bouiltin ● Computers ● DirectionSecurityPrincipals ● Computers ● DirectionSecurityPrincipals 	🗢 🔶 🖻 🔃 👗 💼 🗡 😭	' 🖻 🗟 😫 💷 🦉 🖉 🐚 🤇	7 🚭 📴	
 ● (#4727U201) ● (#4727U201) ● (a) constants ● Builtin ● Computers ● Demain Controllers ● ForeienSecurityPrincipals ● Computers ● Issuer ● Computers ●	Active Directory ユーザーとコンピュー	Users 26 個のオブジェクト		
Image postest Image postes	田 🛄 1米存されたクエリ	名前人	1 種類	説明
Computers Computer	E Duikin	🕵 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
Computers Computers 日 ○ Domain Controllers 日 ○ D	E Computere	👧 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
日本 Domain Control Advances 日本 Domain Control Advances 日本 Deviain Security Principals 日本	Computers Controllers	and the paster of	セキュリティ グループ - ドメイン ローカル	epositilia-positec.gr
Guest User コンピュータ/ドメイ: Guest User コンピュータ/ドメイ: Mill server user GMSS and IAS Servers ビキュリティ グループ - ドメイン ローカル ひがループのドー Schema Admins セキュリティ グループ - ドメイン ローカル ひがループのドー Schema Admins セキュリティ グループ - ゲノン ローカル スキーマの指定され st01 User st02 User TehnetClients 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 Stest=sample02.jp user1 User user user2 user3 User	E SoreignSecurityPrincipals	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
	Poreignoecurity Frincipals	5 Guest	User	コンピュータ/ドメインへのゲ
		1 IMSUsers	セキュリティ グループ - ドメイン ローカル	Mail server user's group
		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
② st01 User ③ st02 User ③ st02 User ③ TehetClients 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パ ③ test-sample02.jp セキュリティグループ - ドメイン ローカル test-sample02.jp ④ user1 User ④ user2 User ④ user3 User		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
図 st02 User 図 TeinetClients 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, 図 test-sample02.jp セキュリティグループ - ドメイン ローカル test-sample02.jp 図 user1 User User 図 user2 User User		🖸 st01	User	
 ・プロトロもClients ・セキュリティグループードメインローカル ・プログループのメンル ・サキュリティグループードメインローカル ・セキュリティグループードメインローカル ・セキュリティグループードメインローカル ・セキュの目的 ・ロッカル ・セキュリティグループードメインローカル ・セキュの目的 ・ロッカル ・セキュリティグループードメインローカル ・セキュの目的 ・ロッカル ・セキュの目的 ・ロッカル ・セキュの目的 ・ロッカル ・ロッカ		🕵 st02	User	
愛test-sample02.jp セキュリティグループ - ドメイン ローカル test-sample02.jp 愛 user1 User 愛 user2 User 愛 user3 User		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
g user1 User g user2 User user3 User		natest-sample02.jp	セキュリティ グループ - ドメイン ローカル	test-sample02.jp
፼ user2 User ፼ user3 User		🖸 user1	User	
🖸 user3 User		🕵 user2	User	
		🛒 user3	User	
		a		
		La.L		i

▲Windows Server 2008 / 2012 の場合

□ Active Directory ユーザーとコンピュー ファイル(F) 操作(A) 表示(V) ヘル ◆ ● 2 面 4 □ ※ □	9- /Ĵ(H)] @ 🔒 🔽 🏹	🐍 🗞 🗃 🍸 💆 🗞				×			
 Active Directory ユーザーとコンビュ・ ・ 係存されたクエリ ・ 語 Uridan Generation ・ 語 Uridan Generation ・ 語 Uridan Controllers ・ ご Domain Controllers ・ ご Domain Controllers ・ ご ForeignSecurityPrincipal: ・ ご Managed Service Accour ・ Users 	全前 ない DnsJpdateP DnsJpdateP DnsJpdateP Domain Co Domain Co Domain Co Domain Gue Domain Users Enterprise A Comp Polic Guest Interprise R Grup Polic Grup Polic Grup Polic Red colup D Red colum D	権類 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・グローバル 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・グローバル 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・グローバル 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・クローバル セキュリティグループ・コニバーサル セキュリティグループ・ユニバーサル セキュリティグループ・ユニバーサル 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・ブローバル セキュリティグループ・ゲムシローカル セキュリティグループ・ゲムシローカル 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・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・グローバル 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・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・フローバル	説明 DNS 管理者グルーブ DHCP サーパーなどの語 ドメインの音文でのワーク ドメインのすべてのワーク ドメインのまずスト ドメインの全ユーザー エンターブライズの管理 このグルーブのメンパーは このグルーブのメンパーは このグルーブのメンパーは このグルーブのメンパーに このグルーブのメンパーに このグルーブのメンパーに このグルーブのメンパーに このグルーブのメンパーに このグルーブのメンパーに このグループのメンパーに このグループのメンパーに このグループのメンパーに このグループのメンパーに このグループのメンパーに このグループのメンパーに	かの ステ user1のブ 学の 所属す 名前 Pon IMSI testt	ロ/(ティ (ヤルイン ニト デスクト・ 住所 っるグループ(M ain Users Jsers vivn3.jp	T 型は ジブ サービスの) アカウント :: Active Dia EPOSTHV EPOSTHV	え プロファイル プロファイル フロファイル rectory ドメイン OColocal/USers Colocal/USers /Users	セッション COM+ 電話 組織 サービスフォルダー	? × リモート制御 フリガナ 所属するクループ
▲ Window	ws Server	7 2022 の場合		道 プライマ ブラ	カロ(D) ?リ グループ: イマリ グルーフ	削除(R Domain l の設定(S) OK) Users Macintosh ク ーションがない 必要はありませ キャンセル	ライアントまたは POS 場合は、プライマリグ がん。 適用(A)	ax 対応のアブリケ ループを変更する へルプ

