HP OpenVMS CIFS Version 1.2 ECO1 管理者ガイド

2011 年 10 月
第 1.0 版

著作権情報

原典

『HP OpenVMS CIFS Version 1.2 ECO1 Administrator's Guide』 2011 Hewlett-Packard Development Company, L.P.

目次

図目次

表目次

例目次

まえがき

このドキュメントは，HP CIFS Server 製品のインストール，構成，および管理方法について説明してます。『The Samba HowTo Collection』および『Using Samba, 2nd Edition』の内容を補足し OpenVMS に関する情報を追加しています。

本書の対象読者

このドキュメントは，OpenVMS のシステム管理者およびネットワーク管理者を対象にしています。HP CIFS Server については下記の URL の HP CIFS の Web サイトおよびドキュメントも参照してください。

http://h50146.www5.hp.com/products/software/oe/openvms/network/cifs/

本書の構成

本書の構成は以下のとおりです。

第1章 HP CIFS Server について

HP CIFS Server のアーキテクチャ，機能の概要，利用できるドキュメント，などについて紹介します。

第2章 HP CIFS Server のインストールおよび構成

HP CIFS Server のインストールおよび構成の手順について説明します。

第3章 HP CIFS の導入モデル

Samba ドメインモデル，HP CIFS Server のみの環境，あるいは Microsoft NT プライマリ・ドメインコントローラ (PDC) を使用した NT ドメイン環境のそれぞれの導入モデルに関して，NT スタイルのドメインで HP CIFS Server が動作するように環境を構成する方法について説明します。

第4章 Kerberos のサポート

Kerberos プロトコルについて説明します。典型的な Kerberos ログインと Kerberos 認証を使用した共有サービス交換の例についても示します。

第5章 LDAP 統合のサポート

HP Enterprise Directory，HP LDAP Integration 製品，および HP CIFS Server ソフトウェア (LDAP 機能のサポート付き) をインストール，構成，確認する方法について説明します。

第6章 ユーザとグループのマッピング

HP CIFS Server でユーザおよびグループを管理する方法について説明します。この章では，HP CIFS Server が Windows あるいは CIFS ドメインのユーザ およびグループを OpenVMS ユーザとリソース ID にマッマッピングする ためのいくつかの方法についても説明します。

第7章 WINBIND のサポート

`winbind` をサポートするように HP CIFS Server を設定および構成する方法について説明します。

第8章 ユーザ，グループ，アカウント・ポリシー，信頼関係の管理

`SAMBA$MANAGE_CIFS.COM` で HP CIFS Server のユーザ，グループ，アカウントの ポリシーおよび信頼を管理する方法について説明します。ユーザ，グループ，アカウントのポリシーおよび信頼を管理するためのコマンドについても説明します。

第9章 共有の管理

HP CIFS Server を使用して共有とプリンタを管理する方法について説明します。

第10章 ファイルとプリントのセキュリティ

HP CIFS Server が Windows パーミッションを OpenVMS ファイル・セキュリティにマップする方法と，リソースへのアクセスを管理する方法について説明します。

第11章 管理ツールのコマンド・リファレンス

pdbedit や smbclient などのネイティブの Samba ユーティリティも含め，HP CIFS for OpenVMS で提供しているいくつかの管理ツールについて説明しています。

第12章 性能に関する注意事項とトラブルシューティング

HP CIFS Server の性能を改善する方法と 性能に関する問題を解決する方法について説明します。

第13章 SMB.CONF パラメータ

HP CIFS Server の変更可能な構成パラメータ，変更できない構成パラメータ，およびサポートされていない構成パラメータ について説明します。

付録 A インストレーションと削除の実行例

HP CIFS Server のインストールと削除の実行例を示します。

本書の表記法

本書では，以下の表記法を使用します。

表 1 表記法

表記法	意味
	例の中でこの水平方向の反復記号が使用されている場合は，次のいずれかを示します。 • 文中のその他のオプション引数が省略されている。 • 先行する 1 つまたは複数の項目を繰り返すことができる。 • パラメータや値などの情報をさらに入力できる。 垂直方向の反復記号は，コードの例やコマンド形式の中で項目が省略されていることを示します。 この反復記号で項目が省略されている場合は，その部分が説明の内容にとって重要ではないことを意味しています。
( )	コマンド形式の記述でこの記号が使用されている場合は，選択オプションを複数個指定するときにそれらの選択オプションを括弧で囲む必要があることを示します。 インストールやアップグレードの表示例では，次に示すように，プロンプトに対する回答の候補を示します。 `Is this correct? (Y/N) [Y]`
[ ]	コマンド形式の記述で項目が大括弧で囲まれている場合は，その項目が選択オプションであることを示します。項目を 1 つ以上選択することも，すべて省略することもできます。コマンド行には，項目を囲んでいるこの大括弧を入力しないでください。 ただし，OpenVMS のディレクトリ指定構文や，代入文の部分文字列指定構文に含まれる大括弧は，省略できません。 インストールやアップグレードの表示例で項目が大括弧によって囲まれている場合は，プロンプトに対するデフォルトの回答を示します。 値を入力しないで **Enter** を押すと，デフォルトの回答が入力されたものとして処理されます。 次に，その例を示します。 `Is this correct? (Y/N) [Y]`
{ }	コマンド形式の記述で項目が中括弧で囲まれている場合は，その項目が必須の選択オプションであることを示します。 少なくとも 1 つの項目を指定する必要があります。 コマンド行には，この中括弧を入力しないでください。
`Example`	この (等幅) フォントは，コード例，コマンド例，または会話操作中の画面出力を示します。 本文中では，OpenVMS コマンドやパス名，PC のコマンドやフォルダ名，または C プログラミング言語の特定要素を示すこともあります。
`italic type`	イタリック体のテキストは，重要な情報，ドキュメントの正式なタイトル，または変数を示します。 変数は，システムからの出力 (たとえば「Internal error `number`」)，コマンド行 (たとえば「/PRODUCER=`name`」)，または本文中のコマンド・パラメータ (たとえば「`dd` はデバイスの種類を表すコードです」) というように，一定でない情報を表します。
UPPERCASE TYPE	大文字の英文テキストは，コマンド，ルーチン名，ファイル名，またはシステム特権の短縮形を示します。 コマンド形式の記述，コマンド行，またはコード行の末尾にあるハイフンは，コマンドや文が次の行まで続いていることを示します。

第1章 HP CIFS Server について

この章では，HP CIFS Server について概要を説明します。 以下の項目について説明します。

- 1.2 項「オープンソース・ソフトウェア Samba Suite」
- 1.3 項「HP CIFS Server のドキュメント: オンライン」
- 1.4 項「HP CIFS Server のディレクトリ構成」

1.1 HP CIFS Server について

HP CIFS Server は，OpenVMS 上で Microsoft Common Internet File System (CIFS) プロトコルに基づいた分散ファイルシステム機能を提供します。

本バージョンの HP CIFS Server は，オープンソース・ソフトウェアである Samba version 3.0.28a をベースにしており，Windows 2000，2003，XP，Vista，および Windows 7 の CIFS クライアントに対してファイル・サービスとプリント・サービスを提供します。

1.1.1 CIFS プロトコルとは？

CIFS (Common Internet File System) は，リモート・ファイルアクセスのための Windows の仕様です。

CIFS は，1980 年代後半，当時開発されていた Ethernet などのローカル・エリア・ネットワーク技術を利用して PC 向けに開発されたファイル共有のための Server Message Block (SMB) プロトコルとも呼ばれるネットワークプロトコルを起源に持ちます。 SMB は Microsoft Windows システムのネイティブのファイル共有プロトコルで，社内ネットワークで多数の PC ユーザがファイルおよびプリンタを共有するための標準的な方法です。

CIFS は SMB を単に名称変更したもので，CIFS と SMB は実質的には同じものです (Microsoft 社は，現在も SMB と呼ぶことがありますが，最近では CIFS と呼ぶことが増えています)。 CIFS は，UNIX，OpenVMS，Macintosh，その他のプラットフォームで広く利用されています。

その名称にも関わらず，CIFS は実際にはファイルシステムではありません。 より正確に言うならば，CIFS は，リモート・システム上のファイルへのアクセスを提供するリモート・ファイルアクセス・プロトコルです。 CIFS は，ホスト・システムのファイルシステム上に存在し，そのファイルシステムに対して機能します。 CIFS はサーバーとクライアントを定義し，CIFS サーバー上のファイルへのアクセスには CIFS クライアントが使用されます。

HP CIFS は OpenVMS 上で CIFS プロトコルを提供し，Windows クライアントから OpenVMS ディレクトリおよびプリンタへのアクセスを可能にしています。

1.2 オープンソース・ソフトウェア Samba Suite

HP CIFS Server のソースは，1991 年にオーストラリアの Andrew Tridgell 氏によって開発されたオープンソース・ソフトウェア (OSS) である Samba をベースにしています。 この節では，Samba 製品について概要を説明します。 Samba については多数の書籍が出版されており，オンラインでも情報が提供されていますので，Samba の詳細についてはそれらのドキュメントを参照することをお勧めします。 いくつかの情報は Samba の開発メンバー自身によって書かれています。

1.2.1 オープンソース・ソフトウェア

Samba は，GNU Public License (GPL) の規約のもとで利用できます。 現在のバージョンの Samba は GPLV3 ライセンスのもとでリリースされています。

GNU Public License についての詳細は下記の URL を参照してください。

http://www.fsf.org

1.2.2 Samba サーバー

1.2.2.1 概要

HP OpenVMS CIFS はオープンソースの Samba ソフトウェアをベースにしています。

http://www.Samba.org では次のように 紹介されています。

「Samba はオープンソースのフリーソフトウェアで， SMB/CIFS クライアントに対してシームレスなファイルサービスおよび プリントサービスを提供します。 Samba は無料で利用でき，SMB/CIFS の他の実装とは異なり， Linux/Unix サーバーと Windows クライアント間の相互運用が可能です。 Samba は，UNIX，Linux，IBM System 390，OpenVMS オペレーティング・システムなど， Microsoft Windows 以外のプラットフォーム上でも実行可能です。 Samba は，ホスト・サーバーにインストールされている TCP/IP プロトコルを使用します。正しく構成されていれば， それらのホストは Windows のファイルおよびプリントサーバーと同じように，Microsoft Windows クライアントあるいはサーバーと通信することができます。」

Samba は Microsoft の Common Internet File System (CIFS) プロトコルに基づいています。 CIFS プロトコルは，ネットワーク経由で別のシステムと通信するのに 主に Server Message Block (SMB) コマンドを使用します。

Samba は世界規模の開発者コミュニティーで開発されているオープンソース製品です。Windows オペレーティング・システムの新しいリリースに対応しており， Windows システムとのシームレスな統合を提供しています。 OpenVMS カスタマーに Windows の新しいリリースに対応した ファイルおよびプリント・サービスを提供するために Open Source Samba が HP OpenVMS にポーティングされました。従来のファイルおよびプリント・サービスである Advanced Server for OpenVMS の 後継製品と位置付けられています。 HP OpenVMS CIFS は，OpenVMS Alpha V8.3 以降および OpenVMS Integrity V8.3 以降でサポートされます。

1.2.2.2 機能

HP OpenVMS CIFS の主な機能は以下のとおりです (本書では，HP OpenVMS CIFS を HP CIFS Server と呼びます)。

- 1.2.2.2.1 項「ドメイン・サポート」
- 1.2.2.2.2 項「認証」
- 1.2.2.2.3 項「クラスタ・サービス」
- 1.2.2.2.4 項「ブラウジング」
- 1.2.2.2.5 項「ファイルおよびプリント・サービス」
- 1.2.2.2.6 項「ファイルおよびプリント・セキュリティ」

以降の項でこれらの機能について詳しく説明します。

1.2.2.2.1 ドメイン・サポート

HP CIFS Server は，ユーザの認証と承認に Kerberos と LDAP を使用して，Active Directory ドメインにおけるネイティブのメンバーサーバーとして機能することができます。 HP CIFS Server は，任意のドメインで NT4 スタイルのメンバーサーバーとしても 機能します。

HP CIFS Server は NT4 スタイルのプライマリ・ドメイン・コントローラ (PDC) として動作することができますが，そのようなドメインでは HP CIFS Server を実行するバックアップ・ドメイン・コントローラ (BDC) のみを 含みます。 同様に，PDC が HP CIFS Server を実行している場合は NT4 スタイルの BDC として動作することができます。 ただし，HP Advanced Server for OpenVMS や Windows ドメイン・コントローラ の場合と異なり，HP CIFS Server を含む Samba ドメインコントローラ間で ユーザアカウント・データベースの自動複製はサポートされません。 Samba ドメイン・コントローラが アカウント・データベースの自動複製を実行するには， LDAP サーバーの支援を必要とします。

LDAP バックエンドを使用するように HP CIFS PDC および BDC を構成することにより， アカウント・データベースは LDAP サーバーと同期して複製されます。 HP CIFS Server は，LDAP バックエンド (HP Enterprise Directory あるいは OpenLDAP サーバーなど) を使用して LDAP ディレクトリのユーザおよびグループ情報を保管および取得することができます。 1 つの LDAP

サーバーを HP CIFS Server PDC および BDC の両方に使用することはできますが，可用性と性能の観点から，別々の LDAP サーバーを使用することをお勧めします。

1.2.2.2.2 認証

HP CIFS Server は，各共有にアクセスする際にパスワードを提供するベーシックで若干安全性に劣る共有レベルのセキュリティと，共有にアクセスする前にユーザ名とパスワードを使用して HP CIFS Server との接続を確立する必要がある，より安全性の高いユーザ・レベルのセキュリティをサポートします。

ユーザ・レベルのセキュリティでは， HP CIFS Server は以下の認証メカニズムをサポートします。

- LM : Windows 95 や Windows 98 システムなどの古い Windows システムで使用されます。
- NTLM : Windows NT 以降で使用されます。
- NTLMv2 : Windows NT 以降で使用されます。
- Kerberos : ネイティブの Active Directory ドメイン・メンバーで使用されます。

HP CIFS Server は以下の機能も提供します。

- NTLM および NTLMv2 認証のための NTLMSSP(NT LAN Manager Security Support Provider) のサポート
- ドメイン・メンバーとドメイン・コントローラ間で，署名付きで暗号化されたセキュリティ・チャネル・データを提供することによるセッションのセキュリティ確保。 64 ビットあるいは 128 ビットの暗号化キーをサポートします。
- SMB サインあるいはセキュリティ署名

1.2.2.2.3 クラスタ・サービス

HP CIFS Server は， OpenVMS Cluster 内の単一のノードにインストールして使用することも，同じディレクトリを共有するマルチノード・クラスタ環境で共有ディレクトリにインストールして使用することも可能です。

単一ノードへのインストールの場合，各クラスタノードで異なるエンティティとして HP CIFS Server をインストールし，HP CIFS Server の任意の役割で機能させることできます。 この結果，各ノードは，クラスタ化されていない OpenVMS システムのように動作します。 このような環境では，HP CIFS Server がインストールされた各ノードは，同じインストール・ディレクトリを共有すべきではなく，また，複数のクラスタ・メンバーからのディレクトリあるいはファイルへの同時アクセスも許可すべきではありません。

複数のクラスタ・メンバーで単一の HP CIFS Server インストレーション，構成ディレクトリ，およびデータ・ファイルを共有するような，一般的なクラスタ構成も可能です。 このような環境では，HP CIFS Server は単一のドメイン・エントリのように機能します。

1.2.2.2.4 ブラウジング

HP CIFS Server は，通常の Windows ブラウザ・サービス機能をサポートします。 このブラウザ・サービス機能は，Windows の「マイネットワーク」の表示の際に使用されます。

1.2.2.2.5 ファイルおよびプリント・サービス

HP CIFS Server は，OpenVMS のファイルおよびプリンタ・リソースをネットワーク・クライアントで共有すること可能にします。これにより，それらの共有されたファイルおよびプリンタが各クライアント・システムにローカルに存在するかのように表示させることができます。このためユーザは，クライアント・システムで利用可なインタフェースを使用して，共有されたファイルおよびプリンタをシームレスに扱うことができます。

HP CIFS Server は，ODS-2 および ODS-5 ボリューム上に存在するファイルをサポートします。 HP CIFS Server は，異なる OpenVMS ファイル形式およびファイル編成のファイルを Windows クライアントにストリーム形式で提供することができます。 この結果，Windows クライアントで異なる形式のファイルが読み取り可能になります。 HP CIFS Server は，Stream，Stream_LF，

Fixed，Undefined など，いくつかの形式でファイルを作成します。 デフォルトでは，HP CIFS Server は ASCII 文字セットをサポートします。 また，ヨーロッパ言語の文字のための拡張 ASCII 文字セット (CP850/ISO-8859-1)，UTF-8 文字セット，および日本語文字のための日本語文字セット (VTF-7) もサポートします。

HP CIFS Server の印刷サービスを使用すると，OpenVMS プリントキューが存在するプリンタ (あるいは OpenVMS ホストに直接接続されたプリンタ) を共有することができます。 これらのプリントキューは，DCPS，TELNETSYM，LAT，あるいは LPD を使用して設定することができます。 HP CIFS Server は，以下のような NT スタイルの印刷機能をサポートします。

- プリンタドライバ・ファイルを Windows クライアントにローカルにダウンロードする。
- プリンタドライバ・ファイルを Windows クライアントから HP CIFS Server へ アップロードする。

1.2.2.2.6 ファイルおよびプリント・セキュリティ

どのようなファイルおよびプリント・サービスにおいても，セキュリティについて考慮することが重要になります。 OpenVMS ベースのセキュリティに加えて NT ACL ベースのファイルおよびプリンタ・セキュリティを提供する Advanced Server for OpenVMS とは異なり，HP CIFS Server は，OpenVMS のファイル・セキュリティを使用してファイルおよびプリンタに対するセキュリティを提供します。 HP CIFS Server は，ファイルおよびディレクトリに適用される Windows セキュリティを OpenVMS のファイル・セキュリティにマッピングします。 ファイルおよびプリンタ・セキュリティの設定は，任意のユーザあるいはグループに対して行うことができます。

HP CIFS Server では独自のセキュリティ監査機能は提供しませんが，OpenVMS の標準の 監査機能が使用できます。

1.2.2.3 HP CIFS Server の構成要素

上記のような機能を提供する HP CIFS Server の主な構成要素は以下のとおりです。

- 1.2.2.3.1 項 「SMBD プロセス」
- 1.2.2.3.2 項 「NMBD プロセス」
- 1.2.2.3.3 項 「WINBIND」

1.2.2.3.1 SMBD プロセス

各クライアント・セッションは新しい SMBD プロセスを生成します。 SMBD プロセスは，クラスタ・サービス，認証，ファイルおよびプリンタ・サービス， および HP CIFS Server ファイル・セキュリティ・マッピング機能をサポートします。

1.2.2.3.2 NMBD プロセス

NMBD プロセスは，NetBIOS 名前登録および解決機能を除き，従来の Windows ブラウザ・サービス機能を提供します。

1.2.2.3.3 WINBIND

WINBIND は，OpenVMS の UIC およびリソース識別子，入れ子グループ (グループ内のグループ)，および信頼機能へ Windows のドメイン・ユーザおよびグループを自動マッピングするための機能です。

Linux などのプラットフォームでは，Samba は WINBINDD と呼ばれるプロセスによって WINBIND 機能を提供しますが，OpenVMS では各 SMBD プロセスに WINBIND 機能が組み込まれています。

1.3 HP CIFS Server のドキュメント: オンライン

HP CIFS Server のドキュメントは以下のサイトで参照できます。

http://h50146.www5.hp.com/products/software/oe/openvms/network/cifs/

また，HP CIFS Server のドキュメント以外に，以下の Samba のドキュメントも参照することをお勧めします。

- 『The Official Samba-3 HOWTO and Reference Guide』 (John H. Terpstra，Jelmer R. Vernooij 著，ISBN: 0-13-145355-6)
- 『Samba-3 by Example Practical Exercises to Successful Deployment』 (John H. Terpstra 著，ISBN: 0-13-147221-6)
- 『Using Samba, 2nd Edition』 (Robert Eckstein，David Collier-Brown，Peter Kelly，Jay Ts 著，O'Reilly 2000，ISBN: 0-596-00256-4)
- 『Samba, Integrating UNIX and Windows』 (John D Blair 著，Specialized Systems Consultants, Inc.,1998，ISBN: 1-57831-006-7)
- Samba の Web サイト: http://www.samba.org/samba/docs .

HP CIFS Server を使用する際には，『The Samba HOWTO Collection』，『Samba-3 by Example』，および『Using Samba, 2nd Edition』を参照することをお勧めします。 これらのドキュメントは，Samba Web Administration Tool (SWAT) でも参照することができます。

重要: 『Using Samba, 2nd Edition』は，Samba の以前のバージョンである Samba V.2.0.4 について説明しています。 ただし，『Using Samba, 2nd Edition』で説明されている情報の多くは，本バージョンの HP CIFS Server にも適用できます。 HP CIFS Server についての最新の情報は SWAT のヘルプ機能で確認することができます。

注記:

- HP が作成したものでない一般の Samba のドキュメントには，Samba の将来のリリースでサポートされる機能について説明している場合があります。 これらのドキュメントの著者は，既存の Samba リリースで提供している機能と将来の Samba リリースで提供する予定の機能とを明確に区別して記述しているとは限りません。
- UNIX/Linux 版 Samba で提供しているすべての機能が HP OpenVMS CIFS でサポートされているわけではありません。 OpenVMS 版で提供している機能については，『HP OpenVMS CIFS リリース・ノート』を参照してください。

1.4 HP CIFS Server のディレクトリ構成

HP CIFS Server 製品のデフォルトのベース・インストレーション・ディレクトリは SAMBA$ROOT です。 HP CIFS の構成ファイルは SAMBA$ROOT:[LIB] ディレクトリにインストールされます。 HP CIFS Server のログ・ファイルおよび一時ファイルは SAMBAS$ROOT:[VAR] ディレクトリに作成されます。

表 1-1 に HP CIFS Server の重要なディレクトリとファイルを示します。

表 1-1 HP CIFS のファイルとディレクトリ

ファイル/ディレクトリ	説明
SAMBA$ROOT:[000000]	HP CIFS Server のベース・ディレクトリです。
SAMBA$ROOT:[SRC]	HP CIFS Server のソース・コードが含まれているディレクトリです。
SAMBA$ROOT:[BIN]	HP CIFS Server のデーモンおよびユーティリティなどのバイナリが含まれているディレクトリです。 システム・ブート時に HP CIFS Server を起動し，システム・シャットダウン時に HP CIFS Server を停止させるためのコマンド・スクリプトも含まれています。
SAMBA$ROOT:[DOC]	PS (PostScript) など種々のフォーマットの HP CIFS Server のドキュメントが含まれています。
SYS$COMMON:[SYSHLP]	HP CIFS Server のリリース・ノートが含まれています。
SAMBA$ROOT:[SWAT]	SWAT (Samba Web Administration Tool) の html およびイメージファイルが含まれています。

表 1-1 HP CIFS のファイルとディレクトリ (続き)

ファイル/ディレクトリ	説明
SAMBA$ROOT:[VAR]	HP CIFS Server のログ・ファイル，および HP CIFS Server が使用するロック・ファイルなど，その他の動的に作成されるファイルが含まれています。
SAMBA$ROOT:[LIB]SMB.CONF	HP CIFS Server の構成ファイルです。
SAMBA$ROOT:[UTILS]	SWAT ユーティリティの OpenVMS 用セーブセットが含まれています。
SAMBA$ROOT:[LICENSES]	このディレクトリには GPLV3 ライセンスについて説明したファイルが含まれています。

第2章　HP CIFS Server のインストールおよび構成

この章では，HP CIFS Server ソフトウェアのインストールおよび構成の手順について説明します。 以下のような項目について説明します。

2.1 HP CIFS Server の要件と制約

HP CIFS Server をインストールする前に，ご使用のシステムが以下の要件および制約を満たすことを確認してください。

2.1.1 必要なディスクスペース

HP CIFS Server のインストレーションには，OpenVMS Alpha の場合は約 32.68 MB， OpenVMS Integrity の場合は約 40 MB のディスク容量が必要です。 HP CIFS Server は，以下のようなコンポーネントで構成されています。

- HP CIFS の実行および監視のためのユーティリティ — 92 KB
- デーモン・プロセス・バイナリ — 13 MB
- HP CIFS のソース・ファイル (.BCK) — 23 MB
- SWAT 管理ツール — 13 MB
- ドキュメント — 1 MB

注記:　HP CIFS Server の実行には HP CIFS Server のソース・ファイルは必要ありません。ソース・ファイルをインストールせずに削除するかどうか選択することができます。ソース・コードのバックアップ・セーブセットは `SAMBA$ROOT:[SRC]` に含まれます。

2.1.2 ソフトウェアの要件

HP CIFS Server のソフトウェア要件は以下のとおりです。

- OpenVMS Alpha V8.3 あるいは 8.4
- OpenVMS Integrity V8.3，8.3-1H1 あるいは 8.4
- TCP/IP Services (あるいは MultiNet もしくは TCPware) — 他のサーバーあるいはネットワーク・クライアントと通信するためのネットワーク・プロトコルをサポートするソフトウェアです。
- Kerberos Version 3.0 以上

注記:

- HP CIFS Server キットをインストールする前に，C RTL (C Run-Time Library) の最新の ECO キットをインストールする必要があります。C RTL の最新の ECO キットは，HP サポートセンターの web サイトからダウンロードしてください。

  http://h20566.www2.hp.com/portal/site/hpsc/

2.2 リリース・ノートについて

『HP CIFS リリース・ノート』には，製品をインストールする前に知っておくべき重要な情報が記載されています。インストールを開始する前に，このリリース・ノートを読むことをお勧めします。

インストール前にキット内のリリース・ノートを取り出す方法は以下のとおりです。

1. ドライブにインストール・キットをロードします。
2. 以下のように，PCSI ユーティリティ・コマンドを入力します。 *file_name.txt* には，リリース・ノートを保管する任意のファイル名を指定します。 *directory-path* には，HP CIFS Server ソフトウェアがあるソース・ドライブのディスクおよびディレクトリ名を指定します (たとえば /SOURCE=SYS$DEVICE:[TEST1])。

   ```
   $ PRODUCT EXTRACT RELEASE_NOTES SAMBA/FILE=file_name.txt -
   _$ /SOURCE=directory-path
   ```

   ファイル名を省略すると，リリース・ノートは現在のディレクトリに CIFS_REL_NOTES.TXT というファイル名で作成されます。 展開先を省略すると，PCSI はリリース・ノートを現在のディレクトリに展開します。

CIFS ソフトウェアがインストール済みのシステムでは，リリース・ノート SYS$HELP:CIFS_REL_NOTES.TXT を参照あるいは印刷できます。

2.3 インストール前の作業

ここでは，お使いのシステムに HP CIFS Server ソフトウェアをインストールする前に実施すべき作業について説明します。

手順 1: ネットワーク・ハードウェアの確認

HP CIFS Server ソフトウェアは，ソフトウェア要件を満たした OpenVMS Alpha システムまたは OpenVMS Integrity サーバーで動作します。 PC ローカル・エリア・ネットワーク (LAN) には，次のものが必要です。

- サポートされているネットワーク・コントローラ・ボード (サーバーおよび各クライアント用)
- 各クライアントとサーバーをネットワークに接続するためのケーブル

手順 2: システムアカウントへのログイン

HP CIFS Server ソフトウェアをインストールする前に，システムアカウントで，またはインストレーション・プロシージャを実行するために必要なすべての権限を持つアカウントで OpenVMS システムにログインする必要があります。

1. Username プロンプトに対し，SYSTEM と入力します。

   ```
   Username: SYSTEM
   ```

2. Password プロンプトに対し，SYSTEM アカウントのパスワードを入力します。

手順 3: 必要なソフトウェアの確認

HP CIFS Server ソフトウェアには，次のものが必要です。

- OpenVMS Alpha Version 8.2，8.3 あるいは 8.4
- OpenVMS Integrity Version 8.2-1，8.3，8.3-1H1 あるいは 8.4
- ネットワーク通信のための TCP/IP Services for OpenVMS (または MultiNet あるいは TCPware)
- 最新の C RTL ECO キット
- Kerberos Version 3.0 以上

手順 4: システムのバックアップ

貴重なデータが失われないように，HP では，あらゆるレイヤード製品のインストールの前に，お使いのシステムのすべてのディスク(または，少なくともシステム・ディスク)のバックアップを取ることを推奨しています。

システム・バックアップを実行するには，OpenVMS BACKUP コマンドを使用します。 詳細は，『HP OpenVMS システム管理ユーティリティ・リファレンス・マニュアル』を参照してください。

手順 5: リリース・ノートの確認

ソフトウェアをインストールする前に，リリース・ノートを必ずお読みください。リリース・ノートの参照方法については，2.2 項「リリース・ノートについて」を参照してください。

手順 6: ディスク容量の確認

インストールに必要なディスク・ブロック数については，2.1.1 項「必要なディスクスペース」を参照してください。システム・ディスク上の空きブロック数を確認するには，次のコマンドを入力します。

`SHOW DEVICE` ***デバイス名***

OpenVMS システムは，空きブロック数など，システム・ディスクに関する情報を表示します。

たとえば，デバイス `NEWTON$DKA0` の空き容量を確認するには，次のようなコマンドを入力します。

```
$ SHOW DEVICE NEWTON$DKA0/unit=bytes
Device Name   Device Status   Error Count   Volume Label   Free Space    Trans Count  Mnt Cnt
NEWTON$DKA0:  Mounted                 0       V083        2.58GB         373          1
```

手順 7: TCP/IP ステータスを確認

次のコマンドを実行して，TCP/IP の状態を確認してください。

```
$ SYS$STARTUP:TCPIP$STARTUP.COM
%TCPIP-I-INFO, TCP/IP Services startup beginning at 17-AUG-2011 19:16:41.78
%TCPIP-I-NORMAL, timezone information verified
%TCPIP-I-NETSTARTED, network already started
%TCPIP-S-STARTDONE, TCP/IP Services startup completed at 17-AUG-2011 19:16:44.80
```

