



LCAD_UG_20100301_1

Linux Connector for ActiveDirectory ユーザーガイド

製作著作

© 2009 Turbolinux, Inc. All rights reserved.

本書の一部、または全部を著作権所有者の許諾なしに、商用目的のために複製、配布することはできません。

Turbolinux、ターボリナックスの名称およびロゴはターボリナックス株式会社の商標または登録商標です。Linux は Linus Torvalds 氏の米国および他の国における商標です。UNIX は The Open Group の米国および他の国における登録商標です。Red Hat、および RPM は Red Hat, Inc. の米国および他の国における登録商標です。X Window System は X Consortium, Inc. の商標です。Microsoft、MS-DOS、Windows は米国 Microsoft Corporation の米国及び他の国における登録商標です。

その他、記載された会社名およびロゴ、製品名などは該当する会社の商標または登録商標です。本ガイドでは、© ® ™ の表示を省略しています。ご了承ください。

改訂履歴

LCAD_UG_20090427	初版	2009/04/27
LCAD_UG_20090513	シングルサインオンの設定例を追加しました。	2009/05/13
LCAD_UG_20090924_1	グループポリシーの反映に関する記述などを補足しました。 付録章にメールサーバー (Postfix、Dovecot) の設定例を追加しました。	2009/09/24
LCAD_UG_20091215_1	ActiveDirectory に複数ドメインコントローラが存在する場合の設定について補足しました。	2009/12/15
LCAD_UG_20100128_1	Dovecot で Maildir 形式を利用する場合の記述を追加しました。	2010/01/28
LCAD_UG_20100301_1	ProFTPD の認証に関する設定例を追加しました。	2010/03/01

目次

第 1 章 はじめに.....	1
1.1 Linux Connector for Active Directory 概要.....	3
1.2 利用環境.....	3
1.3 製品構成.....	4
第 2 章 Turbo ID AIO 管理コンソール.....	5
2.1 概要.....	5
2.2 Turbo ID AIO 管理コンソールのインストールと起動.....	5
2.3 メニューの紹介.....	6
2.4 主要な処理の流れ.....	8
2.5 ActiveDirectory へ接続.....	8
2.6 ActiveDirectory スキーマ拡張機能の配置.....	9
2.7 データの更新.....	12
2.8 ID Aio ユニットの作成.....	12
2.9 ID Aio ユニットの設定.....	14
2.10 ID Aio ユニットの解除.....	17
2.11 グループポリシーの作成.....	18
2.12 グループポリシーの確認と編集.....	19
2.13 グループポリシーの ID Aio ユニットへの適用.....	21
2.14 グループポリシーの削除.....	23
2.15 ID Aio ユニットへのユーザー/グループの追加.....	24
2.16 無効なオブジェクト(ユーザー/グループ)の削除.....	26
2.17 Windows ユーザー、グループ、コンピュータを検索.....	26
2.18 NIS マイグレーションウィザード.....	28
2.19 ID Aio ユーザーの設定変更.....	34
2.20 ID Aio グループの設定変更.....	35
2.21 グループポリシーモジュール.....	36
2.21.1 Linux Crontab.....	36
2.21.2 Firefox Policy.....	41
2.21.3 Sudoer Policy.....	44
2.21.4 Thunderbird Policy.....	46
2.21.5 CUPS Policy.....	51
2.21.6 Turbo AD ConnectorPolicy.....	61
2.21.7 Gconf Policies.....	63
第 3 章 Linux Connector for Active Directory.....	66
3.1 インストールの準備.....	66
3.1.1 システム時刻の確認と同期.....	66
3.2 インストール.....	66
3.3 初期設定.....	68
3.3.1 設定ファイルの編集.....	68
3.3.2 シリアル登録.....	68
3.4 adjoin_cli コマンド.....	69
3.4.1 adjoin_cli コマンドのパラメータ.....	69
3.4.2 adjoin_cli コマンドの使用例.....	70
3.5 adjoin_gui.....	72
3.5.1 シリアル登録.....	73
3.5.2 adbind デーモン管理.....	74
3.5.3 ドメインに参加(JOIN).....	75
3.5.4 OU(組織単位)の選択.....	76
3.5.5 ドメインから離脱.....	77
3.5.6 キーテーブルの設定.....	78
3.5.7 adbind の設定(config.xml).....	79
3.5.8 ヘルプ.....	81
3.6 サービスの管理.....	82
3.6.1 adbind サービスの起動と停止.....	82
3.6.2 adcnetworklogond サービスの起動と停止.....	82
第 4 章 その他の便利な機能.....	84
4.1 複数ドメインの指定.....	84
4.2 デフォルトドメインの省略名.....	84
4.2.1 デフォルトドメインの指定.....	84
4.2.2 省略名の指定.....	84

4.3 AD Connector Netlogon	84
4.3.1 概要.....	84
4.3.2 adcnetlogond.....	84
4.3.3 adc_get_dc.....	85
4.4 オフライン機能	87
4.5 ID Map ヘルパー	87
4.5.1 概要.....	87
4.5.2 SIDとUID/GIDのマッピング情報の検索と削除.....	87
4.5.3 現在のマッピングリストの出力.....	89
4.5.4 現在のUID/GIDを指定範囲に移行.....	89
4.5.5 マッピングテーブルの完全な削除.....	90
第5章 SSO(シングルサインオン)設定例	92
5.1 ApacheのSSO設定	92
5.1.1 前提条件.....	92
5.1.2 設定例.....	92
5.2 SSHサーバーのSSO設定	95
5.2.1 前提条件.....	95
5.2.2 設定例.....	95
第6章 アンインストール	97
6.1 Turbo ID AIO 管理コンソールのアンインストール.....	97
6.2 Linux Connector for Active Directoryのアンインストール.....	97
付録 I. 設定例ご紹介	99
A. Postfix / Dovecot の設定例.....	99
B. ProFTPD の設定例.....	102

第1章 はじめに

本ガイドは、Linux Connector for Active Directory をご使用いただく際に必要な手順を解説しています。ご利用を開始する前に必ずご確認ください。

「Linux Connector for Active Directory クイックスタートガイド」では、システムのインストールおよび最小限の初期設定までを簡単に解説しています。インストール時には合わせてご参照ください。

本ガイドの表記について

本ガイドでの表記方法を以下に示します。

キー

キーは、次のように[]で表記します。

例) 入力したコマンドを実行するには、[Enter]キーを押します。

複数キーの組み合わせは、次のように表記します。

例) コンソール、またはグラフィカルログイン画面に戻るには、[Ctrl]+[Alt]+[BackSpace]キーを押します。

入力する文字列

ユーザーが入力する文字列は、次のように太字で表記します。

例) テキストモードでインストール作業を進めるには、boot: プロンプトで **text** と入力し[Enter]キーを押します。

置き換える文字列

入力の際、ユーザーが置き換える必要のある文字列は、次のように斜体で表記します。

例) *filename* は、実際のファイル名に置き換えます。

コンソールの出力

コンソール上に出力されるコマンドの実行結果やファイルの内容は、次のように表記します。

例) ls コマンドを実行して ディレクトリの内容を確認します。

```
$ ls -l /home/turbo
合計 4
-rw-r--r--  1 turbo  turbo           0  2月 22 14:20 sample.txt
drwxr-xr-x  2 turbo  turbo        4096  2月 22 14:18 sample_dir/
```

プロンプトの表示

本ガイドでは、コマンドプロンプトを、#(スーパーユーザー) と \$(一般ユーザー) のみで表記します。また、# で表記されるコマンドは、スーパーユーザーのみ実行可能です。

コラム

特に注意いただく点、強調したい点として記載するコラムには以下のアイコンを使用しています。



知っていると便利な事項を示します。



ご注意ください事項や最も重要度の高いコラムを示します。

1.1 Linux Connector for Active Directory 概要

Linux Connector for Active Directory は、ターボリナックス株式会社が SSO (シングルサインオン) 実現のために研究開発した製品です。Linux クライアントが Windows ドメインのメンバーとなる機能を持ち、システム管理者は Windows クライアントと同様に Linux クライアントも管理することができますので、管理コストを大幅に削減し、ユーザーの利便性も向上させます。ActiveDirectory の一般的な Windows アカウント (アカウントとパスワード) は、Linux OS / Windows OS を意識することなく任意のクライアントからドメインへログインすることができます。管理者は Windows 上の GUI ツールを使用し Linux クライアントのポリシー定義を行うこともできます。

1.2 利用環境

次の利用環境を準備してください。

● Linux コンピュータ

利用環境は以下ディストリビューションです。いずれかインストールされたコンピュータを準備してください。

Turbolinux 11 Server 32/64 bit

Turbolinux Client 2008

RHEL 5 32/64 bit

CentOS 5 32/64 bit

● Active Directory の構築が完了した Windows サーバー

Windows Server 2003 スタンダード/エンタープライズ SP1 または SP2

Windows Server 2008 スタンダード/エンタープライズ



ActiveDirectory のレルム名 (ドメイン名) に " " (アンダースコア) を含む場合、Linux Connector for Active Directory の Linux クライアントが参加 (Join) する際、正常に DNS への登録が行われません。レルム名には、"_" (アンダースコア) を含めないようにしてください。

● Windows 管理端末

Turbo ID AIO 管理コンソールをインストールする管理用のクライアントです。Active Directory の動作する Windows サーバーで兼用することも可能です。



Turbo ID AIO 管理コンソールを動作させるには、Microsoft .NET Framework 2.0 のインストールが必要です。

1.3 製品構成

Linux Connector for Active Directory の CD-ROM には以下のソフトウェアが含まれています。

ソフトウェア/インストール先	パス	説明
Turbo ID AIO 管理コンソール / Windows 管理端末	Win32/	Windows 管理 PC 用インストーラ(zip ファイル)
Linux Connector for Active Directory / Linux コンピュータ	TLC2008/	Turbolinux Client 2008 用 RPM パッ ッケージファイル
	TL11S/x86_32/	Turbolinux 11 Server 32bit 用 RPM パッケージファイル
	TL11S/x86_64/	Turbolinux 11 Server 64bit 用 RPM パッケージファイル
	RHEL5.2/x86_32/	RHEL 5.2 および CentOS 5.2 32bit 用 RPM パッケージファイル
	RHEL5.2/x86_64/	RHEL 5.2 および CentOS 5.2 64bit 用 RPM パッケージファイル

● Turbo ID AIO 管理コンソール

Windows 管理端末(ActiveDirectory の構築されている Windows サーバーで兼用も可能)にインストールします。ActiveDirectory のアカウントと Linux のアカウントのマッピングや、グループポリシーの定義など ActiveDirectory を GUI 操作で管理します。インストールおよび設定は「[第 2 章 Turbo ID AIO 管理コンソール](#)」を参照ください。

● Linux Connector for Active Directory

Linux コンピュータにインストールします。Linux コンピュータがドメインのメンバーとして JOIN し、ユーザーが ActiveDirectory の認証を使用しログインするための機能を提供します。また、本ソフトウェアの利用に必要なライセンス登録も行います。インストールおよび初期設定は「[第 3 章 Linux Connector for Active Directory](#)」を参照ください。

第2章 Turbo ID AIO 管理コンソール

2.1 概要

Turbo ID AIO 管理コンソールは、Microsoft Windows サーバーを管理するためのソフトウェアです。Windows の管理端末または、Windows サーバー上で動作します。Windowsドメインの管理者は、Turbo ID AIO 管理コンソールを利用してドメインのユーザーとLinux ユーザーのUID/GIDのマッピング指定が可能になります。また、UID/GIDの範囲指定やLinux グループポリシーの定義や設定、NIS ユーザーの移行ウィザードなどの機能も提供します。



NIS サーバーからの移行はサポート対象となりません。ご注意ください。

2.2 Turbo ID AIO 管理コンソールのインストールと起動



Turbo ID AIO 管理コンソールを動作させるには Microsoft .NET Framework Version 2.0 が必要です。あらかじめインストールを完了しておいてください。

以下よりダウンロードが可能です。

<http://www.microsoft.com/downloads/details.aspx?familyid=0856eacb-4362-4b0d-8edd-aab15c5e04f5&displaylang=en>

インストール

Windows システムに管理者権限でログオンし Linux Connector for Active Directory CD-ROM の win32 フォルダにある Turbo ID AIO 管理コンソールのインストーラを解凍します。インストーラ turboIDAiOSetup.exe をダブルクリックし実行します。インストール手順および初期設定の概要については「Linux Connector for Active Directory クイックスタートガイド」を参照してください。

インストール完了後には「[2.4.主要な処理の流れ](#)」を参照し必要な設定を行ってください。

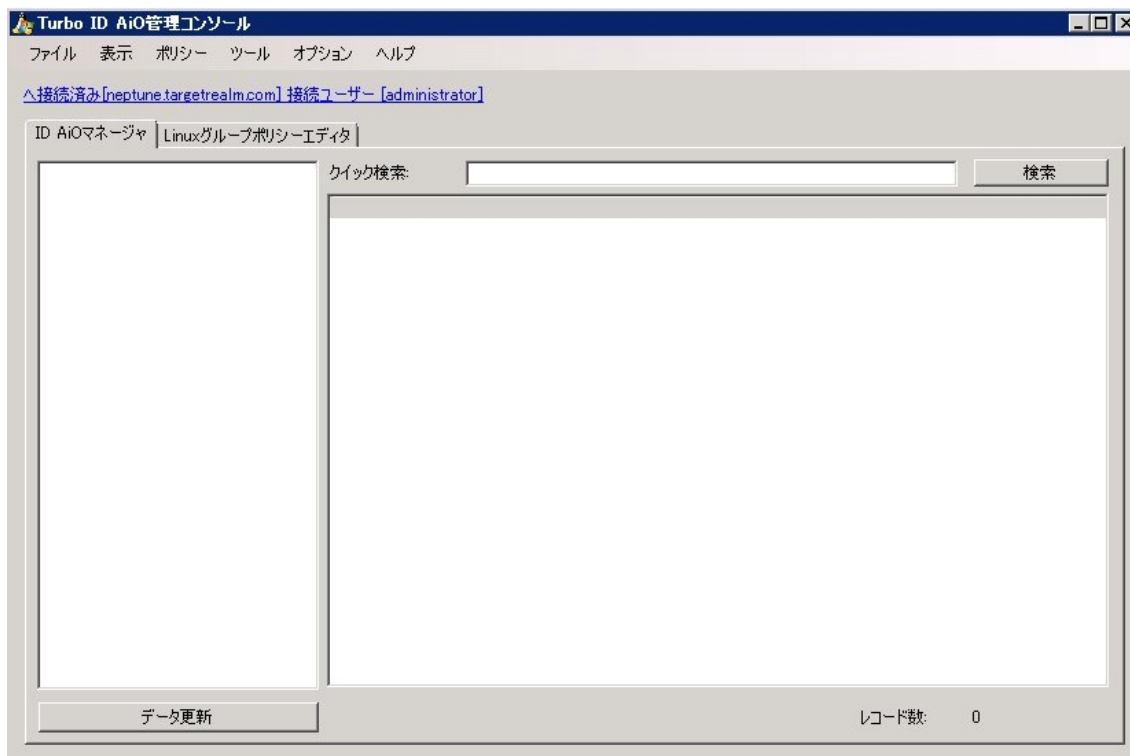
起動



デスクトップの Turbo ID AIO アイコンをダブルクリックするか、スタートメニュー -> “すべてのプログラム” -> “turbo” -> “Turbo ID AIO” -> “Turbo ID AIO administrative console” をクリックし Turbo ID AIO 管理コンソールを起動します。メイン画面が表示されます。ID Aio マネージャとLinux グループポリシーエディタの2つのタブで構成されています。

2.3 メニューの紹介

メイン画面のメニューバーには“ファイル” “表示” “ポリシー” “ツール” “オプション” “ヘルプ” の各メニューが表示されます。各サブメニューの概要について紹介します。



ファイル

サブメニュー	説明
終了	Turbo ID AIO 管理コンソールを終了します。

表示

サブメニュー	説明
標準表示	Turbo ID AIO 管理コンソールのディレクトリツリーの表示モードを標準モードに切り替えます。Windows Server の管理ツール “Active Directory ユーザーとコンピュータ” の表示内容と同じようにすべての OU とサブディレクトリを表示します。
コンパクト表示	Turbo ID AIO 管理コンソールのディレクトリツリーの表示モードをコンパクトモードに切り替えます。作成済み ID Aio ユニットのみ表示します。

ポリシー

サブメニュー	説明
ポリシーの作成	システムに存在するグループポリシーを選択しグループポリシーセットを作成します。デフォルト値で作成されます。ID Aio ユニットにグループポリシーを適用するにはまずポリシーを作成する必要があります。 導入時には十分考慮し適切なグループポリシーを用意してください。適用し

	たグループポリシーは ActiveDirectory に格納されます。
ポリシーを開く	作成したグループポリシーを開いて個々の設定を確認、変更します。グループポリシーはデフォルト値で作成されるので値を変更する場合は“ポリシーを開く”を使用します。 作成済みのポリシー項目は固定されていて項目の追加などの変更はできません。
ポリシーの削除	ポリシーを削除します。既に ID Aio ユニットに配置されている場合は、そのリンクも含めて削除されますので、運用後にグループポリシーを削除する際は十分に注意してください。

ツール

サブメニュー	説明
無効なオブジェクトの削除	ActiveDirectory の管理者がユーザーやグループを削除した場合、ID Aio 上のユーザー/グループも無効になります。これらを検索し削除します。 外部信頼関係にあるドメインは、“信頼する側” “信頼される側”という一方向性の信頼関係であるという特性があります。ID Aio ユニットのユーザー/グループもまたデフォルトで無効ユーザーとして検出されます。
グループのバッチ処理	ID Aio ユニット単位に Windows ユーザー/グループをまとめて適用します。
Windows ユーザー、グループ、コンピュータを検索	Windows ユーザー/グループを検索することができます。
配置	ActiveDirectory スキーマの拡張機能の検出と配置を行います。ドメインでの使用を開始する前に一度必ずこの操作を行い、ActiveDirectory スキーマを拡張する必要があります。 また、一度拡張したスキーマを元に戻すことはできませんのでご注意ください。
NIS マイグレーションウィザード	NIS サーバーで管理していたユーザーとグループを ID AiO ユニットへ移行します。

●“オプション”メニュー

サブメニュー	説明
言語	表示言語を“中文(中国語)”、“English(英語)”、“日本語”から選択します。“自動言語検出”を選択した場合、環境に合わせて自動選択されます。

●“ヘルプ”メニュー

サブメニュー	説明
情報	Turbo ID AIO 管理コンソールに関する情報ダイアログが表示されます。

2.4 主要な処理の流れ

ActiveDirectory で Linux システムのユーザーとドメインを管理するには次の処理を実行します。

1. ActiveDirectory へ接続します。通常の接続先はドメインコントローラです。(「[2.5.ActiveDirectory へ接続](#)」参照)
2. ActiveDirectory のスキーマを拡張します。ドメインでの使用を開始する前に一度必ずこの操作を行い、ActiveDirectory スキーマを拡張する必要があります。Linux ユーザーの使用するスキーマを追加する操作です。(「[2.6.ActiveDirectory スキーマ拡張機能の配置](#)」参照)



一度拡張したスキーマを元に戻すことはできません。ご注意ください。

3. ID Aio ユニットの標準表示し、ID Aio ユニットの作成します。OU (組織単位)を作成しているドメインでは、OU の ID Aio ユニットも作成します。(「[2.8.ID Aio ユニットの作成](#)」参照)
4. グループポリシーを作成します。既存のポリシーを選択してグループポリシーを作成しますが、作成時はデフォルト値が設定されます。(「[2.11.グループポリシーの作成](#)」参照)
5. 作成したグループポリシーを開き環境に合わせて編集します。(「[2.12.グループポリシーの確認と編集](#)」参照)
6. ID Aio ユニットにグループポリシーを適用します。(「[2.13.グループポリシーの ID Aio ユニットへの適用](#)」参照)
7. ID Aio ユニットにユーザーを追加します。(「[2.15.ID Aio ユニットへのユーザー/グループの追加](#)」参照)
8. Linux システムが OU を指定し JOIN すると、OU のユーザーはその Linux システムからログインした際、グループポリシー (ユーザーレベル) が適用されます。グループポリシーは OU に適用されます。OU にグループポリシーが作成されていない場合は、OU のグループポリシーが適用されます。上位の OU にもドメインのメンバーサーバーのデフォルトポリシーが使用されます。

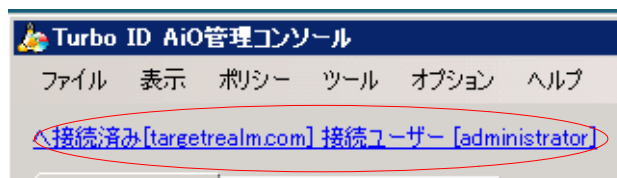


OU に 1 つでもグループポリシーが適用されている場合は、その上位 OU のグループポリシーを使用することはありません。何も適用されていない場合にのみ上位を参照します。


2.5 ActiveDirectory へ接続

Turbo ID AIO 管理コンソールを使用するには、はじめに ActiveDirectory へ接続します。「Turbo ID AIO 管理コンソール」メイン画面の左上に以下のように表示されます。

Turbo ID AIO 管理コンソールを起動すると自動的に現在のユーザーでローカルの Active Directory ドメインサーバーへ接続されます。



青字の“接続済み[targetrealm.com]接続ユーザー[administrator]”は、targetrealm.com へ administrator で接続済みの場合に表示されます。“クリックでドメインへ接続”と表示されている場合は ActiveDirectory へ接続されていません。他の Active Directory ドメインサーバーへ接続するにはこの青地部分をクリックします。次のダイアログが表示されます。



設定項目は以下の通りです。

ドメイン

接続先のドメイン名です。

ユーザー名とパスワードの指定

“カレントユーザーで接続”の選択を解除すると、ドメインに接続する“ユーザー名”“パスワード”“認証の種類”の各項目の指定が可能になります。

カレントユーザーで接続

現在の認証済みユーザーとして接続します。



他のドメインの ActiveDirectory ドメインコントローラへ接続する場合には、“ドメイン”には全体のドメイン名を指定し、“ユーザー名”には“ドメインの NETBIOS 名¥ユーザー名”を指定します。例えば Windows2003j.sh.tlan ドメインから windows2008j.sh.tlan ドメインへ接続する場合、“ドメイン”には、“windows2008j.sh.tlan ”をユーザー名には “:windows2008j¥administrator” のように指定します。

設定完了後、[確定]ボタンをクリックするとドメインへ接続します。ドメインへの接続が成功すると管理が可能になります。

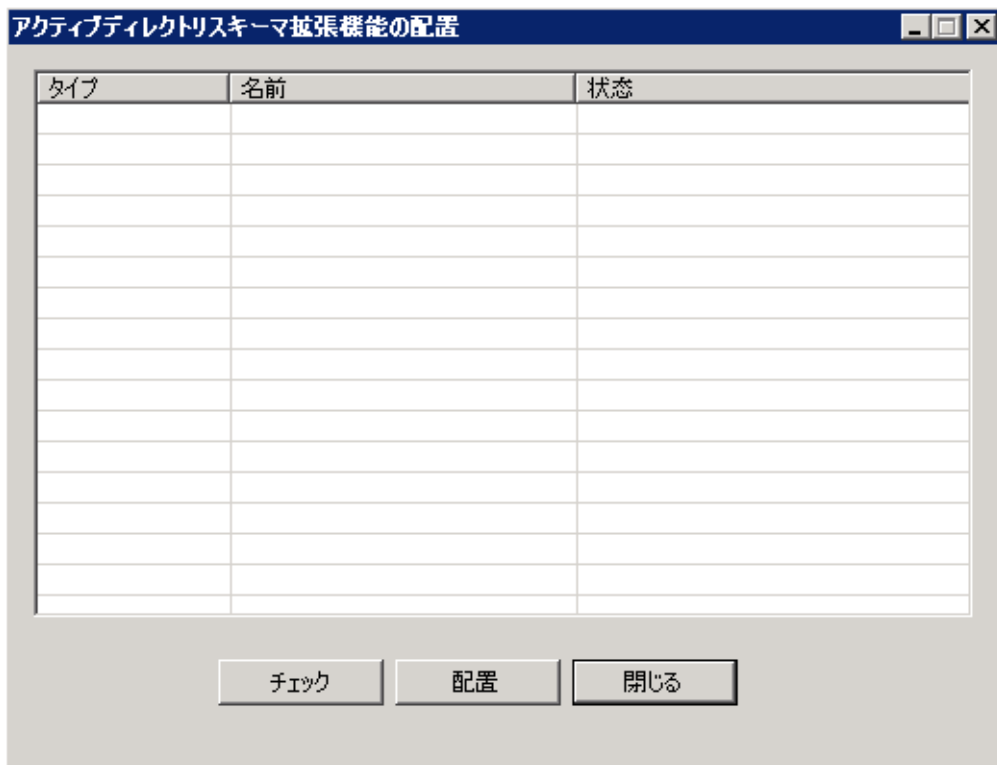
2.6 ActiveDirectory スキーマ拡張機能の配置

使用を開始する前に一度必ずこの操作を行い、ActiveDirectory スキーマを拡張する必要があります。Linux ユーザーの使用するスキーマを追加する操作です。



一度拡張したスキーマを元に戻すことはできません。ご注意ください。

「Turbo ID AIO 管理コンソール」メイン画面のメニューから“ツール”->“配置”を選択します。次の画面が表示されます。



[チェック]ボタンをクリックすると拡張スキーマ拡張機能を検出します。配置していない場合以下のように表示されます。



[配置]ボタンをクリックしてスキーマの拡張を実行してください。成功すると次のように"終了"と緑色の文字で表示されます。



確認をしたら[閉じる]ボタンをクリックしてください。

次のように赤字でが表示されている行はスキーマの拡張に失敗しています。環境を確認し配置し直してください。



スキーマの拡張は初回起動時に1度だけ実施が必要な手順です。緑色で表示され、全てのスキーマの拡張に成功したら、以降は行う必要がありません。

2.7 データの更新

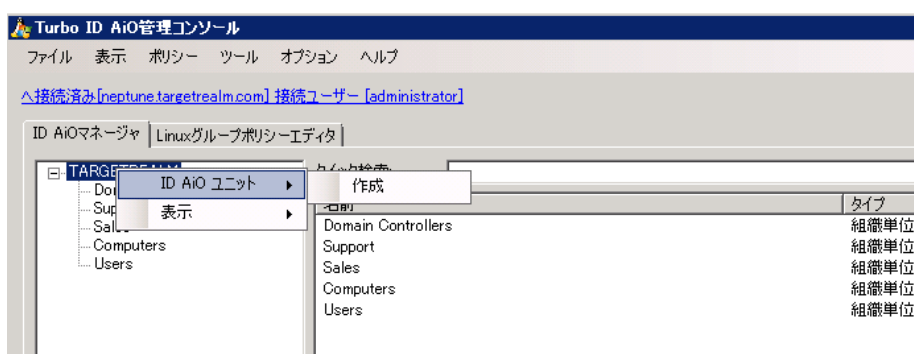
[データ更新]ボタンをクリックするか、メニューの“表示”->“コンパクト表示”をクリックして画面を更新します。

2.8 ID Aio ユニットの作成

ドメインのメンバーサーバーである Linux システムのユーザーとグループが所属する OU (組織単位) に ID Aio ユニットの作成する必要があります。これはまた、OU に所属するメンバーが Linux グループポリシーを使用するためにも必要な操作です。

ID Aio マネージャタブには、デフォルトのコンパクト表示の場合、作成済みの ID Aio ユニットのみがウィンドウに表示されます。新規に作成する場合は「Turbo ID AIO 管理コンソール」メイン画面のメニューから“表示”->“標準表示”を選択してください。

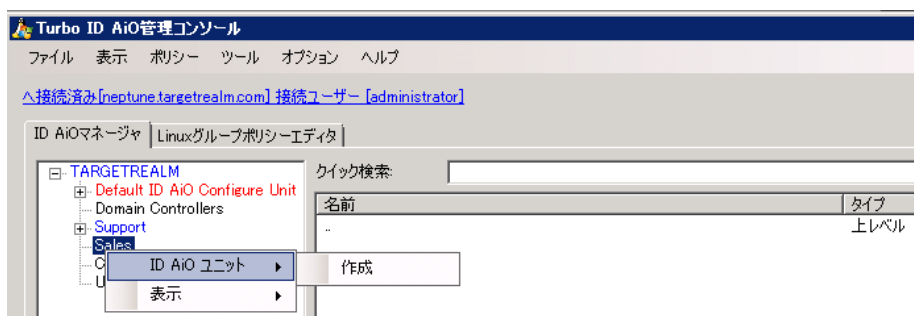
はじめにドメイン名の上で右クリックしメニューから、“ID Aio ユニット”->“作成”を選択します。



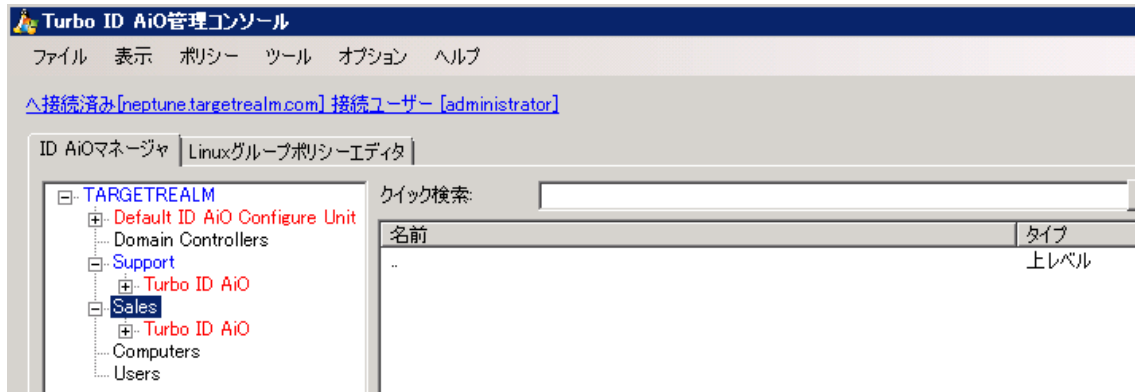
次のように Default ID Aio Configure Unit が作成されます。