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ー」 からユーザーを追加し、追加したユーザーをグループ IMSUsers に所属させます。さら に「Active Directory ユーザーとコンピューター」のグループには、メールドメイン名の セキュリティグループもできているはずですので、そのセキュリティグループにも所属さ せます。

これによって Account Manager 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。 結果的に両者が連動していることを確認することができます。



langua de la companya	יגארבא-א-א	-9			
🦪 ファイル(E) 携	\$ff(A) 表示(Y) ウ	ィンドウ(型) ヘルプ(田)			X
← → 🖻 📧	🛛 🕹 🛍 🗡 🖆	🖻 🖻 😰 🖬 🦉 🖉	🎽 🖓 🍕 🙆		
Active Directory	/ ユーザーとコンピューダ	Users 23 個のオブジェクト			
□ 田 □ 保存された:	5IU	名前	種類	説明	
E Builtin		Administrator	ユーザー	コンピュータバメインの管理	
E Comput	ters	Cert Publishers	セキュリティグル	このグループのメンバは Acti	
🗈 🧭 Doma 🖉	ヴルーナの選択			? ×	
Forei	オブジェクトの種類を遠	訳してください(S):			
	グループ または ビルト	イン セキュリティ プリンシパル		オブジェクトの種類(<u>O</u>)	
	場所を指定してください	۱(<u>F</u>):			
	epost.test			場所(_)	
	選択するオブジェクト名	を入力してください (例)(E):			
	IMSUsers			名前の確認(C)	
	1		7		
	詳細設定(<u>A</u>)			DK キャンセル	4
-				AT 10018/2010/06/218	2
		Contract Clients	ユニリニ わちっロティバル	ヘルノとリホート リーヒスの…	
		Ritest-sample04.in	セキュリティグル	test-sample04.in	
		🖸 user1	ユーザー	Contraction () and () and ()	
		🖸 user2	ユーザー		
		🖸 user3	ユーザー		
1		🖸 user4	ユーザー		

▲ユーザーを追加する場合は、グループ IMSUsers に所属させ、メールドメイン名のセキュリティグループにも所属させるようにする

「複雑さの要件を満たす必要があるパスワード」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「グループポリシーの管理」から呼び出しが可能な「複雑さの要件を満 たす必要があるパスワード」設定(旧「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。

Windows Server 2012 / 2016 / 2019 / 2022 では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。

2008以前は「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。

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。



- INZEPOTO		925
	グループ ポリシーの管理	_ _ ×
(▲ ファイル(F) 操作(A) 表示(V) (● ● 2 前 Q 図 前	バンドウ(W) ヘルプ(H)	_ 8 ×
	フォレスト: EPOSTHVD2.test 内容 名前 風下メイン 通りイト 資ンパレーブポリラーのモデル/作成 近 ウルーブポリラーの相関	
hv2EPST0 (<u>国</u> ファイル(F) 操作(A) 表示(V) ご	グルーブ ポリシーの管理 ł<2とF2(W) ヘルブ(H)	97. X
** 200 0		
 ダループボリシーの管理 ▲ △ フォレスト: EPOSTHVD2.test ▲ 論 ドメイン ▲ 論 EPOSTHVD2.test 	EPOSTHVD2.test 状態 リンカされたグループ ポリシー オブジェクト グループ ポリシーの継承 委任	
📷 Default Domain Pol ▶ 🗃 Domain Controllers ▶ 📑 グループ ポリシ	ママレントンには、このトメークの Active Difectory 2 313 マロビング ションのため あかっ ブポッシーに関係するため)。	Certa (VIV-
▶ ■ WMI フィルター	ブポリシー オブシュかト (GPO) ヘのリンクを進択しました。リンク プロパティへの変更 、ここで行われた変更は GPO にグローバルに適用され、この GPO がリンクされたほか 有タイに影響します。	ユーラーで 変更