注記: 上記のコマンドは TCP/IP Services for OpenVMS 使用している場合の例です。 MultiNet あるいは TCPWare を使用している場合のトランスポートの確認方法は，『MultiNet Installation and Administrator's Guide』あるいは『TCPware Management Guide』を参照してください。

手順 8: OpenVMS クラスタ構成の確認

- HP CIFS Server ソフトウェアを実行するすべてのクラスタ・メンバーがすべて同じ TCP/IP サブネットにあることを確認します。

2.4 OpenVMS Cluster 環境でのインストールについて

HP CIFS Server は，OpenVMS クラスタで以下の構成をサポートします。

- HP CIFS Server をスタンドアロン・エンティティとして各ノードにインストールする。
- クラスタの複数のノードが同じ samba$root ディレクトリおよび共有を共有するような共通 CIFS クラスタとして HP CIFS Server をインストールする。
- 同じ OpenVMS Cluster 内で，スタンドアロンの HP CIFS Server と HP CIFS Cluster を組み合わせる。

  たとえば 3 つのノードを持つクラスタにおいて，2 つのノードが同じ samba$root ディレクトリおよび共有を共有する HP CIFS Cluster を構成し，3 つ目のノードはスタンドアロンの HP CIFS Server インスタンスを実行するように構成することが可能です。

注記: データの破損が発生するため， HP CIFS Server の 2 つのインスタンスがクラスタ内の同じディレクトリおよびファイルを共有することはできません。 これは，HP CIFS Server の各インスタンスが，ファイル・ロックの詳細を HP CIFS Server の他のインスタンスと共有できないためです。

2.4.1 クラスタ環境で HP CIFS Server をスタンドアロン・エンティティとしてインストールする

次のような状況では， クラスタのいずれかのノードで HP CIFS Server をスタンドアロン・エンティティとしてインストールするのが便利です。

- 複数のクラスタ・ノードからのファイルへの同時アクセスが必要なく，負荷バランシングやフェールオーバも必要ない場合。
- 共通の SYSUAF あるいは RIGHTSLIST データベースがない場合。

2.4.2 クラスタ環境で HP CIFS Server を複数のノードにインストールする

負荷バランシングやクラスタ・フェールオーバ機能が必要な場合は，クラスタの複数のノードで共通のエンティティとして HP CIFS Server を実行することができます。 この場合，CIFS クラスタにメンバーとして参加したノードは次のように動作します。

- 同じ samba$root ディレクトリを共有します。
- 同じディレクトリおよびファイルを共有します。
- 個々のノード名の代わりに HP CIFS Server のクラスタ別名に接続することにより， クライアントが CIFS クラスタ・ノードにシングル・エンティティとしてアクセスすることが可能です。

これらの CIFS クラスタ機能をサポートするためには，以下のような前提条件を満たす必要があります。

1. すべての HP CIFS クラスタ・ノードが共通の SAMBA$ROOT ディレクトリ・ツリーを共有する必要があります。 デフォルトでは，HP CIFS Server は SYS$COMMON:[SAMBA] ディレクトリにインストールされます。 すべての HP CIFS クラスタ・ノードからアクセス可能なシステム・ディスク以外のディスクに HP CIFS Server をインストールするには，PRODUCT INSTALL コマンドの /DESTINATION 修飾子を使用してください。

   アーキテクチャの異なるクラスタ・ノード (Alpha および Integrity) が同じ samba$root ディレクトリを共有する CIFS クラスタに参加できるようにするためには， 各ノードで PRODUCT INSTALL コマンドの /DESTINATION 修飾子に同じデストネーション・パスを指定して HP CIFS Server をインストールしてください。

   例：

   2 つの Integrity ノードと 1 つの Alpha ノードを持つクラスタについて考えてみましょう。 3 つのすべてのノードで同じ samba$root ディレクトリを共有できるようにするためには， Integrity ノードのどちらか一方と Alpha ノードで PRODUCT INSTALL コマンドの

/DESTINATION 修飾子に同じインストール先パスを指定して HP CIFS Server をインストールします。

2. OpenVMS システムに最新の C RTL (Run-Time Library) ECO がインストールされていることを確認してください。 この ECO では，HP CIFS Server の動作と信頼性に直接関係する変更が行われています。 OpenVMS ECO を入手する方法の 1 つとして，HP サポートセンターの web サイトから入手する方法があります。

   http://h20566.www2.hp.com/portal/site/hpsc/

3. 同じ `samba$root` インストレーション・ディレクトリを 共有するすべてのクラスタノードが， 共通の `SYSUAF` と `RIGHTSLIST` データベースを使用する必要があります。
4. 共通の CIFS クラスタ別名を選択します。
5. 共通の名前解決手段を選択します。 HP CIFS Server で使用可能な名前解決の手段については， 2.5 項 を参照してください。

2.5 名前解決方法

HP CIFS Server は，クライアントが HP CIFS Server に接続する際に名前を解決する手段として，以下の名前解決方法をサポートします。

- 2.5.1 項 「DNS 名前解決」
- 2.5.2 項 「WINS 名前解決」
- 2.5.3 項 「LMHOSTS 名前解決」

HP CIFS Server がスタンドアロン・エンティティとして構成され， 名前解決に DNS あるいは WINS を使用するようにクライアントが構成されており， DNS あるいは WINS サーバーにより HP CIFS Server 名が解決できる場合は， クライアントおよびサーバー上で必要な操作は特にありません。 ただし，複数のノードで同じ `samba$root` ディレクトリを共有する CIFS クラスタに対しては，さらに設定が必要になります。 これらの設定について，以降の各項で説明します。

2.5.1 DNS 名前解決

複数のノードで同じ `samba$root` ディレクトリを共有するような CIFS クラスタで， 共通の CIFS 別名を使用してクライアントがリソースにアクセスできるようにするためには， さらに設定が必要になります。

まず， OpenVMS クラスタで CIFS が使用するホスト名を設定します。 このホスト名は DNS に登録し，CIFS for OpenVMS が稼働するクラスタ内の個々のノードの IP アドレスと関連付けます。 このホスト名は NetBIOS 名として使用されるので，15 文字を超えない長さにします。 HP CIFS Server は，HP CIFS クラスタ・メンバーにクライアント・セッションを展開する際，TCP/IP と DNS の負荷バランシング・メカニズムを利用します。負荷バランシングおよびフェールオーバ機能を利用するためには，クライアントは HP CIFS クラスタ名を使用している HP CIFS Server に接続する必要があります。

たとえば，CIFS クラスタ別名 CIFSALIAS が次の 3 つのクラスタ・ノードで使用される場合を例に説明します。

```
10.0.0.1 NODEA

10.0.0.2 NODEB

10.0.0.3 NODEC
```

DNS エントリは以下のようになります。

```
10.0.0.1 A NODEA

10.0.0.2 A NODEB

10.0.0.3 A NODEC

10.0.0.1 A CIFSALIAS

10.0.0.2 A CIFSALIAS
```

```
10.0.0.3 A CIFSALIAS
```

DNS はラウンド・ロビン方式でアドレスを提供するため，ある程度の負荷バランシングとフェールオーバを提供します。

システム負荷に基づいたフェールオーバ機能を備えた本来の負荷バランシング機能を利用したい場合，TCP/IP Services for OpenVMS を使用している場合であれば，TCP/IP クラスタ名の作成には Load Broker および METRIC Server で提供される機能を使用すべきです。 Load Broker の構成ファイルで指定する TCP/IP クラスタ名は，DNS ネーム・スペースで登録される CIFS クラスタ別名と同じである必要があります (`SMB.CONF` の NETBIOS NAME パラメータで指定されているのが何であろうと)。 Load Broker および Metric Server の構成についての詳細は，『TCP/IP Services for OpenVMS Management』および『TCP/IP Services for OpenVMS Concepts and Planning』を参照してください。

Multinet あるいは TCPware を実行している場合に負荷バランシングとフェールオーバがどのように実現されるかについては，これらの製品のドキュメントを参照してください。

2.5.2 WINS 名前解決

複数のノードで同じ `samba$root` ディレクトリを共有するような CIFS クラスタで， 共通の名前を使用してクライアントがリソースにアクセスできるようにするために，WINS サーバーで共通の CIFS クラスタ別名を HP CIFS Server が登録できるようにする必要があります。 この処理は以下の操作で実行します。

1. WINS Server の IP アドレスをポイントする HP CIFS Server 構成パラメータ `wins server` を `SMB.CONF` ファイルのグローバル・セクションに追加します。

   ```
   wins server = <IP-address-of-WINS-server>
   ```

   注記: コンマで区切って複数の WINS サーバの IP アドレスを指定することができます。

2. 同じ `samba$root` ディレクトリを共有する クラスタの各ノードの IP アドレスをコンマで区切って， グローバル・セクションの HP CIFS Server 構成パラメータ `cluster addresses` で指定します。

   たとえば，クラスタ内の 2 つのノード NODEA と NODEB が同じ `samba$root` ディレクトリを共有する場合は， `cluster addresses` を次のように指定します。

   ```
   cluster addresses = <IP-address-of-NODEA>,<IP-address-of-NODEB>
   ```

   注記: HP CIFS Server の構成に `SAMBA$CONFIG.COM` 構成ユーティリティを使用している場合，`wins server` および `cluster addresses` パラメータは，構成ユーティリティの「**Generic Options**」メニューから構成できます。

2.5.3 LMHOSTS 名前解決

DNS あるいは WINS 名前解決ではクライアントが HP CIFS Server 名を解決できないようなネットワークでは，LMHOSTS ファイルを使用できます。 この方法は，単一の IP アドレスに対する名前の解決に使用できます。

スタンドアロンの HP CIFS Server ノードでは，この方法は， HP CIFS Server を実行しているノードの IP アドレスに対する HP CIFS Server 名の解決に使用できます。

複数のノードが同じ `samba$root` ディレクトリを共有し 共通の CIFS クラスタ別名を使用する CIFS クラスタでは， LMHOSTS ファイルは， HP CIFS Server を実行しているいずれかのノードの IP アドレスに対する CIFS クラスタ別名を解決するように構成できます。

代替ノードの IP アドレスをポイントするように LMHOSTS ファイルが更新されない限り， クライアントは，CIFS クラスタ別名でポイントされる既存の IP アドレス参照し続けます。 このため LMHOSTS 名前解決は， CIFS クラスタ・ノードの負荷バランシングあるいはフェールオーバには使用できません。

クライアントが LMHOSTS 名前解決を使用したファイル・アクセスのために HP CIFS Server 名あるいは別名に接続できるように，クライアントの LMHOSTS ファイルに次のような行を追加してください。

```
<IP-address-of-CIFS-Server-node> <CIFS-Server-Name-or-Alias> #PRE
```

たとえば，HP CIFS Server 名のエントリに IP アドレスが 10.20.30.40 の PIANO という名前を 追加するには，次のような行を使用します。

```
10.20.30.40 PIANO #PRE
```

Windows システムで LMHOSTS ファイルを更新した後，CMD プロンプトで次のようなコマンドを実行して ネームキャッシュをリロードしてください。

```
nbtstat -R
```

2.6 HP CIFS Server ソフトウェアのインストール

ここでは，PCSI ユーティリティを使用して HP CIFS Server ソフトウェアをインストールする方法について説明します。 PCSI ユーティリティについては，『HP OpenVMS システム管理者マニュアル』を参照しいてください。

インストレーションを開始する前に，2.3 項「インストール前の作業」に示した事前作業が完了していることをご確認ください。

HP CIFS Server ソフトウェアのインストール手順は以下のとおりです。

1. SYSTEM アカウント，または権限のあるアカウントへログインします。
2. 次のように PRODUCT INSTALL コマンドとディレクトリ・パスを入力して，PCSI ユーティリティを起動します。

   ```
   PRODUCT INSTALL SAMBA/DESTINATION=<directory-path>
   ```

   <directory-path> には，HP CIFS Server ソフトウェア・キットをインストールするターゲット・ディスクとディレクトリ名を指定します。 たとえば，`/DESTINATION=SYS$SYSDEVICE:[000000]` のように指定します。

   インストール先を指定しないと，PCSI ユーティリティは，論理名 `PCSI$DESTINATION` で定義されている場所を探します。 この論理名が定義されていない場合，PCSI ユーティリティは，デフォルトのディレクトリである `SYS$SYSDEVICE:[VMS$COMMON]` に HP CIFS Server ソフトウェア・キットをインストールします。

注記:

- インストレーション・プロシージャは `[.SAMBA]` ディレクトリを作成します。 この例の場合，`SYS$SYSDEVICE:[000000.SAMBA]` が作成されます。
- HP CIFS Server は システムディスク以外にインストールすることをお勧めします。 インストレーションの手順については， 12.1 項 を参照してください。

HP CIFS Server のインストール時に，`SAMBA$NMBD`，`SAMBA$SMBD`，`SAMBA$TMPLT` および `SAMBA$GUEST` の 4 つの OpenVMS ユーザアカウントが作成されます。 これらのアカウントの UIC グループ番号は，ユーザ入力，あるいは `SYSUAF` データベースで利用可能なものから動的に割り当てられます。

注記: インストレーションを中止する場合は，**Ctrl+Y** を押してください。 この場合，インストレーション・プロシージャは，作成したファイルを削除せずに処理を終了します。

2.7 HP CIFS Server ソフトウェアのアップグレード

この節では，PCSI ユーティリティによる HP CIFS Server ソフトウェアのアップグレード方法について説明します。 PCSI ユーティリティについての詳細は，『HP OpenVMS システム管理者マニュアル』を参照してください。

インストールを開始する前に，2.3 項「インストール前の作業」に示す準備作業を実行してください。

HP CIFS Server ソフトウェアをアップグレードする際，論理名 SAMBA$ROOT: で定義されている場所にある既存のすべてのイメージおよびスクリプトは，新しいキットのイメージおよびスクリプトで置き換えられます。

警告! サーバーで必要とするその他のファイルの保管とリストアは，システム管理者の責任で行ってください。 SAMBA$ROOT:[LIB]SMB.CONF を参照してファイルを確認することをお勧めします。 また，ローカルで使用するために修正あるいは作成され SAMBA$ROOT: ディレクトリ・ツリーに置かれているスクリプトの保管およびリストアも実施しください。

注記: すでにインストールされている製品をアップグレードする際， PCSI ユーティリティの PRODUCT INSTALL コマンドは， その製品の以前のインストール時に /DESTINATION 修飾子で指定されたインストール先パスを無視し， SYS$SYSDEVICE:[VMS$COMMON] ディレクトリに製品をインストールします。 この問題は OpenVMS V8.4 で修正されています。

OpenVMS V8.4 より前のバージョンを使用している場合は，以下のように対応してください。

1. HP CIFS Server をアップグレードする際に PRODUCT INSTALL コマンドで /DESTINATION 修飾子を使用し， HP CIFS Server の以前のインストールの際に指定したのと同じインストール先パスを指定してください。
2. 最新の PCSI キットがこの問題を解決しているかどうかを確認してください。 確認には，PCSI ECO キットのリリース・ノートを参照してください。 PCSI キットがこの問題を解決していない場合，HP CIFS Server のダウンロード・ページから PCSI の共有イメージをダウンロードしてインストールしてください。 その後，HP CIFS Server をアップグレードしてください。 これにより問題が解決され，PCSI ユーティリティは自動的に正しいインストール先パスを検出します。

HP CIFS Server ソフトウェアのアップグレード手順は以下のとおりです。

1. SYSTEM アカウントあるいは特権アカウントにログインします。
2. HP CIFS Server をシャットダウンします。

```
$ @SYS$STARTUP:SAMBA$SHUTDOWN
```

注記: 同じ SAMBA$ROOT: ディレクトリを共有する複数のクラスタ・メンバーで HP CIFS Server が稼働している場合は，すべてのクラスタ・メンバーの HP CIFS Server をシャットダウンします。

3. PCSI ユーティリティを起動します。

```
$ PRODUCT INSTALL SAMBA
```

注記: 途中でインストールを中止する場合は，**Ctrl+Y** を押してください。

2.8 SAMBA$ROOT ディレクトリの移動

PCSI ユーティリティは，再インストールの際，その製品の以前のインストールで使用されたパスとは異なるインストール先パスに製品をインストールすることはできません。

あるディスクから別のディスクへ SAMBA$ROOT の内容を移動するには，まず BACKUP コマンドで SAMBA$ROOT の内容のバックアップを取ります。 その後，HP CIFS Server を削除し，以下のように /DESTINATION 修飾子を使用して適当な場所に再インストールします。

```
$ PRODUCT REMOVE SAMBA
$ PRODUCT INSTALL SAMBA /DESTINATION=<new-location>
```

この後，/REPLACE 修飾子を指定して SAMBA$ROOT セーブセットの内容を *<new-location>* で指定した場所にリストアします。

上記の手順は，システムディスクが複数存在するクラスタや，異なる SAMBA$ROOT に HP CIFS Server がインストールされて複数のインスタンスを持つクラスタでは，正しく実行できな可能性があります。 また，他のシステム・ディスクに SAMBA$DEFINE_ROOT.COM のコピーが存在するかもしれないという点も考慮する必要があります。インストレーションや構成の状態に応じて，それぞれ注意する必要があります。

2.9 インストール後の作業

インストールが完了したら，次の手順を実行します。

1. 次のコマンドを入力して，SAMBA$ROOT 論理名を確認します。

   ```
   $ SH LOG SAMBA$ROOT
   "SAMBA$ROOT" = "NEWTON$DKA100:[SAMBA.]"
   ```

   この論理名が定義されていない場合は，次のコマンドを実行してください。

   ```
   @SYS$STARTUP:SAMBA$DEFINE_ROOT
   ```

   クラスタ環境で HP CIFS Server をインストールしている場合，この論理名は HP CIFS Server がインストールされているノードでのみ定義してください。

2. @SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS.COM を実行して，すべての HP CIFS ユーティリティで必要となるシンボルを定義してください。このコマンド・プロシージャは，SMBSTART，SMBSTOP，SMBSHOW，SMBVERSION の各シンボルも定義します。

注記: login.com を編集して，次の行を追加してください。

```
$ @SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS.COM
```

これにより，ログイン後，すべての HP CIFS コマンドが有効になります，

OpenVMS クラスタ環境では，以下のような条件に一致する場合，インストレーション・ノードの SAMBA$ROOT:[CLUSTER] ディレクトリににある SAMBA$DEFINE_ROOT.COM，SAMBA$STARTUP.COM，および SAMBA$SHUTDOWN.COM ファイルを クラスタ内の他の各ノードの SYS$COMMON:[SYS$STARTUP] へコピーする必要があります。

- HP OpenVMS CIFS をインストールしたノードと同じインストレーション・ディレクトリをクラスタ内の複数のノードが共有する。
- 同じ samba$root インストレーション・ディレクトリを使用する クラスタ内の各ノードが，別々のシステム・ディスクを使用する。この場合，個別のシステム・ディスクを使用する各ノードへ SAMBA$DEFINE_ROOT.COM，SAMBA$STARTUP.COM， および SAMBA$SHUTDOWN.COM ファイルをコピーしてください。

2.10 HP CIFS Server の構成

HP OpenVMS CIFS ソフトウェアをインストールした後，ご使用の環境に適用される CIFS 設定要件を満たすための構成を行なう必要があります。 構成に関する基本的な要素は以下のものがあります (これがすべてではありません)。

- HP CIFS Server の役割
- HP CIFS Server ドメイン
- HP CIFS Server passdb backend タイプ
- クラスタ環境での HP CIFS Server の構成
- TCP/IP データベースでの CIFS サービスの設定
- 文字セットの要件

HP CIFS Server は，OpenVMS システムから Samba 構成ユーティリティを使用して，あるいは Web ブラウザを通して Samba Web Administration Tool (SWAT) を使用して構成できます。

注記: HP CIFS Server の構成を行なう場合，HP OpenVMS CIFS で提供する Samba 構成ユーティリティ SAMBA$CONFIG.COM か SWAT を使用することをお勧めします。これらは並用することはできません。

2.10.1 Samba 構成ユーティリティによる HP CIFS Server の構成

HP OpenVMS CIFS version 1.2 以降，自動化された Samba 構成ユーティリティ SAMBA$CONFIG.COM を使用して HP CIFS Server を構成することができます。このユーティリティは，HP CIFS Server の基本的な構成を設定するのに使用できます。共有や信頼の設定には使用できません。

2.10.1.1 構成前の作業

Samba 構成ユーティリティを実行するまえに，以下の事前準備を実行する必要があります。

- Samba 構成ユーティリティを実行しようとしているノードで既存の HP CIFS Server が実行中の場合は，HP CIFS Server をシャットダウンします。
- OpenVMS クラスタ環境では，HP OpenVMS CIFS ソフトウェアがインストールされた samba$root インストール・ディレクトリをクラスタ内の複数のノードで共有する必要あるかどうかを判断します。

  たとえば，NODE A，NODE B，NODE C，および NODE D の 4 つのノードを持つクラスタを例に説明します。HP OpenVMS CIFS ソフトウェアが NODE A にインストールされている場合，以下のような判断をする必要があります。

  — NODE A と同じインストール・ディレクトリ samba$root を共有するノードがあるかどうか。NODE A と同じ samba$root インストール・ディレクトリを NODE B および NODE C で共有する場合は，NODE B と NODE C で NODE A と共通の OpenVMS システム・ディスクを使用するかどうかを確認します。NODE A と共通の OpenVMS システム・ディスクを使用しない場合は，NODE A から NODE B および NODE C のそれぞれのノードの SYS$STARTUP ディレクトリへ SYS$STARTUP:SAMBA$DEFINE_ROOT.COM ファイルをコピーします。

  — 既存の HP CIFS 構成で，NODE A，NODE B，および NODE C の各ノードで HP CIFS Server をシャットダウンします。
- SYSTEM アカウントなどの特権付きのユーザ・アカウントで OpenVMS にログインします。

2.10.1.2 構成作業

OpenVMS システムの DCL プロンプトから Samba 構成ユーティリティを実行するには，次のコマンドを実行します。

```
$ @SYS$STARTUP:SAMBA$DEFINE_ROOT.COM
$ @SAMBA$ROOT:[BIN]SAMBA$CONFIG.COM
```

SAMBA$CONFIG.COM ユーティリティを実行すると，以下の処理が行なわれます。

- ヘルプ・テキストの表示
- 構成前の要件に合っているかどうかのチェック
- HP CIFS Server の構成すでに行なわれているかどうかのチェック。既に構成済の場合，次の処理が行なわれます。
  — すべての一時的な TDB ファイルを削除します。
  — 既存の永続的な TDB ファイルのフォーマットを HP OpenVMS CIFS Version 1.2 TDB のファイル・フォーマットに変換あるいは移行します。
  — 現在の HP CIFS Server 構成の情報を収集します。

- Main Menu の表示

注記: HP CIFS Server の構成処理の一部として， SAMBA$CONFIG.COM ユーティリティは以下の処理を行います。

- HOMES，NETLOGON，PRINT$，および PROFILES 共有を追加します。
- HP CIFS Server の役割に適した組み込みの CIFS Server グループを作成します。

以降の項では， Samba 構成ユーティリティを通して設定可能ないくつかの構成オプションについて説明します。

2.10.1.3 Main Menu の構成オプション

Samba 構成ユーティリティの Main Menu では，次のような構成オプションが表示されます。

```
        HP OpenVMS CIFS Main Configuration Options Menu

Configuration options:

        1  - Core environment
        2  - Generic options
        3  - System specific setup
        A  - Configure options 1 - 3
       [E] - Exit Menu

Enter configuration option:
```

これらのオプションについて以下に説明します。

- Core environment オプションでは，サーバーの役割，サーバー・ドメイン，クラスタ別名などの HP CIFS Server の主要な構成を設定することができます。
- Generic options オプションでは，OpenVMS ファイル・フォーマットのサポート，文字セット，サーバー・コメント，ゲスト・アカウント，クラスタ・アドレスなどを構成することができます。
- System specific setup オプションでは，TCP/IP データベースでの CIFS サービス (SMBD および SWAT サービス)，File Server クライアント機能， File Server プロセス (SMBD プロセス) で使用するインタフェースを設定します。

HP CIFS Server をはじめて構成する場合は，オプション A を選択してください。 オプション A は，Main Menu のオプション 1 から 3 のすべてに関して CIFS Server 構成の設定を行ないます。 一度オプション A で HP CIFS Server を構成した後は，将来 HP CIFS Server の再構成が必要になった場合に Main Menu から適切なオプションを選択して構成を行なってください。

複数のノードが同じ samba$root ディレクトリを共有するような OpenVMS クラスタ環境では，Main Menu のオプション A はクラスタ内の 1 つのノードでのみ実行します。 他のノードではオプション 3 を実行してください。

たとえば， NODE A，NODE B，および NODE C が同じ samba$root ディレクトリを共有する CIFS クラスタの場合， NODE A で "Main Menu" のオプション "A" を実行します。 NODE B および NODE C では， "Main Menu" のオプション "3" を使用します。

2.10.1.4 HP CIFS Server のコア環境の構成

Samba 構成ユーティリティの Main Menu で HP CIFS Server のコア環境を構成するには，1 あるいは A のどちらかのオプションを選択します。 どちらの場合も，Samba 構成ユーティリティは次のようなメニューを表示します。

```
HP OpenVMS CIFS Core Configuration Menu

  The CIFS core configuration menu allows you to configure basic server
   configuration parameters and to set the role of the server.

        1. Enable WINBIND mapping: yes
           1A. UIC Group number range:
           1B. POSIX Group IDentifier range:
```

```
        2. Passdb backend: tdbsam
        3. Domain/Workgroup name: LANGROUP
        4. Server role: PRIMARY
        5. Server computer/netbios name: PIANO

Enter item number or press Enter to accept current values [Done]:
```

HP CIFS Server が構成済みの場合は，次のような警告メッセージが表示されます。

```
************************* W A R N I N G *************************
  Changing any of the options in this menu may cause the existing
  databases to be RE-INITIALIZED resulting in the loss of any data
  currently in these databases (for example, user accounts, group
  names, identifier mapping information etc).
 *****************************************************************
```

OpenVMS クラスタでは，HP CIFS Server クラスタ別名を指定するための次のようなオプションが表示されます。

```
6. OpenVMS CIFS cluster alias: PIANO-ALIAS
```

`Core environment` メニューの各サブオプションが以下のように展開されます。

2.10.1.4.1 WINBIND マッピングを有効にする

オプション `1 Enable WINBIND mapping` を使用すると，YES または NO を指定することにより WINBIND マッピングを有効または無効にすることができます。

WINBIND は，自動マッピング，ネストしたグループのサポート，信頼機能などを提供する HP CIFS Server の特別な機能です。 WINBIND の自動マッピング機能 (WINBIND マッピング) により，HP CIFS Server は OpenVMS ユーザあるいはグループ (リソース識別子) を自動的に作成し，対応するドメイン・ユーザあるいはグローバル・グループにマッピングします。OpenVMS ユーザ名あるいはグループ (リソース識別子) は，既存のマッピングが存在しない場合のみ作成されます。 WINBIND と自動マッピング機能についての詳細は，第7章 「WINBIND のサポート」 を参照してください。 このオプションは，HP CIFS Server をメンバーサーバーとして構成した場合に便利です。 このオプションに対し YES を指定して WINBIND マッピングを有効にした場合，`Core environment` オプションは次のようなサブ・オプションを表示します。

```
1A. UIC Group number range:
1B. POSIX Group IDentifier range:
```

WINBIND マッピングが有効な場合，2 つのサブ・オプション "1A" および "1B" に対して値を指定する必要があります。

2.10.1.4.1.1 UIC グループ・メンバーの範囲

`UIC group number range:` で指定した値の範囲は，Samba 構成ファイル・パラメータ *`idmap uid`* にマッピングされます。

`1A. UIC Group number range:` オプションを選択した場合，次のようなメッセージが表示されます。

```
Whenever a domain user connects to CIFS Server, it needs a matching
  OpenVMS username. If no such match exists, winbind can automatically
  create a new OpenVMS username to map the domain user. To achieve this,
  CIFS Server requires that a range of OpenVMS UIC group numbers is
  specified for its exclusive use.

  For example, the range can be specified as 1000-2000

  At the following prompt, enter HELP to obtain more information.

Enter UIC Group number range in decimal: []
```

このプロンプトで HELP を入力すると，`UIC group number range` についての詳細情報が表示されます。

UIC group number range オプションについての詳細は，第7章 「WINBIND のサポート」を参照してください。

2.10.1.4.1.2 POSIX グループ識別子の範囲

POSIX Group IDentifier range で指定した値の範囲は，Samba 構成ファイル・パラメータ *idmap gid* にマッピングされます。

1B. POSIX Group IDentifier range オプションを選択した場合，以下のようなメッセージが表示されます。

```
  Whenever a domain group is referenced by CIFS Server, it needs a matching
  OpenVMS group (resource identifier). If a match is not found, winbind can
  automatically create the corresponding OpenVMS resource identifier. To
  achieve this, CIFS Server requires that OpenVMS resource identifier value
  is provided in POSIX GID format for its exclusive use.

  For example, the range can be specified as 5000-10000

  At the following prompt, enter HELP to obtain more information.

Enter POSIX group identifier range: []
```

このプロンプトで HELP を入力すると，POSIX group identifier range についての詳細情報が表示されます。

POSIX グループ識別子の範囲についての詳細は，第7章 「WINBIND のサポート」 を参照してください。

2.10.1.4.2 Passdb バックエンド

このオプションは，Samba 構成ファイル・パラメータ *passdb backend* のマッピングを行ないます。

オプション 2. Passdb backend を選択すると，構成ユーティリティは以下のようなメッセージを表示します。

```
  Passdb Backend option allows you to choose the backend that will be
  used for storing user and possibly group information. This allows you
  to swap between different storage mechanisms.

  Available backends include -
       tdbsam - The TDB based password storage backend.
       ldapsam - The LDAP based passdb backend.

Enter Passdb Backend to use [TDBSAM/LDAPSAM]: [tdbsam]
```