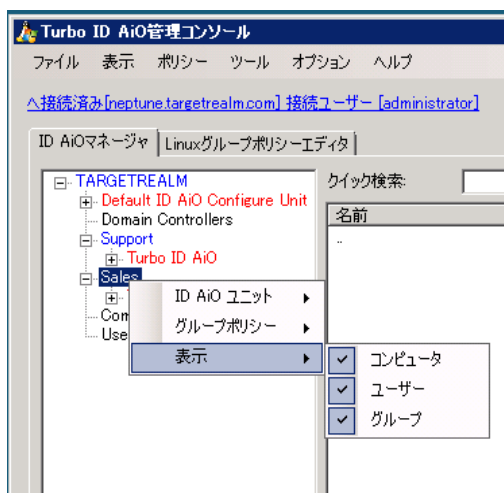
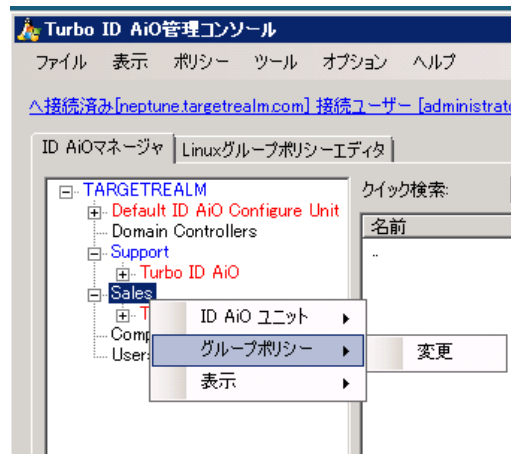
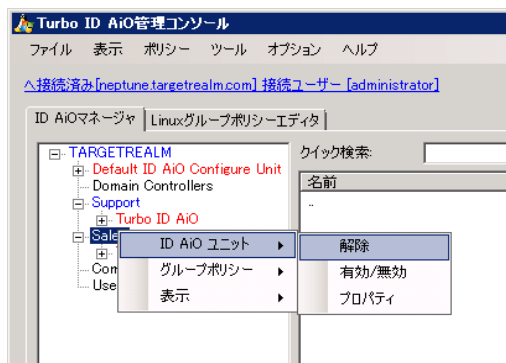
同様に OU の ID Aio ユニットも作成します。OU 上で右クリックしメニューから“ID Aio ユニット”->“作成”を選択します。



ID Aio ユニットの作成が完了した組織は 青色で表示され、サブディレクトリに Turbo ID Aio が作成されます。

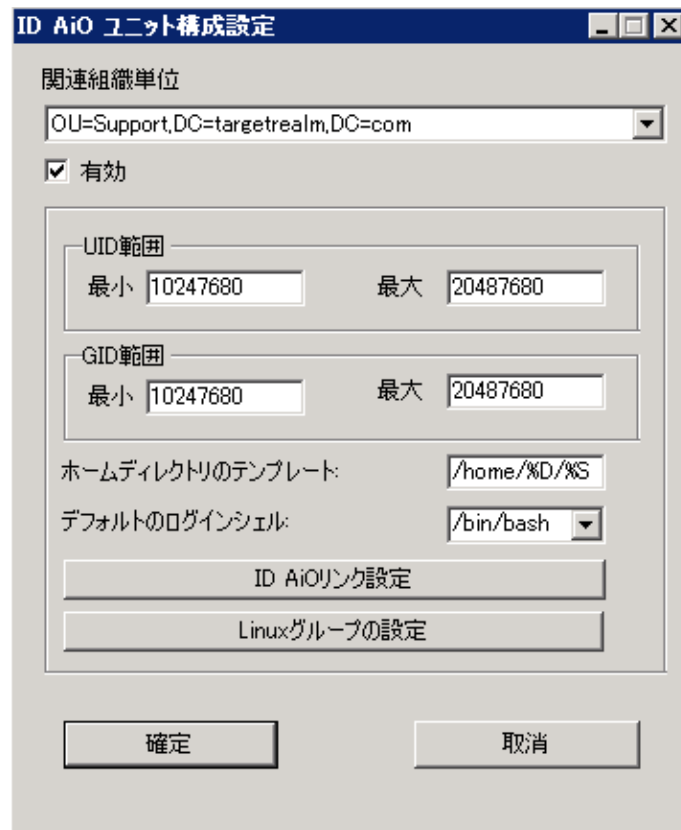


同時に右クリックで表示されるメニューも次のように変わります。



2.9 ID Aio ユニットの設定

OU の ID Aio ユニット上で右クリックし、メニューから “ID Aio ユニット” -> “プロパティ” を選択します。次の「ID Aio ユニット構成設定」画面が表示されます。



ID Aio ユニットについて以下の項目を設定します。

関連組織単位

対象の組織単位が選択されています。プルダウンリストから ID Aio ユニットの選択を変更することも可能です。

有効

選択時は ID Aio ユニットが有効です。選択を解除すると無効になります。ID Aio 管理コンソールの ID ユニット名を右クリックしメニューから “ID Aio ユニット” -> “無効”/ “有効” を選択し切り替えることも可能です。

UID 範囲

この ID Aio ユニットのユーザーにマッピングする UID の最小値と最大値を指定します。ユーザーを有効にする際、この範囲内で自動的に UID が割り当てられます。ID Aio ユニットごと、あるいは信頼関係にあるドメイン内でも重複しない範囲を指定するようにしてください。

GID 範囲

この ID Aio ユニットのグループにマッピングする GID の最小値と最大値を指定します。ユーザーを有効にする際、この範囲内で自動的に GID が割り当てられます。ID Aio ユニットごと、あるいは信頼関係にあるドメイン内でも重複しない範囲を指定するようにしてください。

ホームディレクトリのテンプレート

ID Aio ユニットのユーザーのホームディレクトリパスのデフォルト値です。

デフォルトのログインシェル

ID Aio ユニットのユーザーのログインシェルのデフォルト値です。



上記の指定はデフォルト値で、ユーザー/グループの追加時に明示的に指定を変更しない場合に適用される範囲の指定です。ユーザー/グループを追加する際に、個別に指定を変更することも可能です。

このように同一のユーザーは異なる ID Aio ユニットにおいても同一の ID を使用することができますし、また異なる ID を使用することもできます。

ここまでに指定した値は、以下の通り「ID Aio 管理コンソール」の ID Aio ユニットの “properties” 行をクリックして確認できます。

The screenshot shows the Turbo ID Aio Management Console interface. The window title is "Turbo ID Aio管理コンソール". The main content area is divided into a left sidebar and a main table. The sidebar shows a tree view with "TARGETREALM" expanded, and "Default ID Aio Configure Unit" selected. Underneath, "Properties" is highlighted. The main table displays the following data:

アイテム	値
defaultLoginShell	/bin/bash
disabled	False
homeDirectoryTempl...	/home/%D/%S
maxGID	20487680
maxUID	20487680
minGID	10247680
minUID	10247680

At the bottom of the window, there is a "データ更新" button on the left and "レコード数: 7" on the right.

ID Aio リンク設定

このボタンをクリックすると次の画面が表示されます。



この設定は管理者の操作を簡素化します。例えば上記を Engineer OU の ID Aio ユニットのプロパティから表示している場合、DC=targetrealm,DC=com の OU 上のユーザーは Engineer OU に JOIN している Linux システムからログインすると DC=targetrealm,DC=com のユーザー情報を利用することができます。ユーザーのポリシーは、Linux システムが JOIN している OU のグループポリシーが適用されます。

もしコンピュータが Engineer OU に JOIN している場合は、Engineer OU に設定されているグループポリシーが適用され、もしコンピュータが DC=targetrealm,DC=com に JOIN している場合は、DC=targetrealm,DC=com に設定されているグループポリシーが適用されます。



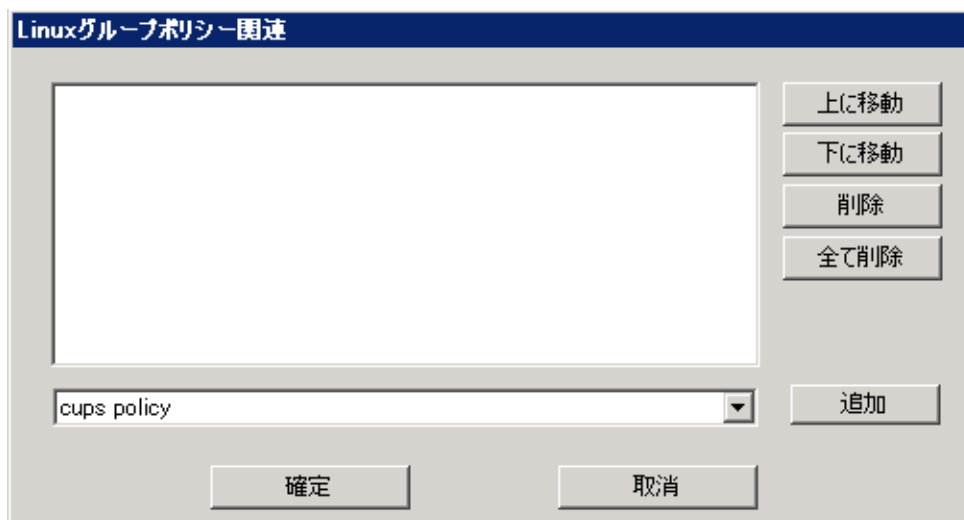
この ID Aio リンク設定では、Engineer OU に JOIN しているコンピュータで、ユーザーとグループ (getent passwd/group コマンド) を取得した場合、DC=targetrealm,DC=com のユーザー/グループはリストされませんがログイン可能となります。DC=targetrealm,DC=com に JOIN しているコンピュータでは DC=targetrealm,DC=com のユーザー/グループがリストされログイン可能です。



ログイン時は、“ID Aio ユニットのリンク設定”画面のリスト上部からマッチする OU のユーザー情報でログインします。リストの OU を選択し [上に移動][下に移動] ボタンで順序を変更します。

Linux グループの設定

このボタンで OU のグループポリシーを設定します。ID Aio 管理コンソールの ID ユニット名を右クリックメニューから“グループポリシー”->“変更”を選択しても同様に操作できます。



下部のリストからグループポリシーを選択し[追加]ボタンで設定します。複数のポリシーを追加した場合、[上に移動][下に移動]ボタンでグループポリシーの順序を変更することが可能です。グループポリシーは上から順に実行され、整合性がとれないポリシーは下にあるグループポリシーで上書きされます。また選択したグループポリシーを削除するには[削除]ボタンを、すべてのグループポリシーを削除するには[全て削除]ボタンをクリックします。



グループポリシーは上から順に実行され、下にあるもので上書きされます。グループポリシーの指定順序には注意してください。

2.10 ID Aio ユニットの解除

ID Aio ユニットの削除は作成時と逆の課程で行います。まずは、Turbo ID Aio ユニットのサブディレクトリのユニット上で右クリックメニューから“解除”を選択しユニットを削除します。Turbo ID Aio ユニットのすべて削除すると Default ID AiO Configure Unit が利用されます。

2.11 グループポリシーの作成

「Turbo ID AIO 管理コンソール」メイン画面のメニューから“ポリシー” -> “ポリシーの作成”を選択します。以下の画面が表示されます。

各項目は以下の通りです。

表示名

グループポリシーの名前定義です。[名前のチェック]ボタンをクリックするとグループポリシー名を ActiveDirectory で使用できるかどうか(競合しないか)を確認することができます。

GUID

ActiveDirectory で一意のグループポリシー ID です。[GUID の変更]ボタンをクリックすると ID を自動生成します。

利用可能なグループポリシーセット

利用できるグループポリシーセットがリストされます。上記画面にはシステムの提供するデフォルトのポリシー (Thunderbird Policy、Linux Crontab、Turbo AD Connector、Sudoer、Cups Policy、GconfGP Module、Firefox Policy) が表示されています。

[参照]ボタンをクリックしてその他のグループポリシーモジュールをロードすることができます。

選択されているグループポリシーセット

選択されているグループポリシーセットがリストされます。“利用可能なグループポリシーセット” のリストから対象のグループポリシーセットをダブルクリックするか、選択し >>>> をクリックするとリストに追加されます。

また、“選択されているグループポリシーセット” 内のグループポリシーセットをダブルクリックするか、選択をして <<<< ボタンをクリックするとリストから削除されて“利用可能なグループポリシーセット” へ移動します。

設定が完了したら[保存]ボタンまたは[保存して編集]ボタンをクリックし保存します。

[保存して編集]ボタンをクリックすると Linux グループポリシーエディタタブで作成したグループポリシーを開いた状態で保存されます。初期状態ではグループポリシーセットはデフォルト値となっているため、すぐに値を変更するには、グループポリシーを開く必要があるため便利です。



グループポリシー作成後にモジュールを変更してロードし直すことはできません。もしモジュールを変更する場合は、グループポリシーを削除してから行ってください。ただし、既に OU の ID Aio ユニットに設定されているグループポリシー定義も含め削除されるので注意してください。

また、モジュールの変更はサポート対象となりません。ご注意ください。

2.12 グループポリシーの確認と編集

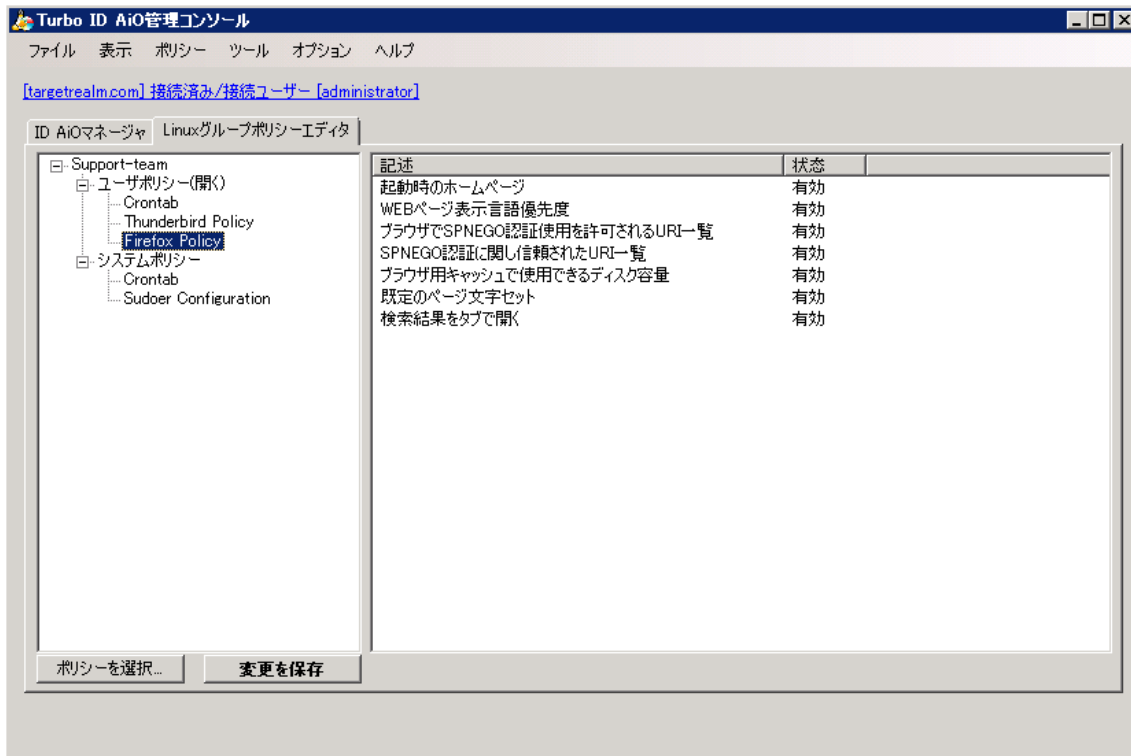
グループポリシーは作成時にはデフォルト値が採用されます。管理者は作成済みのグループポリシーの各項目の値をご利用環境に合わせて変更することができます。グループポリシーを変更する手順は以下の3通りがあります。

1. グループポリシーの作成時に[保存して編集]ボタンをクリックする
2. メイン画面のメニューから“ポリシー”->“ポリシーを開く”を選択する
3. メイン画面で“Linux グループポリシーエディタ”タブを選択し[ポリシーを選択]ボタンをクリックする

いずれかの方法で Linux グループポリシーエディタを開きます。2. 3.の方法で起動すると以下のように「Linux グループポリシーの選択」画面が表示されます。



対象のグループポリシーを選択し[確定]ボタンをクリックします。「Linux グループポリシーエディタ」タブに選択したグループポリシーが表示されます。[プロパティ]ボタンをクリックしてグループポリシーの情報を確認することもできます。





グループポリシーは“ユーザーポリシー”と“システムポリシー”で構成されています。“ユーザーポリシー”は、ユーザーがログインする際に適用され、“システムポリシー”は、ID Aio ユニットに OU の Linux システムが JOIN し adbindd が起動されたタイミングで適用されます。



システムポリシーは adbindd の起動時および“システムポリシーの実行間隔”（デフォルトは 300 秒）ごとに反映されます。“システムポリシーの実行間隔”を変更するにはグループポリシー「Turbo AD Connector」を設定します。

ただし CUPS ポリシーだけは CUPS サービスの再起動が行われるまでは反映されません。詳細は「[2.21.5.4.設定変更の予約](#)」を参照してください。

それぞれ  の部分をクリックすると展開表示されます。値を編集するにはポリシーの各行をダブルクリックしてください。ダイアログが表示され値を更新できます。

例えば  の Firefox Policy をクリックすると右側のウィンドウに各項目が表示されます。“起動時のホームページ”をダブルクリックすると以下のダイアログが表示されます。

ポリシーアイテムの編集

名前: browser.startup.homepage

起動時のホームページ

状態

有効
 無効
 未指定

www.turbolinux.co.jp

デフォルト値: www.turbolinux.co.jp

起動時のホームページの設定

確定 取消

設定変更が完了したら[確定]ボタンをクリックします。設定完了後、Linux グループポリシーエディタタブの [変更を保存]ボタンをクリックして設定が保存されます。

このグループポリシーを適用されたユーザーはログイン時に Web ブラウザ (Firefox) のホームページが “デフォルト値” の URL に設定されます。

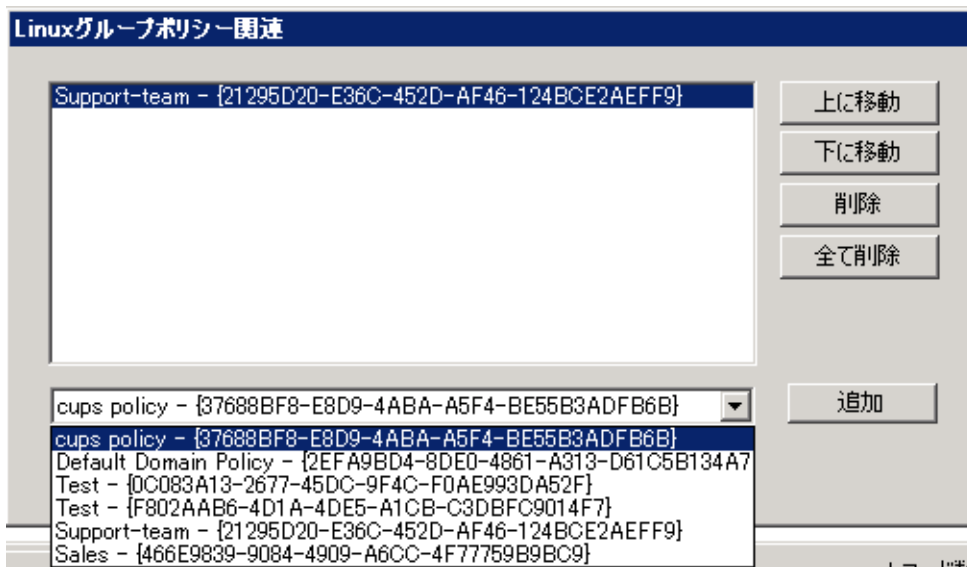
2.13 グループポリシーの ID Aio ユニットへの適用

作成したグループポリシーは ID Aio ユニットに追加することで適用され有効になります。手順は以下の通りです。

ID Aio マネージャタブを表示し、グループポリシーを適用する OU の ID Aio ユニット上で右クリックしメニューから “グループポリシー” -> “変更” をクリックします。次の画面が表示されます。



中央の枠には既に適用されているグループポリシーがリスト表示されます。その下にあるプルダウンリストから既存のグループポリシーを以下のように選択することが可能です。



選択後、[追加]ボタンをクリックすると中央の枠にリストされグループポリシーが適用されます。

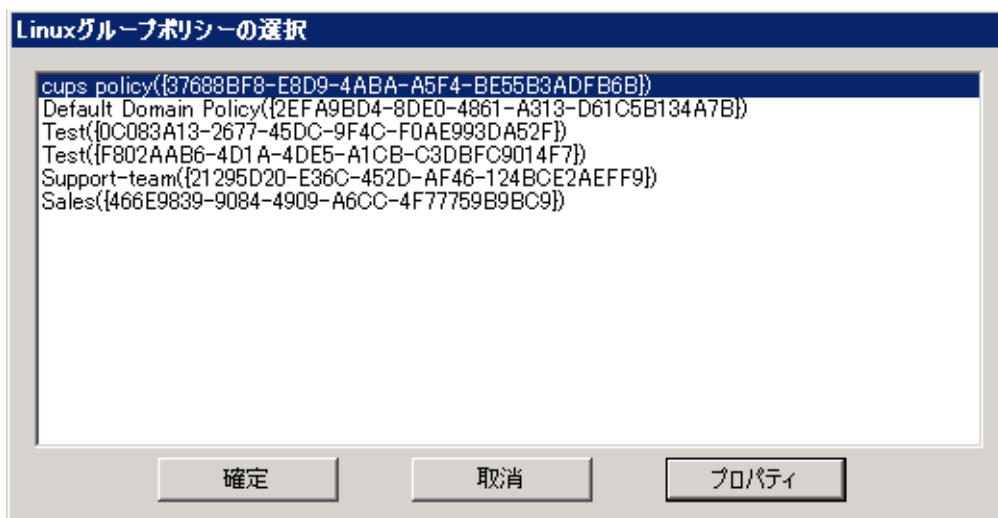
複数のグループポリシーが適用されている場合は、[上に移動] [下に移動]ボタンで順番を変更します。グループポリシーは上から順番に適用され、競合するポリシーが定義されている場合、下にあるグループポリシーで上書きされます。

リストから選択したグループポリシーを削除するには、[削除]ボタンをクリックします。確認のダイアログが表示され、[確定]ボタンをクリックするとリストから削除されグループポリシーが無効になります。

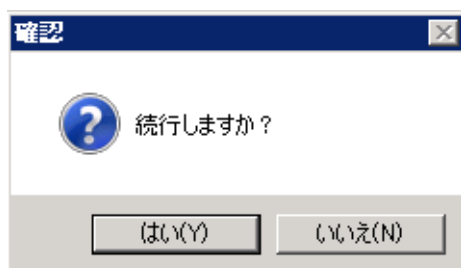
グループポリシーの関連づけをまとめて全て削除するには[全て削除]ボタンをクリックします。

2.14 グループポリシーの削除

「Turbo ID AIO 管理コンソール」メイン画面のメニューから「ポリシー」->「ポリシーの削除」を選択します。
「Linux グループポリシーの選択」画面が表示されます。



対象のグループポリシーを1つあるいは複数選択し[確定]ボタンをクリックします。次の確認のダイアログが表示されたら[はい]ボタンをクリックするとグループポリシーは削除されます。



複数グループポリシーを選択するには[Ctrl]キーを押しながらクリックします。

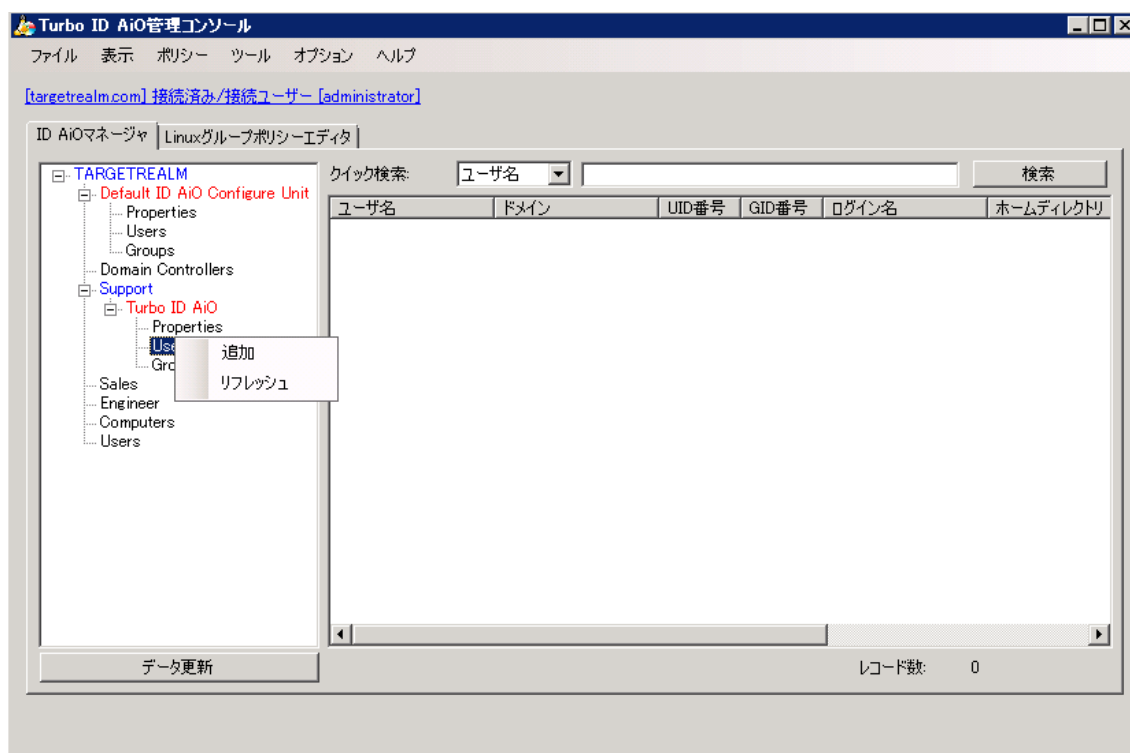
2.15 ID Aio ユニットへのユーザー/グループの追加

ID Aio ユニットの主要な機能には、ユーザーとグループの管理があります。Windows のユーザー/グループを組織単位 (OU) の ID Aio ユニットへ追加すると、Linux システムからログインをしたユーザーにも統一した ID 管理を実現します。グループも同様に統一した GID にて管理することができます。

組織単位の ID Aio ユニットを作成していない場合は、メンバーサーバーからユーザーおよびグループの情報取得要求があった場合、上位のユニットを検索します。もし ID Aio ユニットに存在しないときデフォルト ID Aio ユニット (Default AiO Configure Unit) を検索します。

デフォルト ID Aio ユニット (Default AiO Configure Unit) または、組織単位 (OU) の ID Aio ユニット (組織名下の Turbo ID Aio) およびサブディレクトリの ID Aio ユニットにユーザーを追加するには、「ID Aio マネージャ」タブでユーザーを追加する組織の Users の上で右クリックしメニューから「追加」を選択します。

以下の例は、組織単位 Support にユーザーを追加しています。



次の「Windows ユーザー、グループ、コンピュータを検索」画面が表示されます。

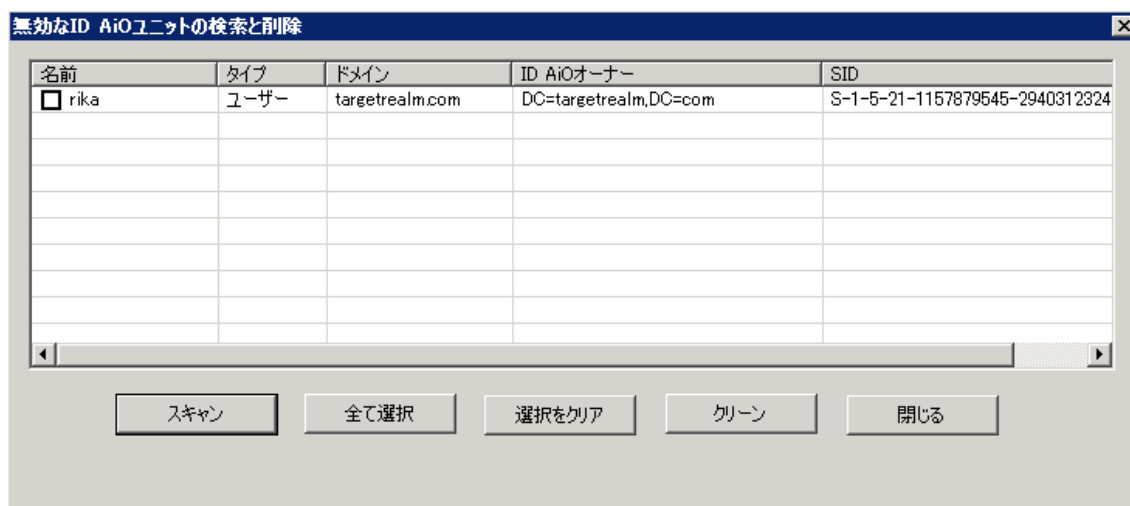
択]ボタンを解除するには[選択をクリア]ボタンをクリックします。

選択後[確定]ボタンをクリックしてください。ID Aio ユニットにユーザーが追加されます。

2.16 無効なオブジェクト(ユーザー/グループ)の削除

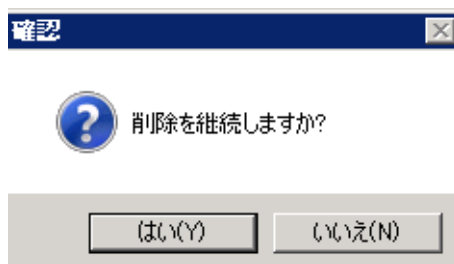
ActiveDirectory の管理ツールでユーザー/グループが削除された場合、このユーザーやグループが ID Aio ユニットに存在していても無効な ID Aio オブジェクトになります。以下の手順でこれら無効な ID Aio オブジェクトを検索しまとめて削除することが可能です。

「Turbo ID AIO 管理コンソール」メイン画面のメニューから「ツール」->「無効なオブジェクトの削除」を選択します。「無効な ID Aio オブジェクトの検索と削除」画面が表示されたら[スキャン]ボタンをクリックします。無効な ID Aio オブジェクトが存在すると以下の例のようにリストされます。



削除対象の無効な ID Aio ユニットの「名前」のチェックボックスをクリックして選択します。検索結果を全て選択する場合は[全て選択]ボタンを、選択を解除するには[選択をクリア]ボタンをクリックします。

選択後、[クリーン]ボタンをクリックすると次の確認のダイアログが表示されます。[はい]ボタンをクリックすると削除が実行されます。



外部信頼関係にあるドメインは、「信頼する側」「信頼される側」という一方向性の信頼関係であるという特性があります。ID Aio ユニットのユーザー/グループもまたデフォルトで無効ユーザーとして検出されます。

2.17 Windows ユーザー、グループ、コンピュータを検索

検索範囲のドメインを指定し、条件にマッチするユーザー、グループ、コンピュータを検索することができます。「Turbo ID AIO 管理コンソール」メイン画面のメニューから「ツール」->「Windows ユーザー、グループ、コンピュータの検索」を選択します。「Windows ユーザー、グループ、コンピュータの検索」画面が表示され

ます。

The screenshot shows a dialog box titled "Windowsユーザー、グループ、コンピュータを検索". It contains the following elements:

- 検索範囲:** A dropdown menu set to "グローバルカタログ".
- 名前:** An empty text input field.
- オブジェクトの種類:** A group box containing three checkboxes: ユーザー, グループ, and コンピュータ.
- 検索:** A button.
- 完全一致:** An unchecked checkbox.
- 検索結果の上限:** A text input field containing "99999".
- 全て選択** and **選択をクリア:** Two buttons.
- Table:** A table with 5 columns: "名前", "ログイン名(Windo...", "ユーザープリンシパル名", "フォルダ", and an empty column. The table is currently empty.
- レコード数:** A label followed by the value "0".
- 確定** and **取消:** Two buttons at the bottom.