6

今すぐ検出(D)







- 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]-[パスワード]の順に展開。
- 6.「複雑さの要件を満たす必要があるパスワード」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。



「複雑さの要件を満たす必要があるパスワード」設定(旧「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。

7ክሳንኑ 🗵]
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>	



複雑さの要件を満たす必要があるパスワードの条件

ユーザーのアカウント名またはフルネームに含まれる3文字以上連続する文字列を使用しない。
 長さは6文字以上にする。
 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、「複雑さの 要件を満たす必要があるパスワード」設定を「無効」にして設定します。 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。

① 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。

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ー	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	$\begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \\ \end{array}$	・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			・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

Active Directory 連携時の連動項目

※1)「Active Directory ユーザーとコンピューター」にある 2003 以降の「ユーザーログオン 名」は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ー」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 (x64)のドメイン名と AD のドメインの関係

E-Post Mail Server (x64)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ー」の Users の中にメール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、「メンバー」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 Directo	ory 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

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。

Windows Server 2008 R2 / 2012 / 2016 / 2019 / 2022 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]項目はイ ンポートできません。そのためインポート後に、AD 側の「Active Directory ユーザーと コンピューター」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 (x64)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強く推奨します。

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。



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 (x64) 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。

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り、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

 \rightarrow SYSTEM

→CurrentControlSet →Services →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、上記の同バージョン以降、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 \rightarrow SYSTEM \rightarrow CurrentControlSet \rightarrow Services \rightarrow EPSTRS \rightarrow ADRetryTime (DWORD) デフォルト 10 (回) \rightarrow EPSTDS \rightarrow ADRetryTime (DWORD) デフォルト 10 (回) \rightarrow EPSTPOP3S \rightarrow ADRetryTime (DWORD) デフォルト 10 (回) \rightarrow EPSTIMAP4S \rightarrow 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 (x64) 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

 \rightarrow SYSTEM

 \rightarrow CurrentControlSet

 \rightarrow Services

 $\rightarrow \text{EPSTRS}$

→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

 ${\rightarrow} CurrentControlSet$

 \rightarrow Services

 \rightarrow EPSTDS

 \rightarrow 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

 ${\rightarrow} CurrentControlSet$

 \rightarrow Services

 \rightarrow 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

 \rightarrow CurrentControlSet



 \rightarrow Services

 \rightarrow 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 とコンピューター」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。

EPSTPOP3S v4.34 以前 および EPSTIMAP4S v4.49 以前の過去バージョンでは、 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 (") や円マ ーク(¥) 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した。2016 年以降の最新差分アップデートによる EPSTPOP3S v4.35 以降 および EPSTIMAP4S v4.50 以降のバージョンでは、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、有効になるよう対策が取られました。

なお、POP3/IMAP4パスワードの長さについては、旧 Windows Server の制限値に合わ せて、E-Post シリーズでは最大 14 文字までの制限が設けられていました。これまでは 15 文字以上の同パスワードは、使用できませんでしたが、2022 年 6 月以降に公開される 最新差分アップデートでは、最大 64 文字まで拡張することが可能となります。



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 (x64)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 (x64)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ー」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:4	Program	files¥EP	OST¥MS"	《Enter》				
4. EPS	TDS サー	ビスのデバ	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

Account Manager 21 -
Administrator 40 -
AD ユーザーとコンピュータ 25 -
Aレコード 18 -
DNS サーバ 17 -, - 18 -
IMSUsers-6-,-9-,-10-,-13-,-16-,-20
-, - 21 -, - 24 -, - 26 -
Mail Control 20 -, - 21 -
MailGroup 6 -, - 21 -, - 23 -
MX レコード 18 -
NT ドメイン 7 -, - 32 -
Virtual Server7 -
アカウント情報 32 -
アカウントフォルダ 20 -
アクティブースタンバイ方式

エイリアス6	3 -
簡単セットアップ 16	3 -
サービス開始 40) -
デバッグモード 40) -
独自アカウント管理 20) -
ドメインコントローラ5-,-7	7 –
ドメインローカルグループ9) -
バーチャルドメイン 6	3 -
パスワード	
の複雑さ 30) -
バッチジョブとしてのログオン 10) -
メール作業フォルダ 19) -
メールボックスフォルダ23	3 -
メンバーマシン	5 -
ライセンス数6	3 -