デフォルトでは，*passdb backend* は TDBSAM に設定されます。 Enter Passdb Backend to use プロンプトで LDAPSAM を指定することにより，*passdb backend* の設定を LDAPSAM に変更することができます。 *passdb backend* が LDAPSAM に設定されている場合，HP CIFS Server は，指定した LDAP サーバーにユーザおよびグループ情報を保管します。 LDAPSAM バックエンドについての詳細は， 第5章 「LDAP 統合のサポート」を参照してください。

LDAPSAM バックエンドは以下の Samba 構成ファイル・パラメータも制御します。

- *ldap admin dn*
- *ldap passwd sync*
- *ldap suffix*

passdb backend に LDAPSAM が指定されている場合，HP CIFS Server のユーザおよびグループ情報を保管するのに HP CIFS Server が使用できる LDAP サーバーについての詳細を提供する必要があります。 *passdb backend* が "LDAPSAM" の場合，LDAP サーバーについての詳細を指定できるように，Samba 構成ユーティリティの Core environment メニューに次のような *passdb backend* の 3 つのサブオプションが表示されます。

- 2A. LDAP Server nodename
- 2B. LDAP Server port

- 2C. LDAP Server Admin dn

LDAP Server nodename

passdb backend として LDAPSAM が選択されている場合，LDAP サーバーをホストするシステムの名前を HP CIFS Server の構成ユーティリティで指定する必要があります。 LDAP サーバーのシステム名には，完全に修飾されたドメイン名 (FQDN: Fully Qualified Domain Name) あるいはシステムの IP アドレスが使用できます。システムの FQDN は，nodename.myorg.dom の形式になります。LDAP サーバーをホストするシステム名の FQDN は，次のようなプロンプトで指定します。

```
Enter Fully Qualified Domain Name of LDAP Server system: []
```

LDAP サーバーのシステム名が FQDN で解決できない場合，LDAP サーバー・システムの IP アドレスを指定するためのプロンプトが表示されます。

LDAP Server port

デフォルトでは，LDAP Server は待ち受けポートとして TCP ポート 389 を使用します。 これとは異なるポートを使用するようにホスト・システムの LDAP Server が構成されている場合，そのポート番号を LDAP Server の待ち受けポートとして指定する必要があります。 ポート番号は，次のプロンプトで指定することができます。

```
Enter the TCP port used by LDAP Server: [389]
```

LDAP Server Admin dn

LDAP Server からユーザ情報を取り出す際，HP CIFS Server は LDAP Server Admin Distinguished Name (DN) を使用します。 この DN は，次の例のような完全な DN でなければなりません。

dc=my-domain,dc=com

構成ユーティリティが次のようなプロンプトを表示したら，LDAP Server Admin DN を指定することができます。

```
Enter LDAP Server Admin DN: [dc=my-domain,dc=com]
```

2.10.1.4.3 ドメイン/ワークグループ名

このオプションでは，Samba 構成ファイルの *workgroup* パラメータをマッピングします。

ドメインとは，共通のアカウント・データベースとポリシーを共有するコンピュータの集まりです。 各ドメインはユニークな名前を持ちます。 ネットワークには多数のドメインを含めることができます。 HP CIFS Server ドメインとは，HP CIFS Server が存在するドメインです。

CIFS Server ドメイン名には，最大 15 文字まで使用できます。 ドメイン名はコンピュータ名とは別でなければなりません。 デフォルトのドメイン名は LANGROUP です。 通常は，企業名やグループ名などをドメイン名として使用します。

Samba 構成ユーティリティが次のようなプロンプトを表示したら，HP CIFS Server ドメインの名前を指定することができます。

```
Enter CIFS Server domain name for this system: [LANGROUP]
```

2.10.1.4.4 サーバーの役割

このオプションでは，Samba 構成ファイルのパラメータ *domain master*，*domain logons*，*add user to group script*，および *delete user from group script* を制御します。 さらに，HP CIFS Server の役割が PDC あるいは BDC の場合，*security* パラメータにも影響を与えます。

ドメインのタイプに従って，HP CIFS Server は PDC，BDC，あるいはマスタ・サーバーとしてドメインに参加できます。あるいは，独立したスタンドアロン・サーバーとして構成することもできます。 それぞれの役割について以下に簡単に説明します。 サーバーの役割についての詳細は 第3章 「HP CIFS の導入モデル」 を参照してください。

プライマリ・ドメイン・コントローラ (PDC)

PDC は，セキュリティ・アカウント・データベースのドメインのマスタ・コピーを保管します。 HP CIFS Server をインストールして新しい Windows NT ドメインを作成する場合，その新しいサーバーはデフォルトでは PDC になります。 サーバー・ソフトウェアをインストールして既存のドメイン名を指定した場合，そのサーバーは BDC あるいはメンバーサーバーとして既存のドメインに参加することができます。

OpenVMS クラスタ環境では，単一のノードが `samba$root` インストール・ディレクトリを使用する場合のみ，HP CIFS Server を PDC として構成できます。

HP CIFS Server を PDC として構成する場合，OpenVMS クラスタ内で同じ `SAMBA$ROOT` インストール・ディレクトリを共有するノードを複数設定することはできません。

バックアップ・ドメイン・コントローラ (BDC)

BDCはドメインに必ず必要なものではありませんが，1 つ以上構成しておくことをお勧めします。 BDC は，ドメインのマスタ・セキュリティ・アカウント・データベースのコピーを保管します。 PDC と BDC は，そのドメインのログイン要求を認証します。

注記: HP CIFS Server は NT4 型の PDC として動作できますが，このようなドメインでは HP CIFS Server を実行する BDC のみを含めることができます。 同様に，PDC でも HP CIFS Server を実行している場合のみ，NT4 型の BDC として機能できます。 ただし，HP Advanced Server for OpenVMS と Windows ドメイン・コントローラの場合と異なり，HP CIFS Server PDC と BDC との間のユーザ・アカウント・データベースの自動複製はサポートされていません。 これを実行するには，HP CIFS Server は LDAP サーバーの支援が必要になります。

LDAP バックエンドを使用するように HP CIFS Server PDC と BDC を構成することにより，LDAP サーバー間の同期化でアカウント・データベースの複製が実現されます。 HP CIFS Server は，LDAP バックエンドを使用して LDAP ディレクトリのユーザおよびグループ・アカウント情報を保管および取得することができます (HP Enterprise Directory あるいは OpenLDAP サーバーなど)。 。 1 つの LDAP サーバーを HP CIFS Server PDC と BDC の両方に使用することもできますが，可用性および性能の観点では，HP OpenVMS CIFS PDC と BDC 用に別々の LDAP サーバーを持つことを強くお勧めします。

メンバーサーバー

メンバーサーバーは，ドメインのセキュリティ・アカウント・データベースのコピーを保管せず，ログイン要求の認証を行ないません。 メンバーサーバーは，メンバーサーバー共有へのアクセスを要求しているユーザの認証に関しては，ドメイン・コントローラに依存します。

HP CIFS Server Version 1.2 以降，Kerberos 認証を使うネイティブ・モードの Active Directory Windows ドメインでメンバーとして参加できます。 HP CIFS Server は，どのドメインでも NT4 型メンバーサーバーとして動作できます。

スタンドアロン・サーバー

スタンドアロン・サーバーは，ネットワーク上のドメイン・コントローラからは独立しています。 ドメイン・メンバーではなく，ワークグループ・サーバーと同じように機能します。 多くの場合，スタンドアロン・サーバーは，提供されているすべてのデータにすべてのユーザが容易にアクセスできるように最低限のセキュリティ制御で構成されます。

CIFS サーバーの役割の変更

HP CIFS Server をはじめて構成する場合，そのドメインにおけるサーバーの役割を選択します。そのサーバーの役割を変更しなければならないような状況が発生することがあるかもしれません。サーバーを変更するのに使用する方法は，そのサーバーの現在の役割と，どの役割に変更したいかに依存します。 役割の変更には Samba 構成ユーティリティが使用できますが，次のような制限があります。

- Samba 構成ユーティリティを使用して，BDC から PDC (あるいはその逆) へサーバーの役割を変更することができます。 役割を変更した後，HP CIFS Server を PDC に変更したの

か BDC に変更したのかに依存して，そのドメインの既存の PDC を手動でシャットダウンするか，別の BDC をそのドメインの PDC に昇格させる必要があります。

- BDC をメンバーサーバーとして再構成した場合，Samba 構成ユーティリティは，そのドメイン・コントローラのドメイン・ユーザおよびグループのアカウント・データベースを自動的に削除します。
- メンバーサーバーを BDC に再構成した場合，Samba 構成ユーティリティは，メンバーサーバーのローカル・ユーザおよびグループのアカウント・データベースを自動的に削除します。

注記: BDC からメンバーサーバー (あるいはその逆) への役割の変更の場合，ローカル・グループ情報が失われるため，いくつかのリソースへのアクセスで影響を受ける可能性があります。ローカル・グループを使用してリソース許可が設定されている場合，これらの許可をリセットする必要があります。 グローバル・グループあるいはグローバル・ユーザ・アカウントを使用してリソース許可が設定されている場合，これらの許可設定は役割を変更した後も有効な状態で残ります。

- サーバーの役割が PDC からスタンドアロン・サーバーに変更された場合，いずれかのワークステーション・アカウントが失われ，ドメインがドメインとして機能しなくなります。代わりに，そのドメインはワークグループとして動作するようになります。
- サーバーの役割がスタンドアロン・サーバーから PDC に変更された場合，そのワークグループはドメインとして機能するようになり，ワークステーション・アカウントとドメイン・グローバル・グループを追加することができます。
- その他のタイプの役割の変更はサポートされていません。

2.10.1.4.5 サーバー・コンピュータ/NetBIOS 名

スタンドアロンの OpenVMS システムでは，このオプションは Samba 構成ファイルの *netbios name* パラメータをマッピングします。 OpenVMS クラスタ環境では，このオプションはそのノードの *netbios aliases* をマッピングします。

ドメイン内のサーバーはこのユニークな名前で識別されます。構成プロシージャの実行時に，この名前を定義するかデフォルト値を使用することができます。他のノードあるいはクラスタが既にその名前を定義しており，その役割で実行中であっても，Samba 構成ユーティリティでは同じ名前の PDC をユーザが指定することを妨げません。 しかし，同じ名前を定義すると名前の解決で矛盾を導くことになります。PDC はドメイン内でユニークでなければなりません。

デフォルトのコンピュータ名は，そのサーバーの SCSNODE 名と同じです。

2.10.1.4.6 OpenVMS CIFS クラスタ別名

このオプションでは，OpenVMS クラスタ環境で Samba 構成ファイルの *netbios name* パラメータをマッピングします。

お使いのサーバーが OpenVMS Cluster のメンバーサーバーの場合，*netbios name* (CIFS cluster alias) は，同じ SAMBA$ROOT インストール・ディレクトリを使用するクラスタ内のすべてのサーバーが共有する名前になります。 この別名により，リモート・ノード (クライアントを含む) がクラスタ内のすべてのメンバーサーバーを単一のサーバーとして扱うことが可能になります。たとえば，クライアント・ユーザは，そのクラスタのサーバーへの接続に HP CIFS Server のクラスタ別名を指定できます。この場合，ユーザは接続時にクラスタ内の個々のノードの名前を知っておく必要はありません。

デフォルトの HP CIFS Server クラスタ別名は nodename-ALIAS です。 nodename は，Samba 構成ユーティリティを最初に実行したクラスタ・メンバーの SCSNODE 名になります。

2.10.1.4.7 メンバーサーバー固有の構成メニュー

HP CIFS Server がメンバーサーバーとして構成されている場合，Samba 構成ユーティリティは次のようなメニューを表示します。

```
Member Server Optional Parameters Configuration Menu

  The Member Server optional parameters configuration menu allows to
  modify Member Server specific parameters which are required for
  successful working of CIFS Server as member in a specified domain.


        1. Enable netlogon secure channel: auto
        2. Require strong session key: no
        3. Security mode: DOMAIN

Enter item number or press Enter to accept current values [Done]:
```

Security mode が ADS の場合，次のメニューも表示されます。

```
    4. Kerberos realm:
```

2.10.1.4.7.1 netlogon セキュリティ・チャネルを有効にする

このオプションは，Samba 構成ファイルの *client channel* パラメータのマッピングを行ないます。

NETLOGON Secure Channel は，ユーザ認証要求とドメイン・コントローラの通信に使用されるセキュリティのレベルを制御する手段を提供します。最も安全なセキュリティは署名 (signing) と暗号化 (sealing) によって提供されます。 以下の 3 つのオプションが用意されています。

- auto — 署名および暗号化を提示しますがそれを強制はしません (デフォルト)
- yes — サーバーが署名と暗号化を提示しない場合アクセスを拒否します。
- no — 署名と暗号化を提示しません。

注記: HP CIFS Server が BDC あるいはメンバーサーバーのどちらかの場合，Samba 構成ユーティリティはこのオプションのプロンプトを表示します。 Advanced Server for OpenVMS ドメインに対する MEMBER あるいは BACKUP として HP CIFS Server を構成している場合は，netlogon secure channel の選択プロンプトに対して NO を指定してください。 それ以外の場合はデフォルトのオプションを選択してください。

2.10.1.4.7.2 ストロング・セッションキーが必要

このオプションは，Samba 構成ファイルの *require strongkey* パラメータのマッピングを行います。

このオプションは HP OpenVMS CIFS 固有のもので，オープンソースの Samba にはこれに相当するパラメータは存在しません。 Require strong session key のセキュリティ設定は，Secure Channel データの暗号化に 128-bit キーを使用するかどうかを決定します。

- yes の場合 — 128-bit 暗号化が実行できなければ Secure Channel は確立されません。
- no の場合 — ドメイン・コントローラと交渉してキーの強さが決定されます。

注記: HP CIFS Server が Windows 2008 ドメインのメンバーとして動作する場合は，Require strong session key オプションの選択プロンプトで YES を選択してください。

2.10.1.4.7.3 OpenVMS ASV ドメインのメンバー

このオプションは，HP CIFS Server 固有のグローバル・セクション構成パラメータ *vms asv domain* を割り当てるためのものです。 Advanced Server for OpenVMS (ASV) ドメインでは，OpenVMS システムあるいは AVS を実行している OpenVMS ノードのクラスタは， そのドメインの PDC として動作します。 HP CIFS Server をそのような ASV ドメインのメンバーとして構成する場合は， "Member in OpenVMS ASV domain" のプロンプトに対して "**YES**" を指定してください。

```
Member in OpenVMS ASV Domain [y/n]: [no]
```

パスワード・サーバーを指定する際，以下のことが必要です。

- 別のドメインの DC を パスワード・サーバーとして指定しないでください。
- セキュリティ・モードを ADS として選択する場合， DC 名は省略せずに完全なドメイン名を指定してください。
- OpenVMS クラスタで ASV PDC が実行されているような Advanced Server for OpenVMS (ASV) ドメインのメンバーサーバーとして HP CIFS Server が構成されている場合は， プロンプトでパスワード・サーバーとして ASV PDC クラスタ別名のみを 指定してください。

```
Enter Password Servers (comma separated): [*]
```

2.10.1.4.7.4 パスワード・サーバー

このオプションは，グローバル構成パラメータ *password server* を割り当てるためのものです。 HP CIFS Server がドメインのメンバーサーバーとして構成される場合は， そのドメイン内のいずれかのドメイン・コントローラのとコンタクトして そのドメインに属するユーザを認証します。ドメイン内のドメイン・コントローラの名前をパスワード・サーバーとして指定することにより， HP CIFS Server はドメイン内の特定のドメイン・コントローラを使用してユーザ名あるいはパスワードの正当性を確認できます。

このオプションでは， 使用するパスワード・サーバーの名前あるいは IP アドレスを設定できます。 このオプションで "*" を設定すると，CIFS Server は， DOMAINNAME<1C> の名前で問い合わせを行い，その結果として 名前解決ソースから IP アドレスのリストとして返された各サーバーにコンタクトすることにより， 認証のためにプライマリあるいはバックアップ・ドメイン・コントローラを 自動検索しようとします。

サーバーのリストに名前/IP と "*" の両方が含まれる場合， そのリストは優先されるドメイン・コントローラ (DC) として扱われますが， 残りのすべての DC の自動検索もそのリストに追加されます。 CIFS Server は，最も近い DC を探してこのリストを最適化するような 処理は行いません。

2.10.1.4.7.5 セキュリティ・モード

このオプションは，Samba 構成ファイル・パラメータ *security* のマッピングを行ないます。 HP CIFS Server をメンバーサーバーあるいはスタンドアロン・サーバーとして構成する場合，セキュリティ・モードを指定することができます。 HP CIFS Server が PDC あるいは BDC として構成する場合，セキュリティ・モードは user に設定されます。

メンバーサーバーとしては，HP CIFS Server は次の 2 つのセキュリティ・モードが指定可能です。

- DOMAIN — このモードでは，HP CIFS Server は，ドメイン・コントローラにユーザ名とパスワードを渡して Windows NT Server と全く同じ方法で認証を行ないます。
- ADS — このモードでは，HP CIFS Server は ADS レルムでドメイン・メンバーとして動作します。 このモードで動作するためには，HP CIFS Server を実行するシステムに Kerberos をインストールし構成しておくことが必要です。 このモードは，Kerberos を使用してクライアントを認証したい場合のみ選択してください。

スタンドアロン・サーバーでは，サーバーへのユーザおよびパスワード情報の転送を行なうかどうか (およびその方法) をどのクライアントが決定できるかに基づいて，HP CIFS Server のセキュリティ・モードを指定できます。 スタンドアロン・サーバーでは以下のセキュリティ・モードが使用できます。

- User (ユーザ・レベルのセキュリティ) — クライアントは，最初に有効なユーザ名とパスワードでログインする必要があります。
- Share — クライアントが共有レベルのセキュリティ・サーバーに接続する場合，共有リソースに接続する前に有効なユーザ名とパスワードでログインする必要はありません。その代わりにクライアントは，共有に接続する際に共有ごとに認証情報 (パスワード) を送信します。

2.10.1.4.7.6 Kerberos レルム

このオプションは，Samba 構成ファイルの *realm* パラメータのマッピングを行ないます。

HP CIFS Server を ADS セキュリティ・モードでメンバーサーバーとして構成する場合，Samba 構成ユーティリティで Kerberos レルムを指定する必要があります。 レルムは Windows ドメインの ADS に相当するものとして使用されます。 通常は，Kerberos サーバーの DNS 名に設定されます。

2.10.1.4.8 ドメイン・コントローラのオプション・パラメータ構成メニュー

HP CIFS Server の役割として PDC が選択されている場合， Samba 構成ユーティリティは，コア構成で次のようなメニューも表示します。

```
Domain Controller Optional Parameters Configuration Menu

  The Domain Controller (DC) optional parameters configuration menu
  allows you to modify DC specific parameters which are required for
  successful working of CIFS Server as a DC in the specified domain.

        1. Logon Drive:
        2. Logon Path:
        3. Logon Script:

Enter item number or press Enter to accept current values [Done]:
```

HP CIFS Server の役割として BDC が選択されている場合， Samba 構成ユーティリティは，Domain Controller Optional Parameters Configuration Menu に 次のような 2 つのオプションも自動表示します。

```
        4. Enable netlogon secure channel: auto
        5. Backup in OpenVMS ASV Domain: no
```

2.10.1.4.8.1 ログオン・ドライブ

このオプションは，HP CIFS Server 構成ファイルに *logon drive* パラメータを割り当てるためのものです。 *logon drive* パラメータは， Windows がホームディレクトリに割り当てるドライブ文字を指定します。ドライブの文字としてはD～Zが使用できます。これはオプションのパラメータです。

2.10.1.4.8.2 ログオン・パス

このオプションは，HP CIFS Server 構成ファイルに *logon path* パラメータを割り当てるためのものです。ログオン・パス指示子は，ユーザがローミング・プロファイルで設定するものです。 この指示子は， 各ユーザのプロファイルの場所に対する Windows ネットワーク・パスを 含まなければなりません。 ユーザのプロファイル・ディレクトリが存在しない場合， プロファイル・ディレクトリは同じ場所に作成されます (そのユーザがそのディレクトリに対する書き込み権限を持っている場合)。

Samba の変数置き換えを利用してアーキテクチャ ごとにユーザのプロファイルを区分することもできます。次のような指示子を使用して，WinXP，WinNT などの Windows の各バージョンに関連してユーザのプロファイルを区分することができます。

```
logon path = \\%L\profiles\%U\%a
```

この機能は，ユーザが，コンピュータごとに異なるバージョンの Windows を 使用しているような場合に便利です。 この場合，指定するログオン・パスはプロファイル共有に対する相対パスです。

ローミング・プロファイルを無効にするためには， *logon path* パラメータに空文字を設定してください。

2.10.1.4.8.3 ログオン・スクリプト

このオプションは，HP CIFS Server 構成ファイルに *logon script* パラメータを割り当てるためのものです。 このログオン・スクリプトは，ユーザ・ログオン時にに実行する オプションのログオン・スクリプトの名前を指定します。 ログオン・スクリプトはバッチ・ファイル

(.BAT あるいは .CMD のファイル拡張子) でも実行プログラム (.EXE のファイル拡張子) でもかまいません。 1 つのログイン・スクリプトを 1 つあるいは複数のユーザ・アカウントに割り当てることができます。 ユーザ・ログオンの際，ログオンを認証するサーバーは， ユーザによって指定されたそのサーバーのログイン・スクリプト・パスに従ってログオン・スクリプトを探します。

このスクリプトは，[netlogon] 共有に対する 相対パスでなければなりません。 [netlogon] 共有が SAMBA$ROOT:[NETLOGON] のパス，および logon script = SCRIPTS\LOGON.BAT を指定する場合， 次のようなファイルがダウンロードされます。

```
SAMBA$ROOT:[NETLOGON.SCRIPTS]LOGON.BAT
```

ユーザ・ログイン時にログオン・スクリプトを実行しないようにするには， *logon script* パラメータに空文字列を設定します。

2.10.1.4.8.4 NETLOGON セキュア・チャネル

このオプションは，HP CIFS Server 構成ファイルで *client schannel* パラメータを割り当てるためのものです。 NETLOGON セキュア・チャネルは， ユーザ認証要求とドメイン・コントローラの通信に使用する セキュリティ・レベルのネゴシエーションの手段を提供します。 最も高いセキュリティは，署名と暗号化を有効にすることにより提供されます。 次の 3 つのオプションがあります。

- auto 署名と暗号化を提供しますが強制はしません (デフォルト)。
- yes サーバーが署名と暗号化を提供しない場合アクセスを拒否します。
- no 署名と暗号化を提供しません。

HP CIFS Server を Advanced Server for OpenVMS に対する BACKUP として構成している場合，NO を指定します。 そうでない場合はデフォルトのオプションを選択します。

2.10.1.4.8.5 OpenVMS ASV ドメインにおけるバックアップ

このオプションは，HP CIFS Server 構成ファイルで *vms asv domain* パラメータを割り当てるためのものです。 ASV ドメインでは， ASV を実行している OpenVMS システムあるいは OpenVMS ノードのクラスタは そのドメインの PDC として動作します。 HP CIFS Server をそのような ASV ドメインのバックアップとして構成する場合， "Backup in OpenVMS ASV domain" プロンプトで "YES" と指定してください。

```
Backup in OpenVMS ASV Domain [y/n]: [no]
```

2.10.1.4.9 コア環境の設定

Core environment メニューでオプションの選択を行なうと，そこで構成を終了することも，先に進むこともできます。 HP CIFS Server が BDC あるいはメンバーサーバーの場合， HP CIFS Server の構成を選択した後，そのドメインの PDC の FQDN (IP address if FQDN fails to resolve to IP) を指定するためのプロンプトが表示されます。 さらに，HP CIFS Server が追加されているドメインに属するユーザの認証情報も提示する必要があります。 提供するドメイン・ユーザ・アカウントは，そのドメインでマシン・アカウントを追加するための特権を持ったものでなければなりません。

HP CIFS Server をはじめて構成する際に，HP CIFS Server を管理するための管理特権を付与したいドメイン・ユーザ・アカウントを指定することができます。

必要な情報を提供したら，Samba 構成ユーティリティは HP CIFS Server のコア構成環境のセットアップを行ないます。 コア環境の構成が完了した後，自動生成される Samba コア構成ファイル SAMBA$ROOT:[LIB]CORE_SMB.CONF あるいは TESTPARM ユーティリティを使用して，それぞれのパラメータ値を参照することができます。 SAMBA$ROOT:[LIB]CORE_SMB.CONF ファイルを手動で編集してパラメータの変更を行なう必要はありません。 さらに，コア環境設定作業の中で，*log file*，*username map*，*printing*，および *load printers* の各パラメータを Samba コア構成ファイルに追加することもできます。

注記: OpenVMS クラスタ環境では，同じ SAMBA$ROOT インストール・ディレクトリを共有するクラスタ・ノードのうち 1 つのノードでのみ core environment メニューを実行してください。

2.10.1.5 HP CIFS Server の Generic オプションの設定

HP CIFS Server のコア環境を設定した後，OpenVMS ファイル・フォーマット・サポート，文字セット，ホーム (パーソナル) 共有などを構成する必要があります。 この設定は，Samba 構成ユーティリティのメイン・メニューでオプション 2 あるいは A を選択して Generic options サブオプションを選択することにより実行できます。 Samba 構成ユーティリティの Main Menu に表示されるオプション 2 あるいは A を使用すると，HP CIFS Server の一般オプションを設定することができます。 どちらのオプションを選択した場合も，次のような Generic options メニューが表示されます。

```
HP OpenVMS CIFS Generic Configuration Menu

This menu allows the administrator to specify character set, guest
account and other generic CIFS Server options.

        1. Character set: ASCII
        2. Guest account: SAMBA$GUEST
        3. Print command: /DELETE
        4. Server Comment String: Samba %v running on %h (OpenVMS)
        5. Enable WINS name resolution: no
        6. Name resolve order: lmhosts,host,wins,bcast

Enter item number or press Enter to accept current values [Done]:
```

2.10.1.5.1 文字セット

このオプションは，Samba 構成ファイル・パラメータ *dos charset* および *unix charset* のマッピングを行ないます。

HP CIFS Server は，ISO-8859-1 および UTF-8 文字セットのファイル名をサポートします。 ヨーロッパの文字は ISO-8859-1 でサポートされ，その他の言語の文字は UTF-8 でサポートされます。 さらに，ヨーロッパの文字のサポートする場合， ユーザ・ローカル・コードページ (そのユーザの Windows コードページ) が CP850 に設定されます。 日本語および中国語の文字をサポートする場合，ユーザ・ローカル・コードページは CP932 に設定されます。 デフォルトのユーザ・ローカル・コードページは ASCII です。ユーザ・ローカル・コードページは SMB.CONF ファイルの *dos charset* パラメータにマッピングされます。

Samba 構成ユーティリティは，文字セットのサポートのための次のようなオプションを表示します。

```
  By default, CIFS is configured to support the ASCII character set.
  For support of some European characters, select the Extended ASCII
  character set.  For support of Japanese characters, select the
  Unicode character set.

        1 - ASCII character support
        2 - Extended ASCII (CP850) character support
        3 - Japanese (CP932) character support

Enter option: [1]
```

ご使用の環境での HP CIFS Server のファイル名文字サポートに応じて，適切なオプションをサポートしてください。

2.10.1.5.2 ゲスト・アカウント

このオプションは，HP CIFS Server 構成ファイルに *guest account* パラメータを割り当てるためのものです。 ゲスト・アカウントは， ゲスト・アクセスが有効 (guest ok) と指定されているサービスにアクセスするための ユーザ名です。 このユーザの特権は，このゲスト・サービスに接続するどのクライアントでも有効です。HP CIFS Server は，指定されたゲスト・アカウントが SYSUAF データベースに存在することを必要とします。 指定されたユーザが SYSUAF データベースに存在しない場合，ユーティリティは， SYSUAF データベースに必要なゲスト・アカウント名を作成することができます。

2.10.1.5.3 Print コマンド

このオプションは，HP CIFS Server 構成ファイルに *print command* パラメータを割り当てるためのものです。 print コマンドでは，OpenVMS の DCL PRINT コマンドの以下の修飾子を 使用することができます。

- /BURST
- /DELETE
- /FEED
- /FLAG
- /FORM
- /HEADER
- /HOLD
- /OPERATOR
- /PAGES
- /PARAMETERS
- /PASSALL
- /PRIORITY
- /RESTART
- /RETAIN
- /SPACE

これらの修飾子についての詳細は， `HELP PRINT <qualifier>` コマンドを実行して DCL ヘルプを参照してください。

プリント・ジョブを OpenVMS システムの特定のスプール・ファイルに送信する際，HP CIFS Server は，指定した print コマンド修飾子を `SYS$SNDJBC` の対応する項目コードに変換します。 *print command* のデフォルト値は /DELETE です。

2.10.1.5.4 サーバー・コメント文字列

このオプションでは，Samba 構成ファイルの *server string* パラメータのマッピングを行ないます。 このサーバーコメント文字は，HP CIFS Server がネットワーク上での存在を通知する場合や，ユーザが有効なサーバーの一覧を表示したりする場合に，HP CIFS Server が表示するテキストです。 デフォルトの文字列は Samba %v running on %h (OpenVMS) です。 実際の表示では，%v は，オープンソースの Samba のバージョンに置き換えられ，%h はノード名に置き換えられます。

2.10.1.5.5 WINS 名前解決を有効にする

このオプションでは，Samba 構成ファイルの *wins server* パラメータのマッピングを行ないます。 HP CIFS Server がドメイン・コントローラなどの他のシステムへのアクセスを開始した場合，HP CIFS Server はまずリモート・システムの NetBIOS 名を解決して IP アドレスを認識する必要があります。 HP CIFS Server は，WINS，LMHOSTS ファイル，ローカル・サブネットでのブロード・キャスト，あるいは場合によっては DNS など，いくつかの手段で NetBIOS から IP アドレスを取得できます。