検索範囲

プルダウンリストから検索対象の範囲を選択します。

オブジェクトの種類

検索対象のオブジェクトのチェックボックスを選択します。

名前

"名前" 欄にオブジェクト名の一部または全部を入力します。

完全一致

"完全一致" を選択すると完全に "名前" の指定と一致するものだけヒットします。

検索結果の上限

検索結果としてリストする上限です。

検索条件を指定し[検索]ボタンをクリックします。次のように結果がリストされます。



検索結果を確認したら[確定]ボタンをクリックしてください。

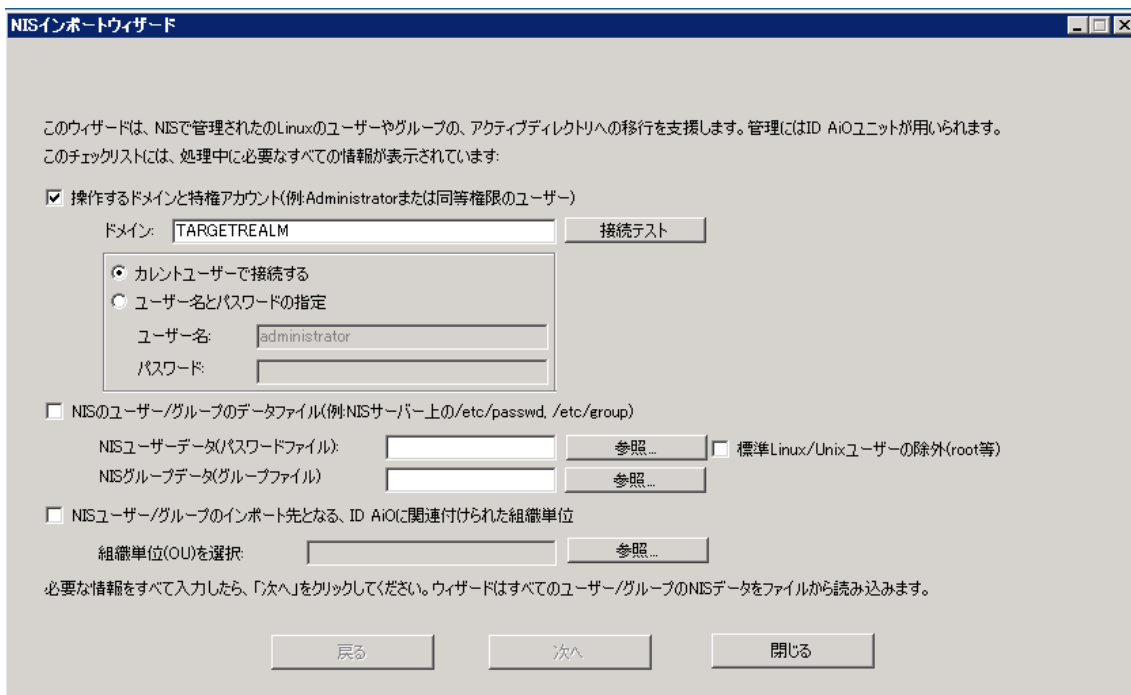
2.18 NIS マイグレーションウィザード

NIS 移行ウィザードは、NIS のユーザー/グループの情報を ActiveDirectory へ移行するためのツールです。

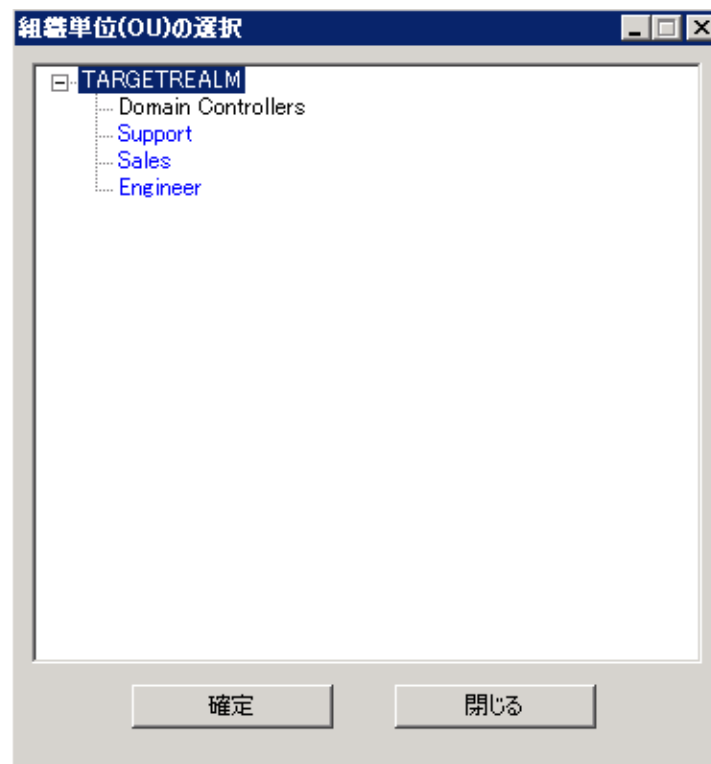
通常、NIS のユーザーおよびグループの情報は、Linux システムの /etc/passwd と /etc/group に格納されています。NIS 移行ウィザードは、これらを Windows の ActiveDirectory へとコピーします。

「Turbo ID AIO 管理コンソール」メイン画面のメニューから「ツール」->「NIS マイグレーションウィザード」を選択します。

次の「NIS インポートウィザード」画面が表示されます。



1. はじめに“操作するドメインと特権アカウント”のチェックボックスを選択して“ドメイン”欄に移行先のドメインを、ドメイン名、NETBIOS名、ドメインコントローラのIPアドレスのいずれかで指定します。“カレントユーザーで接続する”または“ユーザー名とパスワードの指定”のいずれかを選択し管理者権限のあるユーザーを指定します。“ユーザー名とパスワードの指定”を選択した場合は、“ユーザー名”、“パスワード”欄を指定してください。[接続テスト]ボタンをクリックして接続の可否を確認できます。
2. “NIS ユーザー/グループのデータファイル”のチェックボックスを選択します。“NIS ユーザーデータ(パスワードファイル)”には NIS サーバーのユーザーファイル(Linux システムの /etc/passwd ファイル)を、“NIS グループデータ(グループファイル)”には NIS サーバーのグループファイル(Linux システムの /etc/group ファイル)を指定します。[参照]ボタンをクリックしファイルを選択することができます。“標準 Linux /Unix ユーザーの除外(root 等)”を選択すると root ユーザーなど Linux システムのデフォルトユーザー以外の一般ユーザーのみを移行することができます。
3. “NIS ユーザー/グループのインポート先となる、ID Aio に関連づけられた組織単位”のチェックボックスを選択します。移行先の OU を指定します。[参照]ボタンをクリックすると次のウィンドウが表示されて OU を選択することができます。青い文字で表示されているのが ID Aio ユニットを作成済み OU です。選択後[確定]ボタンをクリックしてください。



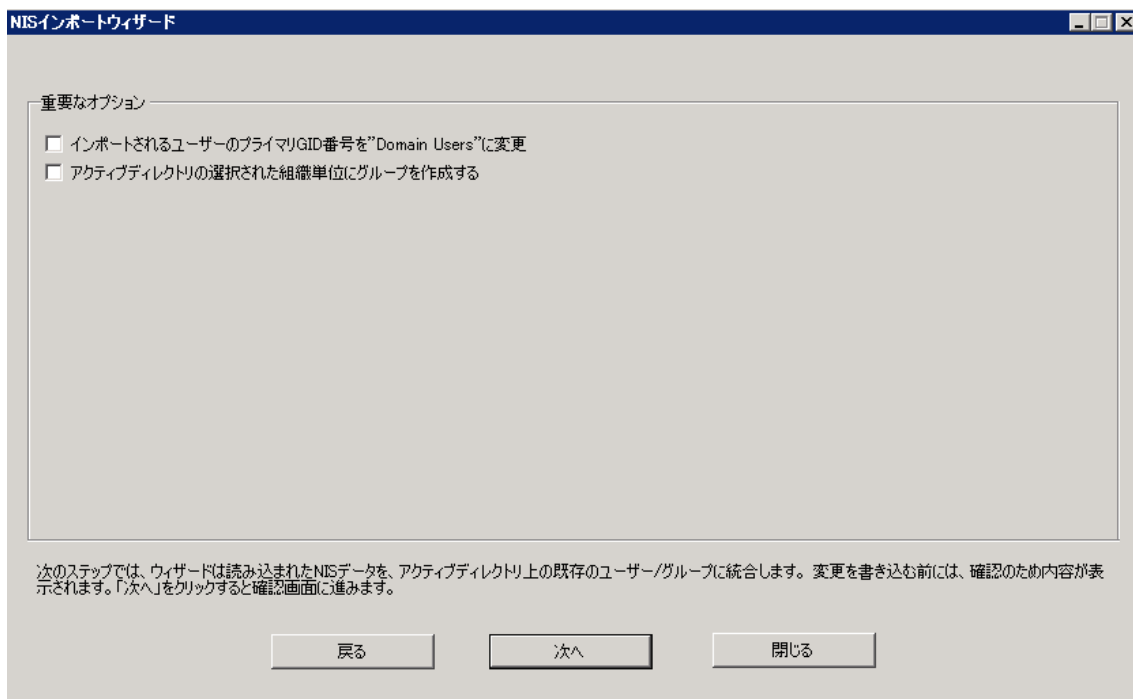
「NIS インポートウィザード」画面に戻り項目の指定が完了したら[次へ]ボタンをクリックします。

次のステップとして passwd /group ファイルの分析結果が次のように表示されます。

移行するユーザーを“UID 番号”欄のチェックボックスで選択します。[すべて選択]ボタンをクリックするとリストがすべて選択され、[すべて選択解除]ボタンで解除されます。



[次へ]ボタンをクリックします。次のステップでは移行オプションを指定します。

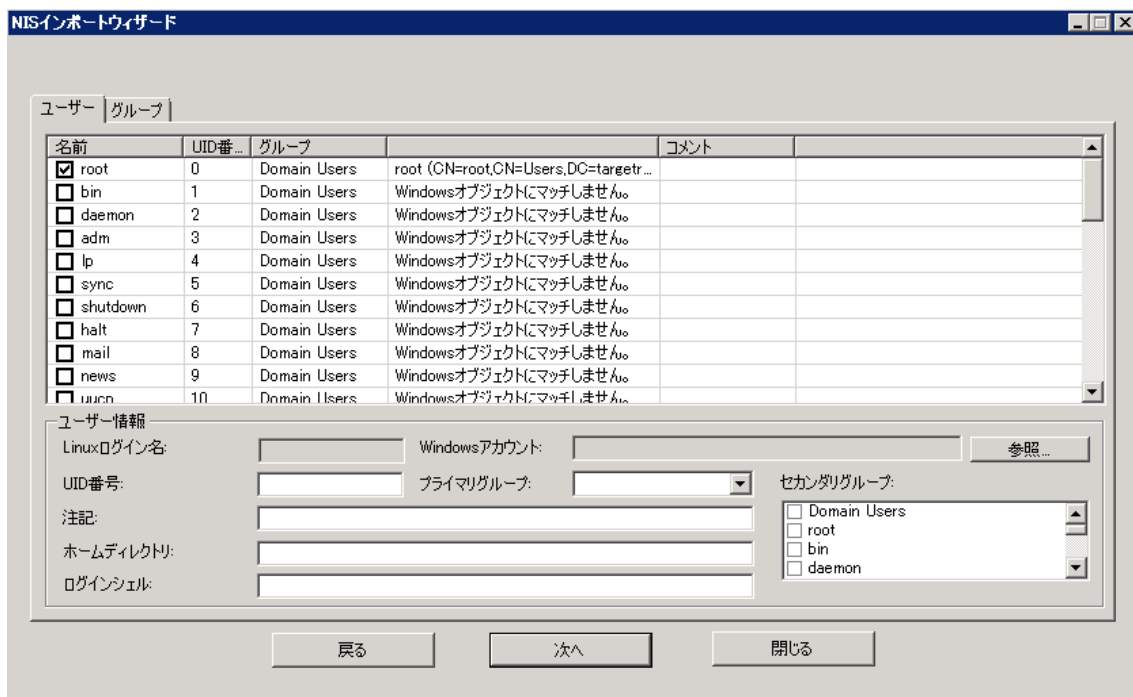


重要なオプションを指定してください。

“インポートされるユーザーのプライマリGID番号を”Domain Users”に変更”を選択すると移行ユーザーのプライマリグループが Domain Users になります。

“アクティブディレクトリの選択された組織単位にグループを作成する”を選択すると ActiveDirectory に移行するグループが存在しないとき、移行先の OU 下にグループを作成する指定です。

指定が完了したら[次へ]ボタンをクリックします。



NIS ユーザー/グループの関連づけを行います。

ユーザータブには NIS ユーザーがリスト表示されます。もし、同ユーザーが ActiveDirectory に存在する場合には自動的に関連づけられて Windows アカウントが表示されます(上記図の root の例を参照)。

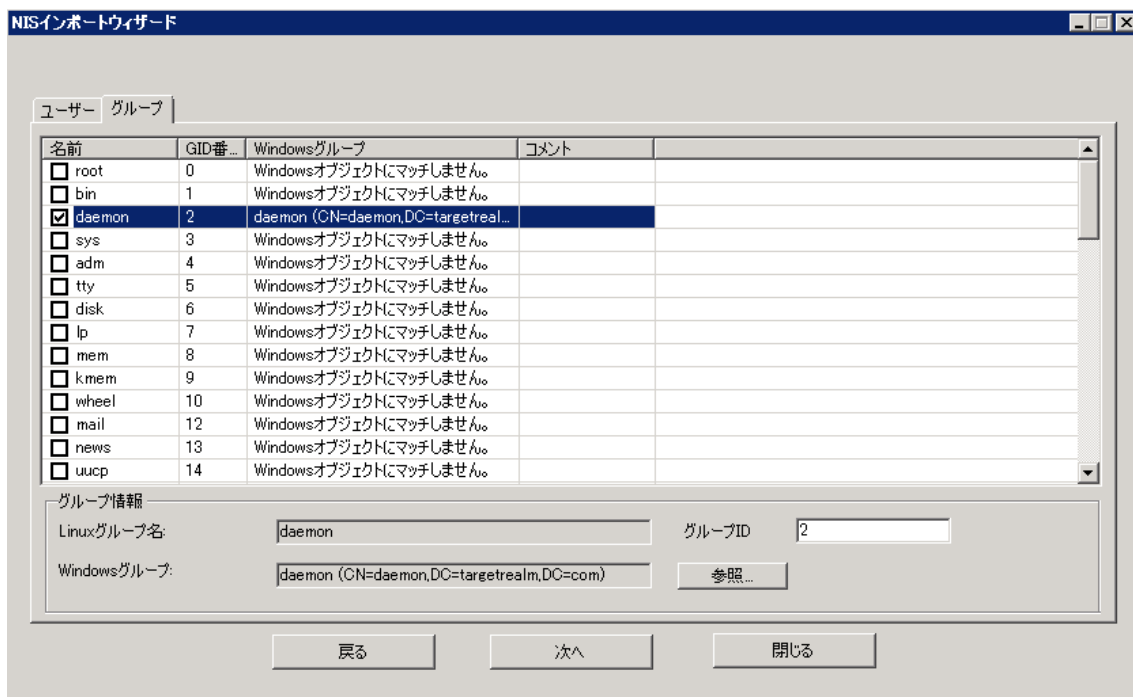
また、自動で関連づけられないユーザーは、[参照]ボタンをクリックして Windows アカウントを選択して手動で指定します。

同名の NIS ユーザーが Active Directory に存在しない場合は "Windows オブジェクトにマッチしません。" とリストに表示されます。ユーザーを選択し、"Windows アカウント" 欄の [参照] ボタンをクリックします。Windows オブジェクトの検索画面が表示されたら検索し、結果一覧から関連づける Windows アカウントを選択、[確定] ボタンをクリックしてください。"UID 番号"、"注記"、"ホームディレクトリ"、"ログインシェル" のデフォルト値を指定します。これらのオプションはユーザーが必要に応じて変更することも可能です。



Windows アカウントと関連づけられていないユーザーはインポートされませんので注意してください。

グループタブは以下の通りです。

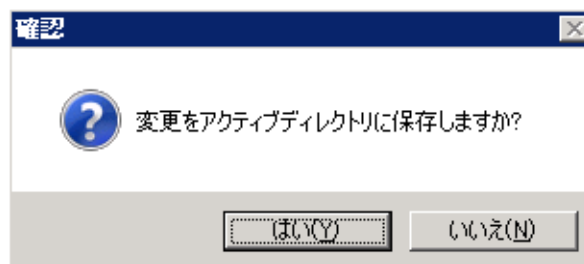


ユーザーと同様に NIS グループと同名の Windows グループが存在する場合は、自動で関連づけられます。存在しないときには、“Windows グループ” 欄に “Windows オブジェクトにマッチしません。”と表示されます。グループを選択し、“Windows グループ” 欄の[参照]ボタンをクリックします。Windows オブジェクトの検索画面が表示されたら検索し、結果一覧から関連づける Windows グループを選択、[確定]ボタンをクリックしてください。



Windows アカウントと関連づけられていないグループはインポートされませんので注意してください。

指定が完了したら[次へ]ボタンをクリックします。次のように確認のダイアログが表示されたら[はい]ボタンをクリックしてください。



マイグレーションが実行され結果が表示されます。確認後[閉じる]ボタンをクリックしてください。

NISユーザーのインポート結果:

NISユーザー	UID番号	GID番号	Windowsユーザー	ホームディレクトリ	ログインシェル
root	0	10247680	root (CN=root,CN=Users,DC=targetrealm,DC=...)	/root	/bin/bash

NISグループのインポート結果:

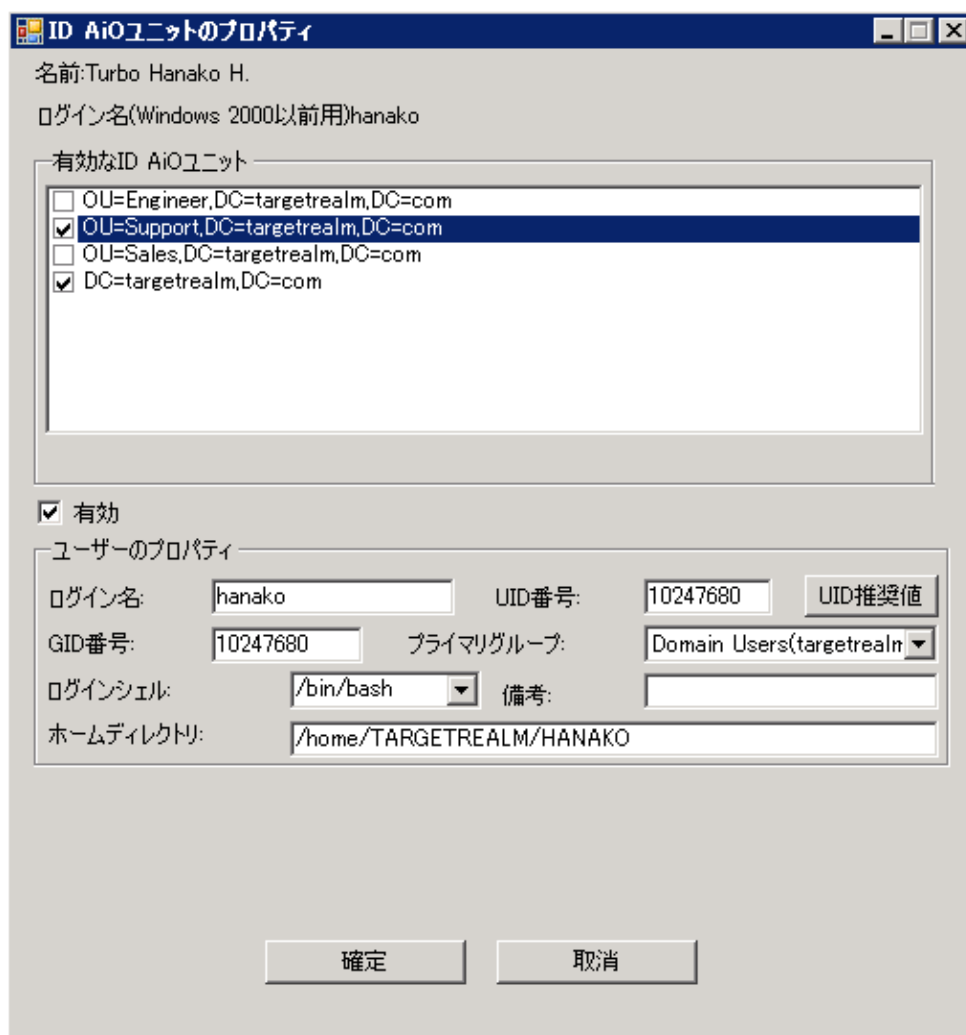
NISグループ	GID番号	Windowsグループ
daemon	2	daemon (CN=daemon,DC=targetrealm,DC=co...)

戻る 次へ 閉じる

2.19 ID Aio ユーザーの設定変更

ID Aio ユーザーの設定を変更するには、「ID Aio マネージャ」タブで設定を変更したいユーザー名の上で右クリックしメニューから「プロパティ」を選択します。

次の画面が表示されます。

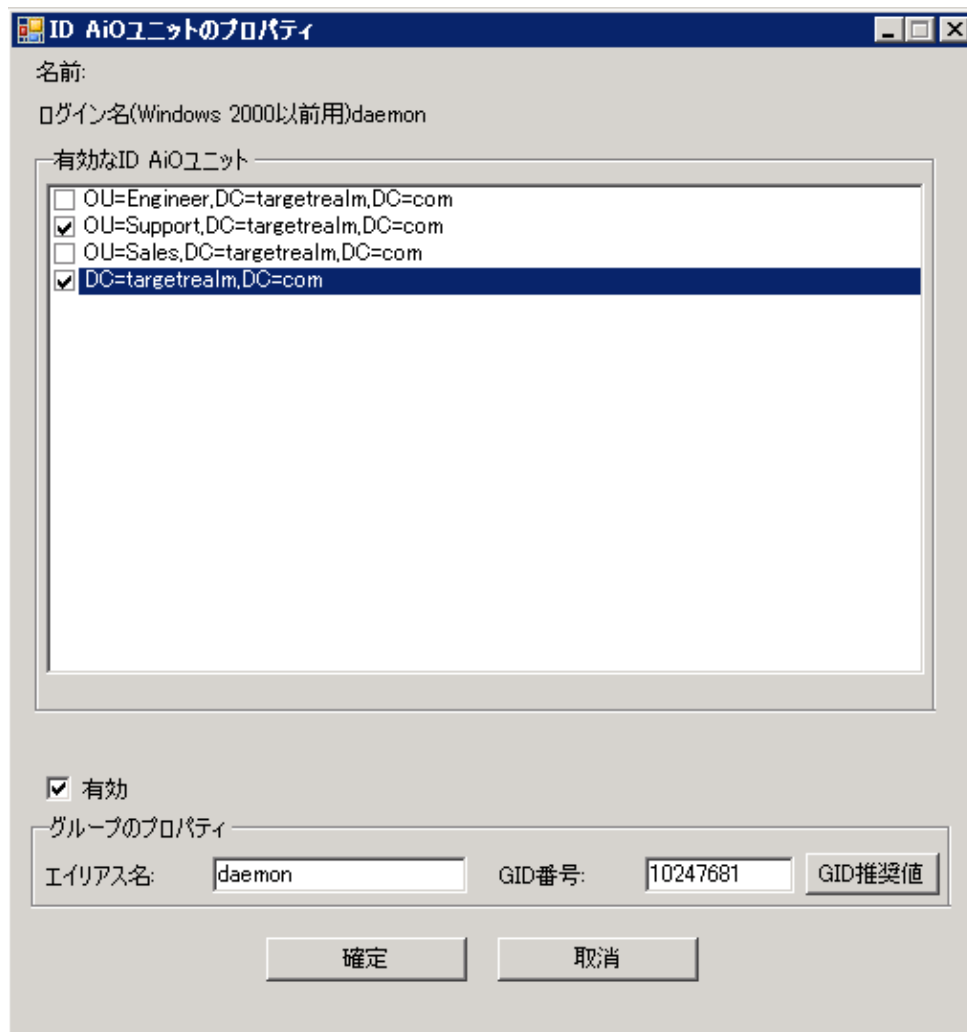


画面上部の“有効な ID Aio ユニット”を選択すると画面下部に関連づけられている Windows アカウントの情報が表示され修正が可能になります。“ログイン名” “UID 番号” “プライマリグループ” “ログインシェル” “備考” “ホームディレクトリ”を必要に応じて編集し[確定]ボタンをクリックしてください。

2.20 ID Aio グループの設定変更

ID Aio グループの設定を変更するには、「ID Aio マネージャ」タブで設定を変更したいグループ名の上で右クリックしメニューから「プロパティ」を選択します。

次の画面が表示されます。



画面上部の“有効な ID Aio ユニット”を選択すると画面下部に関連づけられている Windows グループの情報が表示され修正が可能になります。“エイリアス名”“GID 番号”を必要に応じて編集し[確定]ボタンをクリックしてください。

2.21 グループポリシーモジュール

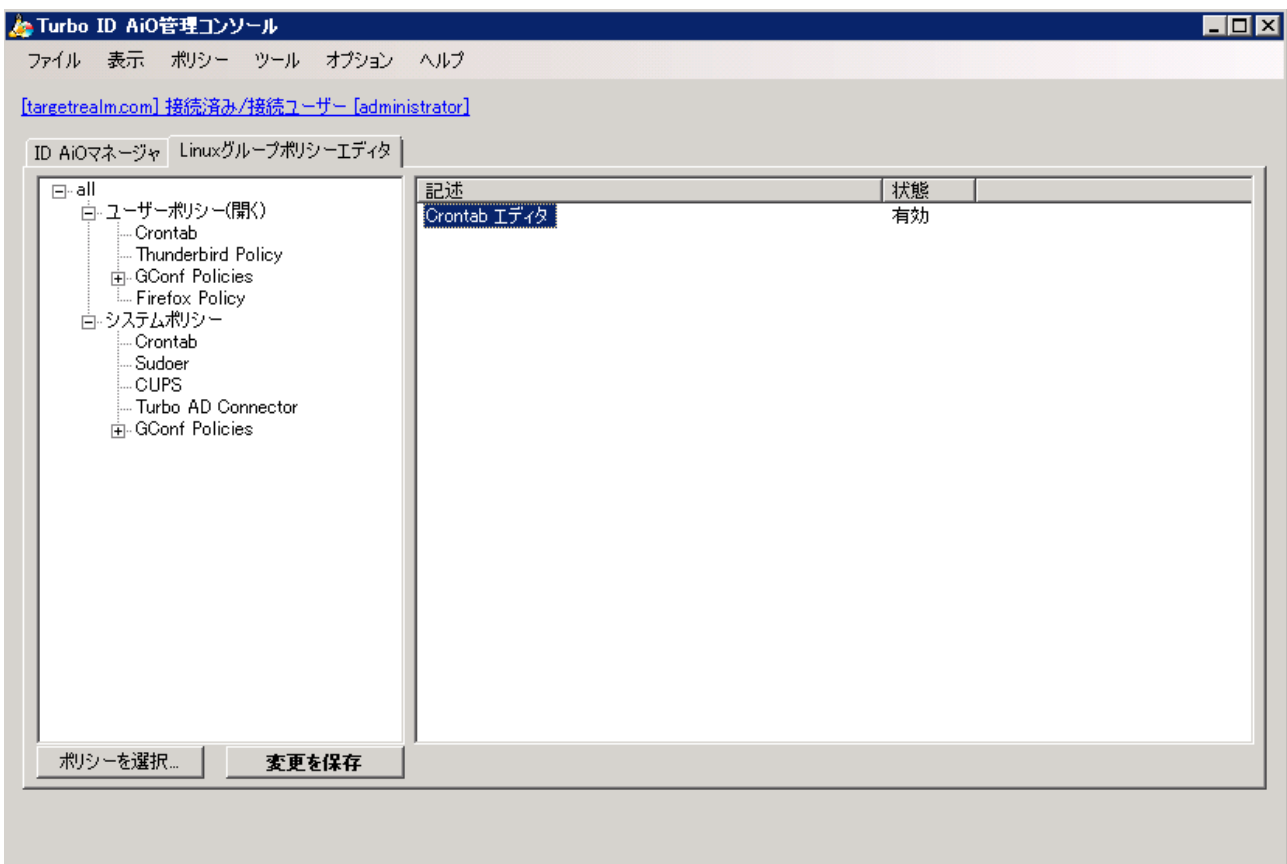
現在、システムの提供するデフォルトのグループポリシーモジュールは、“Linux Crontab”、“Cups Policy”、“Firefox Policy”、“Gconf Policies”、“Sudoer”、“Thunderbird Policy”、“Turbo AD Connector”です。これらの設定項目について解説します。

2.21.1 Linux Crontab

ジョブのスケジューリングと実行のためのグループポリシーモジュールです。ユーザーレベル、システムレベルの crontab 機能を提供します。

「Linux グループポリシーエディタ」タブでポリシーを開きます（「[2.12.グループポリシーの確認と編集](#)」参照）。

ユーザーポリシーまたはシステムポリシーの “Crontab” をクリックし選択すると次のように画面右側のウィンドウに “Crontab エディタ” が表示されます。



右側のウィンドウの “Crontab エディタ” をダブルクリックすると次の設定画面が表示されます。



ポリシーアイテムの設定がすべて完了したら必ず[変更を保存]ボタンをクリックし設定内容を保存してください。

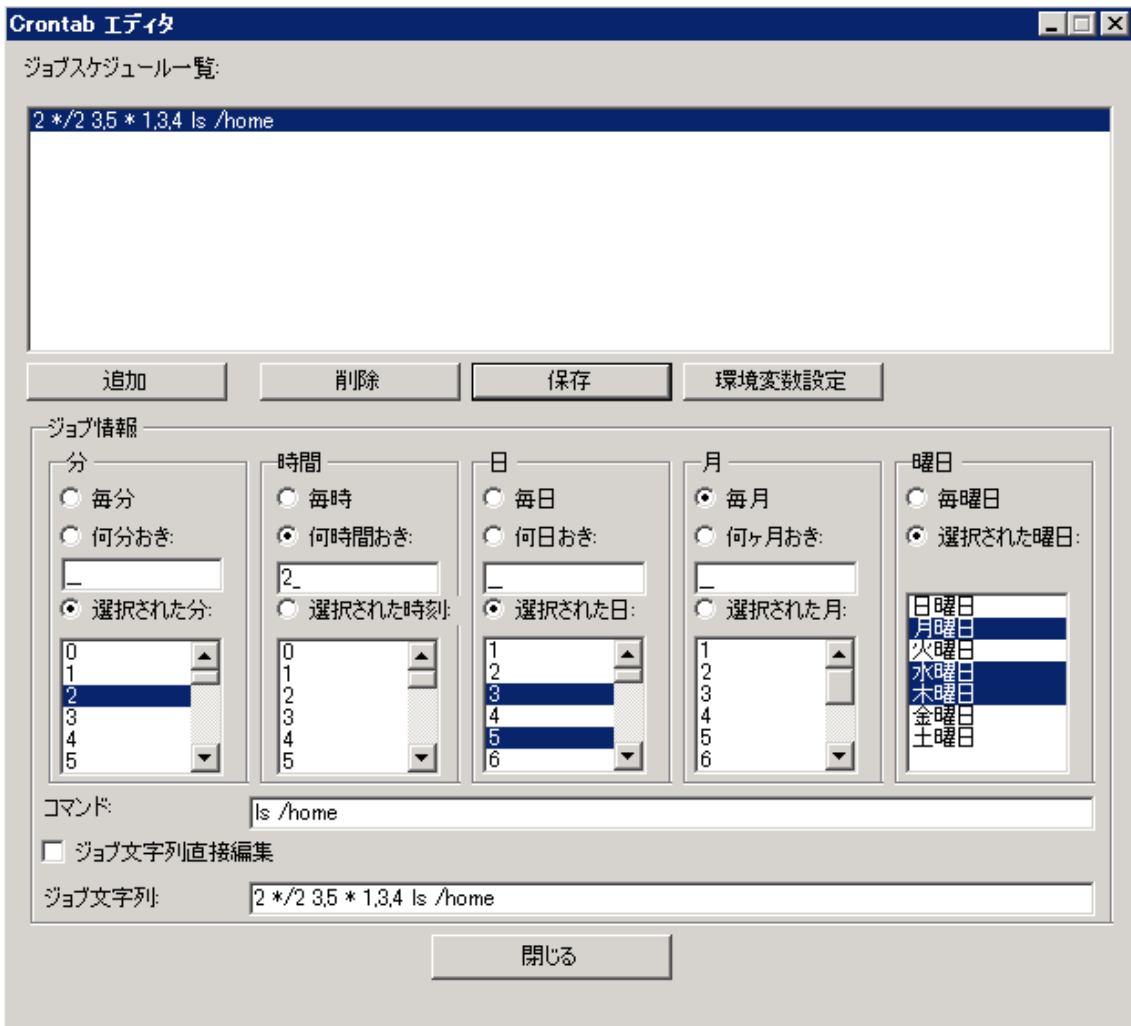


ジョブスケジュールを追加するには[追加]ボタンをクリックします。次のように表示されます。



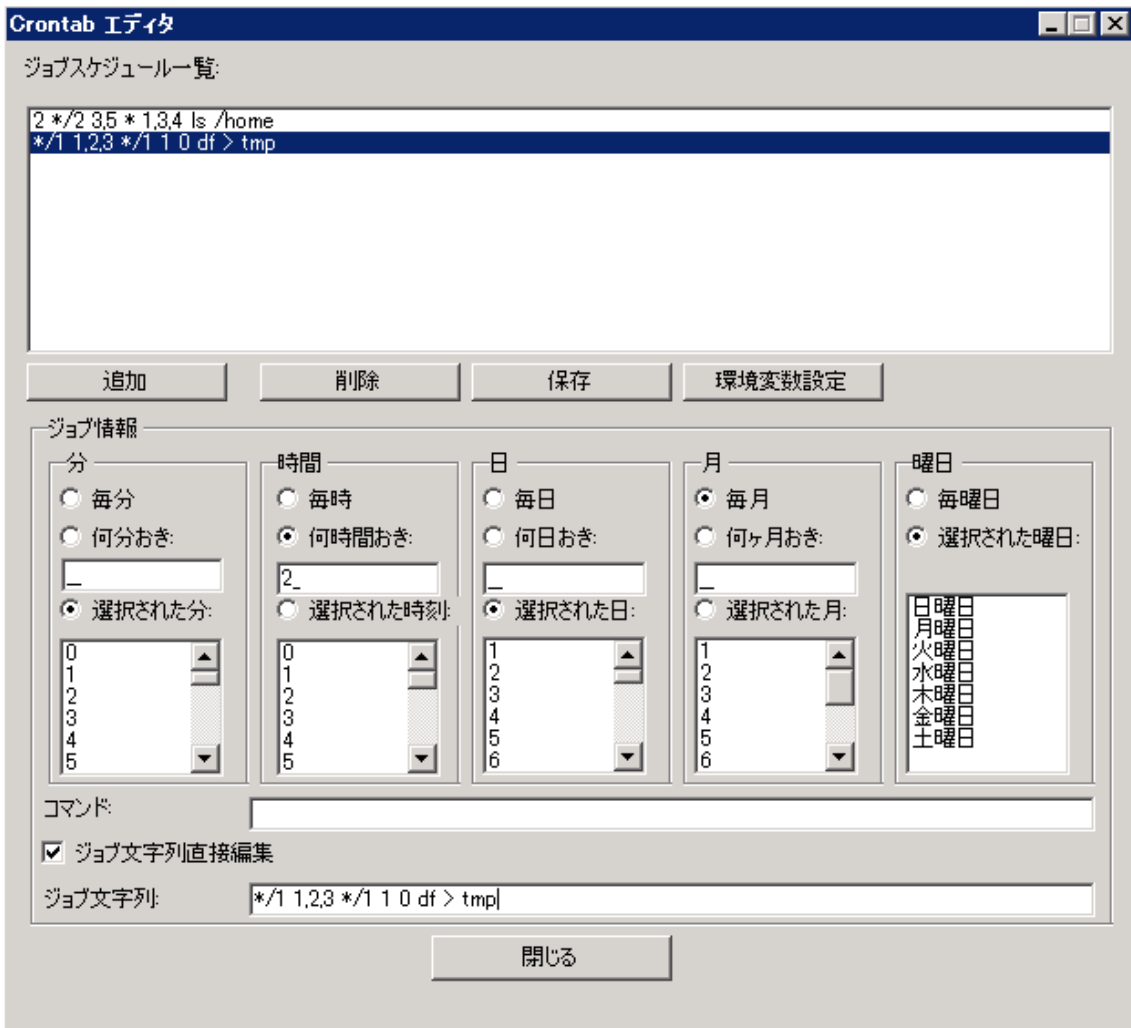
“ジョブスケジューラ一覧”に“***** ジョブ文字の編集”と表示されますので、選択した状態でまずはジョブを実行する時間を指定します。“分”“時間”“日”“月”“曜日”欄を指定します。“XX おき”を選択した場合は、テキストボックス内に間隔を数値で指定します。“選択されたXX”を選択した場合はすぐ下のリストから値を選択してください。コマンド欄には実行するコマンドを入力します。

[保存]ボタンをクリックすると変更は保存され“ジョブ文字列”欄に反映されます。“ジョブ文字列直接編集”を選択すると“ジョブ文字列”欄を直接編集できるようになります。書式は crontab ファイルと同様です。

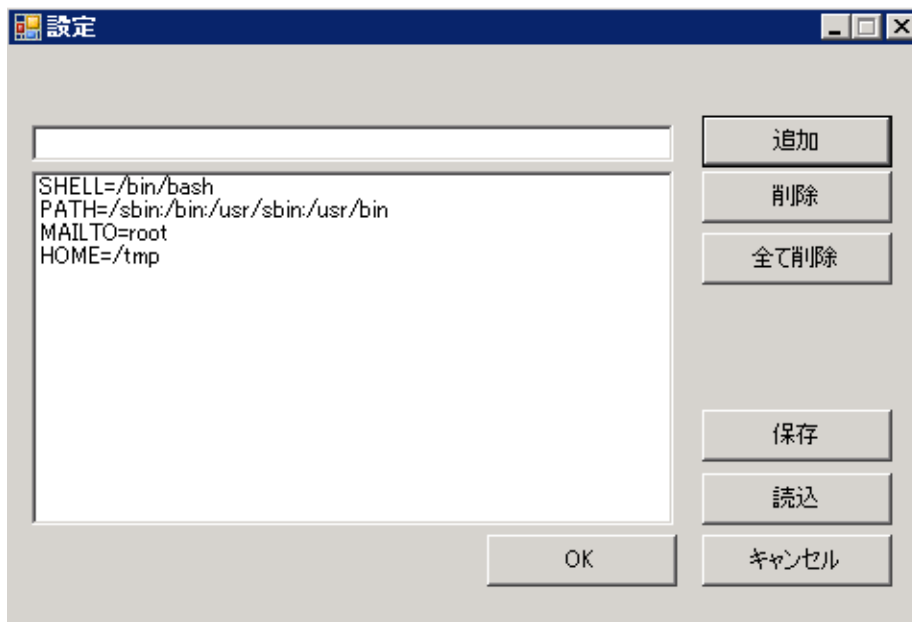


上記の例は、毎月3日、5日および月、水、木曜日の二時間おきの毎2分に ls /home コマンドを実行する指定です。

同様に[追加]ボタンをクリックして他のジョブを追加することも可能です。以下は“ジョブ文字列直接編集”を選択し“ジョブ文字列”欄を直接編集した場合の例です。編集後[保存]ボタンをクリックします。



crontab の環境変数を設定するには [環境変数設定] ボタンをクリックし次の画面を表示します。



上部テキストボックスに環境変数を入力し[追加]ボタンをクリックするとリストに反映されます。リストから選択し[削除]ボタンで削除され、[全て削除]ボタンをクリックして全ての定義を削除することも可能です。定義した内容を[保存]ボタンでファイルに保存しておき、[読込]ボタンでこの定義ファイルを読み込むことができ

ます。

指定が完了したら[OK]ボタンをクリックして有効にします。

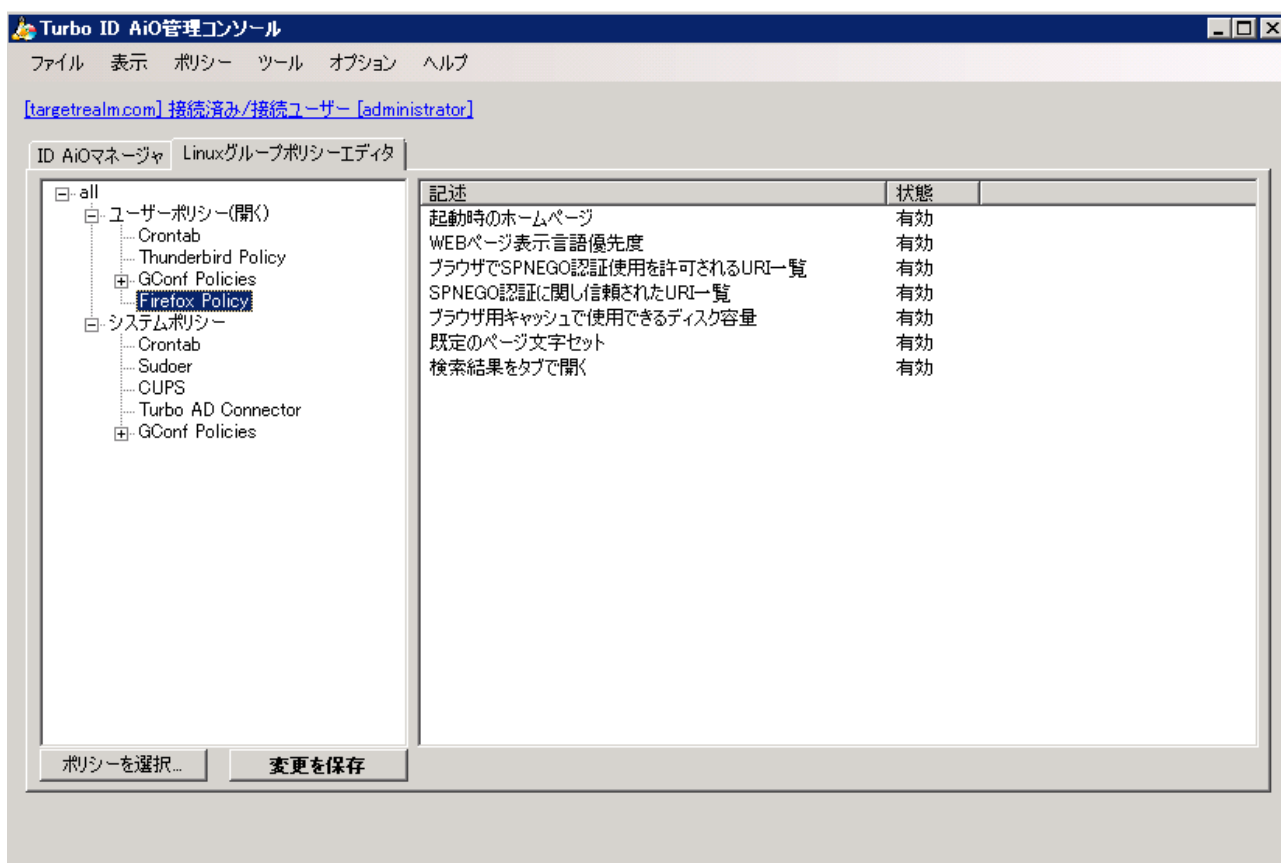
Crontab の設定が完了したら「Crontab エディタ」画面の[閉じる]ボタンをクリックします。

2.21.2 Firefox Policy

Linux システムの Firefox 用ポリシーモジュールです。ユーザーレベルの機能を提供します。

「Linux グループポリシーエディタ」タブでポリシーを開きます(「[2.12.グループポリシーの確認と編集](#)」参照)。

ユーザーポリシーの “Firefox” をクリックし選択すると次のように画面右側のウィンドウに項目が表示されます。



記述	状態
起動時のホームページ	有効
WEBページ表示言語優先度	有効
ブラウザでSPNEGO認証使用を許可されるURI一覧	有効
SPNEGO認証に関し信頼されたURI一覧	有効
ブラウザ用キャッシュで使用できるディスク容量	有効
既定のページ文字セット	有効
検索結果をタブで開く	有効

右側のウィンドウの各項目をダブルクリックすると次のように設定画面が表示されます。



ポリシーアイテムの設定がすべて完了したら必ず[変更を保存]ボタンをクリックし設定内容を保存してください。

次は起動時のホームページの場合です。

ポリシーアイテムの編集

名前: browser.startup.homepage

起動時のホームページ

状態

有効
 無効
 未指定

www.turbolinux.co.jp

デフォルト値: www.turbolinux.co.jp

起動時のホームページの設定

確定 取消

Linux システムからユーザーがログインした際に適用される Firefox (Web ブラウザ) 起動時のホームページ指定です。

Firefox Policy のポリシーアイテム設定画面は以下の構成になっています。

名前

ポリシーアイテム名が表示されます。

状態

この機能を使用するかどうかを指定します。“有効”を選択するとこの機能を使用し中央に指定されているテキストボックスの値を適用します。“無効”はこの機能を使用しません。“未指定”は、この機能を使用しますがデフォルト値を適用します。

ユーザー指定欄(中央のテキストボックス)

ユーザーの指定欄です。

デフォルト値

ユーザー指定欄を省略した場合のデフォルト値です。

概要(画面下部の枠内)

この機能の概要の説明が表示されています。

設定を変更したら[確定]ボタンをクリックして反映します。

2.21.2.1 各項目について

起動時のホームページ

指定した URL を Firefox 起動時のホームページに指定します。デフォルト値は `www.turbolinux.co.jp` です。

Web ページの表示言語優先度

Web ページを表示する際の言語の優先順位を指定します。デフォルト値は、`ja, zh-cn, en-us, en;` です。

ブラウザで SPNEGO を許可される URI 一覧

SPNEGO (Secure Protocol Negotiation) 認証ネゴシエーションを許可する URI を指定します。デフォルト値は、`http://,https://;` です。



Firefox でシングルサインオン機能を使用する場合に、正確な URL を指定した上で有効にしてください。

SPNEGO 認証において信頼された URI 一覧

SPNEGO (Secure Protocol Negotiation) 認証において信頼されるサイトの URI を指定します。デフォルト値は、`http://,https://;` です。



Firefox でシングルサインオン機能を使用する場合に、正確な URL を指定した上で有効にしてください。

ブラウザ用キャッシュで利用できるディスク容量

ページキャッシュの容量(キロバイト単位)を指定します。デフォルト値は 30000 キロバイトです。

規定のページ文字セット

Web ページを表示する際の文字エンコードのデフォルトの指定です。デフォルト値は、UTF-8 です。

検索結果をタブで開く

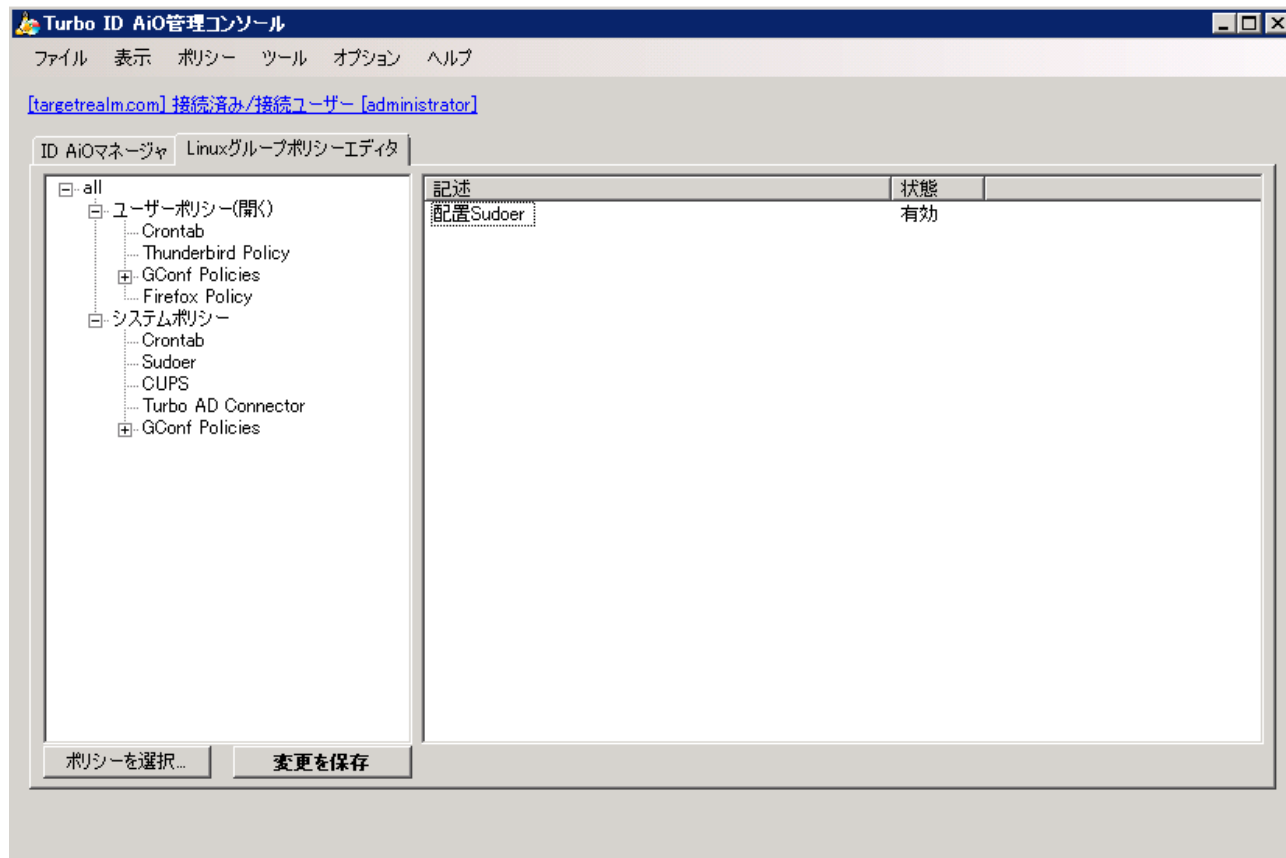
検索結果のページをタブ表示するかどうかの指定です。デフォルト値は、`true`(タブ表示) です。

2.21.3 Sudoer Policy

sudoer のためのグループポリシーモジュールです。システムレベルの機能を提供します。

「Linux グループポリシーエディタ」タブでポリシーを開きます(「[2.12.グループポリシーの確認と編集](#)」参照)。

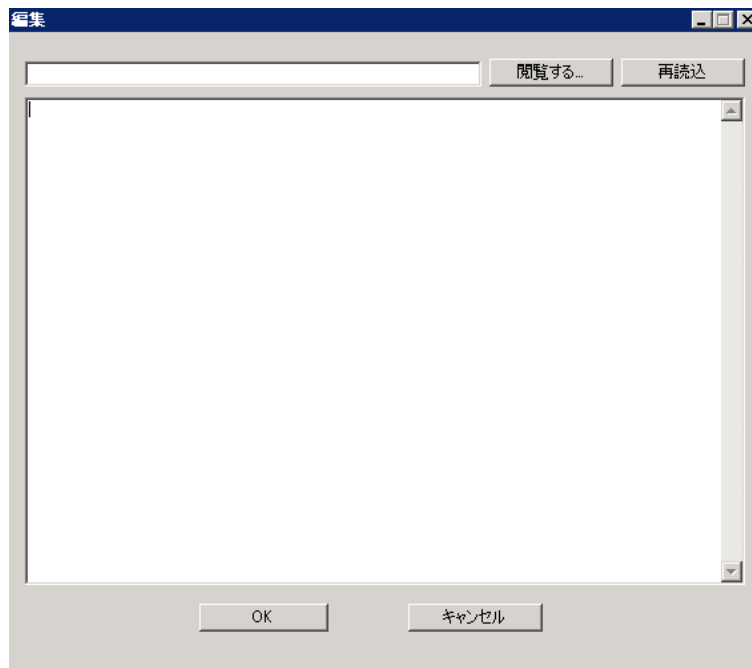
システムポリシーの “Sudoer” をクリックし選択すると次のように画面右側のウィンドウに項目が表示されます。



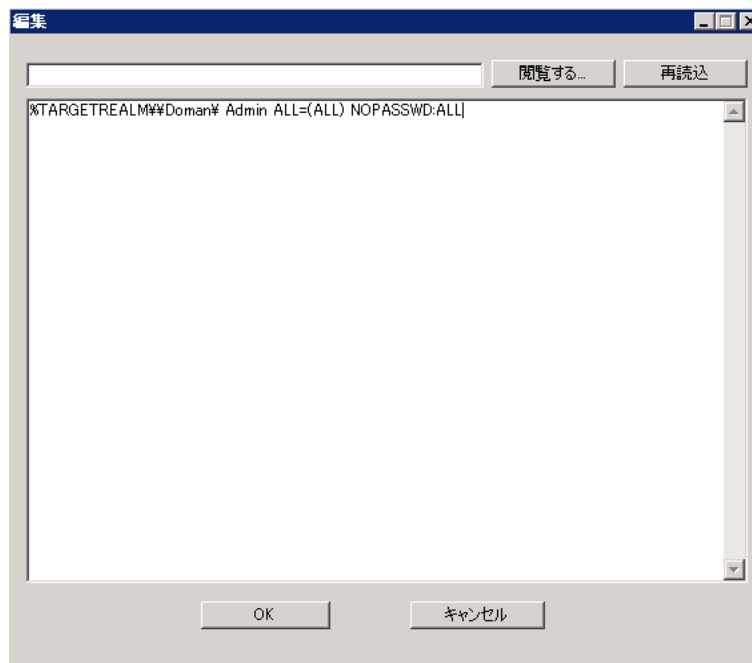
右側のウィンドウの “配置 Sudoer” をダブルクリックすると次のように設定画面が表示されます。



ポリシーアイテムの設定がすべて完了したら必ず[変更を保存]ボタンをクリックし設定内容を保存してください。



[閲覧する]ボタンをクリックして既存の sudoer ファイルのパスを指定することもできます。中央の枠内には開いたファイルの内容が展開され編集も可能です。[再読込]ボタンをクリックするとファイルから再読み込みします。



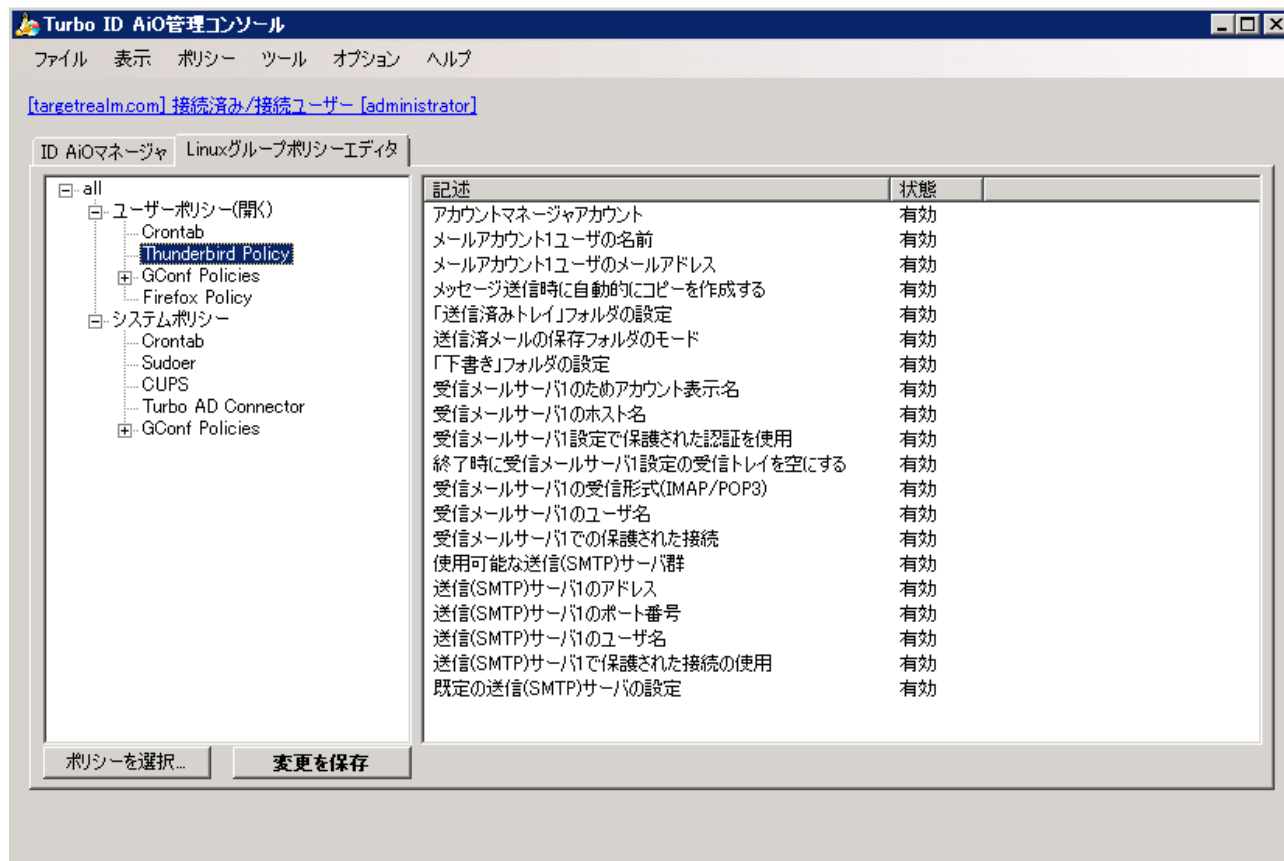
中央のテキスト枠内をクリックして上記例のように直接入力することも可能です。指定が完了したら[OK]ボタンをクリックします。もしも設定にエラーがあると Sudoer グループポリシーは実行されません。

2.21.4 Thunderbird Policy

Linux システムの Thunderbird 用ポリシーモジュールです。ユーザーレベルの機能を提供します。

「Linux グループポリシーエディタ」タブでポリシーを開きます(「[2.12.グループポリシーの確認と編集](#)」参照)。

ユーザーポリシーの “Thunderbird Policy” をクリックし選択すると次のように画面右側のウィンドウに項目が表示されます。



The screenshot shows the Turbo ID AiO Management Console interface. The main window is titled "Linuxグループポリシーエディタ" (Linux Group Policy Editor). On the left, a tree view shows the "Thunderbird Policy" selected under "ユーザーポリシー(開く)" (User Policies). The main area displays a list of policy items with their descriptions and status.