注記: NetBIOS 名によっては DNS ネームスペースには存在しないものもあるため，DNS による名前解決だけは十分でない場合があります。

WINS 名前解決を有効にすることで，WINS サーバー IP アドレスを指定することができます。HP CIFS Server は，この IP アドレスを使用して WINS にアクセスして名前を解決します。`WINS name resolution` オプションを有効にした後，複数の WINS サーバー IP アドレスを指定することもできます。

注記: OpenVMS クラスタでは， *`WINS name resolution`* パラメータが有効な場合，WINS Server の IP アドレスとクラスタ・アドレスを指定できるように 次のようなサブ・オプションが "Generic Options" メニューに表示されます。

```
5A. WINS Server IP address:
5B. Cluster addresses:
```

2.10.1.5.6 クラスタ・アドレス

このオプションは，HP CIFS Server 構成ファイルで *`cluster addresses`* パラメータを割り当てるためのものです。 *`WINS name resolution`* パラメータが有効な場合， クラスタ・アドレス値を入力する必要があります。

OpenVMS クラスタでは，クラスタの複数のノードが同じ `samba$root` ディレクトリを共有する場合， WINS サーバーに共通の CIFS クラスタ別名を登録する必要があります。 この共通の CIFS クラスタ別名は，CIFS クラスタで 同じ `samba$root` ディレクトリを共有する すべてのノードの IP アドレスを示さなければなりません。 これにより，共通の CIFS クラスタ別名を使用して， 登録されているノードにクライアントが接続できるようになります。

WINS サーバーでは， 同じ `samba$root` ディレクトリを共有する OpenVMS クラスタのすべてのノードの IP アドレスを 共通の CIFS クラスタ別名に正しく登録するには， ユーティリティが次のようなメッセージを表示したときに これらのすべてのノードの IP アドレスを コンマで区切って指定する必要があります。

```
IP addresses of cluster nodes sharing same samba$root: []
```

2.10.1.5.7 名前解決の順序

このオプションは，HP CIFS Server 構成ファイルに *`name resolve order`* パラメータを 割り当てるためのものです。 *`Name resolution order`* パラメータは，どのネーミング・サービスを使用して どのような順序で IP アドレスに対するホスト名を解決するかを Samba スイート内のプログラムが決定するのに使用されます。 このオプションは NETBios 名前解決処理を制御します。 名前解決オプションの文字列はコンマで区切って指定します。

オプション文字列としては，lmhosts，host，wins および bcast を使用できます。

たとえば，WINS 名前解決パラメータが有効な場合に，WINS オプションを使用するように名前解決の順序を変更したい といった場合があるかもしれません。

この場合，新しい名前解決順序を次のように指定することができます。

```
wins,lmhosts,host,bcast
```

2.10.1.5.8 一般オプションの設定

一般構成メニューのオプションで値を指定した後，Samba 構成ユーティリティは汎用の Samba 構成ファイル `SAMBA$ROOT:[LIB]GENERIC_SMB.CONF` を作成します。 一般構成メニューで変更できるパラメータだけでなく，Samba 構成ユーティリティはさらに OpenVMS ファイル・フォーマットをサポートするための *`vfs objects`* パラメータを追加することができます。`SAMBA$ROOT:[LIB]GENERIC_SMB.CONF` ファイルのどのオプションも手動では変更しないでください。

注記: OpenVMS クラスタ環境では，SAMBA$ROOT インストール・ディレクトリを共有するクラスタ・ノードのうち 1 つのクラスタ・ノードでのみ Generic options メニューを実行してください。

2.10.1.6 HP CIFS Server システム固有の構成

Samba 構成ユーティリティの Main Menu の 3 つ目のオプションは System specific setup です。 このオプションでは，SMBD や SWAT のような HP CIFS サービス，ファイル・サーバー・クライアント機能，使用するネットワーク・インタフェース，オープン・ファイル・キャッシュ機能などを構成することができます。 Samba 構成ユーティリティの Main Menu でオプション 3 あるいは A を選択すると，次のような構成メニューが表示されます。

```
HP OpenVMS CIFS System Specific Configuration Options Menu

In cluster, you can use this menu to setup node specific CIFS Server
configuration options.

        1. TCP Ports used by CIFS: [445,139]
        2. File Server client capacity: 50
        3. Enable SWAT service: yes
        4. Restrict Network interfaces: no

Enter item number or press Enter to accept current values [Done]:
```

2.10.1.6.1 CIFS が使用する TCP ポート

このオプションでは，Samba 構成ファイル・パラメータ *smb ports* のマッピングを行ないます。 また，TCP/IP データベースで HP CIFS SMBD サービスを設定する方法を制御することもできます。 デフォルトでは，HP CIFS Server サーバーは，TCP ポート 139 (NetBIOS over TCP/IP) および TCP ポート 445 (SMB over TCP/IP) の両方で着信要求を待ち受けます。 ユーザは，HP CIFS Server が着信要求を受けとるのに使用する TCP ポートを 445 あるいは 139 のどちらかに制限することができます。

2.10.1.6.2 ファイル・サーバー・クライアントのキャパシティ

このオプションでは，Samba 構成ファイルの *max smbd processes* パラメータのマッピングを行ないます。 OpenVMS では，*max smbd processes* パラメータはクライアント制限を制御できません。 クライアント制限は，TCP/IP データベースで SMBD サービスを設定する際に Limit 修飾子で制御できます。

クライアント・キャパシティは，HP CIFS Server への同時アクセスが可能なクライアント数の上限で決まります。 Samba 構成ユーティリティを使用すると，このクライアント・キャパシティを指定することができます。 デフォルトでは，HP CIFS Server は TCP/IP ポート 139 および 445 を使用するように設定されます。 HP CIFS Server が使用する TCP/IP ポートが制限されていなければ，各ポートのクライアント・キャパシティが指定された数に設定されます。 たとえば，指定されたクライアント・キャパシティが 100 の場合，HP CIFS Server はポート 139 の上限を 100，ポート 445 の上限を 100 と指定します。 このため，クライアント・キャパシティを 100 と指定すると，HP CIFS Server の最大クライアント数は 200 に設定されます。

2.10.1.6.3 SWAT サービスを有効にする

SWAT (Samba Web Administration Tool) サービスを使用すると，システム管理者は Web ブラウザから HP CIFS のサーバー構成ファイル (SMB.CONF) の参照および変更することができます。 SWAT についての詳細は 2.10.2 項「Samba Web Administration Tool (SWAT) による HP CIFS の構成」 を参照してください。

2.10.1.6.4 ネットワーク・インタフェースを限定する

このオプションでは，Samba 構成ファイルの *bind interfaces only* および *interfaces* パラメータのマッピングを行ないます。 OpenVMS システムのインストール時に HP TCP/IP

Services を使用するように設定されている場合，このオプションによる設定は，TCP/IP データベースの SMBD サービスの設定時に /address 修飾子が使用される方法にも影響を与えます。SMBD サービスは， HP TCPIP Services の TCPIP SET SERVICE コマンドで登録されます。

複数のネットワーク・インタフェースを持つシステムでは，HP CIFS Server が着信要求の待ち受けに使用するネットワーク・インタフェースを Samba 構成ユーティリティで指定できます。使用するネットワーク・インタフェースを制限することを選択した場合，そのインタフェースの IP アドレスを指定するためのプロンプトが表示されます。 コンマを使用すると，複数のインタフェース IP アドレスを指定することができます。

2.10.1.6.5 システム固有構成の設定

システム固有構成メニューで選択されたオプションに基づいて，Samba 構成ユーティリティは TCP/IP データベースの SMBD および SWAT サービスを設定します。 さらに，適用されるパラメータが設定されたノード固有の構成ファイル
SAMBA$ROOT:[LIB]<SCSNODE>_SPECIFIC_SMB.CONF も作成します。 パラメータ値の変更のためこのファイルを手動で編集するのは避けてください。

注記: OpenVMS クラスタ環境では，HP OpenVMS CIFS をインストールしたノードと同じ SAMBA$ROOT インストール・ディレクトリを共有するすべてのノードに対して SAMBA$DEFINE_ROOT.COM をコピーした後，それぞれのノードで Samba 構成ユーティリティを実行するひつようがあります。 このユーティリティを実行する際，Samba 構成ユーティリティの Main Menu のオプション 1，2 および 3 は，同じ SAMBA$ROOT ディレクトリを共有するノードのうちの 1 つのノードでのみ実行する必要があります。 システム固有の構成を実行するためのオプション 3 は，同じ SAMBA$ROOT ディレクトリを共有するすべてのノードで実行する必要があります。

2.10.1.7 Samba 構成ユーティリティの制約

Samba 構成ユーティリティを使用すると，HP CIFS Server の基本的な構成を行なうことができます。 HP CIFS Server の基本的な構成が設定されると，HP CIFS サーバーを起動して接続を行なうことができます。 Samba 構成ファイルに既存の HP CIFS Server 共有がない場合は，アクセスの前に Samba 構成ファイルに共有を明示的に追加する必要があります。 構成ユーティリティでは，共有を追加するためのオプションは用意されていません。 このユーティリティでは，HP CIFS Server が提供している多くの Samba 構成ファイル・パラメータのうち，基本的なパラメータのみが設定されます。 その他のパラメータの追加あるいは修正に関しては，Samba 構成ファイル SMB.CONF を手動で編集する必要があります。

注記:

- HP CIFS Server で共有を構成する方法については， 第9章 「共有の管理」を参照してください。
- 既存の HP CIFS Server 構成ファイルで *lock dir* および *private dir* パラメータを明示的に使用した場合は， Samba 構成ユーティリティを使用すべきではありません。

2.10.2 Samba Web Administration Tool (SWAT) による HP CIFS の構成

SWAT は，Windows から HP CIFS Server を管理するための Web インタフェースです。

このユーティリティを使用するためには，次のコマンドを実行して，
SAMBA$ROOT:[UTILS]SAMBA$SWAT_FILES.BCK ファイルを SAMBA$ROOT:[SWAT...] ディレクトリ以下にリストアする必要があります。

```
$ BACKUP SAMBA$ROOT:[UTILS]SAMBA$SWAT_FILES.BCK/SAVE -
_$ SAMBA$ROOT:[*...]*.*;*/LOG
```

SWAT についての詳細は以下の URL を参照してください。

http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/SWAT.html

2.10.3 HP CIFS 構成ファイル

HP CIFS 構成ファイルのデフォルトのファイル名は SMB.CONF で，この構成ファイルの形式は Windows の .ini ファイルと同じです。 SMB.CONF ファイルはプレーン・テキスト・ファイルであるため，通常使用している編集ツールで編集できます。

SMB.CONF ファイルには，必須の構成パラメータが含まれています。

注記: SMB.CONF ファイルは非常に重要なファイルです。このファイルを編集する際には注意してください。 構成に関する詳細については，次の Web サイトを参照してください。

http://www.samba.org

2.10.3.1 構成ファイルの構造

以下に，構成ファイルの構造の例を示します。

```
[global]
...
[homes]
...
[<file/printer share-name>]
...
```

大括弧内の名前は，SMB.CONF ファイルの固有のセクションを表します。 各セクションは，そのセクションが参照する共有名 (またはサービス名) を指定します。 たとえば，[homes] セクションは特別なディスク共有で，このセクションには，CIFS サーバー上の特定のホーム・ディレクトリに割り当てるオプションが含まれます。 [global] セクションを除き，SMB.CONF ファイルで定義されるセクションはすべて，ディスクまたはプリンタ共有として，HP CIFS Server に接続するクライアントから利用できます。

2.10.3.2 セクションの説明

SMB.CONF ファイル内の各セクションは，HP CIFS Server 上の共有を表しています。 "global" は，ある特定の共有に対してではなく，CIFS サーバー全体に対して適用される設定が含まれている特別なセクションです。 特別なセクションとしては，[global]，[homes] および [<file/printer share-name>] の 3 つがあります。 以下にこれらのセクションについて説明します。

特別なセクション

[global] セクション

このセクションのパラメータは，サーバー全体に適用されるか，対応する項目が特に指定されていない各セクションのデフォルト値となります。

[homes] セクション

構成ファイルに homes というセクションが含まれていれば，クライアント・ユーザ自身のホーム・ディレクトリに接続するサービスを，サーバーによって自動作成できます。

[file/printer share-name>] セクション

指定された名前が共有名になり，Printable パラメータが YES に設定されていると， この共有はプリンタ共有として機能します。 Printable パラメータが NO に設定されていると，この共有はファイル共有またはディスク共有として機能します。

パラメータ

パラメータは，各セクションの特定の属性を定義します。 パラメータは 2 種類あり，次のように呼ばれます。

- グローバルパラメータ - [global] セクション固有のパラメータ。 たとえば，workgroup，security などです。
- サービス・パラメータ - サービスごとの各セクションに固有のパラメータ。 これらはすべてのセクションで使用可能です (たとえば，browsable など)。

注記: 構成ファイル (SMB.CONF) の詳細については，次の Web サイトを参照してください。
http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html

2.10.3.2.1 構成ファイルの検証

次のコマンドを入力して，SMB.CONF の内容を検証します。

```
$ TESTPARM
```

TESTPARM は，SMB.CONF ファイルに構文エラーがないか調べ，エラーが見つかった場合は，お使いのシステムで有効なサービスのリストと共にエラーを出力します。

注記: TESTPARM が何も問題を報告しなくても，構成ファイルで指定したサービスが使用できることあるいは期待どおり動作することを保証するものではありません。

2.10.3.2.1.1 サンプル構成ファイル (SMB.CONF)

```
[global]
server string = Samba %v running on %h (OpenVMS)
security = user
passdb backend = tdbsam
domain master = yes
guest account = SAMBA$GUEST
domain logons = Yes
log file = /samba$root/var/log.%m
log level = 0
load printers = no
printing = OpenVMS
[homes]
comment = Home Directories
browsable = no
read only = no
create mode = 0750
[HPLASER]
path = /samba$root/spool/
printable = yes
min print space = 2000
[test1]
browsable = yes
writeable = yes
```

```
path = /DKA0/users/test1/
```

2.11 HP CIFS Server の起動と停止

ここでは，HP CIFS Server の起動と停止について説明します。

2.11.1 HP CIFS Server を手動で起動

HP CIFS Server を手動で起動するには，次のコマンドを入力します。

```
$ @SYS$STARTUP:SAMBA$STARTUP.COM
```

HP CIFS Server が起動され，次のようなメッセージが表示されます。

```
Creating NMBD Process
[ Creating NMBD Process... ]
%RUN-S-PROC_ID, identification of created process is 0004EA65

[ Enabling SMBD services... ]

[ Successfully enabled TCPIP SMBD services. ]
```

2.11.2 HP CIFS をシステム・ブート時に起動

OpenVMS システムのブート時に HP CIFS Server が必ず自動起動するように設定するには，サイト固有のスタートアップ・ファイル SYS$STARTUP:SYSTARTUP_VMS.COM を編集します。CIFS 起動コマンドを，ネットワーク・トランスポートを起動するすべての行の下に追加します。次に例を示します。

```
$ @SYS$STARTUP:TCPIP$STARTUP.COM
.
.
.
$ @SYS$STARTUP:SAMBA$DEFINE_ROOT.COM
$ @SYS$STARTUP:SAMBA$STARTUP.COM
```

2.11.3 OpenVMS クラスタで CIFS を起動する方法

同じ OpenVMS Cluster 内の複数のノードで HP CIFS Server をインストールし，構成した場合，SYSMAN ユーティリティを使って，すべてのクラスタ・メンバー上で手動で同時に CIFS を起動することをお勧めします。

すべてのクラスタ・ノードで同時に CIFS を起動するには，いずれかのメンバー・ノード上で SYSTEM アカウントへログインしていることを確認してから SYSMAN を実行してください。表 2-1 に SYSMAN ユーティリティについて説明します。

表 2-1 SYSMAN ユーティリティ

入力するコマンド	操作
$ **RUN SYS$SYSTEM:SYSMAN**	SYSMAN ユーティリティを起動します。
SYSMAN> **SET ENVIRONMENT/NODE=(node1,node2,...)**	サーバーを起動する OpenVMS Cluster メンバーを定義します。 たとえば， SYSMAN> **SET ENVIRONMENT/NODE=(SPEEDY,SPIN,SPAN)**
SYSMAN> **DO @SYS$STARTUP:SAMBA$STARTUP.COM**	上記のコマンドで定義したすべてのノードで HP CIFS Server を起動します。
SYSMAN> **EXIT**	SYSMAN ユーティリティを終了します。

2.11.4 HP CIFS Server の停止

HP CIFS Server を手動で停止させるには，次のコマンドを実行します。

```
$ @SYS$STARTUP:SAMBA$SHUTDOWN.COM
```

2.12 インストールおよび構成に関するトラブルシュート

HP CIFS Server のインストールあるいは構成の際に遭遇する可能性のあるいくつかの問題について説明します。

- OpenVMS Integrity システムへの HP CIFS Alpha キットのインストール

  Integrity サーバーへ Alpha キットをインストールしようとした場合，PCSI ユーティリティ・プロシージャは次のようなエラー・メッセージを表示してインストレーションを中断します。

  ```
  HP AXPVMS SAMBA Version 1.2 ECO1 does not run on OpenVMS I64 systems.
  You can install this product on OpenVMS Alpha systems only.
  ```

- OpenVMS Alpha システムへの HP CIFS Integrity キットのインストール

  AlphaServer に Integrity キットをインストールしようとした場合，PCSI ユーティリティ・プロシージャは次のようなエラー・メッセージを表示してインストレーションを中断します。

  ```
  HP I64VMS SAMBA Version 1.2 ECO1 does not run on OpenVMS Alpha
  systems. You can install this product on OpenVMS I64 systems only.
  ```

- HP CIFS ユーティリティ
  - `testparm`

    `testparm` は，`SMB.CONF` ファイルの内容をテストするプログラムです。`SMB.CONF` ファイルを変更した場合は `testparm` ユーティリティを実行する必要があります。

    ```
    $ testparm
    ```

  - SWAT

    SWAT は，Windows システムから HP CIFS Server を構成するための Web ベース・インタフェースです。また，各構成パラメータのオンライン・ヘルプも提供します。詳細は，2.10.2 項「Samba Web Administration Tool (SWAT) による HP CIFS の構成」を参照してください。

- ログ
  - スタートアップ時に NMBD ログ・ファイルが生成されます。`SAMBA$NMBD_<node-name>.log` ファイルが `SAMBA$ROOT:[VAR]` に保管されます。
  - HP CIFS Server を利用する各クライアントに対し SMBD ログ・ファイルが生成されます。デフォルトでは，これらのファイルは `SMB.CONF` パラメータ log files の指定に従って `SAMBA$ROOT:[VAR]` に保管されます。
- 対話モード `"-i"` で実行ファイルを実行すると，画面にすべてのデバッグ・メッセージが表示され，SMBD プロセスがハングした場所あるいはアボートした場所を正確に把握することができます。
- `SAMBA$ROOT:[BIN]SAMBA$GATHER_INFO.COM` - 情報およびデータ・ファイルを収集し，問題のレポートのためのバックアップ・セーブセット・ファイルを作成するコマンド・プロシージャです。
- パケット・スニファー (Wireshark，Microsoft Network Monitor など) を使用すると，クライアントとサーバー間のネットワーク・トレースを記録することができます。
- System Dump Analyzer を使用するとプロセスを詳細に分析することができます。

- サービス・スタートアップ・コマンド・ファイルの名前が，SMBD スタートアップに適切なスタートアップ・プロシージャをポイントしていることを確認してください。確認するには，次のコマンドを実行します。

  ```
  TCPIP SHOW SERVICE SMBD/FULL
  ```

  以下に例を示します。

```
$ TCPIP SHOW SERVICE SMBD445/FULL
Service: SMBD445
State: Enabled
Port: 445    Protocol: TCP     Address: 0.0.0.0
Inactivity: 5  User_name: SAMBA$SMBD    Process: SMBD445
Limit: 500    Active: 0          Peak: 0

File: SAMBA$ROOT:[BIN]SAMBA$SMBD_STARTUP.COM
Flags: Listen
Socket Opts: Rcheck Scheck

Receive: 0 Send: 0
Log Opts: Acpt Actv Dactv Conn Error Exit Logi Logo Mdfy Rjct TimO Addr
TimO Addr
File: SAMBA$ROOT:[VAR]SAMBA$SMBD_STARTUP.LOG

Security
Reject msg: not defined
Accept host: 0.0.0.0
Accept netw: 0.0.0.0
$ TCPIP SHOW SERVICE SMBD/FULL
Service: SMBD
State: Enabled
Port: 139    Protocol: TCP,UDP     Address: 0.0.0.0
Inactivity: 0  User_name: SAMBA$SMBD  Process: SMBD
Limit: 100    Active: 1        Peak: 1

File: SAMBA$ROOT:[BIN]SAMBA$SMBD_STARTUP.COM
Flags: Listen
Socket Opts: None

Receive: 0 Send: 0
Log Opts: Acpt Actv Dactv Conn Error Exit Logi Logo Mdfy Rjct
TimO Addr
File: SAMBA$ROOT:[VAR]SAMBA$SMBD_STARTUP.LOG

Security
Reject msg: not defined
Accept host: 0.0.0.0
Accept netw: 0.0.0.0
```

注記: すべての設定ファイルおよびログ・ファイルにアクセスできることを確認してください。

2.12.1 クライアント接続の確認

クライアント接続を確認する前に，すべてのセキュリティと構成の設定を完了させてください。クライアントからユーザが正しく接続できるかどうかは，以下の手順で確認します。

1. 次のコマンドを実行して NMBD プロセスを開始します。

   ```
   $ @SYS$STARTUP:SAMBA$STARTUP.COM
   ```

2. サーバー名が登録されているかどうか確認するために，クライアント側からコマンド・プロンプトで次のようなコマンドを入力してください。

```
C:\ NBTSTAT -A <IP-address>
```

これにより，そのサーバーの登録済み NetBIOS 名が確認できます。

以下に例を示します。

```
C:\ NBTSTAT -A 16.148.18.31
Local Area Connection:
Node IpAddress: [16.38.47.15] Scope Id: []
NetBIOS Remote Machine Name Table
Name Type Status
---------------------------------------
NEWTON <00> UNIQUE Registered
NEWTON <03> UNIQUE Registered
NEWTON <20> UNIQUE Registered
LANGROUP <00> GROUP Registered
LANGROUP <1C> UNIQUE Registered
LANGROUP <1E> GROUP Registered
MAC Address = 00-00-00-00-00-00
```

3. RUN プロンプトで次のようなアドレスを入力してクライアントから接続します。

   \\<*ip-address-of-CIFS-server*> OR <*name of the server*>

   a. Enter Network Password スクリーンが表示されます。
      - User Name フィールドに domain\user 名を入力し，Password フィールドにパスワードを入力します。
      - 「**OK**」をクリックします。

   b. 共有フォルダの一覧が表示されます。

注記: HP CIFS Server があるドメインのメンバーサーバーとして構成されている場合は，次のようにユーザ名の前にドメイン名を付ける必要があります。

<*domain-name*>\<*user-name*>

2.13 HP CIFS Server の構成に関するその他の問題

2.13.1 HP CIFS Server で NFS を使用している場合の接続

NFS も CIFS も，これらはどちらも複数のシステムからファイル・ストレージへのファイルシステム・アクセス機能を提供します。ただし，ファイルへのアクセス制御，特に書き込みアクセスのためのファイル・オープンは，NFS システムおよび CIFS システムの両方から同時に行うことはできません。 NFS と CIFS はそれぞれ独自のロック・メカニズムを持っており，それらは相互には機能しないため，特定のリソースに対して同時にアクセスすることはできません。

2.13.2 NetBIOS 名は ポート 445 ではサポートされない

HP CIFS Server V1.1 (および Samba 3.0.x) では，ポート 139 の他，ポート 445 で接続することができます。 ただし，ポート 445 接続は SMB over TCP 用で NetBIOS プロトコルはサポートしないため，NetBIOS 名はポート 445 ではサポートされません。 このため，NetBIOS に依存する HP CIFS Server の機能は，このポートでは機能しません。 たとえば， include = /etc/opt/samba/SMB.CONF.%L により他の SMB.CONF.<netbiosname> を参照する virtual server テクニックは機能しません。

サーバーがどのポートで SMB トラフィックを認識するかは SMB.CONF パラメータ smb ports を使用して指定できます。 smb ports に 139 を設定してポート 445 を無効にしてください。 デフォルトでは，smb ports は 445 および 139 に設定されています。

2.13.3 Token sid limit パラメータ

`Token sid limit` は OpenVMS 固有の `SMB.CONF` パラメータで，`[global]` セクション指定します。このパラメータは，ユーザが所属可能なドメイングループの最大数を指定します。デフォルトでは，このパラメータは 750 に設定されます。

2.14 HP CIFS Server ソフトウェアのアンインストール

ここでは，お使いのシステムから HP CIFS Server ソフトウェアを削除する方法を説明します。

クラスタ内の特定のノードで HP CIFS Server 構成を削除する場合は，次のコマンドを入力してください。

```
$ @SAMBA$ROOT:[BIN]SAMBA$REMOVE_CONFIG.COM
```

このコマンド・プロシージャは，そのノードで定義されているすべての HP CIFS Server 論理名の定義を解除し，構成時に設定される SMBD や SWAT などの TCP/IP サービスを削除します。

HP CIFS Server ソフトウェアのアンインストールの手順は以下のとおりです。

1. 特権アカウントでシステムにログインします。
2. 次のコマンドを入力して，NMBD とすべての SMBD プロセスを止めます。

   ```
   $ @SYS$STARTUP:SAMBA$SHUTDOWN.COM
   ```

3. 次のコマンドを入力します。

   ```
   $ PRODUCT REMOVE SAMBA
   ```

この削除コマンドにより，次の処理が行われます。

- 構成ファイルを保管するかどうかのプロンプトが表示されます。ここで言う構成ファイルとは，HP CIFS データベース・ファイル (.tdb)，`SMB.CONF`，`username.map` ファイル，および `LMHOSTS.file` です。
  - プロンプトに対して NO を入力すると，`TDB` ファイルおよび `SMB.CONF` ファイルが削除され，HP CIFS Server 関連の論理名の定義が解除されます。
  - プロンプトに対して YES を入力すると，指定されたファイルが `SYS$COMMON:[SAMBA$SAFETY]` ディレクトリに保管されます。
  - インストール時に作成されたすべての HP CIFS Server アカウントが削除されます。

第3章　HP CIFS の導入モデル

この章では，Samba ドメインモデル，HP CIFS Server のみの構成，あるいは Windows NT / Active Directory ドメインモデルのいずれかのドメインの役割に基づいて HP CIFS Server を構成する方法について説明します。

この章では次のような項目について説明します。

- 3.1 項「ドメインの役割 」
- 3.2 項「Windows ドメインモデル」
- 3.3 項「Samba ドメインモデル」

3.1 ドメインの役割

ここでは，それぞれ異なる役割を持ついくつかのドメイン用に HP CIFS Server を構成する方法について説明します。

3.1.1 プライマリ・ドメインコントローラ

各ドメインには，必ずプライマリ・ドメインコントローラが存在します。プライマリ・ドメインコントローラ (PDC) はドメイン内でいくつかのタスクを担当します。以下にそれらを示します。

- ユーザログオン時の認証，およびドメインメンバーのワークステーションの認証を行います。
- ドメインのユーザアカウントおよびグループ情報を管理します。
- プライマリ・ドメインコントローラにドメイン管理者としてログオンしたユーザは，ドメインに所属する任意のマシンの Windows ドメインアカウント情報を追加，削除，変更できます。
- ドメイン・マスターブラウザおよびその IP サブネットのローカル・マスターブラウザとして機能します。

3.1.2 バックアップ・ドメインコントローラ

バックアップ・ドメインコントローラ (BDC) には以下のような機能があります。

- PDC に接続している広域ネットワーク・リンクがダウンしている場合でも，BDC を利用することにより，ユーザログオンの認証やドメインメンバーであるワークステーションの認証を行うことができます。
- BDC は，ドメインのセキュリティとネットワークの一貫性の面で重要な役割を果たします。
- ローカル・ネットワーク上の PDC の負荷が非常に高くなっている場合に，BDC がネットワーク・ログオン要求を引き受け，ユーザを認証できます。 これによりネットワーク・サービスの堅牢性が向上します。
- PDC で障害が発生したり，サービスの停止が必要な場合には，BDC を PDC に昇格させることができます。 これはドメインコントローラ管理における重要な機能です。

3.1.3 ドメイン・メンバーサーバー

ドメイン・メンバーサーバーは，ドメイン・セキュリティには参加しますが，ドメインアカウント・データベースのコピーは持ちません。各ドメイン・メンバーサーバーは別々にローカルアカウント・データベースを持ちますが，ドメインコントローラあるいはトラステッド・ドメインが管理するアカウントを利用することもできます。

- 以下のメンバーサーバーがサポートされます。
  - Windows NT
  - Windows 2000 および Windows 2003

  - HP CIFS Server
  - Advanced Server for OpenVMS
- ドメインユーザは，ファイル共有やプリンタ共有になどのドメイン・メンバーサーバーのリソースにアクセスすることができます。
- メンバーサーバーは，ユーザ認証要求をドメインコントローラに渡してドメインユーザを認証します。