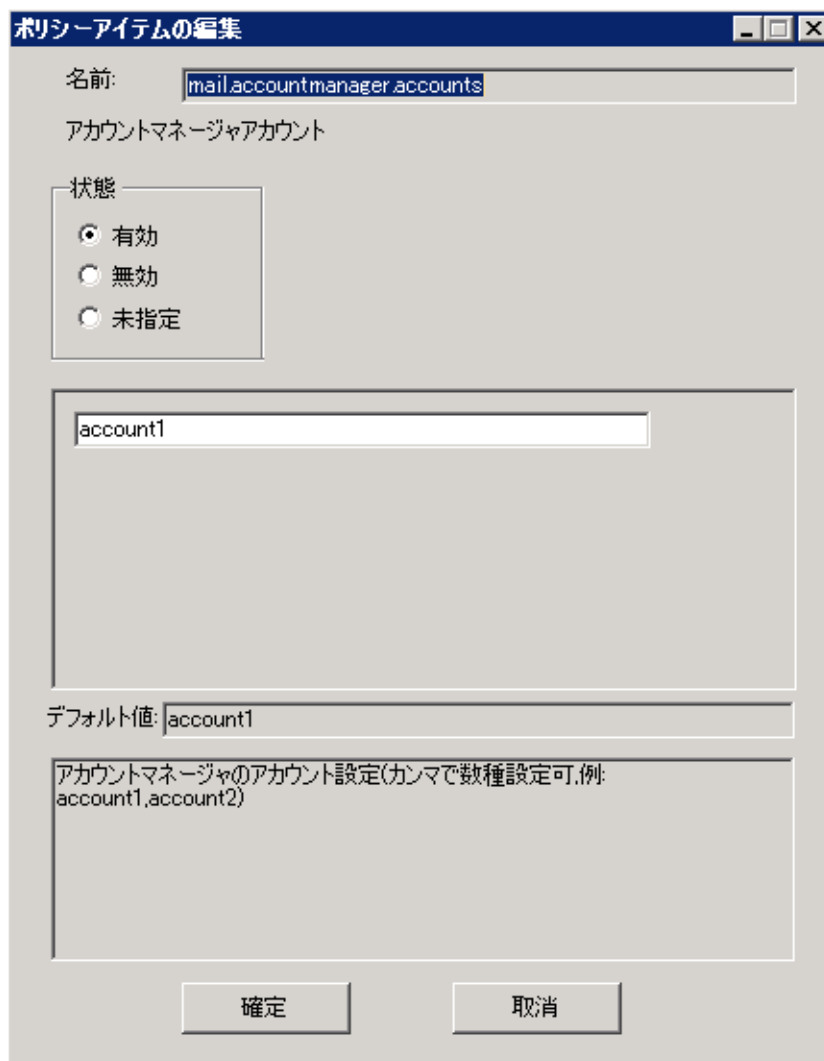
記述	状態
アカウントマネージャアカウント	有効
メールアカウント1ユーザの名前	有効
メールアカウント1ユーザのメールアドレス	有効
メッセージ送信時に自動的にコピーを作成する	有効
「送信済みトレイ」フォルダの設定	有効
送信済みメールの保存フォルダのモード	有効
「下書き」フォルダの設定	有効
受信メールサーバのためアカウント表示名	有効
受信メールサーバのホスト名	有効
受信メールサーバ設定で保護された認証を使用	有効
終了時に受信メールサーバ設定の受信トレイを空にする	有効
受信メールサーバの受信形式(IMAP/POP3)	有効
受信メールサーバのユーザ名	有効
受信メールサーバでの保護された接続	有効
使用可能な送信(SMTP)サーバ群	有効
送信(SMTP)サーバのアドレス	有効
送信(SMTP)サーバのポート番号	有効
送信(SMTP)サーバのユーザ名	有効
送信(SMTP)サーバで保護された接続の使用	有効
既定の送信(SMTP)サーバの設定	有効

At the bottom of the window, there are two buttons: "ポリシーを選択..." (Select Policy...) and "変更を保存" (Save Changes).

右側のウィンドウの各項目をダブルクリックすると次のように設定画面が表示されます。次は「アカウントマネージャアカウント」の設定画面です。



ポリシーアイテムの設定がすべて完了したら必ず[変更を保存]ボタンをクリックし設定内容を保存してください。



Linux システムからユーザーがログインした際に適用される Thunderbird のアカウント設定です。Thunderbird Policy のアイテム設定画面は Firefox Policy と同様に以下の構成になっています。

名前

ポリシーアイテム名が表示されます。

状態

この機能を使用するかどうかを指定します。“有効”を選択するとこの機能を使用し中央に指定されているテキストボックスの値を適用します。“無効”はこの機能を使用しません。“未指定”は、この機能を使用しますがデフォルト値を適用します。

ユーザー指定欄(中央のテキストボックス)

ユーザーの指定欄です。

デフォルト値

ユーザー指定欄を省略した場合のデフォルト値です。

概要(画面下部の枠内)

この機能の概要の説明が表示されています。

設定を変更したら[確定]ボタンをクリックして反映します。

2.21.4.1 各項目について

アカウントマネージャアカウント

Thunderbird のアカウントマネージャで設定するメールアカウントの指定です。以降の各項目でメールアカウント 1 (account1) に関する指定を行いますのでデフォルト値のまま account1 としてください。



複数のアカウントをご利用になるには、"," (カンマ) で区切り account1,account2 のように指定します。ただし、account2 以降のアカウントを定義するには XML ファイル (Turbo ID AiO¥policies¥Thunderbird Policies.xml) の編集が必要になります。関連情報はターボリナックス株式会社の Web サイトをご確認ください。また、同ファイルの編集は、サポートサービスの対象となりません。お客様の責任においてご注意の上行ってください。

メールアカウント 1 ユーザーの名前

メールアカウント 1 (account1) のフルネームの指定です。以下のマクロの使用が可能です。

マクロ	説明
%mail%	ユーザーの E-MAIL アドレス
%samacct%	ユーザーのログイン名 (Windows2000 以前)
%mailnickname%	ユーザーのニックネーム
%displayname%	ユーザーの表示名
%name%	ユーザー名

デフォルト値は%displayname% です。

メールアカウント 1 ユーザーのメールアドレス

メールアカウント 1 (account1) のメールアドレスの指定です。以下のマクロの使用が可能です。

マクロ	説明
%mail%	ユーザーの E-MAIL アドレス
%samacct%	ユーザーのログイン名 (Windows2000 以前)
%mailnickname%	ユーザーのニックネーム
%displayname%	ユーザーの表示名
%name%	ユーザー名

デフォルト値は%mail% です。

メッセージ送信時に自動的にコピーを作成する

メールアカウント 1 (account1) がメール送信時に自動的にコピーを作成するかどうかを指定します。デフォルト値は、true (コピーする) です。

「送信済みトレイ」フォルダの設定

メールアカウント 1 (account1) の「送信済みトレイ」の指定です。デフォルト値は、:imap://%mail%/Sent です。

送信済メールの保存フォルダのモード

メールアカウント 1 (account1) で “「送信済みトレイ」フォルダの設定” で設定をしたフォルダを使用するかどうかの指定です。1 を指定すると使用するです。デフォルト値は、0 (使用しない) です。1 で無いときにはシ

システムのデフォルト指定になります。

「下書き」フォルダの設定

メールアカウント1(account1)の「下書き」フォルダの指定です。デフォルト値は、imap://%mail%/Drafts です。

受信メールサーバー1のためのアカウント表示名

メールアカウント1(account1)のアカウント名です。デフォルト値は、%displayname%'s emails です。

受信メールサーバー1のホスト名

メールアカウント1(account1)の受信メールサーバー1のホスト名指定です。デフォルト値は mail.example.org です。

受信メールサーバー1設定で保護された認証を使用

メールアカウント1(account1)の受信メールサーバー1で保護された認証(APOP、NTLM、CRAM-MD5、ケルベロス)を使用するかどうかの指定です。デフォルト値は、true(コピーする)です。

終了時に受信メールサーバー1設定の受信トレイを空にする

メールアカウント1(account1)の受信メールサーバー1で終了時に受信トレイを空にするかどうかの指定です。デフォルト値は、true(空にする)です。IMAPを使用している場合に効果的です。

受信メールサーバー1の受信形式(IMAP/POP3)

メールアカウント1(account1)の受信メールサーバー1の受信形式を pop3 または imap で指定します。デフォルト値は imap です。

受信メールサーバー1のユーザー名

メールアカウント1(account1)の受信メールサーバー1のユーザー名指定です。以下のマクロの使用が可能です。

マクロ	説明
%mail%	ユーザーのE-MAILアドレス
%samacct%	ユーザーのログイン名(Windows2000以前)
%mailnickname%	ユーザーのニックネーム
%displayname%	ユーザーの表示名
%name%	ユーザー名

デフォルト値は%samacct%です。

受信メールサーバー1での保護された接続

メールアカウント1(account1)の受信メールサーバー1で保護された接続を使用するかどうかの指定です。0(使用しない)、1(可能ならTLSを使用する)、2(TLSを使用する)、3(SSLを使用する)から指定します。デフォルト値は0(使用しない)です。

使用可能な送信(SMTP)サーバー群

Thunderbirdで使用するSMTPサーバーの指定です。以降の各項目でSMTPサーバー1(smtp1)に関する指定を行いますので、1つのSMTPサーバーを指定する場合は**デフォルト値のまま smtp1 としてください。**



複数の SMTP サーバーをご利用になるには、","(カンマ)で区切り smtp1,smtp2 のように指定します。ただし、smtp2 以降の SMTP サーバーを定義するには XML ファイル(Turbo ID AIO¥policies¥Thunderbird Policies.xml)の編集が必要になります。関連情報はターボリナックス株式会社の Web サイトをご確認ください。また、同ファイルの編集は、サポートサービスの対象となりません。お客様の責任においてご注意の上行ってください。

送信 (SMTP) サーバー 1 のアドレス

SMTP サーバー 1 (smtp1) のアドレス指定です。デフォルト値は smtp.example.org です。

送信 (SMTP) サーバー 1 のポート番号

SMTP サーバー 1 (smtp1) のポート番号の指定です。デフォルト値は 25 です。

送信 (SMTP) サーバー 1 のユーザー名

SMTP サーバー 1 (smtp1) のユーザーログイン名の指定です。下のマクロの使用が可能です。

マクロ	説明
%mail%	ユーザーの E-MAIL アドレス
%samacct%	ユーザーのログイン名 (Windows2000 以前)
%mailnickname%	ユーザーのニックネーム
%displayname%	ユーザーの表示名
%name%	ユーザー名

デフォルト値は %mail% です。

送信 (SMTP) サーバー 1 で保護された接続の使用

SMTP サーバー 1 (smtp1) で保護された接続を使用するかどうかの指定です。0 (使用しない)、1 (可能なら TLS を使用する)、2 (TLS を使用する)、3 (SSL を使用する) から指定します。デフォルト値は 0 (使用しない) です。

規定の送信 (SMTP) サーバーの設定

規定の送信 (SMTP) サーバーの指定です。1 つのみを指定している場合は、デフォルト値の smtp1 のままとしてください。smtp1 は、送信 (SMTP) サーバー 1 で定義した SMTP サーバーです。

2.21.5 CUPS Policy

CUPS Policy は Linux システム上に CUPS のプリンタ設定を行うグループポリシーモジュールです。システムレベルの設定機能を提供します。ターゲットサーバー上では、CUPS パッケージをインストールし、サービスを起動しておいてください。

「Linux グループポリシーエディタ」タブでポリシーを開きます（「[2.12.グループポリシーの確認と編集](#)」参照）。

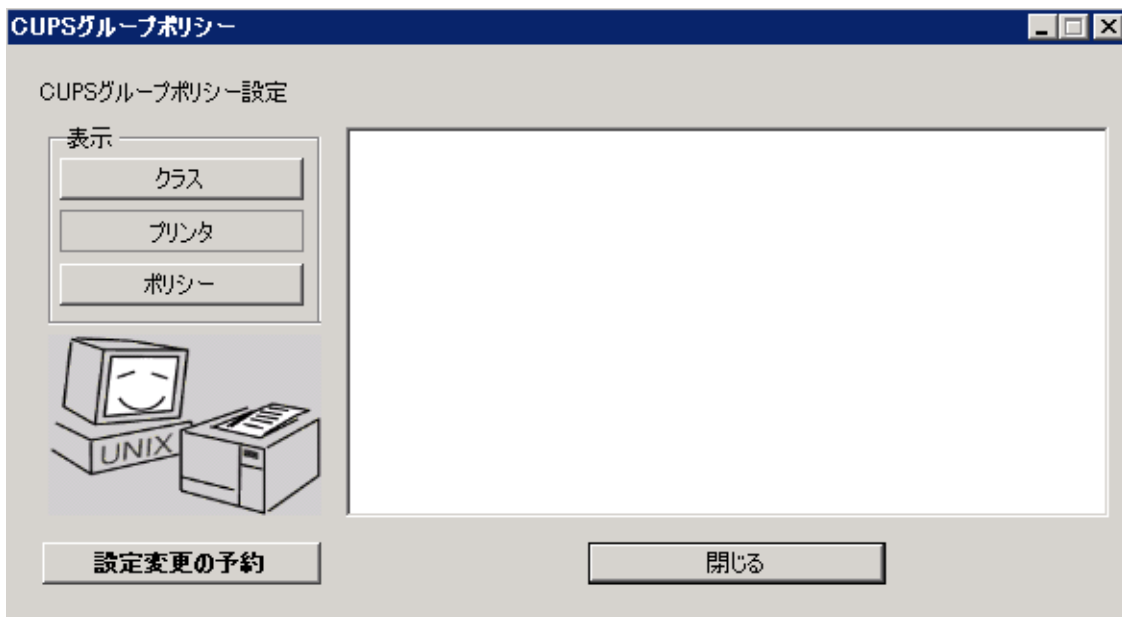
システムポリシーの “CUPS” をクリックし選択すると次のように画面右側のウィンドウに項目が表示されます。



右側のウィンドウの “CUPS” をダブルクリックすると次のように設定画面が表示されます。



ポリシーアイテムの設定がすべて完了したら必ず[変更を保存]ボタンをクリックし設定内容を保存してください。



上記の図のように“クラス” “プリンタ” “ポリシー”の3つのレベルがあります。

一般的にはまずプリンタを定義します。その後、クラスを定義します。デフォルトの状態でも CUPS のポリシーは通常の操作についてアクセス制御を満たしています。もちろん、管理者が CUPS の操作に関するアクセス制御の設定を変更することも可能です。CUPS のポリシーの追加、更新、削除を行った場合は、CUPS サービスの再起動が必要です。[設定変更の予約]ボタンで CUPS サービスの再起動やプリンタおよびクラスの追加、変更、削除を有効にする日時を設定することができます。

2.21.5.1 プリンタの設定

“表示”の[プリンタ]ボタンをクリックします。右側の枠内で右クリックをしてメニューから“新規”を選択します。



次のダイアログが表示されたらプリンタ名を入力し[OK]ボタンをクリックしてください。



プリンタ名は 127 バイト未満の ASCII 文字で指定します。スペースは指定できません。英数_(アンダースコア)などを推奨します。



右側の枠内に Printer1 アイコンが表示されたらダブルクリックをしてください。次の画面が表示されます。

設定項目は以下の通りです。完了後[OK]ボタンをクリックします。

プリンタ名

プリンタの名前です。

プリンタの URI

プリンタの URI です。ipp://hostname/ipp/port1 のように指定してください。

PPD ファイル名

PPD ファイルのパス指定です。/usr/share/ppd/Canon/Canon-BJC-2100-bjc600.ppd.gz のように指定します。例は、foomatic パッケージに含まれる PPD ファイルです。利用環境に合わせて適宜インストールしてください。

プリンタ情報

プリンタに関する簡単な説明です。

場所

場所に関する説明です。

ユーザーアクセス

ユーザーのアクセス制御の指定です。“すべてのユーザーを許可” “リスト内のユーザーを許可” “リスト以外のユーザーを許可” から選択します。“リスト内のユーザーを許可” または “リスト以外のユーザーを許可” を選択した場合は [ユーザーリスト編集] ボタンをクリックし「設定」ダイアログを表示し追加、削除、リストの保存や読込を行えます。リストの編集は「●[ユーザーリスト編集](#)」を参照してください。

ジョブ受け入れ中

選択をすると新規ジョブの受け入れが可能な状態になります。

共有

選択をするとこの CUPS プリンタを共有します。

オペレーションポリシー

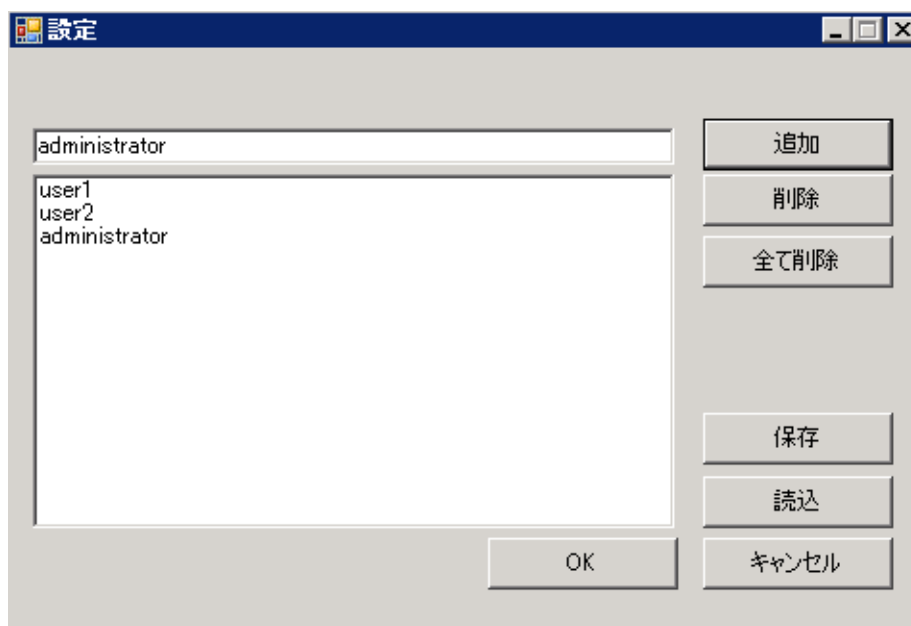
プルダウンリストからオペレーションポリシーを選択します。追加方法は「[6.21.5.3.ポリシーの設定](#)」で説明します。CUPS のデフォルトのオペレーションポリシーを使用する場合は default を選択します。

エラーポリシー

プルダウンリストからエラー発生時の動作について選択します。abort-job (ジョブを中断)、retry-job (ジョブをリトライ)、stop-printer (プリンタを停止) です。

●ユーザーリスト編集

“ユーザーアクセス” の [ユーザーリスト編集] ボタンをクリックすると以下のダイアログが表示されます。



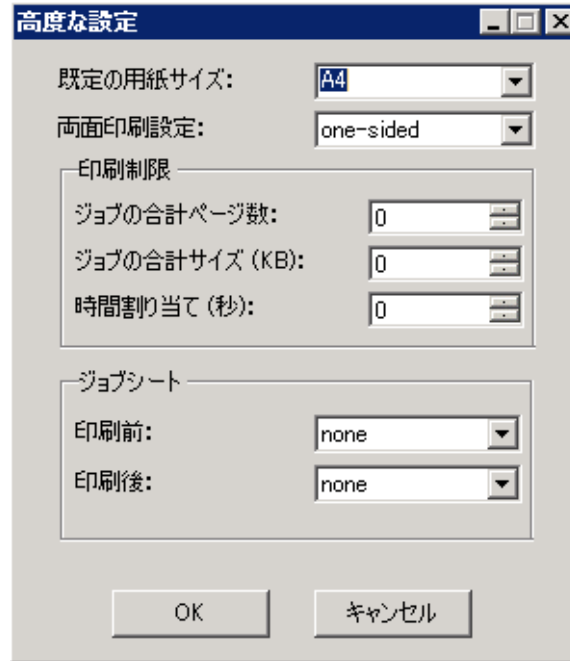
上部テキストボックスにユーザー名を入力し [追加] ボタンをクリックするとリストに反映されます。リストから選択し [削除] ボタンで削除され、[全て削除] ボタンをクリックして全ての定義を削除することも可能です。定

義した内容を[保存]ボタンでファイルに保存しておき、[読込]ボタンでこの定義ファイルを読み込むことができます。

指定が完了したら[OK]ボタンをクリックして有効にします。

● 高度な設定

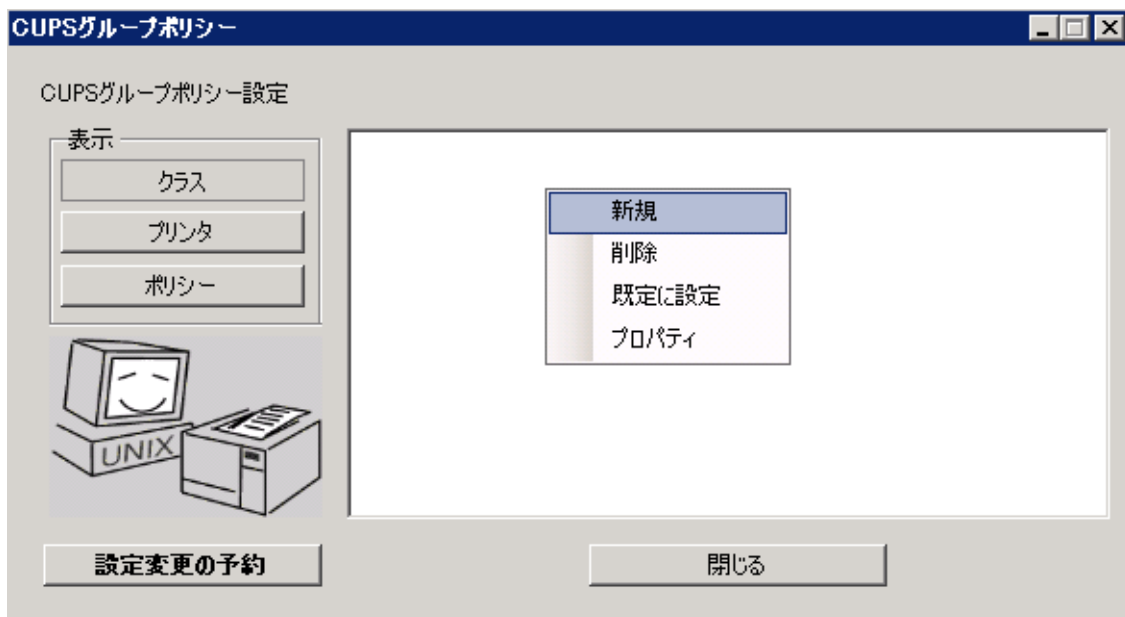
[高度な設定]ボタンをクリックすると以下のダイアログが表示され、プリンタの属性を定義することができます。



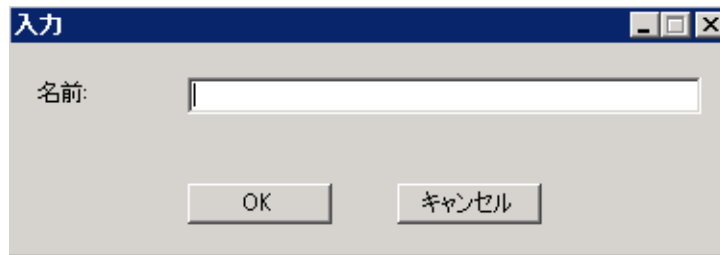
指定が完了したら[OK]ボタンをクリックして有効にします。

2.21.5.2 クラスの設定

クラスを設定する場合は、「CUPS グループポリシー設定」画面、「表示」の[クラス]ボタンをクリックします。右側の枠内で右クリックをしてメニューから「新規」を選択します。



次のダイアログが表示されたらクラス名を入力し[OK]ボタンをクリックしてください。



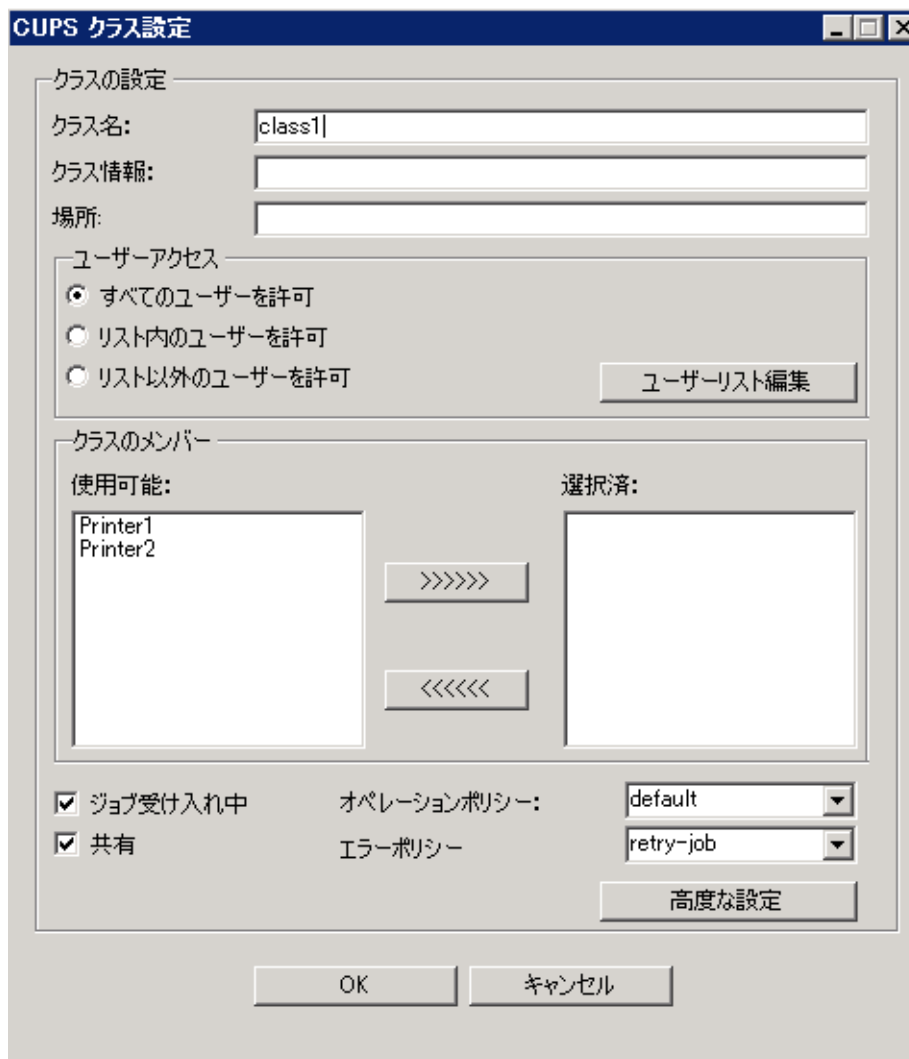
A dialog box titled "入力" (Input) with a text field labeled "名前:" (Name) and two buttons: "OK" and "キャンセル" (Cancel).