3.2 Windows ドメインモデル

Windows ドメインモデルは，次のような環境で使用できます。

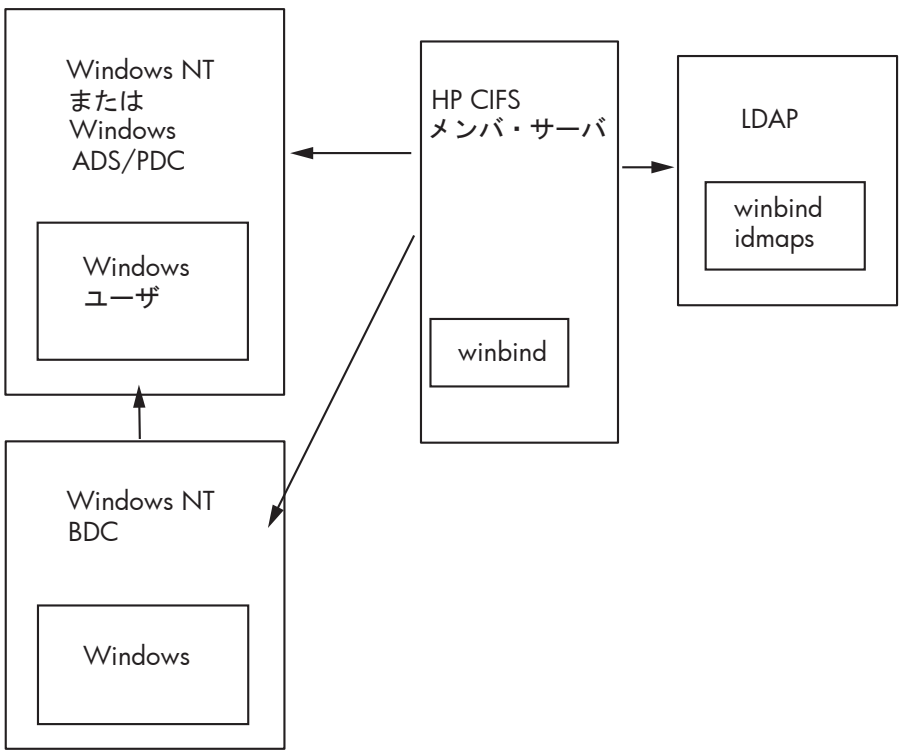
- Windows NT4，Advanced Server for OpenVMS，あるいは Windows 200x サーバーを (NetBIOS 機能を有効にして) 導入している。
- ファイルおよびプリント・サービスを提供する任意の数の HP CIFS メンバーサーバーをサポートする。
- さらに大規模な導入の場合は，複数の HP CIFS Server 間の `winbind` ID マップを保持するために，LDAP Enterprise Directory Server にバックエンドストレージとしてアクセスする。

Windows ドメインモデルには次の利点があります。

- Windows ドメインメンバーのシングルサインオン，ネットワーク・ログオン，および Windows アカウント管理システムを使用できる。
- `winbind` を使用することで，複数の HP CIFS Server 間のユーザ管理を簡単に行える。
- 簡単に機能拡張できる。

図 3-1は，Windows ドメイン導入モデルを示しています。

図 3-1 Windows ドメイン



Windows ドメインモデルでは，HP CIFS Server は，Windows NT または Windows 200x ドメインコントローラの管理下で，Windows ドメインにメンバーサーバーとして参加できます。HP CIFS Server は，Windows ユーザに対して User ID (UID) および Group ID (GID) のマッピング機能を提供するために `winbind` をサポートしています。 大規模な導入の場合は，LDAP ディ

レクトリを使用することで，複数の HP CIFS Server 間でユニークな ID マップを保持することができます。

3.2.1 Windows ドメインモデルのコンポーネント

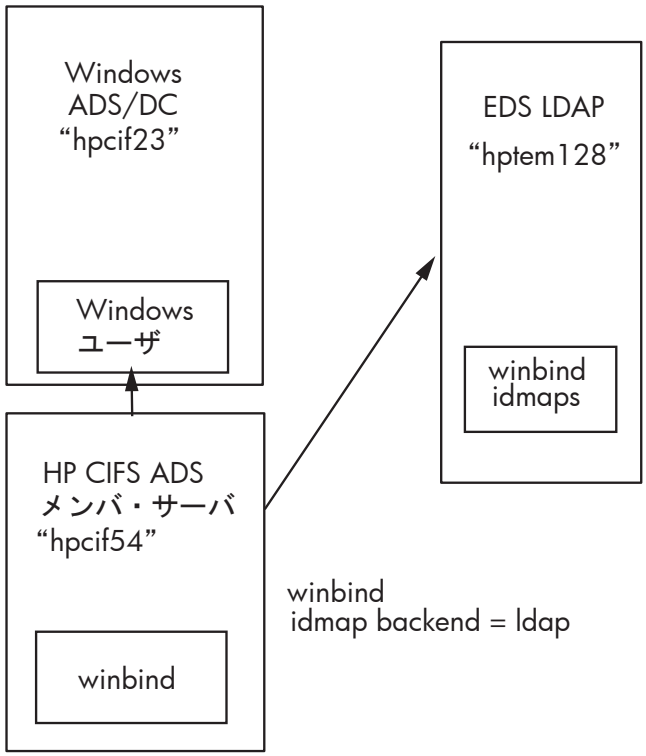
HP CIFS Server は NT ドメインメンバーシップに対して使用される NTLMv1/NTLMv2 セキュリティをサポートするため，Windows 2000/2003 ADS，Windows 200x 混在モード，あるいは NT 環境で HP CIFS Server を管理できます。 HP CIFS Server は標準の SAM データベースをサポートしないため，Windows NT，Windows 2000，または Windows 2003 ドメインでドメインコントローラとして参加することはできません。 HP CIFS Server は `winbind` をサポートします。これを使用して，OpenVMS ユーザとグループを Windows ユーザとグループのマッピングに明示的に割り当てるのを回避することができます。 `winbind` は，Windows ユーザに対して UID と GID の生成機能およびマッピング機能を提供します。 `SMB.CONF` パラメータ `idmap uid = <uid range>` および `idmap gid = <gid range>` を設定してください。 `winbind` についての詳細は，第7章「WINBIND のサポート」を参照してください。 複数の HP CIFS Server を配備する場合は，LDAP ディレクトリを使用して複数のシステム間で一意の ID マップを保持することができます。この処理を行わないと，システム間でユーザマッピングの整合性が取れなくなります。LDAP ディレクトリ内で ID マップを一元管理するには，`SMB.CONF` ファイル内の `idmap backend` パラメータを `ldap:ldap://<ldap server name>` に設定します。

`SMB.CONF` パラメータ `wins server = <Windows or NT WINS server address>` を設定して，マルチサブネット・ネットワーク全体にアクセスできるように構成することもできます。

3.2.2 ADS ドメインモデルの例

図 3-2 は，ドメインコントローラ・マシン `hpcif23`，メンバーサーバーとして機能する HP CIFS Server マシン `hpcif54`，および Enterprise Directory Server システム `hptem128` で構成される Windows 2000/2003 ADS ドメインモデルの例です。

図 3-2 ADS ドメインモデルの例



3.2.3 HP CIFS Server をネイティブの ADS メンバーサーバーとして構成する

HP CIFS Server を ADS メンバーサーバーとして構成するには，次の要件を満たしている必要があります。

- HP CIFS Server が参加する Windows ドメインの PDC の完全修飾ドメイン名が，DNS サーバーを使用して IP を解決できる必要があります。
- Kerberos のクロックスキュー・エラーを避けるために，Windows ドメインの PDC と HP CIFS Server の時間の差は 5 分未満にすべきです。

HP CIFS Server を ADS メンバーサーバーとして追加する手順は 以下のとおりです。

1. Samba 構成ファイル `SMB.CONF` に次のパラメータを設定します。

```
[global]
workgroup = <NetBIOS_domain_name>
security = domain
domain logons = no
domain master = no
netbios name = <NetBIOS_name or CIFS_cluster_alisa>
```

ネイティブの ADS メンバーサーバーとして HP CIFS Server を正しく構成するためには，以下のパラメータを設定する必要があります。これらのパラメータについての説明は，2.10 項「HP CIFS Server の構成」を参照してください。

```
security = ADS
realm = <ADS Realm>
password server = <Windows ドメインのドメインコントローラの大文字の FQDN>
client schannel = <yes/no/auto>
require strongkey = <yes/no>
```

さらに必要に応じて，同じ [global] セクションに以下のパラメータを追加します。

一般的な Samba 構成パラメータを指定するには，以下のパラメータを追加します。

```
server string = Samba %v running on %h (OpenVMS)
username map = /samba$root/lib/username.map
log file = /samba$root/var/%h_%m.log
```

ユーザおよびグループのアカウント情報を保管するための passdb バックエンドとして LDAP を使用する場合は，以下のパラメータを追加します。

```
passdb backend = ldapsam:ldap://<LDAP サーバーを実行しているノード名あるいは IP アドレス >
ldap admin dn = <LDAP Admin DN>
ldap passwd sync = yes
ldap suffix = <LDAP Admin DN>
```

注記: passdb バックエンドとして使用する前に，LDAP を正しく設定しておく必要があります。バックエンドとして LDAP を使用するように HP CIFS Server を構成する方法 については，第5章「LDAP 統合のサポート」を参照してください。

HP CIFS Server を WINS クライアントとして構成して，HP CIFS Server が WINS サーバーを使用して NetBIOS 名を解決できるようにするためには，次のパラメータを追加します。

```
wins server = <WINS サーバー IP アドレス >
name resolve order = wins, lmhosts, bcast, hosts
```

CIFS が，ドメインのユーザおよびグループ・アカウントのための OpenVMS アカウントとリソース識別子を作成できるようにするには，次のパラメータを追加します。これらは，指定しなければマッピングされません。

```
idmap uid = <UID 範囲 >
idmap gid = <GID 範囲 >
```

idmap uid および *idmap gid* の範囲については， 第7章 「WINBIND のサポート」 を参照してください。

OpenVMS ログイン・ディレクトリへのユーザ・アクセスを可能にする homes 共有を設定するには，次のパラメータを追加してください。

```
[homes]
 comment = Users home share
 browseable = no
 read only = no
```

2. `testparm` ユーティリティを実行して， サーバーがメンバーサーバーとして構成されていることを確認します。

```
$ @SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS
$ testparm
```

3. HP CIFS Server を ADS メンバーサーバーに加えます。

```
$ net ads join --user=<username-in-domain>
Password:
```

4. 参加を確認します。

```
$ net ads testjoin
```

5. HP CIFS Server を開始します。

```
$ @SYS$STARTUP:SAMBA$STARTUP
```

3.3 Samba ドメインモデル

次のような環境では Samba ドメイン導入モデルが使用できます。

- HP CIFS Server によってドメインが構成されており，Windows ドメインコントローラが存在しない。
- 相応数のユーザにファイルサービスとプリントサービスを提供する任意の数の OpenVMS サーバーをサポートしている。
- 1 つの HP CIFS Server がプライマリ・ドメインコントローラ (PDC) として構成されており，1 つ以上の HP CIFS Server がバックアップ・ドメインコントローラ (BDC) として動作している。
- ドメインのアカウントは，HP OpenVMS Enterprise Directory Server などで作成された LDAP ディレクトリで管理される。
- PDC および BDC は，ユーザの認証時などには，Samba LDAP バックエンド (ldapsam) を使用して LDAP ディレクトリサーバーにアクセスする。

Samba ドメインモデルには次の利点があります。

- 簡単に規模を拡張できます。
- BDC として動作する HP CIFS Server は，ネットワーク・ログオン要求をピックアップできるので，ネットワーク上で PDC がビジー状態の場合でもユーザを認証できます。
- PDC をサービスから除外する必要のある場合や，PDC に障害のある場合，BDC を PDC に昇格させることができます。 PDC-BDC モデルを使用すると，大規模なネットワークで認証の負荷を分散できます。
- PDC，BDC，およびドメイン・メンバーサーバーは，アカウント・データベースを LDAP ディレクトリに保存するので，ネットワークのサイズに関係なく管理を一元化できる。

図 3-3は，ローカルにパスワード・データベースを持つ PDC として動作するスタンドアロンの HP CIFS Server を示しています。

図 3-3 PDC として動作するスタンドアロンの HP CIFS Server

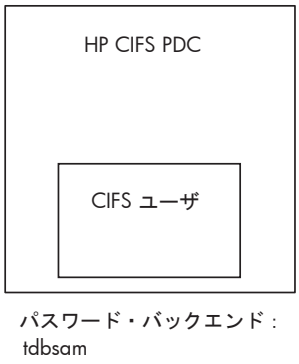


図 3-4 は，LDAP バックエンドとして EDS (Enterprise Directory Server) を使用し，PDC として動作するスタンドアロンの HP CIFS Server を示しています。

図 3-4 EDS バックエンドを使用し，PDC として動作するスタンドアロンの HP CIFS Server

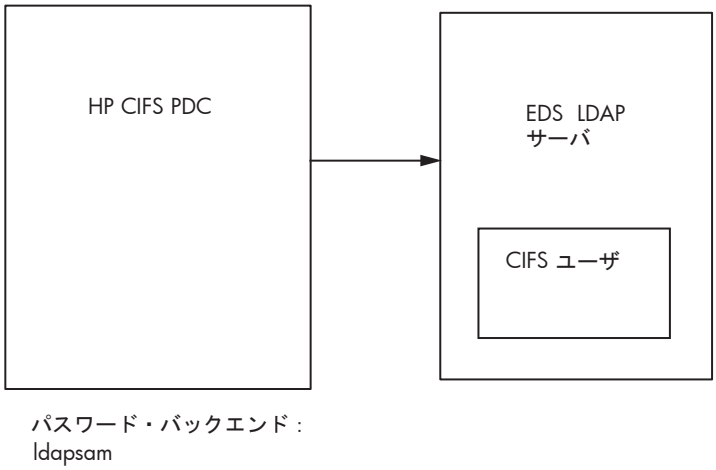
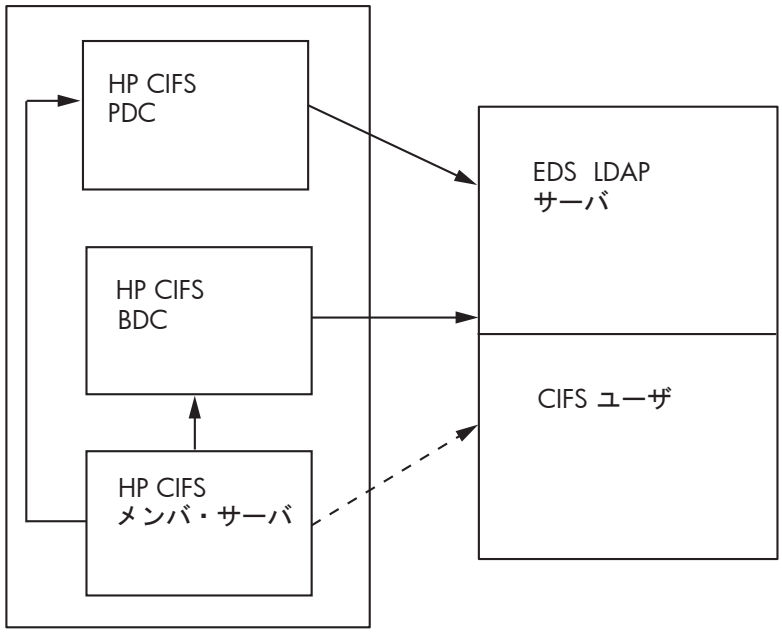


図 3-5は，LDAP バックエンドとして EDS (Enterprise Directory Server) を使用する複数の HP CIFS Server を示しています。

図 3-5 EDS バックエンドを使用する複数の HP CIFS Server



パスワード・バックエンド：
ldapsam

Samba ドメイン導入モデルは，プライマリ・ドメインコントローラ (PDC) として構成された 1 つの HP CIFS Server と，バックアップ・ドメインコントローラ (BDC) として動作する 1 つ以上の HP CIFS Server によって構成されます。 PDC，BDC，およびメンバーサーバーは，一元化された LDAP バックエンドを使用し，LDAP ディレクトリ上で CIFS アカウントを統合しています。

3.3.1 Samba ドメインのコンポーネント

複数のサーバーが必要とされることが多いので，このモデルではディレクトリサーバーと LDAP アクセスを使用します。 POSIX と Windows のユーザ・データを統合管理するのに LDAP サーバーを使用します。 LDAP の設定方法については，詳細は，第5章「LDAP 統合のサポート」を参照してください。

WINS 名前解決

マルチサブネット環境では WINS が使用されます。 マルチサブネット環境では単一の IP サブネットのブロードキャスト制限を超えるため，名前と IP アドレスのマッピングが必要になります。 PC クライアントの構成にも WINS サーバーのアドレスを指定でき，これによって IP サブネット境界の外部にあるシステムのアドレスを認識できます。 HP CIFS Server を WINS クライアントとして構成するには，`SMB.CONF` グローバルパラメータ `wins server` を使用して WINS サーバーの IP アドレスを指定します。 この際，HP CIFS Server が WINS サーバーとなることはできません。

3.3.1.1 PDC として動作する HP CIFS Server

PDC として構成された HP CIFS Server は，ドメイン全体の認証を担当します。 `SMB.CONF` グローバルパラメータ `security = user`，`domain master = yes`，および `domain logons = yes` を設定して，そのサーバーがドメインの PDC となるように指定してください。

CIFS PDC の重要な特性にブラウジング制御があります。パラメータ `domain master = yes` を指定すると，サーバーは，*<domain name>*`1B` という NetBIOS 名を登録します。 `1B` は，ドメイン・マスターブラウザ用に予約されています。 この *<domain name>*`1B` は，他のシステムがドメインの PDC を探す際に使用されます。

単一サーバー構成の場合は，tdbsam パスワード・バックエンドを使用することもありますが，設置する数が多い場合は，LDAP バックエンドを使用して CIFS ユーザを一元的に管理する必要があります。

HP CIFS Server を PDC として構成する方法については， 3.3.2.1 項「PDC として HP CIFS Server を構成」 を参照してください。

3.3.1.1.1 制限事項

PDC のサポートに関しては以下の制限事項があります。

- HP CIFS Server は，SAM (Security Account Management) のアップデート・デルタ・ファイルは作成できません。 HP CIFS Server は，PDC と通信して BDC が持つデルタ・ファイルから SAM の同期化を行うことはできません。
- HP CIFS Server PDC は BDC へのアカウント情報の複製をサポートしていません。 また，BDC を LDAP 以外のバックエンドと共に運用している場合は，SAM データベースの同期が難しくなります。 このため，バックエンドとして LDAP を使用することをお勧めします。 LDAP を使用したドメイン構成については，『Official Samba-3 HOWTO and Reference Guide』の Table 5.1 「Domain Backend Account Distribution Option」を参照してください。

3.3.1.2 BDC として動作する HP CIFS Server

BDC の構成は PDC の構成とよく似ています。 SMB.CONF グローバルパラメータ security = user，domain master = no，および domain logons = yes を設定して，そのドメインの BDC としてサーバーを指定します。 これにより BDC がネットワークログイン処理の大部分を実行できるように構成することができます。 このため，ローカルネットワーク上で PDC がビジー状態の場合でも，ローカルセグメント上の BDC がログオン要求を処理し，ユーザを認証します。 セグメントの負荷が大きくなると，役割が他のセグメントの BDC や PDC に移され，負荷が分散されます。 したがって，ネットワーク全体に BDC をディプロイすることで，リソースを最適化し，ネットワークサービスの堅牢性を向上させることができます。

SMB.CONF 内で local master パラメータを yes に設定すると，ブラウジングをネットワーク全体に広げることもできます。

使用している PDC のサービスを停止させる必要のある場合や，PDC が機能しなくなった場合は，BDC の 1 つを PDC に昇格させることができます。BDC を PDC に昇格させるには，domain master パラメータを no から yes に変更します。

PDC と BDC は，一元化された LDAP ディレクトリを使用し，LDAP ディレクトリに共通の CIFS アカウントを格納します。 BDC として動作している HP CIFS Server を LDAP ディレクトリと統合する場合は，HP LDAP ソフトウェアをインストールして，LDAP クライアントを構成する必要があります。 BDC は，Windows 認証用の LDAP ディレクトリにアクセスできます。

HP CIFS Server を BDC として構成する方法については， 3.3.2.1 項「PDC として HP CIFS Server を構成」 を参照してください。

HP CIFS Server は真の SAM データベースだけでなくその複製も実装していません。 HP CIFS Server の BDC の実装は PDC と非常に良く似ていますが，重要な違いが 1 つあります。 BDC は，smb.conf パラメータ domain master を no に設定しなければならない点を除き，PDC と同じように構成されます。

注記:

`security`
Windows ユーザ，クライアント・マシンアカウント，およびパスワードを `passdb backend` で保管および管理するには，このパラメータに `user` を設定してください。

`domain master`
HP CIFS Server を BDC として機能させるには，このパラメータに `no` を設定してください。

`domain logon`
netlogon サービスを提供するには，このパラメータには `yes` を設定してください。

`Encrypt passwords`
このパラメータに `yes` を設定するとユーザ認証に使用するパスワードが暗号化されます。HP CIFS Server を BDC として構成する場合は，このパラメータに `yes` を設定する必要があります。

3.3.1.2.1 BDC および PDC 間のアカウント・データベースの同期化

Advanced Server と Windows ドメインコントローラの場合と異なり，HP CIFS PDC および HP CIFS BDC 間のユーザアカウント・データベースの自動複製機能は提供されません。 HP CIFS 環境で自動複製を実現するには LDAP サーバーの助けを必要とします。 LDAP バックエンドを使用するように HP CIFS PDC および各 HP CIFS BDC を構成することにより，LDAP サーバー間で発生する同期化の結果としてアカウント・データベースの複製が可能になります。 HP CIFS は LDAP バックエンドを使用して，LDAP ディレクトリ (HP Enterprise Directory あるいは OpenLDAP サーバー) でユーザおよびグループアカウント情報を保管および入手することができます。 1 つの LDAP サーバーを HP CIFS PDC と BDC の両方として使用することは可能ですが，可用性と性能の観点から，HP CIFS PDC と BDC には別の LDAP サーバーを使用することをお勧めします。

`passdb backend` として `tdbsam` が指定されている場合，BDC と PDC 間の複製は下記のコマンドを実行することにより実現できます。

```
NET RPC VAMPIRE -S [NT netbios name or IP] -W [domainname] -U
administrator%password
```

3.3.1.3 メンバーサーバーとして動作する HP CIFS Server

HP CIFS Server は，Samba ドメインに参加させることができます。Windows の認証要求は，LDAP，`tdbsam`，またはその他のバックエンドを使用して，PDC または BDC によって管理されます。サーバーをメンバーサーバーとして指定する場合は，`SMB.CONF` グローバルパラメータ `security = domain`，`domain master = no`，および `domain logons = no` を設定してください。 HP CIFS Server を Samba Domain に参加させる方法については，3.3.2.3 項「HP CIFS Server をメンバーサーバーとして構成」 を参照してください。

メンバーサーバーにおける `SMB.CONF` の構成は，PDC や BDC での構成とは異なります。 メンバーサーバーでは SMB グローバルパラメータ `"security = domain"` を設定する必要があります。これにより，メンバーサーバーがドメインコントローラに認証要求を送信することが可能になります。 PDC に制御を渡すには，`domain master` パラメータに `no` を設定してください。 PDC および BDC の場合と同様に，`passdb backend` パラメータに `tdbsam` を設定するとローカルの HP CIFS Server データベースにメンバーサーバー・アカウントが保管され，`ldapsam` を設定すると HP Enterprise Directory Server for OpenVMS などで作成された LDAP ディレクトリにアカウントが保管されます。

3.3.1.4 スタンドアロン・サーバーとして HP CIFS Server を構成

スタンドアロン・サーバーはネットワーク上でドメインコントローラには依存しません。定義によると，これは，ユーザおよびグループがローカルに作成および制御され，ネットワーク・

ユーザ ID がローカルユーザ・ログインと一致しなければならないことを意味します。サーバーをスタンドアロン・サーバーとして指定するには，SMB.CONF グローバルパラメータ security = user および and domain logons = no を設定してください。

3.3.2 HP CIFS Server を手動で構成する

HP CIFS Server は，3.1 項「ドメインの役割 」で説明している種々の役割を持つように， 自動構成ユーティリティを使用して， あるいは Samba 構成ファイルを手動で編集して構成できます。 HP CIFS Server の構成に使用できる Samba 構成ユーティリティは SAMBA$ROOT:[BIN]SAMBA$CONFIG.COM です。 このユーティリティを使用して HP CIFS Server を構成する方法については， 2.10 項「HP CIFS Server の構成」 を参照してください。

以下の項では， Samba 構成ファイル SAMBA$ROOT:[LIB]SMB.CONF を手動で編集して HP CIFS Server を構成する手順を説明しています。 このファイルには， HP CIFS Server を種々の役割を持つように構成するのに必要な Samba 構成パラメータとその値が記述されています。 同じパラメータを SWAT ユーティリティから選択して HP CIFS Server を構成することもできます。

注記: 以降の項で説明するパラメータについての詳細は， 2.10 項「HP CIFS Server の構成」 を参照してください。

3.3.2.1 PDC として HP CIFS Server を構成

HP CIFS Server を PDC として構成する手順は以下のとおりです。

1. SMB.CONF ファイルに 以下のパラメータを追加します (山括弧 < > で示した箇所は適切な値で置き換えます)。

```
[global]
 workgroup = <NetBIOS ドメインあるいはワークグループ名 >
security = user
 domain logons = yes
 domain master = yes
netbios name = <NetBIOS コンピュータあるいはクラス別名 >
add user to group script = @samba$root:[bin]samba$addusertogroup %g %u
 delete user from group script = @samba$root:[bin]samba$deluserfromgroup %g %u
```

さらに，必要に応じて同じ [global] セクションに次のパラメータを追加します。

一般的な Samba 構成パラメータを指定する場合は，下記のように追加します。

```
server string = Samba %v running on %h (OpenVMS)
 username map = /samba$root/lib/username.map
 log file = /samba$root/var/%h_%m.log
```

ユーザおよびグループ・アカウント情報を保管するための passdb バックエンドとして LDAP を使用するためには，次のパラメータを追加します。

```
passdb backend = ldapsam:ldap://<LDAP サーバーを実行しているノード名あるいは IP アドレス >
ldap admin dn = <LDAP Admin DN>
ldap passwd sync = yes
 ldap suffix = <LDAP Admin DN>
```

注記: LDAP を passdb バックエンドとして使用する前に LDAP の設定を行う必要があります。 バックエンドとして LDAP を使用して HP CIFS Server を構成する方法については，第5章「LDAP 統合のサポート」 を参照してください。

ワークスステーションをドメインに参加させるために， 次のパラメータを追加して WINBIND マッピングを有効にします。

```
idmap uid = <UID 範囲 >
idmap gid = <GID 範囲 >
```

注記: *idmap uid* および *idmap gid* パラメータについての詳細は，第7章「WINBIND のサポート」を参照してください。

HP CIFS Server を WINS クライアントとして構成して HP CIFS Server が WINS を使用して NetBIOS 名を解決できるようにするには， 以下のパラメータを追加します。

```
wins server = <WINServer1 IP アドレス > <WINServer2 IP アドレス >
name resolve order = wins, lmhosts, bcast, hosts
```

プロファイルのローミングを有効にするには，次のように追加してください。

```
logon path = \\%L\profiles\%U
```

プロファイルのローミングについては，3.3.2.1.2 項「ローミングプロファイル」を参照してください。 3.3.2.1.2 項 で説明するように， SMB.CONF に [PROFILES] 共有を追加することもできます。

ユーザがドメインにログインする際に実行する netlogon スクリプトを指定するには， 次のようなパラメータを追加します。

```
logon script = < ログオン・スクリプトのパス >
```

ドメインへのユーザログイン時にユーザログオン・スクリプトが 実行されるように netlogon 共有を設定るるには， 以下のパラメータを追加します。

```
[netlogon]
 comment = Netlogon share
 path = /samba$root/netlogon
 read only = yes
 browseable = no
 guest ok = yes
 vms path names = no
 write list = @administrators, cifsadmin
```

netlogon 共有についての詳細は， 3.3.2.1.3 項「ユーザログオン・スクリプトの構成」を参照してください。

ユーザが OpenVMS ログイン・ディレクトリにアクセスできるようにするための homes 共有の設定には，次のパラメータを追加します。

```
[homes]
 comment = Users personal share
 browseable = no
 read only = no
```

2. `testparm` ユーティリティを実行して，サーバーが PDC として構成されていることを確認します。

```
$ @SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS
$ testparm
```

3. 次のコマンドを実行して HP CIFS Server を起動します。

```
$ @SYS$STARTUP:SAMBA$STARTUP
```

3.3.2.1.1 HP CIFS ドメインへの Windows クライアントの追加

ここでは，HP CIFS PDC を持つドメインへ Windows クライアントを追加する方法について説明します。

1. Windows クライアント用の OpenVMS アカウントを作成します。 アカウント名はクライアント・コンピューターと同じにし，ドル記号 ($) を後に 1 つ付与する必要があります。このドル記号はこのアカウントがマシンアカウントであることを示しています。 次に例を示します。

```
$ MC AUTHORIZE ADD winstatn01$$ /FLAG=NODISUSER/UIC=[1000,1]
```

注記: HP CIFS Server が PDC として構成されている場合，HP CIFS Server PDC に追加するワークステーション名は 11 文字を超えてはいけません。この制限は，OpenVMS ユーザ名の長さが SYSUAF データベースで 12 文字に制限されているために存在します。

2. クライアント・コンピューター用の HP CIFS マシンアカウントを作成します。pdbedit ツールを使用してアカウントを作成し，それがマシンアカウントであることを指定します(マシン名の末尾にはドル記号は含めないでください。ドル記号は pdbedit が自動的に追加します)。このアカウント名は，上記の手順 1 でそのマシンに対して作成された OpenVMS アカウントと同一でなければなりません。

   ```
   $ pdbedit -am winstatn01
   ```

   このアカウントは他のアカウントと同じように表示することができますが，その際はドル記号を含む完全なアカウント名を指定する必要があります。次に例を示します。

   ```
   $ pdbedit --list --verbose winstatn01$
   ```

注記: Samba 構成ファイル SMB.CONF で 有効な範囲の *idmap uid* および *idmap gid* が指定されている場合，「手順 1」 および「手順 2」 は省略できます。

3. アカウントを作成した後，ドメインへ Windows ワークステーションを追加できます。Windows クライアントから以下の手順を実行してください。
   a. 任意のユーザとしてログインします。
   b. 「**マイ コンピューター**」 右クリックし，「**プロパティ**」を選択します。
   c. 「**コンピュータ名**」タブを選択します。
   d. 「**変更**」ボタンをクリックします。
   e. "次のメンバー" セクションで「**ドメイン**」オプションを選択し，HP CIFS ドメインの NetBIOS ドメイン名を指定します。「**OK**」をクリックします。
   f. プロンプトに対してドメイン管理者の認証情報を入力します。成功したら，システムは welcoming you to the domain メッセージを表示します。「**OK**」をクリックします。
   g. 「**OK**」 をクリックし，システムリブートに関するメッセージに同意します。
   h. 「**OK**」 のクリックにより，名前の変更が完了しリブートが行われます。

      システムリブートの後，Windows Security ログイン・スクリーンが表示されます。ドメインの 'username' および 'password' を入力してください。「**Logon to** 」ドロップダウン・ボックスからドメイン名を選択します。「**Logon to**」ボックスが存在しない場合，「**Options**」ボタンをクリックして表示させてください。

3.3.2.1.2 ローミングプロファイル

PDC として構成された HP CIFS Server は，以下の特徴を持つローミングプロファイルをサポートしています。

- ユーザの環境設定，基本設定，デスクトップ設定などが HP CIFS Server に保存されます。
- ローミングプロファイルは共有として作成でき，Windows クライアント間で共有可能です。
- ユーザがドメイン内のワークステーションにログオンした場合，PDC として構成された HP CIFS Server の共有からローカル・マシンにローミングプロファイルがダウンロードされます。ログアウト時には，ローカル・マシンのプロファイルがサーバーにコピーされます。

3.3.2.1.2.1 ローミングプロファイルの構成

ローミングプロファイルの構成手順は以下のとおりです。

1. SMB.CONF ファイルのグローバルパラメータ logon path を使用して，ローミングプロファイルを変更または使用可能にします。例を次に示します。

```
[global]
 #%L substitutes for this server's NetBIOS name, %U is the user name
 logon path = \\%L\profiles\%U
```

2. ローミングプロファイル用の [profiles] 共有を作成します。ユーザプロファイル・ファイル用に使われるプロファイル共有に対して，profile acls = yes を設定します。 通常の共有では，共有上に作成されるファイルの所有権が不正なものとなるため，profile acls = yes を設定しないでください。 [profiles] 共有の構成例を以下に示します。

```
[profiles]
 profile acls = yes
 path = /samba$root/profiles
 read only = no
 create mode = 04600
 directory mode = 04770
 writeable = yes
 browseable = no
 guest ok = no
 vms path names = no
```

注記: SAMBA$CONFIG.COM ユーティリティを使用して HP CIFS Server を構成している場合は， デフォルトで PROFILES 共有を追加できます。

3.3.2.1.3 ユーザログオン・スクリプトの構成

ユーザログオン・スクリプトの構成は，以下の要件を満たしている必要があります。

- ユーザログオン・スクリプトは，HP CIFS Server 上のファイル共有 [netlogon] に保存されている必要があります。
- OpenVMS 実行可能権限が設定されている必要があります。
- ログオン・スクリプトには，Windows クライアントが認識できる有効なコマンドが含まれていなくてはなりません。
- ログオン・スクリプトを実行するログオン・ユーザは，適切なアクセス権限を持っている必要があります。

ユーザ・ログイン・スクリプトの構成例を以下に示します。

```
[global]
 logon script = %U.bat
[netlogon]
 path = /samba$root/netlogon
 browseable = no
 guest ok = no
```

注記: SAMBA$CONFIG.COM ユーティリティを使用して HP CIFS Server を構成している場合は， デフォルトで NETLOGON 共有が追加されます。

3.3.2.2 HP CIFS Server を BDC として構成する

HP CIFS Server を BDC として構成するには，以下の手順を実行します。

1. Samba 構成ユーティリティ SMB.CONF で以下のパラメータを設定します。

```
[global]
 workgroup = <NetBIOS ドメイン名 >
 security = user
 domain logons = yes
 domain master = no
 netbios name = <NetBIOS コンピュータあるいはクラスタ別名 >
 add user to group script = @samba$root:[bin]samba$addusertogroup %g %u
 delete user from group script = @samba$root:[bin]samba$deluserfromgroup %g %u
```

さらに，必要に応じて同じ [global] セクションに以下のパラメータを追加します。

一般的な Samba 構成パラメータを追加するために以下のように追加します。

```
server string = Samba %v running on %h (OpenVMS)
username map = /samba$root/lib/username.map
log file = /samba$root/var/%h_%m.log
```

ユーザおよびグループ・アカウント情報を保管するための passdb バックエンドとしてデフォルトの SAM データベースバックアップ (tdbsam) の代わりに LDAP を使用する場合，以下のパラメータを追加します。

```
passdb backend = ldapsam:ldap://<LDAP サーバーを実行しているノード名あるいは IP アドレス >
ldap admin dn = <LDAP Admin DN>
ldap passwd sync = yes
ldap suffix = <LDAP Admin DN>
```

注記: passdb backend として使用する前に， LDAP を正しく設定しておく必要があります。LDAP をバックエンドとして使用するための HP CIFS Server の構成に関する情報については， 第5章 「LDAP 統合のサポート」 を参照してください。

PDC からアカウントを複製するには，以下のパラメータを追加することにより WINBIND マッピングを有効にします。

```
idmap uid = <UID range>
idmap gid = <GID range>
```

注記: *idmap uid* および *idmap gid* パラメータについての情報は，第7章「WINBIND のサポート」 を参照してください。

(HP CIFS Server が WINS を使用して NetBIOS 名を解決できるように) HP CIFS Server を WINS クライアントとして構成するには， 以下のパラメータを追加します。

```
 wins server = <WINS サーバー IP アドレス >
 name resolve order = wins, lmhosts, bcast, hosts
```

ドメインへのユーザ・ログイン時に実行される netlogon スクリプトを指定するには， 次のように追加します。

```
logon script = < ログオン・スクリプトのパス >
```

ドメインへのユーザ・ログイン時にユーザ・ログオン・スクリプトを実行できるように netlogon 共有を設定するには，次のように追加します。

```
[netlogon]
 comment = Netlogon share
 path = /samba$root/netlogon
 read only = yes
 browseable = no
 guest ok = yes
 vms path names = no
```

netlogon 共有についての詳細は， 3.3.2.1.3 項「ユーザログオン・スクリプトの構成」を参照してください。

ユーザが OpenVMS ディレクトリに追加できるように homes 共有を設定するには，次のように追加します。

```
[homes]
 comment = Users share
 browseable = no
 read only = no
```

2. testparm ユーティリティを実行して サーバーが BDC として構成されていることを確認します。

```
$ @SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS
$ testparm
```

3. WINS クライアントとしては構成されておらず， ドメイン PDC が HP CIFS Server BDC とは別のサブネットの場合， BDC の SAMBA$ROOT:[LIB]LMHOSTS．ファイルに 次の 3 つのエントリが含まれている必要があります。

```
<PDC-IP-Address> <PDCname>
<PDC-IP-Address> <Domainname>#1b
<PDC-IP-Address> <Domainname>#1c
```

<PDC-IP-Addess> にはドメイン PDC の IP アドレスを指定し， *<PDCname>* には PDC のコンピュータ名を指定し， *<Domainame>* には SMB.CONF の *workgroup* パラメータに指定されている名前を指定します。

たとえば，HP CIFS ドメイン VMSCIFSDOM の HP CIFS Server PDC の名前が ROX3 で，その IP アドレスが 10.20.20.40 の場合， 次のような LMHOSTS. エントリが必要になります。

```
10.20.20.40 VMSCIFSDOM#1b
10.20.20.40 VMSCIFSDOM#1b
10.20.20.40 ROX3
```

4. 管理者認証情報とともに PDC の名前を指定して NET RPC JOIN コマンドを実行し，ドメインに参加します。 以下に例を示します。

```
$ net rpc join -S <PDCname> --user administrator
Password:
```

5. 次のコマンドで参加を確認します。

```
$ net rpc testjoin
```

6. 次のコマンドで HP CIFS Server を起動します。

```
$ @SYS$STARTUP:SAMBA$STARTUP
```

7. HP CIFS Server BDC を構成し起動した後， BDC，PDC，および BDC 間でアカウント・データベースを同期化する必要があります。 同期化の方法については 3.3.1.2.1 項「BDC および PDC 間のアカウント・データベースの同期化」 を参照してください。

3.3.2.3 HP CIFS Server をメンバーサーバーとして構成

ここでは，HP CIFS Server をドメインへ参加させる手順を説明します。 ドメインのメンバーとなるためには，そのドメインで HP CIFS Server がアカウントを必要とします。 このアカウント名は，SMB.CONF ファイルの "netbios name" パラメータで定義された HP CIFS Server の NetBIOS 名と一致する必要があります。 "netbios name" パラメータがデフォルト値である %h に設定されている場合，この環境変数 %h はローカル・システムのホスト名に変換されま

す。アカウント名にはドル記号が追加され，それがマシンアカウントであることが明示されます。 複数のクラスタ・メンバーが同じ SMB.CONF ファイルを共有する HP CIFS クラスタ環境では，そのクラスタに対する単一のマシンアカウントが必要になり，その名前は SMB.CONF ファイルの "netbios name" パラメータで指定した値と一致しなければなりません。

マシンアカウントは，HP CIFS Server をドメインに追加する前か，HP CIFS Server をドメインに追加する最中のいずれかのタイミングで作成されます。前者の場合，管理者は次に示すように適切な方法を使用して，PDC タイプに依存するドメインにコンピューターを追加します。

- Windows Active Directory Domain (Windows 2000 以降)

  「Active Directory Users and Computers」管理インタフェースを使用して，新しいコンピューターアカウントを追加します。「Add Computer」ウィザードで，HP CIFS Server の NetBIOS 名 (ドル記号は省略) を指定し，「**Assign this computer account as a pre-Windows 2000 computer**」チェック・ボックスのみを選択します。

- Advanced Server for OpenVMS

  ADMIN インタフェースを使用して，次のようにコンピューターアカウントを追加します。

  ```
  $ ADMIN ADD COMPUTER/TYPE=SERVER <CIFS server name>
  ```

  上記の例で，最後の $ 記号は自動的に追加されるので指定しません。

- HP OpenVMS CIFS

  3.3.2.1.1 項「HP CIFS ドメインへの Windows クライアントの追加」で説明した方法で，OpenVMS アカウントと CIFS マシンアカウントを追加します。

- Windows NT PDC

  Server Manager アプリケーションを使用してドメインにコンピューターを追加できます。トップ・メニューから，「**Computer**」を選択し「**Add to Domain**」を選択します。「**Windows NT Workstation or Server**」ラジオ・ボタンをクリックし，HP CIFS Server の NetBIOS 名 (ドル記号は省略) を指定して「**Add**」 をクリックします。

HP CIFS Server がドメインに参加する前にコンピューターアカウントが作成されている場合，HP CIFS Server の管理者は，ドメインにコンピューターを追加するための権限を持つアカウントのドメイン・ユーザ名とパスワードを指定する必要はありません。

ドメインに参加する前に HP CIFS Server のコンピューターアカウントが作成されていない場合，管理者は，ドメインにコンピューターを追加するための権限を持つドメインアカウントのユーザ名とパスワードを指定する必要があります。 たとえば Administrator アカウントなど。

3.3.2.3.1 HP CIFS Server を NT スタイル (ダウンレベル) メンバーサーバーとしてドメインに追加する

HP CIFS Server を NT スタイル (ダウンレベル) メンバーサーバーとしてドメインに追加するには， 以下の手順を実行します。

1. Samba 構成ユーティリティ・ファイル SMB.CONF に以下のパラメータを設定します。

   ```
   [global]

   workgroup = <NetBIOS ドメイン名 >
   security = domain
   domain logons = no
   domain master = no
   netbios name = <NetBIOS 名あるいは CIFS クラスタ別名 >
   ```

   HP CIFS Server をそのドメインの NT スタイル (ダウンレベル) のメンバーサーバー として正しく構成するためには， 以下のようなパラメータが必要になります。

   これらのパラメータについては， 2.10 項 「HP CIFS Server の構成」 を参照してください。

```
password server = < パスワード・サーバー名 >
client schannel = <yes/no/auto>
require strongkey = <yes/no>
vms asv domain = <yes/no>
```

さらに，必要に応じて同じ [global] セクションに 以下のパラメータを追加してください。

一般的な Samba 構成パラメータを指定するには，以下のように追加します。

```
server string = Samba %v running on %h (OpenVMS)
username map = /samba$root/lib/username.map
log file = /samba$root/var/%h_%m.log
```

ユーザおよびグループ・アカウント情報を保管するための passdb バックエンドとして LDAP を使用するには，以下のパラメータを追加します。

```
passdb backend = ldapsam:ldap://<LDAP サーバーを実行しているノード名あるいは IP アドレス >
ldap admin dn = <LDAP Admin DN>
ldap passwd sync = yes
ldap suffix = <LDAP Admin DN>
```

注記: passdb バックエンドとして使用する前に， LDAP は正しく設定しておく必要があります。バックエンドとして LDAP を使用するように HP CIFS Server を構成する方法については，第5章 「LDAP 統合のサポート」 を参照してください。

HP CIFS Server が WINS サーバーを使用して NetBIOS 名を解決できるように HP CIFS Server を WINS クライアントとして構成するには， 以下のパラメータを追加します。

```
wins server = <WINS サーバー IP アドレス >
name resolve order = wins, lmhosts, bcast, hosts
```

ドメイン・ユーザおよびグループ・アカウントに対する OpenVMS アカウントとリソース識別子は 明示的にはマッピングされませんが， CIFS がこれらを作成できるようにするには， 以下のようなパラメータを含めます。

```
idmap uid = <UID 範囲 >
idmap gid = <GID 範囲 >
```

注記: *idmap uid* および *idmap gid* の範囲については， 第7章 「WINBIND のサポート」 を参照してください。

OpenVMS ログイン・ディレクトリに対するユーザ・アクセスを可能にするために homes 共有を設定するには， 次のように追加してください。

```
[homes]
 comment = Users home share
 browseable = no
 read only = no
```

2. testparm ユーティリティを実行して， サーバーがメンバーサーバーとして構成されていることを確認してください。

```
$ @SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS
$ testparm
```

3. WINS クライアントとして構成されておらず， ドメイン PDC が HP CIFS Server と同じ IP サブネットに存在しない場合， SAMBA$ROOT:[LIB]LMHOSTS. ファイルに次のようなエントリが必要になります。

```
<PDC の IP アドレス > < ドメイン名 >#1b
```

```
<PDC の IP アドレス > < ドメイン名 >#1c
<PDC の IP アドレス > <PDC 名 >
```

たとえば，ドメイン ACCOUNTSDOM の PDC の名前が PIANO でその IP アドレスが 10.20.30.40 の場合， 次のような LMHOSTS. エントリを追加する必要があります。

```
10.20.30.40 ACCOUNTSDOM#1b
10.20.30.40 ACCOUNTSDOM#1c
10.20.30.40 PIANO
```

4. 次のように，HP CIFS Server を NT スタイル (ダウンレベル) のメンバーサーバーとして参加させます。

```
$ net rpc join -S <PDC name> --user=<domain administrator account name>
Password:
```

5. 参加を確認します。

```
$ net rpc testjoin
```

注記: HP CIFS Server をネイティブな Active Directory メンバーサーバーとして構成するには，3.2.3 項「HP CIFS Server をネイティブの ADS メンバーサーバーとして構成する」を参照してください。

6. HP CIFS Server を起動します。

```
$ @SYS$STARTUP:SAMBA$STARTUP
```

注記:

1. NET RPC JOIN コマンドを実行する前に HP CIFS を開始する必要はありません。
2. 前述のように，このコマンドは，WINS (SMB.CONF に有効な wins サーバー・エントリが含まれる場合)，lmhosts. ファイルのエントリ，あるいはローカル・サブネットにおけるブロードキャストなどの標準の NetBIOS 名前解決手法を使用してドメインの PDC を探す機能に依存しています。 NetBIOS 名前解決が有効かどうかを確認するには，第11章「管理ツールのコマンド・リファレンス」で説明する nmblookup ツールを使用してください。
3. 別の方法として，NET RPC JOIN には，ドメイン PDC の名前 (-server) あるいは IP アドレス (-ipaddress) を指定するためのオプションが用意されています。 名前が指定されている場合，NET RPC JOIN は NetBIOS 名前解決を使用してその IP アドレスを解決します。
4. NET RPC JOIN コマンドは，SMB.CONF ファイルに指定されている場合 "password server" パラメータを使用しません。
5. ドメインに参加した後，サーバーがドメインに正しく参加しているかどうか確認するには，NET RPC TESTJOIN コマンドを使用してください。

3.3.2.4 HP CIFS Server をスタンドアロン・サーバーとして構成する

HP CIFS Server をスタンドアロン・サーバーとして構成するには，以下の手順を実行します。

1. Samba 構成ファイル SMB.CONF に以下のパラメータを設定します。

```
[global]
 workgroup=<NetBIOS ワークグループ名 >
 security =user
 domain logons = no
 domain master = no
 netbios name = <NetBIOS コンピュータあるいはクラスタ別名 >
```

さらに，必要に応じて同じ [global] セクションに以下のパラメータを追加します。

一般的な Samba 構成パラメータを指定するには，次のように追加します。

```
 server string = Samba %v running on %h (OpenVMS)
```

```
 username map = /samba$root/lib/username.map
 log file = /samba$root/var/%h_%m.log
```

ユーザおよびグループ・アカウント情報を保管するための passdb バックエンド として LDAP を追加するには，以下のパラメータを追加します。

```
passdb backend = ldapsam:ldap://<LDAP を実行しているノードの名前あるいは IP アドレス >
 ldap admin dn = <LDAP Admin DN>
 ldap passwd sync = yes
 ldap suffix = <LDAP Admin DN>
```

注記: passdb バックエンドとして使用する前に，LDAP は正しく設定しておく必要があります。バックエンドとして LDAP を使用するように HP CIFS Server を構成する方法については，第5章「LDAP 統合のサポート」を参照してください。

WINS を使用して NetBIOS 名を解決できるように HP CIFS Server を WINS クライアントとして構成するには，以下のパラメータを追加します。

```
wins server = <WINS サーバー IP アドレス >
 name resolve order = wins, lmhosts, bcast, hosts
```

ユーザが OpenVMS のログイン・ディレクトリにアクセスできるように homes 共有を設定するには，以下のように追加してください。

```
[homes]
 comment = Users home share
 browseable = no
 read only = no
```

2. スタンドアロンの HP CIFS Server では WINBIND は必要ないため，以下のシステム論理名を定義して WINBIND を無効にします。

```
$ DEFINE/SYSTEM WINBINDD_DONT_ENV 1
```

注記: システムをリブートしても論理名が存続し続けるように，SYS$MANAGER:SYLOGICALS.COM に上記の行を追加してください。

3. testparm ユーティリティを実行して，サーバーがスタンドアロン・サーバーとして構成されていることを確認してください。

```
$ @SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS
$ testparm
```

4. HP CIFS Server を起動します。

```
$ @SYS$STARTUP:SAMBA$STARTUP
```

第4章 Kerberos のサポート

Kerberos プロトコルは，IETF RFC 1510 で規定されています。 Kerberos は，Microsoft によって Windows 2000 に採用され，Windows 2000/2003 ドメイン (および，これらのドメイン内に存在する Windows 2000/XP クライアントも含む) ではデフォルトの認証プロトコルになっています。 HP CIFS Server では，Kerberos 認証は，Windows 2000/2003 ドメインでのサーバーメンバーシップの認証にだけ使われ，また HP CIFS Server に"`security = ads`"を構成している場合にだけ使われます。

この章では，Kerberos についての概要と， HP CIFS Server が Kerberos セキュリティプロトコルを利用する 他の OpenVMS アプリケーションと共存している場合にも適用できる 各種の Kerberos 構成情報について説明します。

この章では，次の内容について説明します。

- 4.1 項 「Kerberos の概要」
- 4.2 項 「Kerberos の CIFS 認証の例」

4.1 Kerberos の概要

Kerberos は，認証者，認証対象者，および認証対象者がアクセスする必要があるリソース間で使われる鍵を複合化するために，共有シークレットと暗号化を利用する認証プロトコルです。 HP CIFS Server の場合に該当するのは以下のとおりです。

- Windows Key Distribution Center (KDC): 認証者
- Windows クライアント: 認証対象者
- HP CIFS Server: リソース

CIFS 関連の Kerberos の情報については，HP のホワイトペーパー 『HP CIFS Server and Kerberos』を参照してください。: http://docs.hp.com/en/netcom.html 。

プロトコル交換では，実際に回線上でパスワードが渡されるわけではないので，パスワードを傍受して復号化され，リソースへのアクセスに使われることはありません。回線上で渡されるのは暗号化された鍵であり，3 つのプリンシパル (KDC，Windows クライアント，CIFS サーバー) のそれぞれが，定義済みのシークレットを使って鍵を複合化して，アクセスを許可します。シークレットが送信されることはありません。交換における主要なコンポーネントは，以下のとおりです。

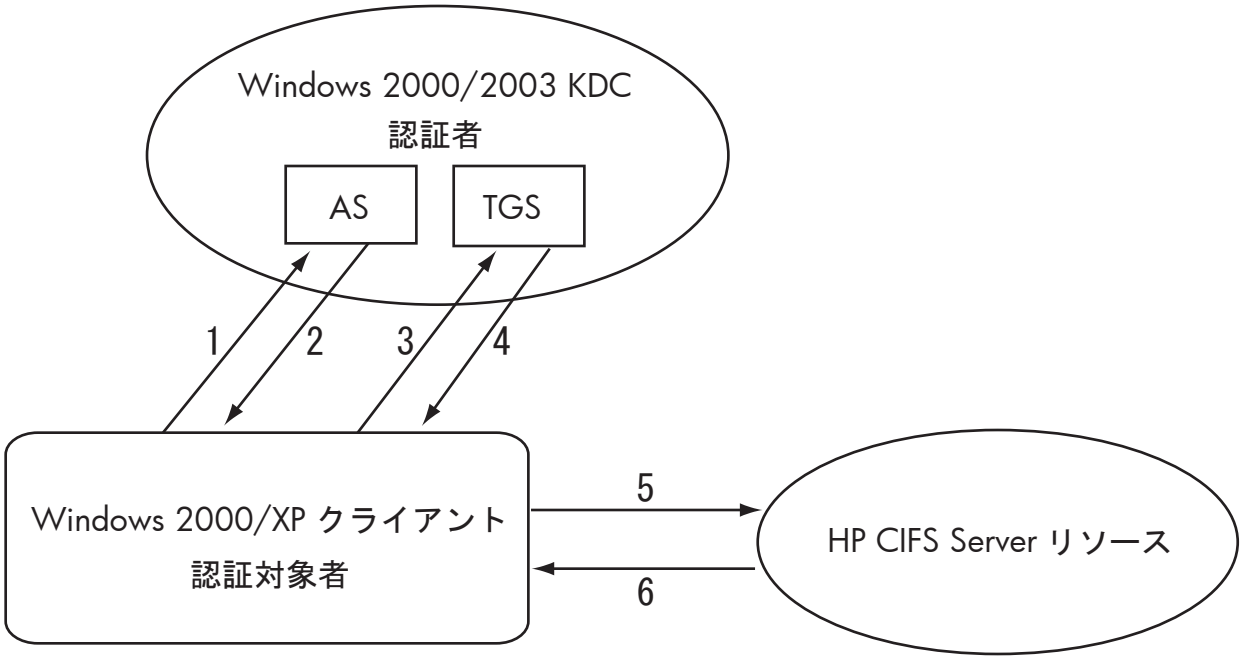
- Windows Key Distribution Center (KDC): ドメインでの Kerberos の中央認証局
- 長期鍵: クライアントのパスワードから計算される固定鍵
- セッション鍵: 期限切れになるまで認証で使われる短期鍵
- チケット認可チケット (TGT): クライアントが TGS からサービスチケットを取得できるように，KDC へのアクセスを許可する
- チケット認可サービス (TGS): クライアントが CIFS サーバーのサービスにアクセスできるようにする交換機能
- 認証サービス: クライアントの KDC へのアクセスを実際に許可する交換機能

Microsoft の Kerberos 実装に関するホワイトペーパーについては，以下の Web サイトを参照してください。

http://www.microsoft.com/technet/prodtechnol/windows2000serv/deploy/confeat/kerbers.mspx

4.2 Kerberos の CIFS 認証の例

図 4-1 Kerberos 認証環境



ここでは，図 4-1 「Kerberos 認証環境」 に示す Windows 2000/2003 ドメイン環境での Kerberos 認証で使われる，典型的な Kerberos のログオンおよび共有サービス交換について説明します。

1. Windows クライアントは，ユーザが `netlogon` コマンドを実行したときに，プリンシパル名とパスワードを認証サーバー (AS) に送信します。
2. AS はプリンシパルが正当であることを確認すると，チケット認可チケット (TGT) と，Windows KDC へのアクセスをクライアントに許可する関連付けられたセッション鍵を含む，資格証明を Windows クライアントに送信します。
3. Windows クライアントは，セッション鍵と TGT を使って，チケット認可サービス (TGS) に対して共有サービスのためのサービスチケットを要求します。
4. TGS は，Windows クライアントに対して，サービスチケットとその他の情報を送信します。
5. Windows クライアントは，サービスチケットを HP CIFS Server に送信して，共有サービスを要求します。
6. HP CIFS Server は受信した情報を確認し，サーバーの共有へのアクセスを Windows クライアントに許可します。

Kerberos 認証を使用するように HP CIFS Server を構成した場合，`TESTPARAM` ユーティリティを実行すると次のようなパラメータ値が表示されます。

```
[global]
workgroup = MYREALM
realm = MYREALM.HP.COM
netbios name = atcux5
server string = Samba Server
security = ADS
password server = HPWIN2K3.MYREALM.HP.COM
```

これらのパラメータ値は，HP CIFS Server の keytab の構成に使用されます。設定した構成は，HP CIFS Server を起動し，クライアントでドメインへログオンし，HP CIFS 共有をマウントすることにより有効になります。

注記: OpenVMS のインストール時に Kerberos を構成するかどうかは任意ですが，HP CIFS Server で Kerberos 認証をサポートするためにはシステムに Kerberos キットがインストールされていることが必須になります。

第5章　LDAP 統合のサポート

この章では，HP CIFS Server の LDAP 統合について説明します。 LDAP の利点，パスワード・バックエンドとして LDAP を使用するように HP CIFS Server ソフトウェアを構成する手順などについても説明します。

5.1 概要

LDAP (Lightweight Directory Access Protocol) とは，集中管理インフラストラクチャを構築するための枠組みを提供するものです。LDAP は，アプリケーション，サービス，ユーザアカウント，Windows アカウント，および構成情報を集中管理するための LDAP ディレクトリに統合することによって，ディレクトリ対応のコンピューティングをサポートします。

多数のユーザとサーバーを抱えた環境で HP CIFS を使用する場合は，HP CIFS Server と LDAP サポートを統合することが望ましい場合があります。 複数の CIFS サーバーが LDAP ディレクトリサーバーと通信できるように構成することにより，ユーザ・データベースを集中的かつスケーラブルに管理できるようになります。 HP CIFS Server を OpenVMS 上の LDAP 製品と統合する場合，HP CIFS Server は Enterprise Directory Server 上にユーザアカウント情報を保管することができます。 LDAP データベースは `tdbsam` あるいは NT サーバーのユーザ・データベースに取って変わることができます。

これまで `passdb.tdb` ファイルに格納されていた Windows ユーザ情報を LDAP ディレクトリに格納することができます。 LDAP パスワード統合機能を使用するように HP CIFS Server が構成されている場合，`SMBD` プログラムは 認証および承認処理の際に LDAP ディレクトリを使用して Windows ユーザ情報を調べることができます。 また，ユーザ情報の追加，削除，変更のために `pdbedit` プログラムを起動する際，`tdbsam` バックエンドが使用する `passdb.tdb` ファイルではなく，LDAP ユーザ・データベースのアップデートが行われます。

LDAP サポートは，HP CIFS Server の構成パラメータを使用することで有効にすることができます。 `SMB.CONF` の `passwd backend` パラメータに `ldapsam` を設定している場合，HP CIFS Server は LDAP ディレクトリサーバーにあるパスワード，ユーザ，グループ，およびその他のデータにアクセスします。

5.1.1 HP CIFS Server の特長

LDAP をサポートする HP CIFS Server には次の特長があります。

- LDAP がユーザ・データベースを集中管理するため，複数の CIFS サーバーでユーザアカウント情報を管理する必要性が低減されます。
- 複数の CIFS サーバーやユーザを容易に LDAP ディレクトリ環境に追加できます。これによって HP CIFS Server のスケーラビリティが大幅に向上します。
- LDAP ディレクトリでユーザアカウント情報の保存および検索が可能です。
- `tdbsam` ファイルに保存される情報には限りがあり，追加的な属性を保存することができません。LDAP サポートでは，スキーマを拡張することができるので，より多くのユーザ情報を LDAP ディレクトリに保存できます。また，これによって社員やユーザのデータベースを別途用意する必要もなくなります。

5.2 ネットワーク環境

HP CIFS Server は，さまざまなネットワーク環境をサポートしています。WINS，ブラウザ制御，ドメイン・ログオン，ローミングプロファイルなど，多くの機能は引き続き利用可能であ