クラス名は 127 バイト未満の ASCII 文字で指定します。スペースは指定できません。英数 (アンダースコア) などを推奨します。



右側の枠内に **class1** アイコンが表示されたらダブルクリックをしてください。次の画面が表示されます。



A dialog box titled "CUPS クラス設定" (CUPS Class Setup) with the following sections and controls:

- クラスの設定** (Class Settings):
 - クラス名: class1
 - クラス情報:
 - 場所:
- ユーザーアクセス** (User Access):
 - すべてのユーザーを許可
 - リスト内のユーザーを許可
 - リスト以外のユーザーを許可
 - ユーザーリスト編集
- クラスのメンバー** (Class Members):
 - 使用可能: Printer1, Printer2
 - 選択済:
 - >>>>>
 - <<<<<
- ジョブ受け入れ中:
- 共有:
- オペレーションポリシー: default
- エラーポリシー: retry-job
- 高度な設定

Buttons: OK, キャンセル

設定項目は以下の通りです。完了後[OK]ボタンをクリックします。

クラス名

クラスの名前です。

クラス情報

クラスに関する簡単な説明です。


場所

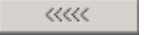
場所に関する説明です。

ユーザーアクセス

ユーザーのアクセス制御の指定です。“すべてのユーザーを許可” “リスト内のユーザーを許可” “リスト以外のユーザーを許可” から選択します。“リスト内のユーザーを許可” または “リスト以外のユーザーを許可” を選択した場合は[ユーザーリスト編集]ボタンをクリックし「設定」ダイアログを表示し追加、削除、リストの保存や読込を行えます。リストの編集は「[2.21.5.1.プリンタの設定](#)」の「[●ユーザーリスト編集](#)」を参照してください。

クラスのメンバー

クラスのメンバーであるプリンタが右側の“選択済み” 枠内にリストされます。左側の“使用可能” のリストから対象のプリンタをダブルクリックするか、選択し  をクリックするとリストに追加されます。

また、“選択済” 内のプリンタをダブルクリックするか、選択をして  ボタンをクリックするとリストから削除されて“使用可能” へ移動します。

選択をすると新規ジョブの受け入れが可能な状態になります。

ジョブ受け入れ中

選択をすると新規ジョブの受け入れが可能な状態になります。

共有

選択をするとこのクラスのプリンタを共有します。

オペレーションポリシー

プルダウンリストからオペレーションポリシーを選択します。追加方法は「[6.21.5.3.ポリシーの設定](#)」で説明します。CUPS のデフォルトのオペレーションポリシーを使用する場合は default を選択します。

エラーポリシー

プルダウンリストからエラー発生時の動作について選択します。abort-job (ジョブを中断)、retry-job (ジョブをリトライ)、stop-printer (プリンタを停止) です。

高度な設定

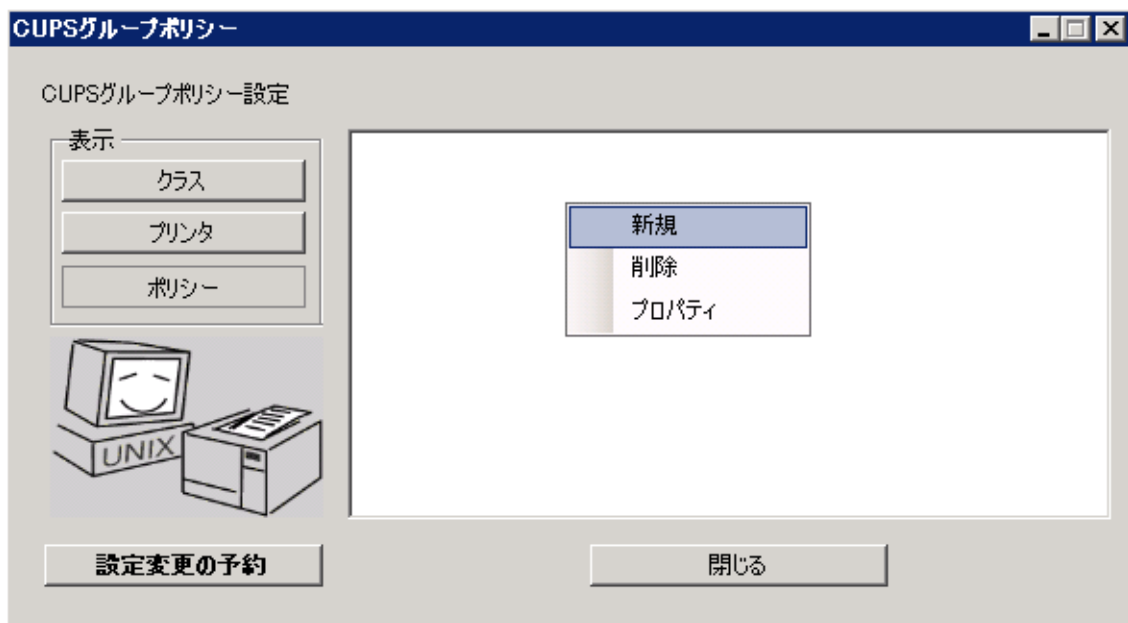
「[2.21.5.1.プリンタの設定](#)」の「[●高度な設定](#)」と同様ですので参照してください。

2.21.5.3 ポリシーの設定

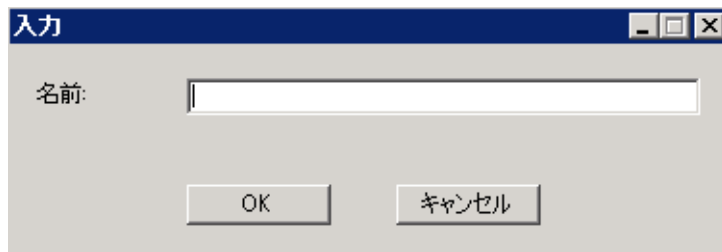
CUPS のサポートする IPP 関連のコマンド操作のアクセス制御を行います。特定の権限をユーザーごとに制限することもできます。プリンタおよびクラスに対し特別な運用ポリシーを定義します。root または CUPS のシステムグループに対してはプリンタの管理権限 (CUPS-Add-Modify-Printer、CUPSDelete-Printer、CUPS-Add-Modify-Class、CUPS-Delete-Class、CUPS-Set-Default 等) を必ず持たせるようにしてください。

詳細は CUPS のオンラインマニュアル等をご確認ください。

ポリシーを設定する場合は、「CUPS グループポリシー設定」画面、“表示” の[ポリシー]ボタンをクリックします。右側の枠内で右クリックをしてメニューから“新規” を選択します。



次のダイアログが表示されたらポリシー名を入力し[OK]ボタンをクリックしてください。



ポリシー名は 127 バイト未満の ASCII 文字で指定します。スペースは指定できません。英数_(アンダースコア)などを推奨します。



右側の枠内に policy1 アイコンが表示されたらダブルクリックをしてください。次の画面が表示されます。



設定項目は以下の通りです。完了後[OK]ボタンをクリックします。

ポリシーサブセット

[サブセット追加]ボタンをクリックして作成したポリシーが“ポリシーサブセット”欄にリストされます。リストのサブポリシーセットを選択し[サブセット削除]ボタンをクリックして削除も可能です。

サブセットの説明

追加したポリシーサブセットは Policy Subset という名前でもリストされます。これを選択した状態で“サブセットの説明”欄に名前を入力し変更します。

オペレーション

ポリシーサブセットに挿入する制限対象のオペレーションをリストから選択します。“よく使われるオペレーション”のプルダウンリストから対象を選択し[選択]ボタンを選択するとオペレーションをまとめて選択できます。

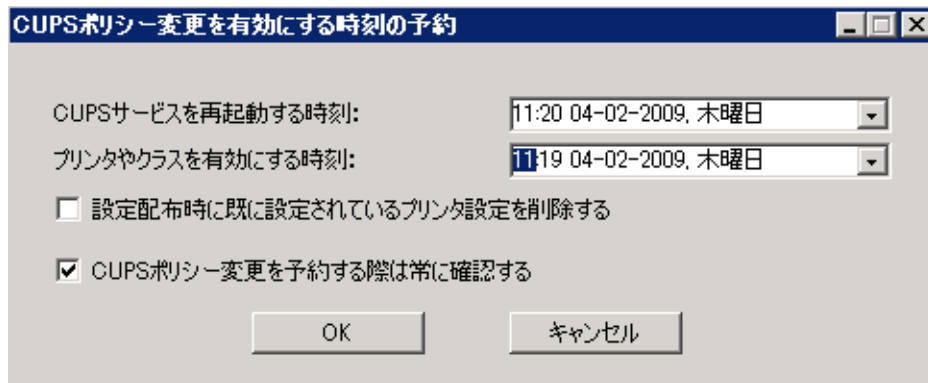
ディレクティブ

オペレーションに対するディレクティブを指定します。中央の枠内にリストされます。“よく使われるディレクティブ”からまとめて選択することもできます。“ディレクティブ”の上部テキストボックス内に直接値を入力し[ディレクティブ追加]ボタンでリストに追加することも可能です。リストのディレクティブを選択し[ディレクティブ削除]でディレクティブを削除することも可能です。

2.21.5.4 設定変更の予約

CUPS の設定はユーザーのログイン時にすぐ反映されません。システムに展開する必要があります。

設定が完了したら「CUPS グループポリシー設定」画面に戻り、[設定変更の予約]ボタンをクリックして、CUPS サービスの再起動、プリンタ/クラスの設定を有効にする日時の指定を行います。次の画面が表示されます。



設定項目は以下の通りです。完了後[OK]ボタンをクリックします。

CUPS サービスを再起動する時刻

CUPS サービスの再起動時間を指定します。CUPS グループポリシーを全て有効にするには CUPS サービスの再起動が必要です。

プリンタやクラスを有効にする時刻

CUPS のプリンタやクラスの指定を有効にする時間を指定します。もしプリンタやクラスの設定を変更した場合は、ここで必ず指定してください。

設定配布時に既に設定されているプリンタ設定を削除する

設定を適用する際に、既存のプリンタやクラスの設定(プリンタ名で検索)を削除するかどうかの指定です。選択を解除した状態では削除しません。

CUPS ポリシー変更を予約する際は常に確認する

管理者が設定変更をして[閉じる] ボタンをクリックした際に、「CUPS ポリシー変更を有効にする時刻の予約」画面を表示するかどうかの確認ダイアログを表示する指定です。変更時に有効にするための設定を忘れないように警告します。

CUPS の設定が反映されるタイミング



Linux システムがドメインへ JOIN し「CUPS ポリシー変更を有効にする時刻の予約」画面での設定以降に反映されます。

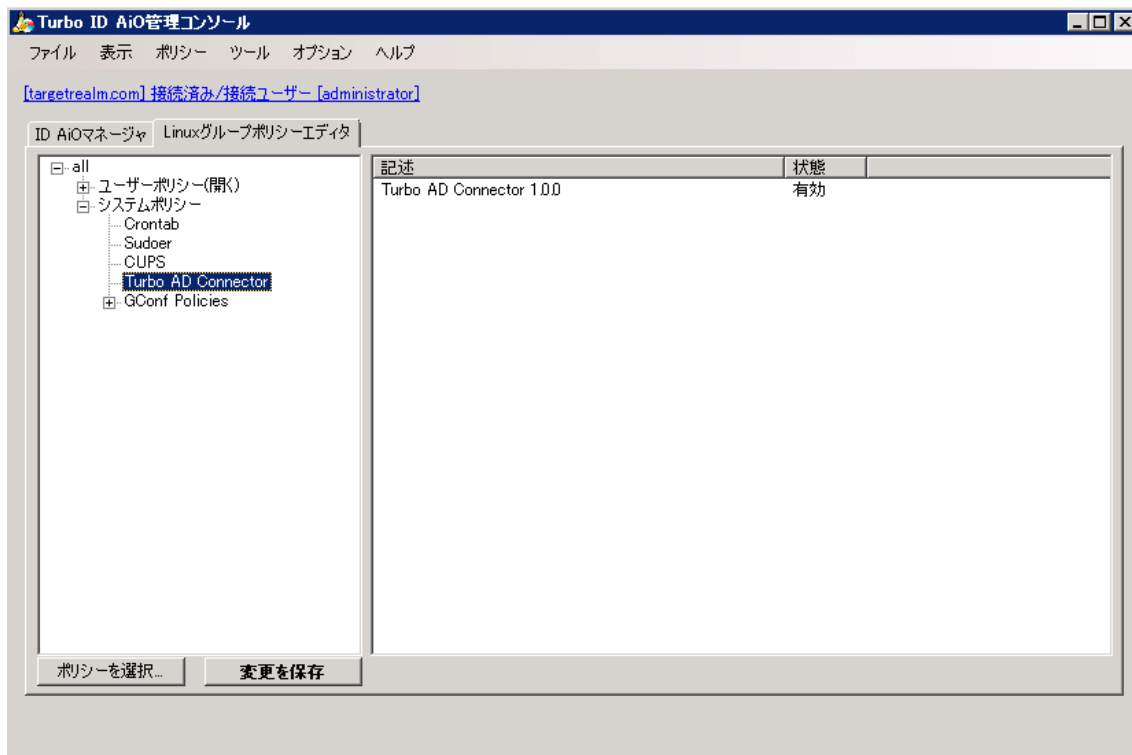
ただし、実際に有効になるのは CUPS サービスの再起動後です。反映されない場合は、CUPS サービスを手動で再起動してください。また、プリンタやクラスなどの設定内容に誤りがあると正常に反映されません。設定を見直してください。

2.21.6 Turbo AD ConnectorPolicy

Linux システムの adbindd デーモン用ポリシーモジュールです。システムレベルの機能を提供します。

「Linux グループポリシーエディタ」タブでポリシーを開きます(「[2.12.グループポリシーの確認と編集](#)」参照)。

システムポリシーの “Turbo AD Connector” をクリックし選択すると次のように画面右側のウィンドウに項目が表示されます。

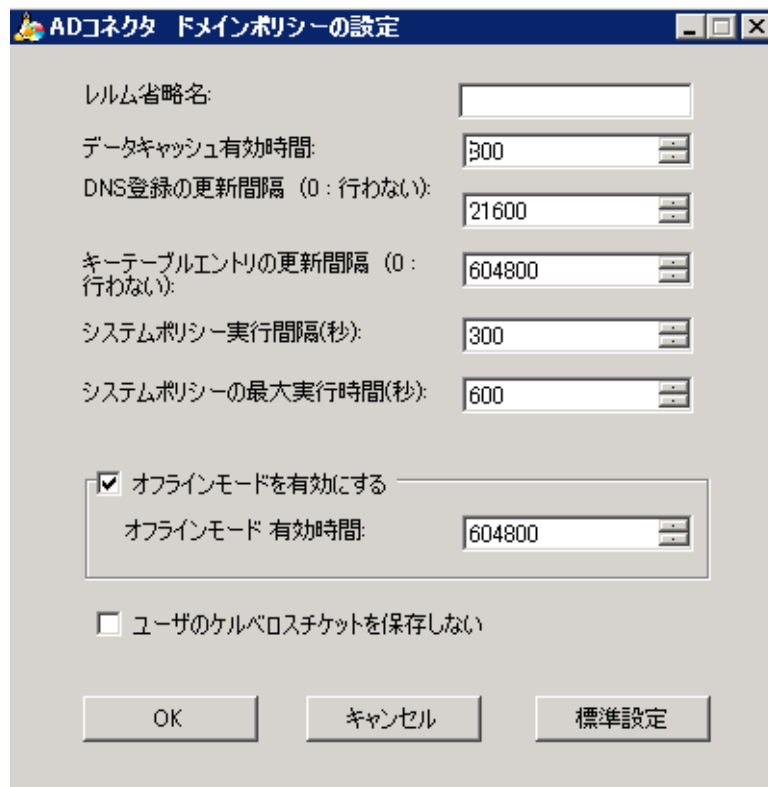


右側のウィンドウの各項目をダブルクリックすると次のように設定画面が表示されます。



ポリシーアイテムの設定がすべて完了したら必ず[変更を保存]ボタンをクリックし設定内容を保存してください。

次は Turbo AD Connector 1.0.0 の場合です。



設定項目は以下の通りです。完了後[OK]ボタンをクリックします。

レルム省略名

ユーザーがログインする際に指定するドメイン名(レルム名)の省略名を指定できます。ここで指定した省略名を指定しログインができるので便利です。

データキャッシュ有効時間

処理を高速化するためにデータキャッシュを保持しますが、このキャッシュの有効時間を指定します。キャッシュが無効な場合は、Active Directory を参照します。

DNS 登録更新間隔(0:行わない)

adbindd が自動的に DNS を更新する間隔を指定します。行わない場合は 0 と指定します。

キーテーブルエントリの更新間隔(0:行わない)

adbindd が自動的にケルベロスの keytable を更新する間隔を指定します。行わない場合は 0 と指定します。

システムポリシー実行間隔(秒)

システムレベルのグループポリシーを adbindd が適用する間隔です。適用したシステムレベルのグループポリシーはこの期間で有効になります。

システムポリシー最大実行時間(秒)

システムレベルのグループポリシーを adbindd が適用し続ける最大時間の指定です。システムレベルのポリシーが長い期間適用されたままになるのを防ぐ目的です。期間の制限を設けています。

オフラインモードを有効にする

オフラインモードを有効にするかどうかの指定です。

オフラインモード有効時間

オフラインモードの有効期間の設定です。

ユーザーのケルベロスチケットを保存しない

ユーザーのログインドメインのケルベロスチケットを保存するかどうかの指定です。デフォルトは、保存(選択を解除)しています。これはシングルサインオン機能を有効にしています。

2.21.7 Gconf Policies



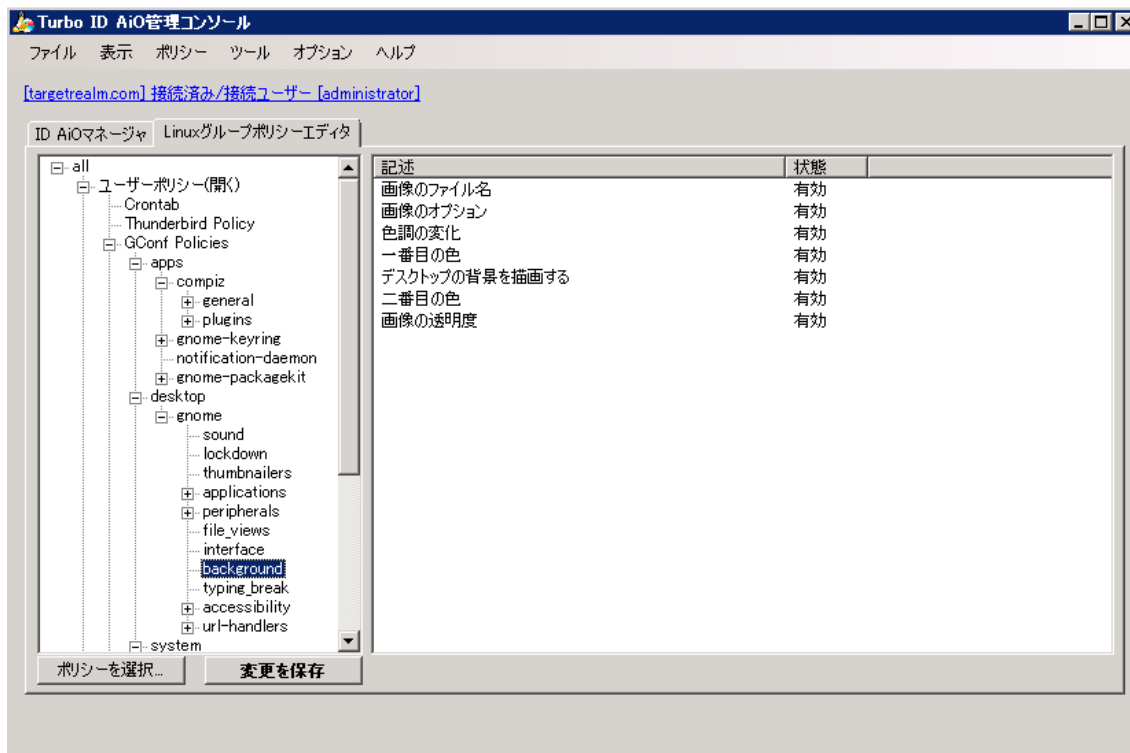
Gconf Policies は Linux クライアントのディストリビューションが混在していない環境での利用を前提としています。

デフォルトの状態は Turbolinux Client 2008 用のポリシーアイテムを装備しています。その他のディストリビューションの存在する環境ではご利用いただけません。もしご利用になる場合は、「[2.21.7.1.gconf convert ツール](#)」を参照し環境に合わせた設定を必ず行ってください。

Gconf Policies は Linux システム上に Gconf の設定を行うグループポリシーモジュールです。ユーザーレベルのグループポリシーモジュールですが、システムレベルでも同様に使用いただけます。いずれのレベルの場合も同じ設定項目を持ち、同じ項目に異なる値を指定することでシステムレベルの設定とユーザーごとの設定を変えることも可能です。

「Linux グループポリシーエディタ」タブでポリシーを開きます(「[2.12.グループポリシーの確認と編集](#)」参照)。

システムポリシーまたはユーザーポリシーの “Gconf Policies” をクリックするとサブディレクトリが展開されます。サブディレクトリ以下の項目を選択すると次のように画面右側のウィンドウにはそれぞれの設定項目が表示されます。



右側のウィンドウの各項目をダブルクリックすると次の設定画面が表示されます。

次は “/desktop/gnome/background/draw_background” の “デスクトップの背景を描画する” の設定画面です。



ポリシーアイテムの設定がすべて完了したら必ず[変更を保存]ボタンをクリックし設定内容を保存してください。

ポリシーアイテムの編集

名前: /desktop/gnome/background/draw_background

デスクトップの背景を描画する

状態

有効
 無効
 未指定

true

デフォルト値: true

GNOME にデスクトップの背景を描画させるかどうかです。

確定 取消

GNOME デスクトップの背景を描画するかどうかの設定です。

Gconf Policies のアイテム設定画面は、Thunderbird Policy や Firefox Policy と同様に以下の構成になっています。

名前

ポリシーアイテム名が表示されます。

状態

この機能を使用するかどうかを指定します。“有効”を選択するとこの機能を使用し中央に指定されているテキストボックスの値を適用します。“無効”はこの機能を使用しません。“未指定”は、この機能を使用しますがデフォルト値を適用します。

ユーザー指定欄(中央のテキストボックス)

ユーザーの指定欄です。

デフォルト値

ユーザー指定欄を省略した場合のデフォルト値です。

概要(画面下部の枠内)

この機能の概要の説明が表示されています。

設定を変更したら[確定]ボタンをクリックして反映します。



Gconf Policies を拡張するには XML ファイル(Turbo ID AiO¥policies¥gconf_schema.xml)の編集が必要になります。関連情報はターボナックス株式会社の Web サイトをご確認ください。また、同ファイルの編集は、サポートサービスの対象となりません。お客様の責任においてご注意の上行ってください。

2.21.7.1 gconf_convert ツール

Turbolinux Client 2008 以外のディストリビューションでご利用になるには、gconf_convert ツールを使用し環境にあった XML ファイルを抽出、生成する必要があります。gconf_convert ツールは、Linux Connector for Active Directory をインストールした Linux システムでご利用が可能です。

まずは Linux システム上でコンソールから root ユーザーで次のように実行します。

```
# gconf_convert gconf_schema.xml
```

カレントディレクトリに gconf_schema.xml ファイルが生成されます。これを Turbo ID AIO 管理コンソールのインストールされている Windows システムの Turbo ID AiO¥policies¥gconf_schema.xml ファイルにコピーしてください。ポリシーを開く際に読み込まれ、ご利用いただけます。



Turbo ID AiO¥policies¥gconf_schema.xml ファイルの置換する際は、あらかじめバックアップをとってください。



gconf_convert ツールは、Linux クライアントのディストリビューションが統一されている環境でご利用ください。また、サポートサービスの対象となりません。お客様の責任においてご注意の上行ってください。

2.21.7.2 デフォルトの Gconf Policies の内容

必要な項目は Linux ディストリビューションにより異なりますが、デフォルトの状態では Turbolinux Client 2008 を前提に装備しています。apps、desktop、system の 3 つの大きなカテゴリがあり、それぞれに小さなカテゴリがツリー構造になっています。



デフォルトの Gconf Policies については Linux クライアントが Turbolinux Client 2008 の場合にのみご利用ください。

第3章 Linux Connector for Active Directory

Linux Connector for Active Directory は、Linux コンピュータがドメインのメンバーとして JOIN し、ユーザーが ActiveDirectory の認証を使用しログインするための機能を提供します。また、本ソフトウェアの利用に必要なライセンス登録も行います。

3.1 インストールの準備



Linux ディストリビューションのインストールタイプ(インストールするパッケージの組み合わせ)によっては追加でパッケージのインストールが必要になる場合があります。環境に合わせてパッケージを追加インストールしてください。Linux Connector for Active Directory の RPM パッケージを rpm コマンドでインストールした際、パッケージの依存関係が確認され、不足している RPM パッケージがあるとエラーメッセージとともにリストされます。



各ディストリビューションに関する情報は「Linux Connector for Active Directory クイックスタートガイド」を参照ください。

3.1.1 システム時刻の確認と同期

ActiveDirectory では認証にケルベロスを採用しています。ケルベロスを利用する際にはクライアント側の PC(プリンシパル)と KDC(ドメインコントローラ)との時刻差が大きいとサービスを受けることができません。Windows サーバーとクライアントの時間差が大きくないかを事前に確認し、必要な場合は同期をとるよう調整してください。また、運用時には NTP システムを導入するか、定期的にシステム時間を確認、調整する必要があります。

3.2 インストール

Linux コンピュータに root でログインをするか、ログイン後に root ユーザーになります。

```
ログイン: root
パスワード: <- root のパスワードを入力
#
```

Linux Connector for Active Directory の CD-ROM をマウントし、ご利用のディストリビューション用の 3 つの RPM パッケージをインストールします。次は Turbolinux 11 Server 32bit 版の場合の例です。

```
# mount /mnt/cdrom
# cd /mnt/cdrom/TL11S/x86_32/
# ls
turboadconnector-1.0.0-2.i586.rpm
turboadconnector-gp-1.0.0-2.i586.rpm
turboadconnector-netlogon-1.0.0-2.i586.rpm
```



ディストリビューションごとに RPM パッケージが異なります。格納されているディレクトリは「[1.3.製品構成](#)」を参照し、必ずご利用になる環境に合った RPM パッケージを指定してください。



パッケージ名の 1.0.0-2 の部分はバージョン番号、i586 の部分はアーキテクチャです。ご利用環境に合わせて適宜読み替えてください。



RPM パッケージをインストールすると /etc/pam.d/system-auth、/etc/openldap/ldap.conf、/etc/nsswitch.conf を自動的に更新します。あらかじめバックアップを作成してください。

コンソールから root ユーザーで次のように実行します。

```
# rpm -ivh turboadconnector-1.0.0-2.i586.rpm ¥
turboadconnector-netlogon-1.0.0-2.i586.rpm ¥
turboadconnector-gp-1.0.0-2.i586.rpm

準備中... ##### [100%]
1:turboadconnector ##### [ 33%]
2:turboadconnector-netlogon##### [ 67%]
3:turboadconnector-gp ##### [100%]
```



ディストリビューションごとに RPM パッケージが異なります。ご利用環境に合わせて適宜読み替えてください。

インストールは完了です。続いて「[3.3.初期設定](#)」を参照し必要な設定を行ってください。

3.3 初期設定



設定ファイルの編集およびシリアル登録について詳細は「Linux Connector for Active Directory クイックスタートガイド」を参照ください。

なお、/etc/turboadc/config.xml ファイルは GUI ツールで設定も可能です。詳細は「[3.5.adjoin_gui](#)」を参照ください。

3.3.1 設定ファイルの編集

/etc/krb5.conf ファイルの編集

ケルベロスの設定ファイル /etc/krb5.conf ファイルにレルム名 (realm) を指定します。ActiveDirectory では、レルム名としてドメイン名を使用します。ActiveDirectory に複数のドメインコントローラが存在する場合、kdc 行を複数記述しておきますと指定順に使用されます。

[realms] セクションおよび [domain_realm] セクションを以下例の太字部分のように環境に合わせて指定します。

```
[realms]
TARGETREALM.COM = {
  kdc = kdc.targetrealm.com:88
  kdc = kdc2.targetrealm.com:88
  admin_server = kdc.targetrealm.com:749
}

[domain_realm]
targetrealm.com = TARGETREALM.COM
.targetrealm.com = TARGETREALM.COM
```

/etc/resolv.conf ファイルの編集

/etc/resolv.conf に Windows ドメインで使用している適切なネームサーバーが指定されていることを確認します。

```
nameserver 192.168.0.1
```

/etc/turboadc/config.xml ファイルの編集

/etc/turboadc/config.xml ファイルを編集しレルム名を指定します。

```
<realm>
  <fqdn>TARGETRELM.COM</fqdn>
  <netbiosname>TARGETRELM</netbiosname>
  <IDAiOTech>1</IDAiOTech>
</realm>
```

3.3.2 シリアルの登録

クライアントの NETBIOS 名と Linux Connector for Active Directory 製品に付属のシリアル番号を使用して製品使用のための登録を行います。利用を開始するには必ず実行しなければなりません。詳細は「Linux Connector for Active Directory クイックスタートガイド」および「[3.4.2.adjoin_cli コマンドの使用例](#)」、「[3.5.1.シリアルの登録](#)」を参照ください。

3.4 adjoin_cli コマンド

3.4.1 adjoin_cli コマンドのパラメータ

adjoin_cli コマンドは、Linux クライアントが Active Directory へ参加する際に使用します。次のパラメータを指定することができます。

パラメータ	説明
-h --help	ヘルプメッセージ
-j --join	ドメインへ JOIN します。実行時にはドメインの選択とドメインコントローラの administrator パスワードの入力が必要です。 JOIN に成功したら、adbind デーモンを再起動し情報を更新します。
-l --leave	ドメインから削除します。実行時にはドメインの選択とドメインコントローラの administrator パスワードの入力が必要です。
-r --regist	DNS サーバーへ登録します。実行時にはドメインの選択とドメインコントローラの administrator パスワードの入力が必要です。
-u <i>username</i> --user= <i>username</i>	ドメインの管理権限を持つユーザー名を指定します。指定を省略した場合は、administrator が適用されます。
-p <i>password</i> --password= <i>password</i>	パスワードを指定します。省略した場合には、コマンド実行時にパスワードの入力を促されます。
-o <i>OU</i> --orgunit= <i>OU</i>	OU (組織単位) を指定します。OU が存在しないとき、コマンドの実行時に失敗します。-t または --list パラメータで存在する OU を確認することができます。
-i --info	adbind デーモンに関する情報を表示します。また、メンバーとなっているドメイン、ドメインの SID、クライアントのマシン OU、JOIN した時間などを確認できます。
-t 0 1 --listou=0 1	ドメインの組織をツリー表示します。0 を指定した場合、DN (OU=Domain Controllers,DC=targetrealm,DC=com など) を表示し、1 は DN の表示を省略します。実行時にはドメインの選択とドメインコントローラの administrator パスワードの入力が必要です。
-q <i>SAM アカウント名</i> --qsam= <i>SAM アカウント名</i>	指定した SAM アカウント名の情報を表示します。
-s --testjoin	Linux システムがドメインへ JOIN 可能かどうかテストします。 Testjoin returned success / failure のように可否が結果として表示されます。
-T --servertime	Windows サーバーのシステム時間を取得し、クライアントとの時間差を表示します。実行時にはドメインの選択とドメインコントローラの administrator パスワードの入力が必要です。
-x --register	システムの登録および登録情報の確認をします。登録済みの場合は "Netbios name" "Serial number" "Expire time" が画面に表示されます。登録時には "Netbios name" "Serial number" "register server" を指定します。"Serial number" は、製品に同梱されているものを使用してください。