り，さまざまなネットワーク環境をサポートできます。LDAP 統合により，HP CIFS ユーザ認証のための新たな解決策が利用できるようになります。

5.2.1 ドメインモデルのネットワーク

5.2.1.1 プライマリ・ドメインコントローラ (PDC) として動作する HP CIFS Server

PDC は Windows 認証を担当しているため，PDC として構成された HP CIFS Server は，tdbsam を LDAP 対応のディレクトリサーバーに置き換えて Windows 認証を実現します。Samba に関するその他の構成項目は変更する必要はありません。

5.2.1.2 Samba PDC のバックアップ・ドメインコントローラ (BDC) として動作する HP CIFS Server

BDC もまた Windows 認証に使用されるため，BDC として構成された HP CIFS Servers は，ユーザ認証のために LDAP ディレクトリにアクセスできます。 BDC では `SMB.CONF` の `domain master` パラメータを `no` に設定できる点を除き，BDC の構成は PDC の構成と似ています。

5.2.1.3 メンバーサーバーとして動作する HP CIFS Server

ドメインモデルのネットワーク環境でメンバーサーバーとして動作する HP CIFS Server は，個々の Samba 構成を変更することなくそれぞれメンバーサーバーとして動作し続けることができます。 Windows の認証要求は，LDAP を使用しているか `tdbsam` を使用しているかに関係なく，引き続き PDC によって管理されます。

メンバーサーバー (`security = domain`) が LDAP を使用するように構成されている場合，PDC 経由で認証を行おうとします。 PDC 認証が失敗した場合，自身の `SMB.CONF` 構成ファイルに設定されている LDAP ディレクトリサーバー経由で直接認証を試みます。

5.2.2 ワークグループモデルのネットワーク

LDAP が有効になっている場合，ユーザモードの認証が失敗すると，認証は LDAP サーバーにフェール・バックします。 スタンドアロンのユーザモード・サーバーとして構成された HP CIFS Server は，tdbsam を LDAP ディレクトリサーバーに置き換えることができます。

5.2.3 LDAP 統合による CIFS 認証

LDAP 統合により，複数の HP CIFS Server が単一の LDAP ディレクトリサーバーを共有できるようになり，ユーザ・データベースを集中管理できます。HP CIFS Server は，LDAP ディレクトリにアクセスして Windows のユーザ情報を検索し，ユーザ認証を行うことができます。図 5-1 は，LDAP ネットワーク環境での CIFS 認証を示しています。

図 5-1 LDAP 統合による CIFS 認証

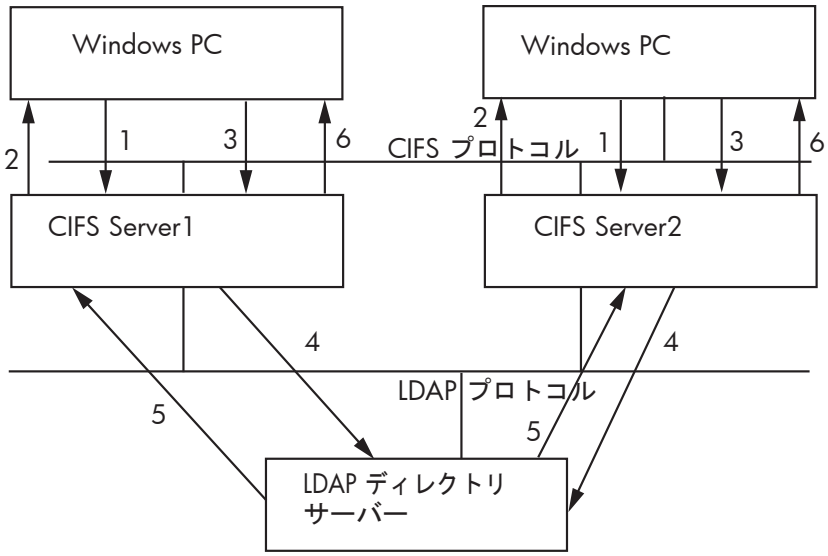


図 5-1 「LDAP 統合による CIFS 認証」 に示された，Windows PC，CIFS Server，および LDAP ディレクトリサーバーの間で行われるユーザ認証のためのメッセージ交換について以下に説明します。

1. Windows ユーザが接続を要求します。
2. CIFS Server は，Windows PC クライアントに `challenge` を送信します。
3. Windows PC クライアントは，ユーザパスワードと `challenge` 情報に基づいて `response` パケットを CIFS Server に送信します。
4. CIFS Server は，LDAP ディレクトリサーバーを調べてユーザデータを検索し，パスワード情報などのデータ属性を要求します。
5. CIFS Server は，LDAP ディレクトリサーバーからパスワード情報などのデータ属性を受け取ります。そのパスワードと `challenge` 情報が，クライアントの `response` パッケージに含まれる情報と一致すれば，Samba ユーザの認証は成功です。
6. ユーザ認証が成功し，有効な OpenVMS ユーザに適切にマッピングできたら，CIFS Server は，ユーザのトークンセッション ID を Windows PC クライアントに返します。

5.3 Directory Server のインストールと構成

ここでは，HP OpenVMS Enterprise Directory の設定および構成方法について説明します。

5.3.1 Directory Server のインストール

まだインストールされていない場合は，HP OpenVMS Enterprise Directory Server を設定する必要があります。 Directory Server のインストール方法については，『HP OpenVMS Enterprise Directory Installing』を参照してください。

5.3.2 Directory Server の構成

HP OpenVMS Enterprise Directory は，HP CIFS で LDAP バックエンドをサポートするために Samba Schema ファイルでアップデートされています。 これは，HP OpenVMS Enterprise Directory が HP CIFS の LDAP バックエンドとして動作するのを想定したものです。 LDAP の構成方法については，『HP OpenVMS Enterprise Directory Management Guide』を参照してください。

HP CIFS パスワード・バックエンドとして LDAP を構成する手順は以下のとおりです。

1. 以下のように，特権アカウントから Network Control Language (NCL) を起動し，次のコマンドを入力して HP CIFS 固有のネーミング・コンテキストを作成します。

```
$ MC NCL

NCL> CREATE DSA NAMING CONTEXT "/DC=<domcompnentname>"
```

/DC は，LDAP (X500) ツリーで作成された DIT (Directory Information Tree) 構造で指定されているドメイン名です。

2. DXIM を起動し，次のコマンドを入力して HP CIFS 固有のディレクトリ・エントリを作成します。

```
$ DXIM /I=C

DXIM> CREATE "/DC=<domcomponentname>"ATTRIBUTES -
_DXIM> objectClass=domain,DC=<domcomponentname>
```

/DC は，LDAP (X500) ツリーで作成された DIT 構造で指定されるドメイン名です。

3. 次のコマンドを実行します。

```
DXIM> SET PASSWORD "/DC=<domcomponentname>"
```

初回時の場合， Old Password> プロンプトで **Enter** キーを押します。

New Password> プロンプトに対し，新しいパスワードを指定します。

Verify Password> プロンプトに対し，確認のために新しいパスワードを再入力します。

5.4 HP CIFS Server の構成

HP CIFS Server で LDAP 機能のサポートを有効にするために，LDAP サーバーにアクセスする際に次のコマンドを使用して， 5.3.2 項「Directory Server の構成」 手順 3 で作成した LDAP の admin アカウントのパスワードを HP CIFS で使用するために SAMBA$ROOT:[PRIVATE]SECRETS.TDB ファイルに追加し，HP CIFS Server の設定および構成を行なう必要があります。

```
smbpasswd -"W" <ldap-admin-password>
```

5.4.1 LDAP 構成パラメータ

表 5-1に示すのは，LDAP を有効にして HP CIFS Server を構成する際に使用できる新しいグローバルパラメータです。 これらのパラメータは，SAMBA$ROOT:[LIB]SMB.CONF ファイルの global セクションで設定します。

ここで定義したグローバル設定は，LDAP サポートを備えた HP CIFS Server によって使用されます。

表 5-1 LDAP 関連のグローバルパラメータ

パラメータ	説明
ldap port	LDAP ディレクトリサーバーに接続するために使用する TCP ポート番号を指定します。デフォルトでは，このパラメータは 389 に設定されています。
ldap server	LDAP サーバーのホスト名あるいは IP アドレスを指定します。
ldap suffix	ユーザとマシンのアカウント情報を追加するディレクトリ・ツリーのベースを指定します。LDAPにエントリーの検索開始位置を指示する検索ベースの識別名 (dn) としても使用されます。 たとえば，ベース DN が "dc=org, dc=hp, dc=com" の場合，ldap suffix = "dc=org, dc=hp, dc=com" を使用してください。

表 5-1 LDAP 関連のグローバルパラメータ (続き)

パラメータ	説明
`ldap user suffix`	ユーザ情報を追加するディレクトリ・ツリーのベースを指定します。 このサフィックス文字列には，ldap suffix の文字列があらかじめ適用されますので，それらの識別名 (dn) を指定する必要はありません。 このパラメータを指定しなければ，`ldap suffix` の値が使用されます。 たとえば，HP CIFS Server を PDC として構成する場合， `SMB.CONF` で `ldap user suffix = sambaDomainName=<workgroup>` のように指定します。 HP CIFS Server をメンバーサーバーとして構成する場合，`ldap user suffix = sambaDomainName=<netbios name>` のように指定します。
`ldap group suffix`	グループ情報を追加するディレクトリ・ツリーのベースを指定します。 このサフィックス文字列には，ldap suffix の文字列があらかじめ適用されますので，それらの識別名 (dn) を指定する必要はありません。 このパラメータを指定しなければ，`ldap suffix` の値が使用されます。 たとえば，HP CIFS Server を PDC として構成する場合，`ldap group suffix = sambaDomainName=<workgroup>` in `SMB.CONF` のように指定します。 HP CIFS Server をメンバーサーバーとして構成する場合， `ldap group suffix = sambaDomainName=<netbios name>` のように指定します。
`ldap admin dn`	ユーザのアカウント情報を取り出すときに HP CIFS Server が LDAP ディレクトリサーバーに接続するために使用するユーザの識別名 (dn) を指定します。 `ldap admin dn` は，`secrets.tdb` ファイルに保管されているパスワードと組み合わせて使用されます。 たとえば `ldap admin dn = "cn = directory manager cn=users, dc=org, dc=hp, dc=com"` のように設定します。
`ldap delete dn`	ldapsam の削除オペレーションで，エントリー全体を削除するか，または Samba 固有の属性だけを削除するかを指定します。 デフォルト値は **No** で，Samba 属性だけを削除します。
`ldap passwd sync`	HP CIFS Server が，パスワード変更時に通常のアカウントについて，NT および LM のハッシュと LDAP のパスワードを同期させるかどうかを指定します。このオプションには，以下の値のいずれかを設定します。 • **Yes**: LDAP，NT，LM のパスワードをアップデートし，`pwdLastSet` 時刻をアップデートします。 • **No**: NT と LM のパスワードをアップデートし，`pwdLastSet` 時刻をアップデートします。 • **Only**: LDAP パスワードだけをアップデートし，後は LDAP サーバーにまかせます。 デフォルト値は，**No** です。
`ldap replication sleep`	CIFS は，読み取り専用の LDAP レプリカへの書き込みを要求されると，その要求を読み書きマスターサーバーにリダイレクトします。このサーバーは変更をレプリケートし，ローカルサーバーに戻します。レプリケーションには，特に遅いリンク上であれば，数秒の時間がかかります。書込みが「成功」しても LDAP のバックエンドデータにはすぐに変更が反映されないため，クライアントによっては動作が混乱することがあります。このオプションを指定すると，LDAP サーバーの処理が追い着くまで，CIFS がしばらく待つようになります。値はミリ秒単位で指定します。最大値は，5000 (5 秒) です。デフォルトでは，`ldap replication sleep = 1000` (1 秒) です。
`ldap timeout`	LDAP サーバーがダウンしているか到達不可能の場合に，HP CIFS Server が，接続要求に対する LDAP サーバーからの応答を待つ時間 (秒単位) を指定します。デフォルト値は，15(秒) です。

表 5-1 LDAP 関連のグローバルパラメータ (続き)

パラメータ	説明
`ldap idmap suffix`	idmap マッピングを保管する際に使用されるサフィックスを指定します。 このパラメータが未設定の場合，代わりに ldap サフィックスの値が使用されます。 このサフィックス文字列には，ldap suffix の文字列があらかじめ適用されますので，それらの識別名 (dn) を指定する必要はありません。 デフォルトは `ldap idmap suffix =` です。 たとえば `ldap idmap suffix = ou=Idmap` のように設定します。
`ldap machine suffix`	ldap ツリーのどこにマシンを追加するかを指定します。 このパラメータが未設定の場合，代わりに ldap サフィックスの値が使用されます。 このサフィックス文字列には，ldap suffix の文字列があらかじめ適用されますので，それらの識別名 (dn) を指定する必要はありません。 デフォルトは `ldap machine suffix =` です。 たとえば `ldap machine suffix = ou=Computers` のように設定します。

第6章　ユーザとグループのマッピング

この章では以下のような内容について説明します。

6.1 概要

HP CIFS Server は， CIFS あるいは SMB プロトコルを使用するファイル・サーバーとして，Windows のユーザおよびグループ・アカウントをベースにした Windows のようなファイル・セキュリティを提供する必要があります。 その一方で， HP CIFS Server はホスト・システムのファイル・セキュリティに依存しているため， UIC およびリソース識別子をベースにした OpenVMS のファイルセキュリティを使用する必要があります。ユーザおよびグループ・アカウントのセキュリティ識別子 (SID) と ACL に基づく Windows のファイル・セキュリティの実装は， ユーザ UIC，リソース識別子，OpenVMS ACL に基づく OpenVMS のファイル・セキュリティとは異なります。 HP CIFS Server は，これら 2 つの異なるオペレーティング・システムのファイル・セキュリティの橋渡しを，次のようなマッピングによる方法で提供します。

- Windows のユーザおよびグループを OpenVMS のユーザ名 (UIC) およびリソース ID にマッピングする。
- Windows での権限を OpenVMS の権限にマッピングする。

この章では， HP CIFS Server が Windows あるいは CIFS ドメインのユーザとグループを OpenVMS のユーザおよびリソース識別子にマッピングするための いくつかの方法について説明します。 第10章 「ファイルとプリントのセキュリティ」 では， Windows から OpenVMS へのファイル・セキュリティのマッピングについて説明します。

ユーザおよびグループ・マッピング技術を使用すると，HP CIFS Server は CIFS ドメイン・ユーザを OpenVMS ユーザ名に割り当て， CIFS ドメイン・グループを OpenVMS リソース識別子に割り当てます。 内部的には， CIFS ドメイン・ユーザ SID と OpenVMS UIC，ならびに，CIFS ドメイン・グループ SID と OpenVMS リソース識別子値との間で マッピングが行われます。

6.2 CIFS ドメイン・ユーザとグループ

CIFS ドメイン・ユーザおよびグループは， 以下のデータベースのいずれかの ユーザおよびグループ・アカウントを参照することができます。

- HP CIFS Server が PDC あるいは BDC の場合， HP CIFS Server ドメイン・データベースあるいは HP CIFS Server が信頼するドメインの ユーザおよびグループ・アカウントを， CIFS ユーザおよびグループとして使用することができます。
- HP CIFS Server がメンバーサーバーの場合， 以下のいずれかのユーザおよびグループ・アカウントを， CIFS ユーザおよびグループとして使用することができます。
  - HP CIFS Server ローカル・データベース
  - HP CIFS Server がメンバーサーバーとなっているドメインの ユーザおよびグループ・アカウント
  - HP CIFS Server がメンバーサーバーとなっているドメインが信頼するドメインの ユーザおよびグループ・アカウント
- HP CIFS Server がスタンドアロン・サーバーの場合， HP CIFS Server のローカル・データベースに存在するユーザおよびグループ・アカウントを CIFS ユーザおよびグループとして使用できます。

読みやすくするため，この章では， CIFS ドメイン・ユーザおよびグループの OpenVMS ユーザ名 (UIC) およびリソース識別子へのマッピングのことを， 単にユーザおよびグループのマッピングと呼びます。

この章では，ユーザ・マッピングのいくつかの方法について説明し，その後，グループのマッピングについて説明します。 ユーザのマッピングは必須ですが， ファイル・セキュリティが OpenVMS のリソース識別子に基づいており マップされた OpenVMS ユーザ名にこれらのリソース識別子が SYSUAF で直接与えられていれば，グループのマッピングはオプションです。これについては，6.4 項「グループ・マッピングの別の方法」で詳しく説明します。 HP CIFS Server のファイル・セキュリティが， マップされた OpenVMS ユーザ識別子 (UIC) およびリソース識別子をベースに 設定されている場合， ファイル・セキュリティを確立する前に ユーザとグループのマッピングに関して理解しておくことが重要です。

HP CIFS ファイル・セキュリティの実装についての詳細は 第10章 「ファイルとプリントのセキュリティ」 を参照してください。

6.3 ユーザのマッピング

ユーザのマッピングとは，CIFS ドメイン・ユーザを OpenVMS ユーザ名 (UIC) へマッピングすることです。 HP CIFS Server が CIFS ドメイン・ユーザを OpenVMS ユーザ名にマッピングする際に使用する方法には 3 種類の方法があります。

1. 「WINBIND によるユーザの自動マッピング」

   この方法は， HP CIFS Server がメンバーサーバーとして構成されている場合，あるいは，他のドメインを信頼している CIFS ドメインで， ドメイン・コントローラとして構成されている場合のみ適用可能です。

2. 「暗黙のユーザ・マッピング」

   HP CIFS Server のユーザ名と OpenVMS ユーザ名が同一で 明示的なマッピングが存在しない場合， 暗黙のユーザ名マッピングが発生します。 HP CIFS Server のユーザ・アカウントを作成する前に (PDBEDIT ユーティリティを使用)，同じ名前の OpenVMS アカウントが存在しており， ユニークな識別子が割り当てられていなければなりません。

3. 「明示的なユーザ・マッピング」

   ユーザの Windows アカウント名が OpenVMS アカウント名と同一でない場合は，SMB.CONF の *username map* パラメータで定義したテキスト・ファイルを使用して，アカウントをマッピングできます。

注記: HP CIFS Server は，各ユーザ・アカウントが RIGHTLIST データベースに UIC 識別子を持っていることを前提とします。

たとえば， マップされる OpenVMS ユーザ名が GANGA で UIC が [600,600] の場合， UIC [600,600] の対応する識別子が RIGHTLIST データベースに存在する必要があります。

以降の項で，上記のユーザ・マッピング方法について説明します。

6.3.1 ユーザの自動マッピング

WINBIND が利用でき，SMB.CONF ファイルの idmap UID の範囲が 有効であれば， CIFS がメンバーとなっている Windows ドメインに属するユーザ， あるいはそのドメインが信頼するドメインのユーザは， 自動的に OpenVMS ユーザ名にマップされます。 このマッピング方法は，HP CIFS Server が PDC あるいは BDC の場合， 信頼されているドメインに属するユーザ・アカウントにも使用できます。 自動マッピングについての詳細は， 第7章 「WINBIND のサポート」 を参照してください。

6.3.2 暗黙のユーザ・マッピング

名前が同一であれば， CIFS ドメイン・ユーザを OpenVMS ユーザ名に暗黙にマップすることができます。

たとえば Windows ユーザ ANITA は， OpenVMS ユーザ名 ANITA が存在すれば，これに暗黙にマップされます。

デフォルトでは，同じ名前の OpenVMS アカウントが存在すれば HP CIFS Server のローカル・ユーザの作成のみが可能で， HP CIFS Server のローカル・ユーザは OpenVMS ユーザ名に暗黙にマップされます。

たとえば，HP CIFS Server データベースでユーザ STEFFI を作成するには， 最初に OpenVMS ユーザ名 STEFFI を作成するか， すでに SYSUAF データベースに存在することを確認してください。 この上で，HP CIFS Server データベースにユーザを作成したい場合は， 以下の条件を満たす必要があります。

- HP CIFS Server のユーザ名が OpenVMS のユーザ名の命名規則に準拠している。 すなわち，ユーザ名がアルファベット文字，ドル記号 ($)，アンダースコア (_) のみで 構成される。 ユーザ名の先頭に数字は使用できない。
- OpenVMS ユーザ名の長さは 12 文字を超えることはできない。 このため，HP CIFS Server のローカル・ユーザ・アカウント名は 最大 12 文字に制限される。

6.3.3 項 では，この制限を回避する代替方法について 説明しています。

HP CIFS Server データベースにおけるユーザ・アカウントの作成および管理の 詳細については， 第8章 「ユーザ，グループ，アカウント・ポリシー，信頼関係の管理」 を参照してください。

6.3.3 明示的なユーザ・マップング

明示的なユーザ・マッピングにより，以下のことが可能になります。

- Windows ユーザ名と OpenVMS ユーザ名が同一でない場合， Windows ユーザ名を OpenVMS ユーザ名にマッピングします。
- 6.3.2 項で説明した 暗黙のユーザ・マッピングにおける制限事項を回避できます。

Windows ユーザ名と OpenVMS ユーザ名が同一でない場合，SMB.CONF の *username map* パラメータで定義されているテキスト・ファイルを使用して，それらのユーザ名を明示的にマッピングすることができます。

たとえば，CORP ドメインの Windows ユーザ名 Andrew Smith を OpenVMS ユーザ・アカウント ASMITH にマッピングするには， SAMBA$ROOT:[LIB]USERNAME.MAP を編集して次のような行を追加します。

```
asmith=corp\Andrew Smith
```

OpenVMS ユーザ名の命名規則の制限を回避するには， HP CIFS Server のローカル・アカウントを作成する際に， まず必要な OpenVMS と CIFS Server のローカル・アカウントを作成し，その後，Windows アカウントを OpenVMS アカウントにマッピングするように ユーザ名マップファイルにエントリを追加します。

たとえば，Windows ユーザ・アカウント Andrew Smith を作成する場合，以下の手順で行います。

1. ユニークな UIC で，たとえば ASMITH などの OpenVMS アカウントを作成します。
2. SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM ユーティリティあるいは PDBEDIT ユーティリティのどちらかを使用して， ASMITH という名前の HP CIFS Server ローカル・アカウントを作成します (この名前は，手順 1 で作成した OpenVMS アカウントと同一でなければなりません)。
3. username.map ファイルに対し，Windows ユーザ名 Andrew Smith を OpenVMS ユーザ名 ASMITH にマッピングするようなエントリを追加します。 以下に例を示します。

```
$ EDIT samba$root:[lib]username.map
asmith=Andrew Smith
```

Windows ユーザが Andrew Smith のユーザ名でセッションを確立すると，そのユーザは OpenVMS ASMITH アカウントにマッピングされます。

注記:

1. 手順 3 では，SMB.CONF ファイルの [global] セクションに 次のような行が存在していることを想定しています。

```
username map = samba$root:[lib]username.map
```

2. SAMBA$CONFIG.COM ユーティリティで HP CIFS Server を構成すると，テンプレートファイル samba$root:[lib]username.map が作成され，*username map* パラメータが SMB.CONF ファイルに追加されます。
3. ユーザ名マップファイルとして使用するために別のファイルを作成する場合，そのファイルは Stream レコード・フォーマットで作成する必要があります。 また，SMB.CONF ファイルの *username map* パラメータの値を，作成したファイルのパスと名前に変更してください。

HP CIFS は，複数のドメイン・ユーザから単一の OpenVMS ユーザ名への マッピングをサポートしています。 この場合，単一の OpenVMS ユーザにマッピングした各ドメイン・ユーザは同じユーザ属性を共有するため，同じセキュリティ属性を共有することになります。 複数の CIFS ドメイン・ユーザを単一の OpenVMS ユーザ名にマッピングするこの方法は，ファイル・セキュリティによる影響を理解した上で使用してください。 CIFS Server のアカウント・データベースに存在するユーザ・アカウントに関しては， 複数の CIFS Server ユーザを単一の OpenVMS ユーザ・アカウントにマッピングすることはできません。

CIFS ドメイン・ユーザを明示的にマッピングする際， マップファイルは 1 行ずつ解析されます。 明示的なユーザ・マッピングを行う際には，以下のような点に注意してください。

- 各行には，等号 (=) をはさんで左側に 1 つの OpenVMS アカウント，右側に CIFS ドメイン・ユーザ名のリストが含まれていなければなりません。
- 等号 (=) の前後にスペースは入れません。 たとえば， ASMITH = Andrew Smith のように記述することはできません。
- 番号記号 (#) あるいはセミコロン (;) で始まる行はコメント行として扱われ，無視されます。 たとえば，次の 2 行はコメント行として扱われます。

```
#this file contains explicit user mapping entries for use by CIFS
#Server
```

- CIFS Server がメンバーサーバーとなっているドメイン (仮に WINDOM)，あるいはその WINDOM が信頼するいずれかのドメインにユーザ・アカウントが存在する場合，マッピングの際には，ユーザ・アカウントの先頭にはドメイン名とスラッシュ\を含める必要があります。 CIFS Server が PDC あるいは BDC の場合，信頼されるドメインのユーザ・アカウントに対しても同様の構文を使用する必要があります。たとえば，ドメイン WINDOM のユーザ GangaR を OpenVMS アカウント GANGA にマッピングする場合，次のように記述します。

```
ganga=windom\GangaR
```

- HP CIFS Server に接続するすべてのドメイン・ユーザを 1 つの OpenVMS ユーザ・アカウントにマッピングすることができます。 この設定により，1 つの OpenVMS ユーザ・アカウントにマッピングされるすべてのユーザが同じユーザ属性，つまり同じセキュリティ属性を共有することに注意してください。 次の例では，すべての Windows ユーザが OpenVMS ユーザ・アカウント CIFS$DEFAULT にマッピングされます。

```
cifs$default=*
```

- 行が '!' で始まる場合，その行によるマッピングが行われると， その行の後で処理が停止します。 行の先頭が '!' でない場合は，各行が処理されてマッピングが続行されます。 '!' の使用が便利なケースとしては， ファイルの後ろの方にワイルドカード・マッピングがあるような場合があります。たとえば，マッピング・ファイルに下記のようなマッピング・

エントリがある場合， !ganga=windom\gangar の行の後ろでマッピング処理が停止します。 この場合，Windows ユーザ GangaR は， CIFS$DEFAULT の代わりに OpenVMS ユーザ・アカウント GANGA にマッピングされます。

```
!ganga=windom\gangar
cifs$default=*
```

- 複数のドメイン・ユーザ・アカウントを 1 つの OpenVMS ユーザ・アカウントにマッピングする場合，次のようにドメイン・ユーザ・アカウントをスペースあるいはコンマで区切ります。

```
tunga=windom\kaveri,windom\neela
```

- ユーザ名自体にスペースが含まれる場合は，マッピング時にはユーザ名を引用符で囲む必要があります。

  たとえば， ユーザ Andrew Smith を OpenVMS アカウントにマッピングする場合の例を次に示します。

```
asmith="Andrew Smith"
```

6.3.4 ユーザ認証とホスト・マッピングの処理の流れ

図 6-1 「ユーザ認証とホストのマッピング処理の流れ」 に示すのは， メンバーサーバー環境におけるユーザ認証とホスト・マッピングの処理の流れです。

図 6-1 ユーザ認証とホストのマッピング処理の流れ

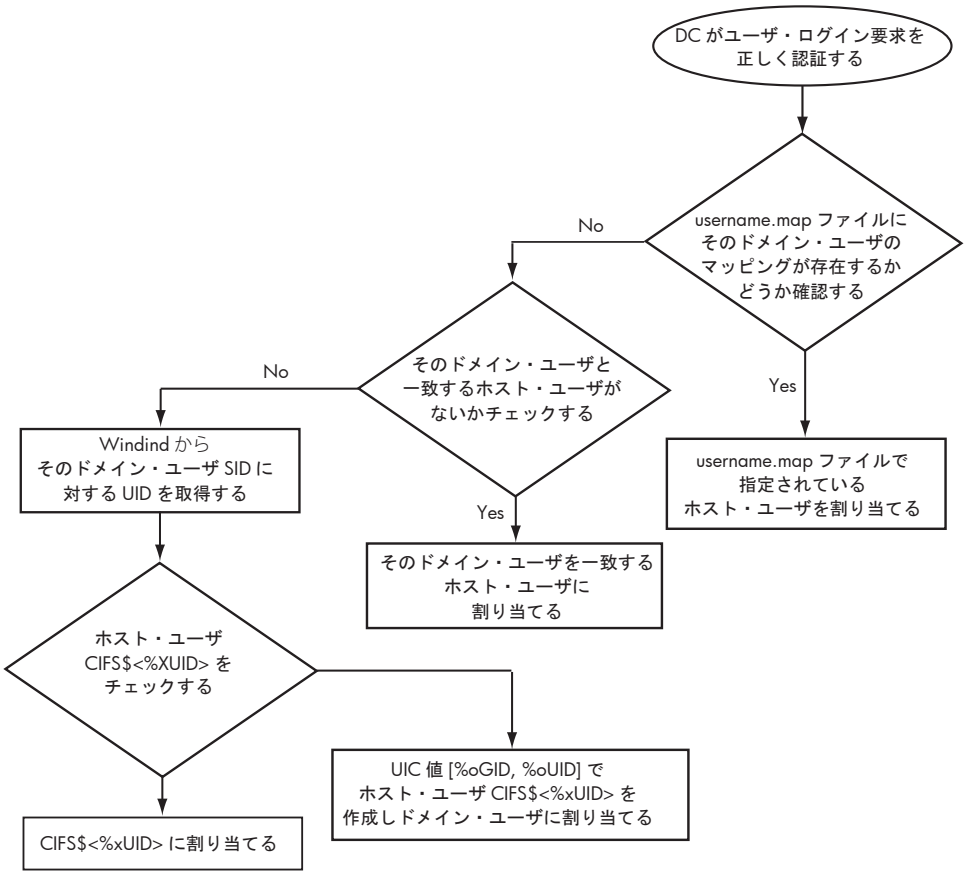


図 6-1の ユーザ認証とホスト・マッピングの処理について，以下に説明します。

1. ドメイン・ユーザがドメイン・コントローラから正しく認証されます。 あるいはユーザにもとづいて ACL が追加されています。

2. HP CIFS Server は，そのドメイン・ユーザに対するマッピングが ユーザ名マッピング・ファイルに存在するかどうか確認します。 対応するマッピングが存在する場合，CIFS はマップされているユーザを使用します。
3. マッピングが存在しない場合，HP CIFS は， そのドメイン・ユーザと一致する 対応するホスト・ユーザがないか確認します。 一致するものがある場合，CIFS はそのホスト・ユーザを使用します。
4. 対応するホスト・ユーザが存在しない場合， 利用可能であれば `winbind` から， ドメイン・ユーザ SID に対する UID を取得します。
5. 取得した UID で，HP CIFS は `CIFS$<hexadecimal-value-of-UID>` の形式でホスト・ユーザを確認します。 ホスト・システム・データベースにユーザがすでに存在する場合は， HP CIFS はそのユーザにマッピングします。
6. ホスト・アカウントが存在しない場合， HP CIFS は，UIC 値 `[%oUID,%oUID]` を使用して `CIFS$<%XUID>` という名前で作成し， ドメイン・ユーザにマッピングします。