<pre>-kKEYTABLE:SPN --setspnkt=KEYTABLE:SPN</pre>	<p>ケルベロスキーテーブルの更新と作成を行います。KEYTABLE:SPN は keytable ファイル:SPN の形式で指定をします</p> <p>(例: mykey.tab:HTTP/hostname.realm.com または HOST/hostname.realm.com)</p> <p>指定を省略した場合は/etc/krb5.keytab が使用されます。(このファイル名はシステム環境に依存します。)</p> <p>実行時にはドメインの選択とドメインコントローラの administrator パスワードの入力が必要です。</p>
---	--

3.4.2 adjoin_cli コマンドの使用例

● 登録(-x / --register)

利用を開始する前に 1 度実行しシステムを登録する必要があります。次のように実行します。

はじめにクライアントマシンの NETBIOS 名を指定してください(例では kevin)。続いて製品に同梱されているシリアル番号を入力してください。シリアル番号はハイフン(-)を含めます(例では 1234-123456-123456)。最後にレジストサーバーを入力します。通常はそのまま[Enter]キーを押してください。

```
# adjoin_cli -x
Please input machine's netbios name: kevin
Please input serial number(for example: XXXX-XXXXXX-XXXXXX):<- 1234-123456-123456
Please input register server[auth.turbolinux.co.jp]: <- そのまま[Enter]キー
Register is running. Please wait a moment.
Register correct. Please enjoy turbo adbind.
```

Register correct と表示されれば成功です。

登録済みの場合、実行すると登録情報が表示され確認することができます。Expire time 欄には、使用期限が表示されます。

y と入力すると上書きで再度登録が可能です。n を入力するとキャンセルされます。

```
# adjoin_cli -x
*****
You have registered the system. The register info as follow:
Netbios name :kevin
Serial number :1111-111111-111111
Expire time :2010-04-27
*****
Would you register again[Y|N]:y
```

● JOIN(-j / --join)

Linux システムをドメインに参加(JOIN)させます。root ユーザーで次のように実行します。

```
# adjoin_cli -j
Configured Realms List:
0 - TARGETREALM
1 - WINDOWS2008J
```

TARGETREALMやIINDOWS2008Jの部分は実際に指定されているレルム名(ドメイン名)が表示されます。次のように表示されたらレルム名の前の番号を入力しJOIN先ドメインを指定します。

```
Choose which realm to use by id:0
```

続いて administrator のパスワードを入力します。

```
TARGETREALM is chosen  
administrator's password: <-パスワードを入力
```

次のように表示されればドメインへの JOIN と DNS サーバーへの登録は成功です。

```
joining domain is a success, also registering dns  
successfully registered dns  
Please restart adbind service
```



次のように `-p password` (administrator のパスワード) を指定した場合は、administrator のパスワード入力は省略されます。

```
# adjoin_cli -j -p password
```

OU(組織)を指定する場合は次の通りです。`-o OU`には OU(組織)名を指定します。例は TARGETREALM です。

```
# adjoin_cli -j -o TARGETREALM -p password
```



ドメインへの JOIN や離脱を行ったら、adbind サービスを再起動してください。

```
# /etc/init.d/adbind restart
```

3.5 adjoin_gui

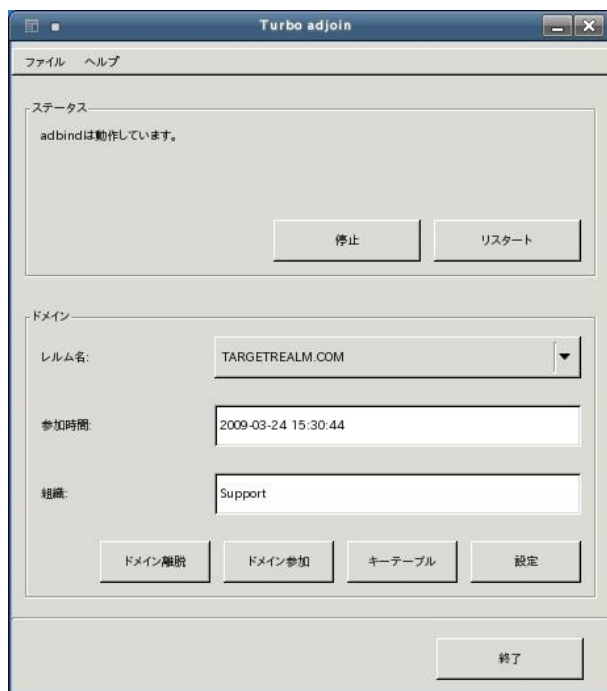
adjoin_gui コマンドは、Linux クライアントが Active Directory への参加する際に使用するツールです。adjoin_cli と同等の機能を GUI による操作で実現します。

起動するには X 上で root ユーザーになってから次のように実行します。

あるいは root 権限で X を起動している場合、メニューに“アクティブディレクトリへ接続”が表示され選択いただけます。

```
# adjoin_gui
```

次のメイン画面が表示されます。



メニューバー“ファイル”メニューの“情報登録”ではシステムの登録や終了を選択できます。画面上部の“ステータス”欄には adbind の状態が表示され[停止]/[開始]、[リスタート]ボタンでデーモンの停止/起動、再起動を実行します。

画面下部の“ドメイン”欄には“レルム名”に接続先ドメイン名、“参加時間”には JOIN した日時、“組織”欄には OU (組織単位) が表示されます。また [ドメイン離脱] [ドメイン参加] [キーテーブル] [設定] の各ボタンでドメイン削除、JOIN、キーテーブルの作成/更新、設定ファイルの編集の操作が可能になっています。

3.5.1 シリアルの登録

メイン画面のメニューバーから“ファイル” -> “情報登録” をクリックします。次の画面が表示されます。



情報登録

NETBIOS名:

シリアルナンバー: - -

登録サーバー:

キャンセル 情報登録

“NETBIOS 名” 欄にクライアントマシンの NETBIOS 名を、“シリアルナンバー” 欄には、製品に同梱されているシリアル番号を入力します。“登録サーバー” 欄はレジストサーバーを指定しますが通常は auth.turbolinux.co.jp のままです。指定が完了したら[情報登録]ボタンをクリックします。

登録済みの場合、実行すると登録情報が表示され確認することができます。Expire time 欄には、使用期限が表示されます。[再登録]ボタンをクリックすると上書きで再登録が可能です。



情報登録

NETBIOS名: Kevin

シリアルナンバー: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX

有効期限: 2010-04-10

キャンセル 再登録

登録に成功すると次のダイアログが表示されます。



3.5.2 adbind デーモン管理

adbind デーモンの起動/停止/再起動を実行します。メイン画面上部の“ステータス”枠内はデーモンが停止状態の時以下のように表示されます。



[開始]ボタンをクリックするデーモンを起動します。起動に成功すると成功のダイアログが表示されます。

画面上部の“ステータス”枠内はデーモンが起動状態の時以下のように表示されます。



[停止]ボタンをクリックするデーモンを停止し、[リスタート]ボタンをクリックするとデーモンを再起動します。それぞれ成功すると成功のダイアログが表示されます。



adbind デーモンが停止中は、接続ドメインの情報はリアルタイムに更新されません。

3.5.3 ドメインに参加 (JOIN)

ドメインに参加 (JOIN) するには、メイン画面下部の [ドメイン参加] ボタンをクリックします。以下の「ドメインに参加」画面が表示されます。



次の項目を指定します。

レルム名

プルダウンリストから接続先ドメインのレルム名を選択します。「ドメイン名」欄には選択したドメインの NETBIOS 名が表示されます。

ユーザー名

ドメインの管理権限を持つユーザー名を入力します。(例: administrator)

パスワード

管理権限を持つユーザーのパスワードを指定します。

組織

ドメインの OU (組織単位) へ JOIN する場合にはここで OU 名を指定します。



ボタンをクリックして接続先ドメインの組織のリストを表示することも可能です。詳細は「[3.5.4.OU \(組織単位\) の選択](#)」を参照してください。


指定が完了したら [ドメイン参加] ボタンをクリックします。JOIN に成功すると以下のダイアログが表示されます。





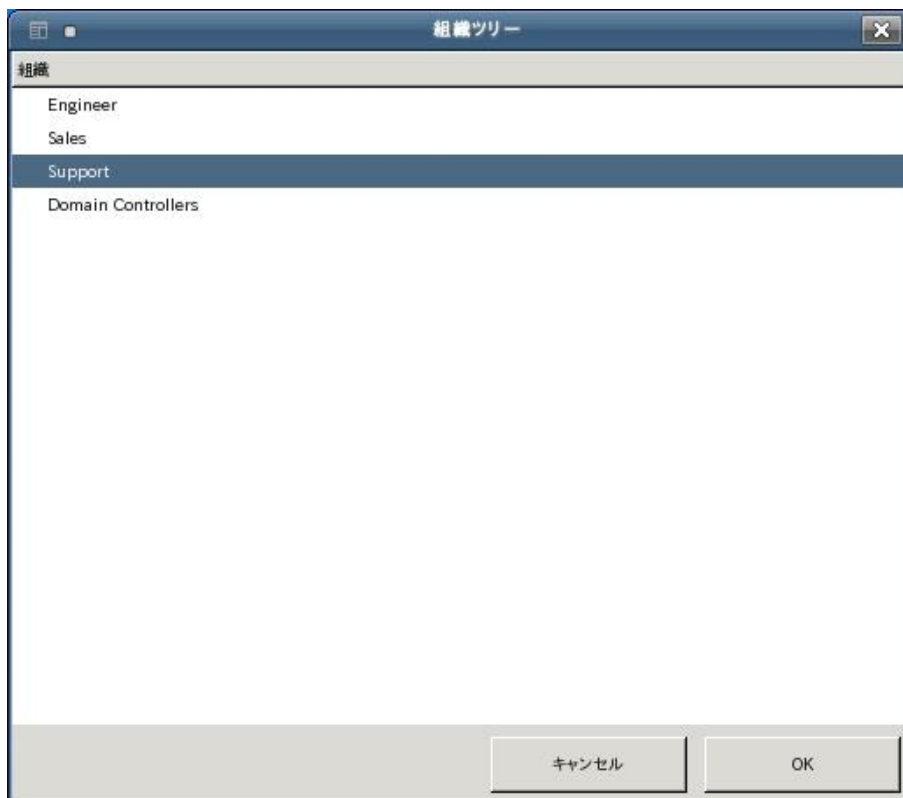
ドメインへの JOIN や離脱を行ったら、adbind サービスを再起動してください(「[3.5.2.adbind デーモン管理](#)」参照)。

3.5.4 OU(組織単位)の選択

ドメインに参加 (JOIN) する際に、OU(組織単位)の指定が可能です。「ドメインに参加」画面の「組織」項  ボタンをクリックし次の「組織リンク」画面を表示します。ユーザー名とパスワードを入力し[OK]ボタンをクリックします。



次のようにドメインの OU 一覧が表示されてリストから選択が可能になります。



選択後[OK]ボタンをクリックします。「ドメインに接続」画面の「組織」欄に選択した OU が表示されます。

3.5.5 ドメインから離脱

ドメインから削除するには、メイン画面下部の[ドメイン離脱]ボタンをクリックします。以下の「ドメインから離脱」画面が表示されます。



次の項目を指定します。

レルム名

離脱するドメインのレルム名を指定します。

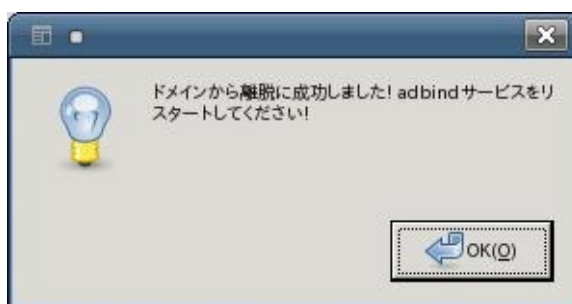
ユーザー名

ドメインの管理権限を持つユーザー名を入力します。(例: administrator)

パスワード

管理権限を持つユーザーのパスワードを指定します。

指定が完了したら[ドメイン離脱]ボタンをクリックします。離脱に成功すると以下のダイアログが表示されます。



ドメインへのJOINや離脱を行ったら、adbindサービスを再起動してください(「[3.5.2.adbind デーモン管理](#)」参照)。

3.5.6 キーテーブルの設定

ケルベロスキーテーブルの更新と作成を行います。メイン画面下部の[キーテーブル]ボタンをクリックします。次の画面が表示されます。

指定を省略した場合は/etc/krb5.keytab が使用されます。このファイル名はシステム環境に依存します。



The dialog box titled "ケルベロス キーテーブル" (Kerberos Key Table) contains the following fields and controls:

- レルム名:** A dropdown menu with "TARGETREALM.COM" selected.
- ドメイン名:** A text field containing "TARGETREALM".
- Spn:** An empty text field.
- キータブファイル:** An empty text field.
- A note below the keytab field: "キータブファイル設定が空なら、システムのデフォルトキータブファイルを使用します。" (If the keytab file setting is empty, the system's default keytab file will be used.)
- Buttons for "キャンセル" (Cancel) and "OK".

次の項目を指定します。

レルム名

対象ドメインのレルム名を指定します。"ドメイン名"欄には選択したドメインの NETBIOS 名が表示されます。

Spn

SPN を指定します。

キータブファイル

キータブファイル名を指定します。

指定が完了したら[OK]ボタンをクリックします。続いて以下のダイアログが表示されたらドメインの管理権限を持つユーザー名とパスワードを入力し[OK]ボタンをクリックしてください。



The dialog box titled "ケルベロス キーテーブル <2>" contains the following fields and controls:

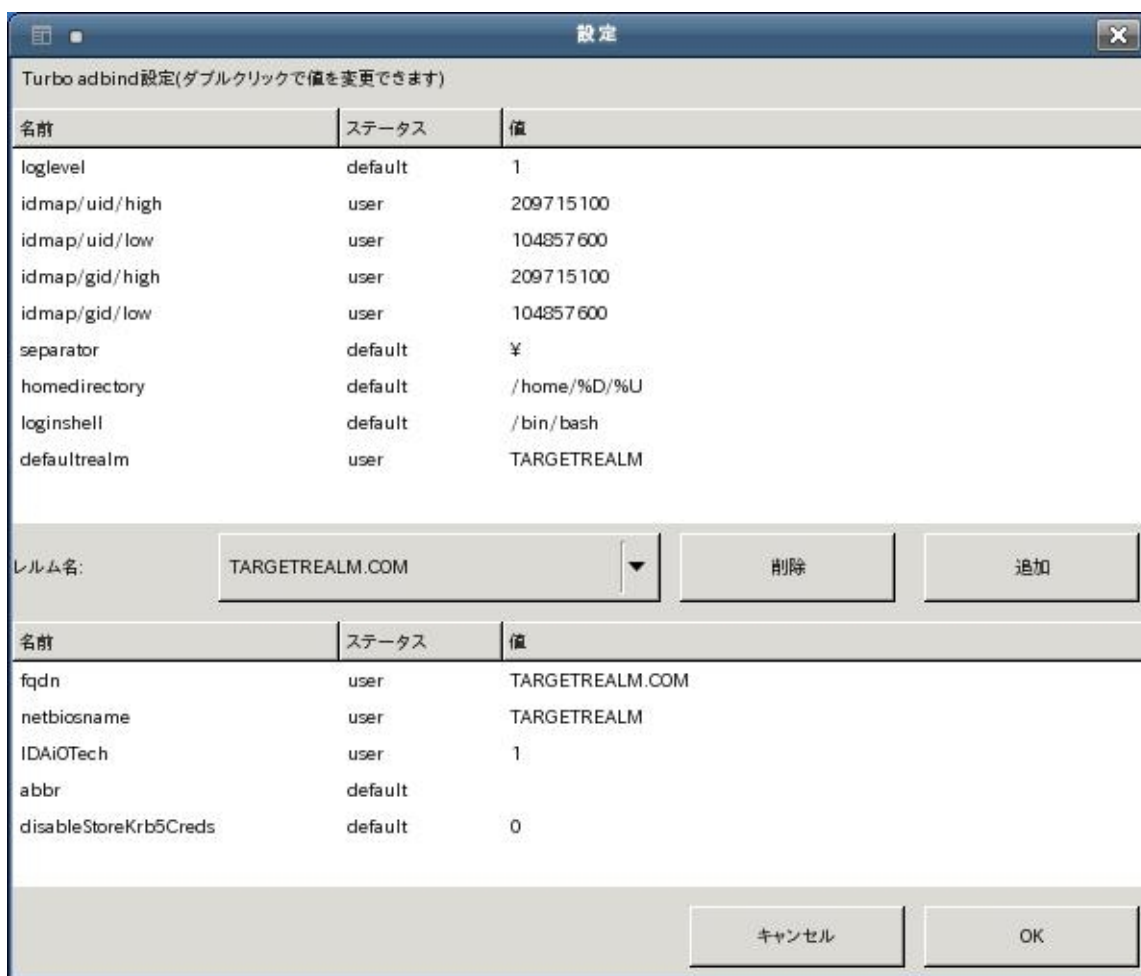
- ユーザ名:** A text field containing "administrator".
- パスワード:** A password field with 12 dots and a cursor.
- Buttons for "キャンセル" (Cancel) and "OK".

成功すると以下のダイアログが表示されます。



3.5.7 adbind の設定 (config.xml)

adbind の設定ファイル (/etc/turboadc/config.xml) を編集します。メイン画面下部の [設定] ボタンをクリックします。以下の画面が表示されます。



画面上部は、adbind 全体に関する設定です。中央の“レルム名”プルダウンリストから設定対象のレルム名を選択します。画面下部は選択しているレルムの設定が表示されます。新たにレルムを追加するには中央の [追加] ボタンを、既存のレルム設定を削除するには [削除] ボタンをクリックします。

また、画面中の“名前”は設定項目が表示され、“ステータス”に“user”と表示されている行はユーザーによって“値”が設定されています。“ステータス”に“default”と表示されている行は指定が省略されているため default 値が適用されている項目です。各行をダブルクリックし、値を変更することができます。

adbind 全体に関する各設定項目は以下の通りです。

loglevel

syslog へ出力するログレベルの指定です。通常は 0 ですが、更に詳細を記録するには 1、2 を指定します。

idmap/uid/high

自動的に割り当てられる UID の最大値の指定です。“idmap/uid/low” より大きい値を指定する必要があります。

idmap/uid/low

自動的に割り当てられる UID の最小値の指定です。“idmap/uid/high” より小さい値で、システムの使用する UID より大きい値を指定する必要があります。

lidmap/gid/high

自動的に割り当てられる GID の最大値の指定です。“idmap/gid/low” より大きい値を指定する必要があります。

idmap/gid/low

自動的に割り当てられる GID の最小値の指定です。“idmap/gid/high” より小さい値で、システムの使用する GID より大きい値を指定する必要があります。

separator

ドメイン名とユーザー名のセパレータの指定です。デフォルトは ¥(バックスラッシュ)です。1 文字のみ指定可能で、ドメイン名やユーザー名に使用される文字は指定することができません。変更する場合は、* や ^ など通常使用されない文字としてください。

homedirectory

ユーザーのホームディレクトリのテンプレートの指定です。

logonshell

ログインシェルへのデフォルト指定です。

defaultrealm

デフォルトのドメイン(レルム)名指定です。

各ドメイン(レルム)に関する各設定項目は以下の通りです。

fqdn

ドメインの FQDN 指定です。

netbiosname

ドメインの NETBIOS 名の指定です。

IDAiOTech

IDAio ユニットを使用するかどうかの指定です。1(有効)、0(無効)です。

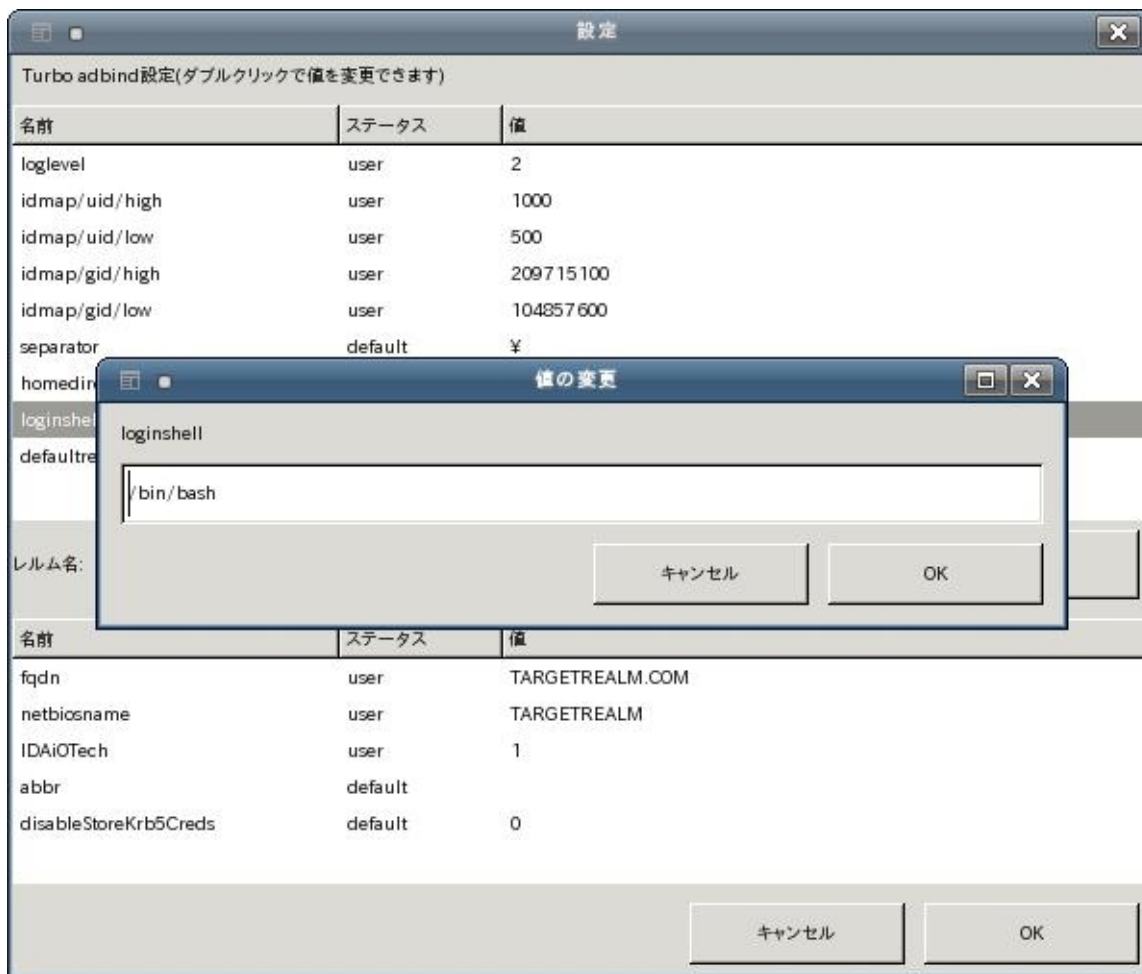
abbr

短縮したドメイン名の指定です。

disableStoreKrb5Creds

ケルベロスの資格情報を保存するかどうかの指定です。0(保存)、1(保存しない)です。デフォルトは 0 です。

値を変更するには、対象の行でダブルクリックします。以下のように値を入力するためのダイアログが表示されます。



3.5.8 ヘルプ

メイン画面メニューバー“ヘルプ” -> “情報” をクリックすると次のダイアログが表示されます。ソフトウェアのバージョン情報や、機能概要、開発元などの情報を確認いただけます。



3.6 サービスの管理

Linux Connector for Active Directory を構成する adbind および adcnologond デーモンのサービス管理について解説します。

3.6.1 adbind サービスの起動と停止

Linux システムが ActiveDirectory へ JOIN したら、必ず adbind サービスを起動する必要があります。adbind サービスによって、Linux クライアントからユーザーが ActiveDirectory へログインすることができるのです。

adbind サービスを起動するには root ユーザーでコンソールから以下の通り実行します。

```
# /etc/init.d/adbind start
Starting adbindd services: OK
```

adbind サービスを停止するには root ユーザーでコンソールから以下の通り実行します。

```
# /etc/init.d/adbind stop
Shutting down adbindd services: OK
```

adbind サービスを再起動するには root ユーザーでコンソールから以下の通り実行します。

```
# /etc/init.d/adbind restart
Restarting adbindd services: Shutting down adbindd services: OK
Starting adbindd services: OK
done.
```



adbind_gui から adbind サービスを制御することもできます。詳細は「[3.5.2.adbind デーモン管理](#)」を参照してください。

システム再起動後も adbind サービスを有効にするには root ユーザーでコンソールから以下の通り実行します。

```
# chkconfig adbind on
```

3.6.2 adcnologond サービスの起動と停止

ActiveDirectory にバックアップドメインコントローラが存在する場合、adcnologond サービスの起動と連携することで adbind サービスが最適なドメインコントローラの IP アドレスを取得し処理の高速化をはかることが可能です。



adcnologond について詳細は「[4.3.AD Connector Netlogon](#)」を参照してください。

adcnetlogond サービスを起動するには root ユーザーでコンソールから以下の通り実行します。

```
# /etc/init.d/adcnetlogon start
Starting adcnetlogond services: OK
```

adcnetlogond サービスを停止するには root ユーザーでコンソールから以下の通り実行します。

```
# /etc/init.d/adcnetlogon stop
Shutting down adcnetlogond services: OK
```

adcnetlogond サービスを再起動するには root ユーザーでコンソールから以下の通り実行します。

```
# etc/init.d/adcnetlogon restart
Restarting adcnetlogond services: Shutting down adcnetlogond services: OK
Starting adcnetlogond services: OK
done.
```

システム再起動後も adcnetlogond サービスを有効にするには root ユーザーでコンソールから以下の通り実行します。

```
# chkconfig adcnetlogon on
```

第4章 その他の便利な機能

4.1 複数ドメインの指定

Linux Connector for Active Directory は、1 台の Linux コンピュータの複数ドメインへの参加をサポートしています。このような場合、ドメインユーザーは、この Linux コンピュータ上から同時にどちらへもログインすることができます。

4.2 デフォルトドメインの省略名

4.2.1 デフォルトドメインの指定

adbind_gui の「設定」画面の "defaultrealm" または /etc/turboadc/config.xml ファイルの defaultrealm ディレクティブに デフォルトドメインの NETBIOS 名を指定し、adbind を再起動します。デフォルトドメインへのログイン時にユーザーは、ドメイン名の指定を省略することができます。

ドメイン名とユーザー名の区切り文字が¥(デフォルト値)の場合、ドメイン NETBIOS 名 TARGETREALM に管理者でログインをするには、"TARGETREALM¥administrator" と指定しますが、"defaultrealm" 指定後は、"TARGETREALM¥" の部分を省略し、"administrator" だけでこのデフォルトドメインへログインすることができます。

4.2.2 省略名の指定

adbind_gui の「設定」画面で各レームごとの "abbr" または /etc/turboadc/config.xml ファイルの abbr ディレクティブにドメイン名の省略名を指定し、adbind を再起動します。各ドメインへのログイン時にユーザーは、ドメイン名の省略名を指定することができます。

例えば、ドメイン TARGETREALM1 と TARGETREALM2 が存在し、それぞれに TG1、TG2 という省略名を指定します。ドメイン名とユーザー名の区切り文字が¥(デフォルト値)の場合、それぞれのドメインへ管理者でログインをするには、"TARGETREALM1¥administrator" "TARGETREALM2¥administrator" と指定しますが、"abbr" 指定後は、"TG1¥administrator" "TG2¥administrator" だけでドメインへログインすることができます。長いドメイン名指定によるタイプミスなどの誤りを防ぐことができます。

4.3 AD Connector Netlogon

4.3.1 概要

AD Connector Netlogon はドメイン名解決機能を提供します。主な機能としては、ドメイン名の入力に対し、最適なドメインコントローラの IP アドレスを返すことで処理を高速化します。サーバー機能の adcnetlogond および libadcnetlogon.so とクライアントの adc_get_dc により実装しています。adbindd デーモンは libadcnetlogon.so を通じて adcnetlogond と通信し最適なドメインコントローラの IP アドレスを入手します。AD Connector Netlogon サービスが無効な場合、adbindd デーモン自身がドメインコントローラの IP アドレスを解析しますが、必ずしも最適とは限りません。

4.3.2 adcnetlogond

4.3.2.1 adcnetlogond オプション

adcnetlogond には以下のオプションがあります。

パラメータ	説明
-h	ヘルプメッセージ

<code>--help</code>	
<code>-i</code> <code>--interactive</code>	インタラクティブ(対話型)モードで実行します。デフォルトはデーモンモードです。
<code>--l logFilePath</code> <code>--logfile logFilePath</code>	指定パスにログ出力します。デフォルトは syslog へ出力です。
<code>-d debugLevel</code> <code>--debuglevel debugLevel</code>	ログレベルの指定です。error、warning、info、verbose、debug を指定します。

4.3.2.2 設定ファイル

adcnetlogond の設定ファイルは /etc/turboadc/netlogon.conf です。

設定項目は "cache_entry_timeout" のみで、ここに解析したドメインの情報をキャッシュする期間を設定します。指定を省略した場合デフォルト値は 30 秒です。最大値は 1 日、最小値は 1 秒です。以下の場合、5 分です。

```
# Turbo ADC Netlogon
#
# Time value suffixes:
# d - days
# h - hours
# m - minutes
# s - seconds
#
[cache]
# Default: 30s
# Minimum: 1s
# Maximum: 1d
cache_entry_timeout = 5m
```

4.3.2.3 サービスの起動

adcnetlogond サービスを起動するには root ユーザーでコンソールから以下の通り実行します。

```
# /etc/init.d/adcnetlogon start
Starting adcnetlogond services: OK
```



サービス管理については「[3.6.2.adcnetlogond サービスの起動と停止](#)」を参照してください。

4.3.3 adc_get_dc

4.3.3.1 概要

adc_get_dc は adcnetlogon が正常に動作しているかを検証するクライアント側ツールです。書式は以下の通りです。

```
adc_get_dc -d target domain FQDN [options]
```

パラメータの指定は以下の通りです。

パラメータ	説明
-d <i>domainname FQDN</i> --domain <i>domainname FQDN</i>	ターゲットドメインの FQDN です。必須指定項目です。

[options]に指定可能なオプションは以下の通りです。

オプション	説明
-h --help	ヘルプメッセージ
-F --fresh	キャッシュからではなく強制的に DNS サーバーからの情報を取得します。adcnetworklogond は高速化のため一度取得した情報はキャッシュし期限内はこの情報を使用します。このオプション指定時はキャッシュデータを使用しません。-F オプションと -C オプションは同時に指定できません。
-C --cache-only	キャッシュの期限に関わらずキャッシュから情報を取得します。何もキャッシュデータが存在しない場合は、DNS から取得します。-F オプションと -C オプションは同時に指定できません。
-D --dc	指定ドメインのドメインコントローラ (DC) の IP アドレスを検索します。DNS の "_ldap._tcp.dc._msdcs.ドメイン名" または "_ldap._tcp.ドメイン名" レコードを取得します。
-G --gc	指定ドメインのグローバル・カタログサーバー (GC) の IP アドレスを検索します。DNS の "_ldap._tcp.gc._msdcs.ドメイン名" または "_gc._tcp.ドメイン名" レコードを取得します。
-P --pdc	指定ドメインのプライマリドメインコントローラ (PDC) の IP アドレスを検索します。必ずしも最適なドメインコントローラとは限りません。 DNS の "_ldap._tcp.pdc._msdcs.ドメイン名" または "_pdc._tcp.ドメイン名" レコードを取得します。
-K --kdc	指定ドメインのケルベロスコントローラ (KDC) の IP アドレスを検索します。 DNS の "_kerberos._tcp.dc._msdcs.ドメイン名" または "_kerberos._tcp.ドメイン名" レコードを取得します。



-F オプションと -C オプションは同時に指定できません。いずれも指定が無い場合は、adcnetworklogond はキャッシュ情報を検査し、期限内の場合に採用します。



-D -G -P -K の各オプションを同時に指定できません。いずれも指定が無い場合は -D オプションが有効です。

次の例のように実行します。例は targetrealm.com ドメインのドメインコントローラの情報を取得しています。

```
# adc_get_dc -d targetrealm.com
Domain targetrealm.com information:
Domain Controller Name = neptune.targetrealm.com
Domain Controller Address = 172.16.37.244
```

4.4 オフライン機能

adbindd デーモンのサポートするオフラインモードは、ネットワーク障害などで接続が不可能なとき、あるいは帰宅後など ActiveDirectory へ接続できない状態の時に Linux システムへログインし利用を可能にします。

ドメインユーザーのパスワード認証とログインはサポートしますが、ユーザーグループリストの取得 (getent passwd / group / shadow コマンド) やユーザーのパスワード変更は未サポートです。

オフラインモードの時、これらの情報はキャッシュから取得します。キャッシュデータは最後のログイン時から計算されます。キャッシュ時間は Turbo ID AIO 管理コンソールのグループポリシーを使用している場合、「オフラインモード」「オフラインモード有効期間」設定（「[2.21.6.Turbo AD ConnectorPolicy](#)」参照）の値によります。デフォルトは 7 日間 (604800 秒) です。

4.5 ID Map ヘルパー

4.5.1 概要

ID Map ヘルパーは管理者用の ID マッピングメンテナンスツールです。ID Aio モジュールを使用しない環境下でユーザー/グループの SID (Windows でユーザー/グループが管理されている SID: Security Identifier) と UID、GID のマッピング情報を管理します。主な機能は以下の通りです。

- SID と UID/GID のマッピング情報の検索と削除
- 現在のマッピングリストの出力
- 現在の UID/GID を指定範囲に移行
- マッピングテーブルの完全な削除

本ツールを利用し ID マッピングテーブルを操作するには root 権限が必要です。ID マッピングテーブルはデフォルトでは、/var/cache/turboadc/idmap_adbindd.db です。



データの整合性を確保するために、adbind サービスを停止後に /var/cache/turboadc/idmap_adbindd.db のバックアップをとり、更新操作をするようにしてください。強く推奨します。

4.5.2 SID と UID/GID のマッピング情報の検索と削除

このメンテナンスツールは現在の ID マッピング情報の検索や削除を行うために次の 2 種類の方法を提供します。

- UID/GID に対応する Windows ユーザー/グループの SID (S-1-5-21-xxxx-xxxx-xxxx-rrr のような形式の ID) を検索/削除
- Windows ユーザー/グループの SID に対応する UID/GID を検索/削除 (U12345 は、UID の 12345、G45678 は GID の 45678 を表します。)

4.5.2.1 検索

```
# idmap_helper --src /var/cache/turboadc/idmap_adbindd.db -q query
```

パラメータ	説明
--src <i>targetdatapath</i>	ターゲットのマッピングテーブルファイルのパスを指定します。
-q <i>query</i>	<i>query</i> に指定した値を検索します。

SID (例は S-1-5-21-3233604394-866250274-1751313351-500) にマップされている UID を検索するには次のように実行します。

```
# idmap_helper --src /var/cache/turboadc/idmap_adbindd.db \  
-q S-1-5-21-3233604394-866250274-1751313351-500  
UID 104857600
```

上記は結果から UID 104857600 がマッピングされていることを確認できます。

次の例の場合、GID 104857608 のグループがマッピングされています。

```
# idmap_helper --src /var/cache/turboadc/idmap_adbindd.db \  
-q S-1-5-21-3233604394-866250274-1751313351-515  
GID 104857608
```

次は UID を指定した場合の例です。SID S-1-5-21-3233604394-866250274-1751313351-502 にマッピングされています。

```
# idmap_helper --src /var/cache/turboadc/idmap_adbindd.db \  
-q U104857604  
S-1-5-21-3233604394-866250274-1751313351-502
```

次は GID を指定した場合の例です。SID S-1-5-21-3233604394-866250274-1751313351-502 にマッピングされています。

```
# idmap_helper --src /var/cache/turboadc/idmap_adbindd.db \  
-q G104857608  
S-1-5-21-3233604394-866250274-1751313351-515
```

4.5.2.2 削除

```
# idmap_helper --src /var/cache/turboadc/idmap_adbindd.db -r query
```

パラメータ	説明
--src <i>targetdatapath</i>	ターゲットのマッピングテーブルファイルのパスを指定します。
-r <i>query</i>	<i>query</i> に指定した値とマッチするエントリを削除します。

GID104857608 を削除するには次のように実行します。

```
# idmap_helper --src /var/cache/turboadc/idmap_adbindd.db \  
-r G104857608
```

4.5.3 現在のマッピングリストの出力

現在のマッピングリストを出力します。書式は次の通りです。

```
# idmap_helper --src /var/cache/turboadc/idmap_adbindd.db -p file
```

パラメータ	説明
--src <i>targetdatapath</i>	ターゲットのマッピングテーブルファイルのパスを指定します。
-p <i>file</i> --dump <i>file</i>	<i>file</i> に指定したファイル名でマッピングリストを出力します。

ファイル (例は output.txt) に出力するには次のように実行します。

```
# idmap_helper --src /var/cache/turboadc/idmap_adbindd.db -p output.txt
```

画面に出力するには次のように実行します。

```
# idmap_helper --src /var/cache/turboadc/idmap_adbindd.db -p -
```

4.5.4 現在の UID/GID を指定範囲に移行

現行の UID と GID 範囲を指定範囲に移行することが可能です。

UID と GID 単独の移行ではなく、合わせての移行のみをサポートしています。

はじめに移行後のマッピングテーブルを作成します。書式は次の通りです。

```
# idmap_helper --src /var/cache/turboadc/idmap_adbindd.db ---dst newdbpath \  
-u min-UID -U max-UID -g min-GID -G max-GID --dump file
```

パラメータ	説明
--src <i>targetdatapath</i>	ターゲットのマッピングテーブルファイルのパスを指定します。
--dst <i>newdbpath</i>	移行後のマッピングテーブルファイルのパスを指定します。
-u <i>min-UID</i>	移行後の UID の最小値
-U <i>max-UID</i>	移行後の UID の最大値

<code>-g min-GID</code>	移行後の GID の最小値
<code>-G max-GID</code>	移行後の GID の最大値
<code>-p file</code> <code>--dump file</code>	<i>file</i> に指定したファイル名で実行結果を出力します。

UID 範囲を 1024～4096、GID 範囲を 1024～4096 に変更し、`idmap_adbindd_new.db` へ出力するには次のように実行します。

```
# idmap_helper --src /var/cache/turboadc/idmap_adbindd.db --dst \
  idmap_adbindd_new.db -u 1024 -U 4096 -g 1024 -G 4096 --dump result.txt
```

移行前の UID、Windows の SID、新 ID は `result.txt` ファイルに次の例のように出力されます。

```
UID 9000004 S-1-5-21-27361763-1365178067-2276120260-1105 1028
GID 800000 S-1-5-21-27361763-1365178067-2276120260-513 1024
```



存在する UID/GID 数と比較して移行先 UID/GID 範囲(使用できる ID の数)を少ない値で指定すると正常に移行できず不整合が生じます。ご注意ください。

移行後の UID/GID 範囲を Linux Connector for Active Directory で使用するには、`adbindd` サービスを停止してから、生成したマッピングテーブルファイル(例は `idmap_adbindd_new.db`)をマッピングテーブルファイル(デフォルトは `/var/cache/turboadc/idmap_adbindd.db`)に上書きします。

`adbindd` サービスを再起動すると有効になります。



`/var/cache/turboadc/idmap_adbindd.db` ファイルを置換する際は、あらかじめバックアップをとってください。

4.5.5 マッピングテーブルの完全な削除



使用中のマッピングテーブルを削除する場合は、`adbindd` デーモンを停止してから実行してください。

マッピングテーブルを完全に削除します。書式は次の通りです。

```
# idmap_helper --src idmap_adbindd_new.db --purge
```

パラメータ	説明
<code>--src targetdatapath</code>	ターゲットのマッピングテーブルファイルのパスを指定します。

<code>--purge</code>	マッピングテーブルを削除します。
<code>-p file</code> <code>--dump file</code>	<i>file</i> に指定したファイル名で実行結果を出力します。

ファイル(例は output.txt)に出力するには次のように実行します。

```
# idmap_helper --src idmap_adbindd_new.db -purge -p output.txt
```

第5章 SSO (シングルサインオン) 設定例

5.1 Apache の SSO 設定

5.1.1 前提条件

Apache に mod_auth_kerb モジュールがインストールされていること、コンパイル時に “--without-krb4” が指定されていることを確認してください。



TurboLinux 11 Server の場合、インストールタイプ “標準サーバー” ではインストールされません。アップデートサイトまたは製品付属の CD-ROM から mod_auth_kerb パッケージをインストールしてください。パッケージ管理について詳細は「TurboLinux 11 Server ユーザーガイド」をご確認ください。

5.1.2 設定例

5.1.2.1 Windows サーバー (ActiveDirectory ドメインコントローラ)

1. ドメインコントローラのコマンドプロンプトから setspn コマンドを実行し、HTTP サーバーの SPN (サービスプリンシパル名) を登録します。

```
c:\> setspn -A http/hostname.targetrealm.com hostname
```

2. 登録結果を次の通り確認できます。例のように HTTP/hostname.targetrealm.com の部分が登録されていることを確認してください。

```
c:\>setspn -L hostname
http/hostname.targetrealm.com
host/hostname.targetrealm.com
host/hostname
CIFS/hostname.targetrealm.com
CIFS/hostname
```



setspn コマンドについて詳細は、マイクロソフト社の Web サイトなどを参照してください。

5.1.2.2 Linux サーバー

1. Apache 設定ファイルの編集

/etc/httpd/conf/httpd.conf または、/etc/httpd/conf.d 以下の各ファイル等に次の例のような記述を確認してください。“<Directory “/var/www/html/ssotest/”>” の部分は環境に合わせて読み替えてください。

```
LoadModule auth_kerb_module modules/mod_auth_kerb.so

<Directory “/var/www/html/ssotest/”>
AllowOverride All
</Directory>
```



Turbolinux 11 Server の場合は、`/etc/httpd/conf.d/auth_kerb.conf` ファイル(以下記述)が読み込まれており、モジュールのロードは有効になっています。

```
LoadModule auth_kerb_module modules/mod_auth_kerb.so
```

その他の項目も適切に設定を完了してください。

2. .htaccess の編集

例の場合、`/var/www/html/ssotest/`以下に `.htaccess` ファイルを作成し以下を記述します。

```
AuthType Kerberos
AuthName "Kerberos"
KrbMethodNegotiate on
KrbMethodK5Passwd off
KrbVerifyKDC off
Krb5Keytab /etc/httpd/conf/httpd.tab
KrbAuthRealms TARGETREALM.COM
require valid-user
```

3. keytab ファイルの生成

次の通り実行しケルベロスの keytab ファイルを作成します。

```
# adjoin_cli -k /etc/httpd/conf/httpd.tab:HTTP/hostname.targetrealm.com
```

4. apache サービスが keytab ファイルへアクセスできるように次の通り実行します。

```
# chmod a+r /etc/httpd/conf/httpd.tab
```

5. サービスの起動

設定が完了したら `httpd` を起動します。Turbolinux 11 Server の場合は次のように実行します。

```
# /etc/init.d/httpd start
```

他のコンピュータからドメインにログインをしているユーザーは、`http://hostnmae.targetrealm.com/ssotest/`へアクセスする際に再度ログイン ID とパスワードを入力する必要がなくなり、シングルサインオンを実現します。

Firefox を使用してシングルサインオンに失敗する場合はロケーションバーに "about:config" と入力し次の "設定名" の "値" が "http://,https://" となっているか確認してください。



```
network.negotiate-auth.delegation-uris  
network.negotiate-auth.trusted-uris
```

これらの値は、グループポリシー "Firefox Policy" の "ブラウザで SPNEGO を許可される URI 一覧" "SPNEGO 認証において信頼された URI 一覧" を有効に設定することでユーザーのログイン時に自動的に設定することも可能です。詳細は「[2.21.2.Firefox Polic](#)」を参照ください。

5.2 SSH サーバーの SSO 設定

5.2.1 前提条件

OpenSSH のバージョン 4.2 以降をインストールしてください。



Turbolinux 11 Server の場合、インストールタイプ“標準サーバー”でバージョン 4.7p1 がインストールされますが、必ず “4.7p1-8” 以降にアップデートしてください。パッケージ管理について詳細は「Turbolinux 11 Server ユーザーガイド」をご確認ください。

5.2.2 設定例

5.2.2.1 Windows サーバー (ActiveDirectory ドメインコントローラ)

1. ドメインコントローラのコマンドプロンプトから `setspn` コマンドを実行し、SSH サーバーの SPN (サービスプリンシパル名) の登録を確認します。例のように `host/hostname.targetrealm.com` の部分が登録されていることを確認してください。

```
c:\>setspn -L hostname
http/hostname.targetrealm.com
host/hostname.targetrealm.com
host/hostname
CIFS/hostname.targetrealm.com
CIFS/hostname
```

2. 登録されていない場合は次のように実行し登録します。

```
c:\> setspn -A HOST/hostname.targetrealm.com hostname
```



`setspn` コマンドについて詳細は、マイクロソフト社の Web サイトなどを参照してください。

5.2.2.2 Linux システム (SSH サーバー)

1. `/etc/ssh/sshd_config` (SSH サーバーの設定ファイル) の編集
次の記述を確認してください。

```
GSSAPIAuthentication yes
GSSAPICleanupCredentials yes
```

2. `keytab` ファイルの生成

次の通り実行しケルベロスの `keytab` ファイル (`/etc/krb.keytab`) を作成します。

```
# adjoint_cli -k host/hostname.targetrealm.com
```

3. .k5login ファイルの編集

ログイン先 SSH サーバーのホームディレクトリ下に .k5login ファイルを用意しサーバー側のユーザー (administrator や taro など)のエントリを追加してください。

例えば、taro ユーザーのホームディレクトリが/home/TARGETREALM/TARO/ の場合、/home/TARGETREALM/TARO/.k5login ファイルに以下を記述します。

```
taro@TARGETREALM.COM
```

4. SSH サーバーのホストネーム

SSH サーバーのホストネームが適切に設定されいていることを確認してください。hostname コマンドを実行して確認できます。

5. SSH サーバーでサービスの起動

設定が完了したら sshd を起動します。Turbolinux 11 Server の場合は次のように実行します。

```
# /etc/init.d/sshd start
```

5.2.2.3 Linux システム (SSH クライアント)

6. /etc/ssh/ssh_config (SSH クライアントの設定ファイル) の編集

次の記述を確認してください。

```
GSSAPIAuthentication yes  
GSSAPIDelegateCredentials yes
```

7. SSH クライアントの逆引き指定 (SSH クライアント)

DNS サーバーまたは/etc/hosts ファイルを設定し SSH クライアントの逆引き名前解決が確実に行えるようにしてください。逆引きに問題があると SSO に失敗します。

SSH クライアントに taro がログインをしているとき、ssh hostname.targetrealm.com コマンドを実行しユーザー名/パスワード無しでリモートログインが可能となりシングルサインオンを実現します。

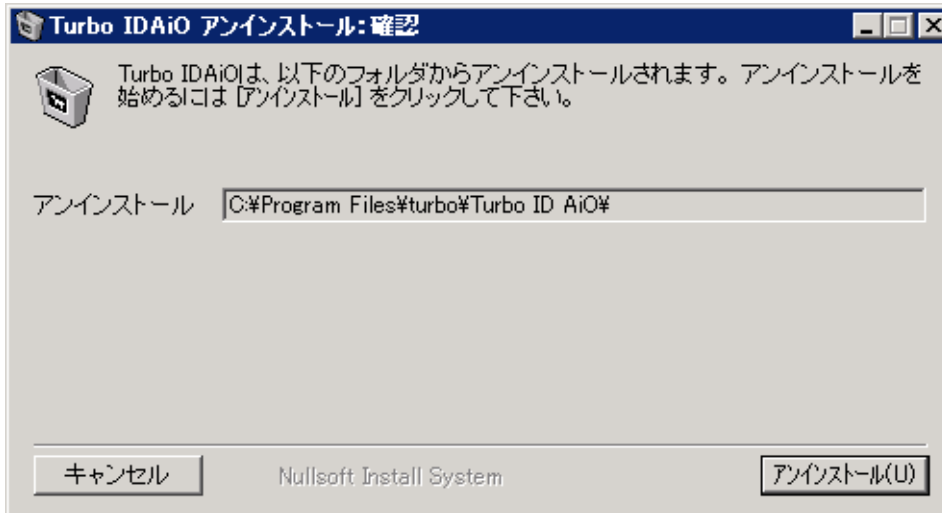
セパレーターが¥(バックスラッシュ)の場合、指定形式は以下のようになります。

```
$ ssh DOMAINNAME¥\USERNAME@HOSTNAME
```

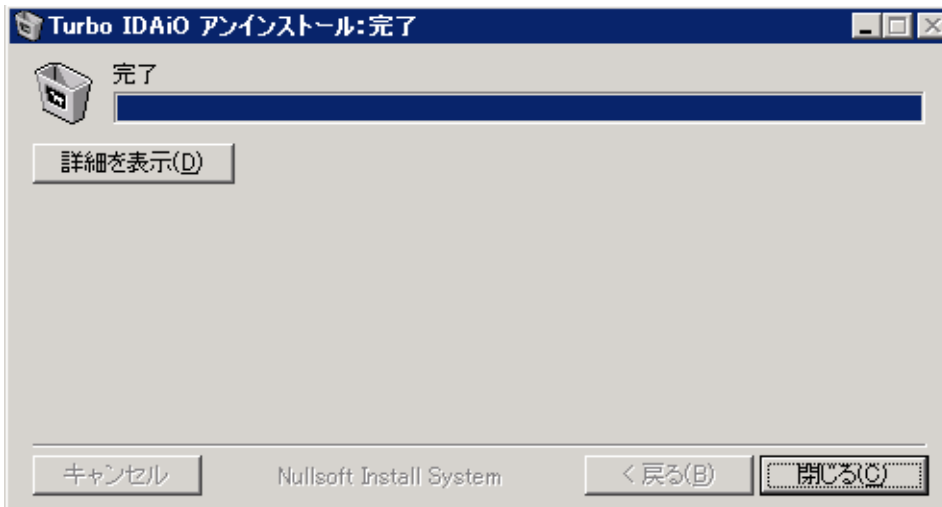
第6章 アンインストール

6.1 Turbo ID AIO 管理コンソールのアンインストール

管理者権限のユーザーで Windows システムにログインし、スタートメニュー -> “すべてのプログラム” -> “turbo” -> “Turbo ID AIO” -> “アンインストール Turbo ID AIO 管理コンソール” をクリックします。次の画面が表示されたら[アンインストール]を選択します。



次のように表示されたら[閉じる]ボタンをクリックして終了してください。



パッケージをアンインストールしても、拡張した ActiveDirectory のスキーマは削除されません。通常はそのままの状態でも問題はありませんが、元の状態に戻す場合は、試用前のバックアップから ActiveDirectory のデータベースを復元してください。

6.2 Linux Connector for Active Directory のアンインストール

/etc/krb5.confファイルの設定(「[3.3.2.設定ファイルの編集](#)」参照)を元に戻してから、root ユーザーで次のように実行し RPM パッケージをアンインストールします。

```
# rpm -e turboadconnector-gp turboadconnector turboadconnector-netlogon
```

付録 I. 設定例ご紹介



ここでは、設定例をご紹介します。最新の情報は、ターボリナックス社の Web サイトも合わせて参照してください。

<http://www.turbolinux.co.jp/>

A. Postfix / Dovecot の設定例

ActiveDirectory によって 認証されたアカウントは Linux サーバー上で “**レルム名¥ユーザー名**” として認識されます。通常、メールボックス形式のメールサーバーではメールスプールが /var/sppol/mail/**ユーザー名** のように扱われるので、いくつかの設定が必要になります。Postfix + Dovecot の環境で POP および IMAP 認証を行う際の基本的な設定方法について解説します。

● 環境

本ガイドは以下の環境を前提としています。

- Postfix
- Dovecot(1.2.4-1 以降)

Dovecot のバージョンについて



Turbolinux 11 Server の場合は、必ず 1.2.4-1 以降を使用してください。また、Dovecot.1.1-8 未満の場合、Linux Connector for Active Directory による POP / IMAP 認証に失敗しますので、他のディストリビューションでご利用の場合も、必ず 1.1-8 以降にアップデートするようにしてください。



Turbolinux 11 Server の場合、デフォルトで UW IMAP がインストールされますが、Linux Connector for Active Directory による認証を行うためには Dovecot のインストールが必要です。turbo+ を利用して Dovecot をインストールしてください。パッケージ管理については「Turbolinux 11 Server ユーザーガイド」をご確認ください。

既に、UW-IMAP を有効にしている場合、/etc/xinetd.d/ipop3 および /etc/xinetd.d/imap ファイルの以下部分を編集し無効に設定してください。

```
disable = yes
```

設定を変更した場合は、xinetd を再起動し反映します。

```
# /etc/init.d/xinetd restart
```

● Linux Connector for Active Directory の設定

Linux システムで “**レルム名¥ユーザー名**” のレルム名を省略して “**ユーザー名**” として扱えるようにするために /etc/turboadc/config.xml ファイルの <defaultrealm> にデフォルトのレルム名を以下例のように指定します。

```
<?xml version="1.0" encoding="UTF-8"?>
<turboadcconnector>
  <config>
    <adbindd>
```

```

<idmap>
  <uid>
    <high>209715100</high>
    <low>104857600</low>
  </uid>
  <gid>
    <high>209715100</high>
    <low>104857600</low>
  </gid>
</idmap>
<defaultrealm>TARGETREALM</defaultrealm>
<useoffline>1</useoffline>
<offlinetime>360000</offlinetime>
</adbindd>
<realms>
  <realm>
    <fqdn>TARGETREALM.COM</fqdn>
    <netbiosname>TARGETREALM</netbiosname>
    <IDAiOTech>1</IDAiOTech>
  </realm>
</realms>
</config>
</turboadconnector>

```

設定を変更した場合は必ず adbindd を再起動してください。

```
# /etc/init.d/adbind restart
```

● Dovecot の設定



Dovecot のインストールは完了し、環境に合わせた適切な設定は完了している前提です。以降は、`/var/spool/mail/ユーザー名` にスプールするメールボックス形式のメールメールサーバーで Linux Connector for Active Directory による認証を行う際に、関連する項目について解説しています。

次の例のように `/etc/dovecot.conf` の該当部分を編集します。

```

protocol imap {
  mail_executable = /etc/dovecot_imap
}

protocol pop3 {
  mail_executable = /etc/dovecot_pop3
}

passdb pam {
  args = session=yes dovecot
}

```

上記で指定した `/etc/dovecot_imap`、`/etc/dovecot_pop3` (パス名は任意)を以下の内容で用意します。**TARGETREALM**には実際に取り除くレルム名を指定してください。例は、セパレータにデフォルト値の `'¥'` を使用し、メールスプール (`/var/spool/mail/ユーザー名`)、mbox をホームディレクトリの `mbox` ディレクトリとしている場合です。セパレータを変更している場合や、メールスプールなどの設定は環境に合わせて適宜読み替えてください。

/etc/dovecot_imap の例

```
#!/bin/sh
export MAIL=mbox:~/mail:INBOX="/var/spool/mail/${USER#TARGETREALM}\'"
exec /usr/libexec/dovecot/imap $*
```

/etc/dovecot_pop3 の例

```
#!/bin/sh
export MAIL=mbox:~/mail:INBOX="/var/spool/mail/${USER#TARGETREALM}\'"
exec /usr/libexec/dovecot/pop3 $*
```

設定が完了したら Dovecot を起動します。

```
# /etc/init.d/dovecot start
```



再起動するには以下の通り実行します。

```
# /etc/init.d/dovecot restart
```

次のシステム起動時にも有効にするには以下の通り実行します。

```
# chkconfig dovecot on
```



Maildir 形式の場合、レールム名を取り除くための設定は必要ありません。以下の例のように /etc/dovecot.conf のコメント記号を削除して mail_location を適切に設定し、passdb pam の設定を行ってください。

```
mail_location = maildir:~/Maildir
...
passdb pam {
  args = session=yes dovecot
}
```

● 制限事項

Maildir 形式の場合は、メールサーバーにメールアカウントのホームディレクトリが作成されるまではメールの受信を行うことができません。メールアカウントではじめて POP 認証を行った時またはメールサーバーにログインした時には自動でホームディレクトリが作成されます。

B. ProFTPD の設定例

ActiveDirectory メンバーサーバーの提供する FTP サービスへのアクセスに、ActiveDirectory のユーザー 認証を利用する場合の設定例を紹介します。

● 環境

本ガイドは以下の環境を前提としています。

- ProFTPD (FTP サーバー)

● Linux Connector for Active Directory の設定

ftp クライアントからのログイン時、“レルム名¥ユーザー名”のレルム名を省略して“ユーザー名”として扱えるようにするためには /etc/turboadc/config.xml ファイルの <defaultrealm> にデフォルトのレルム名を以下例のように指定します。

```
<?xml version="1.0" encoding="UTF-8"?>
<turboadconnector>
  <config>
    <adbindd>
      <idmap>
        <uid>
          <high>209715100</high>
          <low>104857600</low>
        </uid>
        <gid>
          <high>209715100</high>
          <low>104857600</low>
        </gid>
      </idmap>
      <defaultrealm>TARGETREALM</defaultrealm>
      <useoffline>1</useoffline>
      <offlinetime>360000</offlinetime>
    </adbindd>
    <realms>
      <realm>
        <fqdn>TARGETREALM.COM</fqdn>
        <netbiosname>TARGETREALM</netbiosname>
        <IDAiOTech>1</IDAiOTech>
      </realm>
    </realms>
  </config>
</turboadconnector>
```

設定を変更した場合は必ず adbindd を再起動してください。

```
# /etc/init.d/adbind restart
```



defaultrealm を指定しない場合、“レルム名¥ユーザー名”と入力してログインする必要があります。

● ProFTPD の設定



ProFTPD のインストールは完了し、環境に合わせた適切な設定は完了している前提です。

/etc/proftpd.conf の mod_auth.c モジュールに関連する次のディレクティブを編集します。例は、Turbolinux 11 Server の場合で、CreateHome と PersistentPasswd ディレクティブを追加します。

CreateHome ディレクティブを有効に設定することで、認証されたユーザーのホームディレクトリが存在しないとき、新たに作成します。

```
# Use pam to authenticate (default) and be authoritative
AuthPAMConfig          proftpd
AuthOrder               mod_auth_pam.c* mod_auth_unix.c
CreateHome              on
PersistentPasswd       off
```

設定が完了したら proftpd を起動します。

```
# /etc/init.d/proftpd start
```



再起動するには以下の通り実行します。

```
# /etc/init.d/proftpd restart
```

次のシステム起動時にも有効にするには以下の通り実行します。

```
# chkconfig proftpd on
```

ftp クライアントからアクセスし動作を確認してください。