注記: WINBIND から取得した UID を OpenVMS ユーザ名の自動作成とマッピングにどのように使用するのかについては， 第7章 「WINBIND のサポート」 を参照してください。

6.3.5 グループのマッピング

グループのマッピングでは，CIFS ドメイン・グループを OpenVMS リソース識別子に割り当てます。 HP CIFS Server が CIFS ドメイン・グループを OpenVMS リソース識別子に割り当てる方法には 2 種類の方法があります。

1. WINBIND によるグループの自動マッピング

   この方法は， HP CIFS Server がメンバーサーバーである場合， ローカル・ドメインのドメイン・グローバル・グループに対して使用します。 また，HP CIFS Server ドメインの役割に関係なく，信頼されたドメインにおけるドメイン・グローバル・グループに対しても使用できます。 グループ・アカウントの自動マッピングについての詳細は， 第7章 「WINBIND のサポート」 を参照してください。

2. 明示的なグループ・マッピング

   この方法は，HP CIFS Server のどの役割のサーバーにおいても， HP CIFS Server データベースにおけるグループ・アカウントの 作成およびマッピングに使用できます。

6.3.5.1 明示的なグループ・マッピング

HP CIFS Server を PDC あるいは BDC として構成する場合， 2 種類のタイプのグループ，すなわちローカル・グループおよびグローバル・グループを作成することができます。 グローバル・グループはドメイン・グループとも呼ばれます。 HP CIFS Server がメンバーサーバーあるいはスタンドアロン・サーバーの場合， ローカル・グループのみが作成できます。 どちらの場合も， HP CIFS Server 管理ユーティリティ `SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM` あるいは NET GROUPMAP ADD コマンドを実行することにより， グループ・アカウントを HP CIFS Server データベースに作成でき， 同時に OpenVMS リソース識別子に割り当てることができます。 グループ・アカウントの作成およびマッピングの際， OpenVMS リソース識別子が存在しない場合は， HP CIFS Server 管理ユーティリティで追加作成することもできます。

HP CIFS Server データベースでの グループ・アカウントの作成および管理についての詳細は，第8章「ユーザ，グループ，アカウント・ポリシー，信頼関係の管理」を参照してください。

デフォルトでは，明示的なグループ・マッピングは `SAMBA$ROOT:[VAR.LOCKS]GROUP_MAPPING.TDB` ファイルに保管されます。

6.3.5.2 グループ・マッピング処理の流れ

図 6-2 に示すのは， メンバーサーバー環境におけるグループ・マッピング処理の流れです。

図 6-2 グループ・マッピング処理の流れ

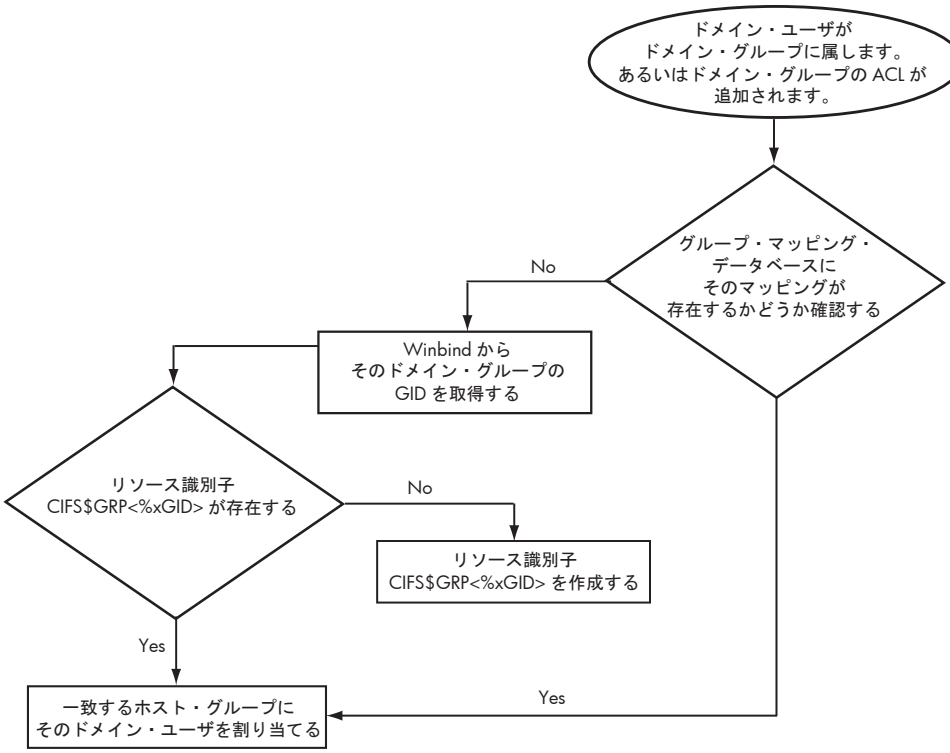


図 6-2 のグループ・マッピング処理の流れについて以下に説明します。

1. 認証されたドメイン・ユーザはグループに属します。 あるいは有効な ACL がグループに追加されています。
2. HP CIFS は，`winbind` から ドメイン・グループの GID を取得します。
3. HP CIFS は，`CIFS$GRP<%XGID>` の形式のリソース識別子を確認します。 一致するものがある場合， HP CIFS はドメイン・グループを一致しているリソース識別子に割り当てます。
4. 対応するリソース識別子が存在しない場合， HP CIFS は `CIFS$GRP<%XGID>` の形式で リソース識別子を作成します。

注記: WINBIND から取得した GID を OpenVMS リソース識別子の自動作成あるいはマッピングに使用する方法については， 第7章 「WINBIND のサポート」 を参照してください。

6.4 グループ・マッピングの別の方法

上記で説明したグループ・マッピング方法の代わりに，管理者は，単に，メンバーとなる CIFS ドメイン・ユーザの マッピングされた OpenVMS アカウントのリソース識別子を集めることで，セキュリティ・グループを設定することもできます。これらのリソース識別子は，リソースへのアクセスを制御するために ACL で使用されます。 ただしこの方法では，リモートからサーバーを管理する場合は，そのサーバーをグループに追加することはできません (Windows クライアントから権限を設定している場合それらを参照できません)。 管理目的でクライアント・システムからグループにアクセスできるようにするには， 前述のいずれかのグループ・マッピング方法でマッピングする必要があります。

6.5 ユーザ属性 (ペルソナ) の作成

HP CIFS Server は， クライアントが HP CIFS Server への新しいセッションを正常に確立したときに， CIFS ドメイン・ユーザおよびグループから OpenVMS UIC およびリソース識別子へのマッピング情報を取得します。 マッピングが無く，WINBIND の自動マッピングが有効な場合， 必要な OpenVMS ユーザとリソース識別子が作成および割り当てられます。

WINBIND で自動マッピング可能な CIFS ユーザおよびグループについては， 第7章「WINBIND のサポート」 を参照してください。

ユーザが認証されると，HP CIFS Server はそのユーザの OpenVMS ペルソナを作成します (そのユーザのセキュリティ・プロフィールを定義します)。 そのユーザに代わって，SMBD プロセスがこのペルソナを使用して ファイル，ディレクトリ，プリント・キューなどの オブジェクトにアクセスします。

ユーザ属性は，以下の属性を継承します。

- 割り当てられる OpenVMS アカウントの UIC および識別子と， そのユーザがメンバーとなるマッピング・グループのリソース識別子
- 割り当てられる OpenVMS ユーザ・アカウントのデフォルトの特権

ユーザがオブジェクトにアクセスする際，OpenVMS は，マッピングされた OpenVMS ユーザのペルソナをもとに オブジェクトへのアクセス権を与えます。 唯一の例外は， HP CIFS Server 構成ファイルの *admin users* パラメータのリストに そのユーザが含まれている場合です。 *admin users* リストに含まれているユーザのペルソナは， UIC，識別子， SAMBA$SMBD アカウントのデフォルトの特権を 継承します。 SAMBA$SMBD アカウントの デフォルトの特権にはすべての特権が含まれています。

注記:

- HP CIFS Server は，ユーザの認証の際に OpenVMS アカウントのパスワードは使用しません。
- SAMBA$SMBD アカウントは， HP OpenVMS CIFS キットのインストール時に HP CIFS Server によって作成されます。

第7章 WINBIND のサポート

この章では，HP CIFS winbind 機能について説明し，使用方法と最適な構成方法について説明します。

7.1 概要

ユーザとグループの識別に，OpenVMS と Microsoft Windows では異なる技術を使用しています。HP CIFS Server を使用すると，この問題が解消されます。Windows に実装されたユーザとグループのセキュリティ ID である SID を OpenVMS に実装されたユーザとグループの ID である UID/GID にマップする機能として，CIFS では複数の方法が用意されています。WINBIND もその 1 つです。 winbind の目的は，UID と GID を自動生成し，最小限の ID 管理作業で Windows SID との対応を維持することです。

ご使用の環境に対して適切な構成を選択することが IT 管理上の問題を最小限に抑えるために重要となるため，HP CIFS Server の構成を行う前に WINBIND について理解しておくことが必要です。 ディレクトリとファイルは，所有者の ID に基づく権限に従ってファイルシステムで管理されるため，ご使用中の環境で最善のマッピング方法を選択することが重要です。最初から適切な構成を選択しておかないと，時間が経つに連れてユーザマップを変更することが難しくなります。この章は，winbind を理解し，HP CIFS を適切に構成する際に役立ちます。

winbind についての詳細は，以下の URL の『Samba 3.0 HOWTO and Reference Guide』を参照してください。

http://us3.samba.org/samba/docs/man/Samba-HOWTO-Collection/

注記: HP CIFS for OpenVMS でも winbind の機能がそのまま提供されているので『Samba 3.0 HOWTO and Reference Guide』の winbind に関する説明はそのまま参照できます。ただし，機能の実装方法については異なっています。

7.2 WINBIND の特長

WINBIND には，以下の特長があります。

- ユーザ ID およびグループ ID の割り当て

  対応する UID/GID を持たない Windows SID が winbind に対して提供されると，winbind は UID/GID を生成します。構成の内容に依存して，winbind は以下のアルゴリズムを使用して ID を作成します。

  — ローカルインクリメント

  WINBIND のデフォルト設定を使用すると，ID の値には定義された範囲内で現在最も大きな値に単純に 1 を加えた値が割り当てられます。値の保管場所は，ローカル HP CIFS Server に限定されます。

  警告!

  - idmap ファイルをバックアップしておくと，UID と GID のマップを再作成せずにリストアすることができます。ローカルインクリメントモデルでは，idmap ファイルを定期的にバックアップする必要があります。
  - このソリューションには，同一の Windows ユーザに対する UID/GID の値がシステムにより異なるという欠点があります。また，idmap ファイルが再作成された場合に UID と GID のマップが以前のマップとは異なり，重大なセキュリティ上の問題 (ファイル所有者の変更) を発生させる原因となる可能性があります。

- ID マッピング

  WINBIND は，特定の Windows SID と，それに対応する OpenVMS UID/GID 間のマッピングを作成します。WINBIND は上記のいずれかの方法を使って，OpenVMS UID/GID と Windows SID 間のマッピングを作成します。winbind は，Windows SID を使って既存の UID/GID マップを検出するか，または既存のマップがない場合には新しいマップを作成します。

- ID の格納

  winbind はデータベースを管理し，そこに OpenVMS UID/GID と Windows SID 間のマッピングを格納します。最も単純なケースでは，winbind は，SAMBA$ROOT:[VAR.LOCKS] ディレクトリの winbind_idmap.tdb という名前のローカルの Trivial Data Base (TDB) ファイルでデータベースを維持します。

7.3 winbind の処理フロー

図 7-1 に示すのは，メンバーサーバーとして HP CIFS を構成した Windows ドメイン環境における winbind の処理フローです。

図 7-1 winbind の処理フロー

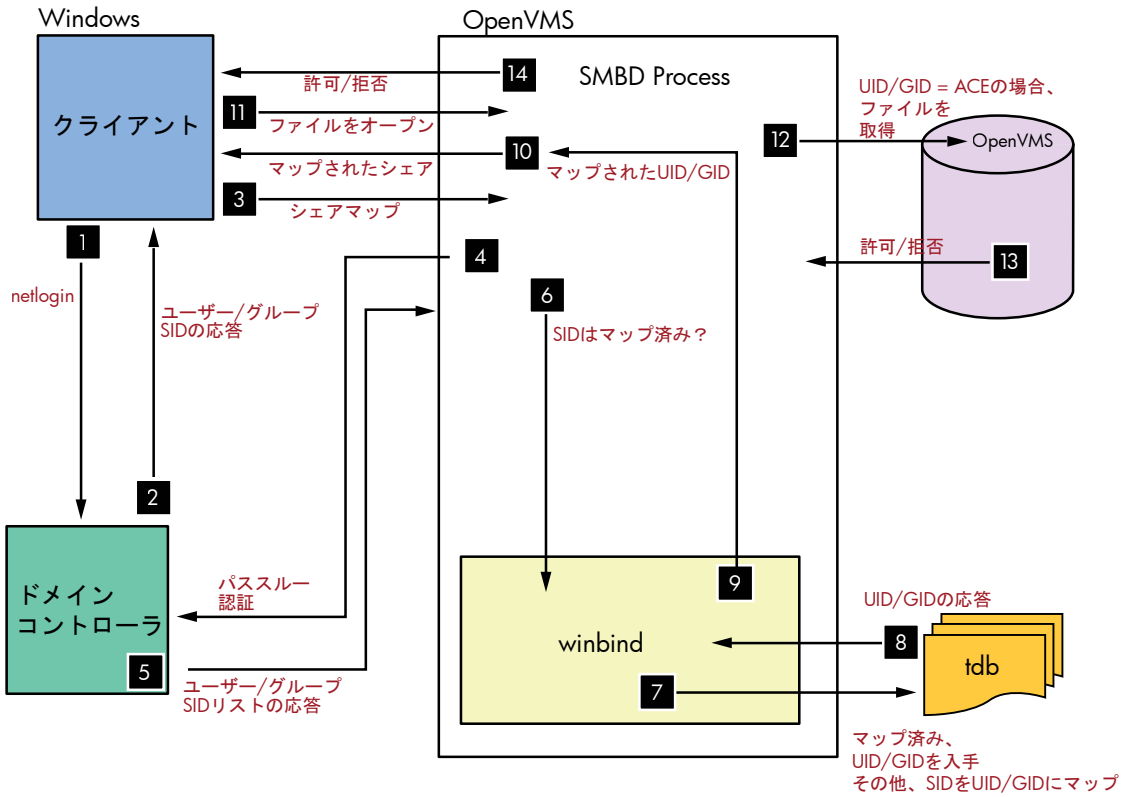


図 7-1に示した winbind の処理フローを以下に示します。

1. Windows クライアントが，ドメインへログインします (認証)。
2. Windows ドメインコントローラがクライアントを認証し，ユーザ・セキュリティ・データを返します。
3. Windows クライアントは，HP CIFS 共有をマップします。
4. HP CIFS メンバーサーバーが Windows ドメインコントローラにユーザ名を渡し，そのユーザがドメインメンバーかどうか確認します。
5. Windows ドメインコントローラは，ユーザ認証リストとメンバー SID リストを返します。
6. smbd プロセスが SID とユーザ情報を winbindd モジュールに渡します。
7. WINBIND が，SID およびユーザ名を ID マッピング・データベースの ID マッピング・データで確認します。 WINBIND は，既存の Windows SID と OpenVMS UID/GID 間のマップを探します。既存のマップがない場合には新しいマップを作成します。
8. TDB データベースからマップされた UID または GID を返します。
9. WINBIND は，smbd に UID/GID マッピングを返します。
10. HP CIFS Server はマップされた共有を Windows クライアントに提示します。
11. Windows クライアントは，HP CIFS Server 共有のファイルを開きます。
12. UID と GID が ACL のファイル所有者，グループ，およびその他の ACE と比較されます。
13. 手順 12 の結果によって，ファイル・オープン操作の許可あるいは拒否がなされます。
14. HP CIFS Server が Windows クライアントへオープン状況を返します。

7.4 WINBIND の機能

WINBIND は，次のような機能を提供する HP CIFS Server の特別な機能です。

- 自動マッピング

  HP CIFS Server がメンバーサーバーとなっているドメインあるいは 信頼されているドメインに対しては， WINBIND は対応する OpenVMS ユーザおよびグループ (リソース識別子) を 自動的に作成しマッピングします。

- 入れ子グループのサポート

  入れ子グループを使用すると，信頼されたドメインからのものも含め，ドメイン・グローバル・グループは ローカル・グループのメンバー (あるグループ内のグループ，あるいは入れ子グループ) となることができます。 入れ子グループは，サーバーの役割には関係なく，任意のサーバーで使用できます。

- 信頼

  CIFS が PDC あるいは BDC の場合， WINBIND はすべての信頼機能で必要になります。

CIFS Server が提供する WINBIND 機能は，論理名 WINBNDD_DONT_ENV で制御されます。また，`idmap uid` および `idmap gid` パラメータの有効な範囲が，HP CIFS Server 構成ファイルで指定されていなければなりません。 これらのパラメータが省略されている場合，自動マッピング機能は使用できません。 この論理名が無効あるいは未定義の場合，HP CIFS Server は WINBIND 機能を提供します。次のようにこの論理名に 1 を定義すると，すべての WINBIND 機能が無効になります。

```
$ DEFINE/SYSTEM WINBINDD_DONT_ENV 1
```

デフォルトでは，WINBINDD_DONT_ENV 論理名は定義されていません。WINBIND 機能は，CIFS サーバーがメンバーとなるドメインあるいは信頼されたドメインに属するようなユーザおよびグループの処理において重要な役割を果たすため，スタンドアロン・サーバーである場合を除き， WINBIND 機能は無効にしないことをお勧めします。

7.4.1 自動マッピング

WINBIND は，OpenVMS ユーザ・アカウントとリソース識別子 (POSIX GID 形式) を作成し，適切な Windows SID に対するそれらの対応を維持して ID 管理のための労力を最小化します。

WINBIND ID マッピング・データベース・ファイル

`SAMBA$ROOT:[VAR.LOCKS]WINBINDD_IDMAP.TDB` は，Windows SID と OpenVMS ユーザ・アカウントおよびリソース識別子との間のマッピングを維持します。Windows SID と OpenVMS ユーザ・アカウントあるいはリソース識別子との間のマッピングは，このデータベース・ファイルに既存のマッピング・エントリが無い場合のみ作成されます。必要なマッピングが無い場合，以下のような状況で， OpenVMS ユーザ・アカウントとリソース識別子の自動作成とマッピングが発生します。

- ユーザが正常に認証された後，HP CIFS Server は， そのユーザと，そのユーザがメンバーとなっているすべてのグループを， OpenVMS ユーザ名 (UIC) およびリソース識別子にマッピングしようとします。ドメイン・グループあるいは CIFS Server グループは， 入れ子グループあるいは認証されたユーザが直接属するグループの どちらでも対応可能です。マッピングが存在しない場合， あるいは認証されたユーザが存在する場合 (かつ，このユーザが CIFS Server がメンバーとなっているドメイン・ユーザの場合) または信頼されたドメインのユーザが存在する場合， WINBIND は必要とされる OpenVMS ユーザ・アカウントを自動的に作成することができ，その後，その OpenVMS ユーザ名を認証されたユーザに割り当てます。
- ファイルおよびディレクトリのセキュリティを設定する際，権限を付与するセキュリティ・プリンシパル (対象) が CIFS Server がメンバーとなっているドメインもしくは信頼されたドメインの ユーザあるいはグローバル・グループの場合， WINBIND は必要な OpenVMS ユーザ名 (UIC) あるいはリソース識別子を作成し， ドメイン・ユーザあるいはグループ SID に割り当てることができます。

- CIFS サーバーが PDC の場合，ワークステーションを CIFS ドメインに追加する際，OpenVMS ユーザ名が自動的に作成され，作成されたワークステーション・アカウントに割り当てられます。 この場合，ワークステーション・アカウント名は OpenVMS ユーザの命名規則に準拠していなければなりません。

各 OpenVMS アカウントごとにユーザ名と UIC が必要です。 WINBIND は，HP CIFS Server 構成パラメータ `idmap uid` で指定された範囲から，新しいアカウントのユーザ名と UIC を取得します。 この範囲の開始値および終了値は，ハイフンで区切られた整数で指定されます。 次に例を示します。

```
idmap uid = 1000 - 2000
```

同様に，WINBIND は， HP CIFS Server 構成パラメータ `idmap gid` で指定された範囲から，名前と OpenVMS (POSIX グループ) リソース識別子の値を取得します。 次に例を示します。

```
idmap gid = 1000 - 2000
```

以下の項では WINBIND がどのように自動処理を実行するかを説明しています。

7.4.1.1 自動マッピングが必要になる場合

- HP CIFS Server は WINBIND を使用して， ドメイン (CIFS Server がメンバーとなっているドメインあるいは信頼されたドメイン) のグローバル・グループ名を OpenVMS リソース識別子にマッピングします。 WINBIND 機能は，ドメインのグローバル・グループに基づいてファイルおよびディレクトリに許可モードを設定する場合に便利です。
- HP CIFS Server が PDC の場合，まず OpenVMS アカウントが存在していなければ， CIFS アカウント・データベースにコンピュータ・アカウントは作成できません。 WINBIND は，コンピュータがドメインに参加する際に， 必要な OpenVMS アカウントと関連する CIFS アカウントを作成することができます。 WINBIND を使用しない場合，管理者は，コンピュータがドメインに参加する前に他の方法で OpenVMS アカウントが作成されていることを確認する必要があります。

7.4.1.2 自動マッピングが必要ない場合

以下の状況に当てはまる場合は，WINBIND による自動マッピングを使用する必要はありません。

- HP CIFS Server に接続する際に HP CIFS Server がメンバーとなっているドメイン あるいは信頼されているドメインに属するすべてのユーザは，明示的あるいは暗黙のどちらかの方法で OpenVMS ユーザ名にマッピングされます。
- オブジェクトの許可リストに， (ローカル・ドメインあるいは信頼されるドメインのいずれにも) ドメイン・グローバル・グループが含まれていない。
- HP CIFS Server が PDC の場合， ドメインに参加するシステムのコンピュータ・アカウントは， ドメインに参加しようとする前に作成されている。

ドメイン・グローバル・グループの許可モードを設定するには，以下のいずれかの方法を使用します。

1. ローカル・グループを表す OpenVMS リソース識別子を作成します。 `SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM` あるいは `NET GROUPMAP ADD` コマンドを使用して， CIFS ローカル・グループを作成し OpenVMS リソース識別子に割り当てます。 `SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM` あるいは `NET [RPC | ADS] GROUP ADDMEM` コマンドを使用して， ローカル・ドンメインあるいは信頼されるドメインの ドメイン・グローバル・グループとドメイン・ユーザを追加するか， ローカルの CIFS ユーザとグループをグループ・メンバーとして追加します。 ドメイン・グローバル・グループを CIFS Server ローカル・グループにメンバーとして追加する方法については，8.3 項「グループの管理」 を参照してください。
2. 6.4 項「グループ・マッピングの別の方法」で説明する方法を使用して，CIFS ドメイン・ユーザに割り当てられた OpenVMS ユーザ名に OpenVMS リソース識別子を付与してください。

7.4.1.3 OpenVMS ユーザ・アカウントの作成とマッピング

WINBIND は，idmap uid の値を使用して 新しいアカウントの OpenVMS ユーザ名と UIC を取得します。 uid の値は 16 進値に変換され，文字列 CIFS$ に追加されて， OpenVMS ユーザ名が導き出されます。 この uic の値は 8 進に変換され，この 8 進値が UIC グループおよびメンバー番号として使用されます。

注記: UIC グループ番号の最大値は 8 進で 37776 (すなわち，10 進で 16382) に制限されるため， `idmap uid` 値の範囲の上限は 16382 です。 同様に，UIC グループ番号の 8 進 376 未満は HP がリザーブしているため， `idmap uid` の下限は 255 よりも小さくならないようにすることをお勧めします。

例として，次のような HP CIFS Server 構成ファイル・パラメータについて説明します。

```
idmap uid = 1000-2000
```

WINBIND はまず uid 1000 を割り当て，この値を 16 進 (3E8) および 8 進 (1750) に変換し，ユーザ名が CIFS$3E8 で UIC が [1750,1750] の OpenVMS アカウントを作成します。

WINBIND が作成したアカウントは対話型ログインが許可されておらず， NETMBX および TMPMBX 特権のみが付与されています。 OpenVMS アカウントが正常に作成されると， ユーザのドメイン・アカウント SID に割り当てられた uid (上記の例では 1000) のマッピング情報は，SAMBA$ROOT:[VAR.LOCKS]WINBINDD_IDMAP.TDB ファイルに保管されます。 このファイルは，オブジェクトのセキュリティを維持するために重要なファイルなので， 必要なマッピング情報の損失を避けるために定期的にバックアップを取る必要があります。

7.4.1.4 リソース識別子の作成とマッピング

WINBIND は `idmap gid` の次の整数値を使用して，OpenVMS リソース識別子 (グループ) の名前と値を導き出します。 `idmap gid` 値は 16 進値に変換され， リソース識別子に割り当てられる値として使用されるとともに， 文字列 `CIFS$GRP` に追加され， これによりリソース識別子の名前が導き出されます。

注記: WINBIND は POSIX のグループ・リソース識別子 (POSIX GID) を作成するため， 最大値は %xFFFFFF あるいは %d16777215 に制限されます。下限は 1 です。 OpenVMS は，選択された値に自動的に %xA4000000 を加算します。 値 1616777200 - 16777215 は HP CIFS Server が使用するためにリザーブされています。 このため，idmap gid の範囲の上限が 167777199 を超えないようにします。

例として，次のようなパラメータを含む SMB.CONF について説明します。

```
idmap gid = 5000-10000
```

WINBIND まず GID 5000 を割り当て，CIFS$GRP1388 という名前の OpenVMS リソース識別子を作成します。

識別子が正常に作成されると， 割り当てられた gid (5000) に対応するドメイン・グループ SID へのマッピングが SAMBA$ROOT:[VAR.LOCKS}WINBINDD_IDMAP.TDB に保管されます。 オブジェクトのセキュリティを維持するのに必要なマッピングを失わないように， このファイルは定期的にバックアップを取ることが重要です。

注記:

- idmap uid および idmap gid パラメータの上限値はこの範囲を超えて増やすことができますが，下限値は変更すべきではありません。 たとえば，1000 - 2000 の範囲を 1000 - 3000 に変更して， WINBIND による割り当てのためにさらに 1000 uid を用意することができます。 WINBIND は，WINBIND ID マッピング・データベース・ファイルに現在のマッピング・エントリを残したまま，idmap uid の既存の範囲を自動的に調整します。 これにより，既存のマッピング・エントリをもとに設定されたファイルとディレクトリの既存のセキュリティ設定は，維持されます。
- ユーザおよびグループのマッピング処理の流れについては， 第6章「ユーザとグループのマッピング 」 を参照してください。

7.4.1.5 WINBIND で作成したユーザとグループの管理

WINBIND は，OpenVMS ユーザ名およびリソース識別子を作成する際， CIFS Server 構成ファイルの idmap uid および idmap gid パラメータで範囲指定された値を使用します。 WINBIND をこれらのいずれかの idmap 範囲を超えて実行すると， CIFS クライアント・ログ・ファイルにエラーが出力されます。 クライアント・ログ・ファイルは，デフォルトでは SAMBA$ROOT:[VAR] ディレクトリに作成されます (作成場所は HP CIFS Server 構成ファイルの log file パラメータで指定されます)。

WINBIND で作成された OpenVMS ユーザ名とリソース識別子と，それらに対応するドメイン・ユーザおよびグループへのマッピングを表示するために，WBINFO ユーティリティが提供されています。 WBINFO ユーティリティは，以下のように実行することができます。

```
$ @SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS.COM
$ WBINFO --hostusers-to-domainusers
$ WBINFO --hostgroups-to-domaingroups
```

--hostusers-to-domainusers オプションを指定すると， CIFS ドメイン・ユーザとそれらにマッピングされている OpenVMS ユーザ名が表示されます。
--hostgroups-to-domaingroups オプションを指定すると， CIFS ドメイン・グループとそれらにマッピングされている OpenVMS リソース識別子が表示されます。 これらの 2 つのオプションは，割り当てられたユーザとグループを表示するためのオプションです。 すべてのユーザおよびグループの表示には使用できません。

1 つの OpenVMS ユーザ名あるいはリソース識別子 (グループ) とドメイン・ユーザあるいはグループのマッピングを確認するには，次のようなコマンドを実行します。

```
WBINFO --hostname-to-domainname=<OpenVMS-identifier>
```

<OpenVMS-identifier> には，OpenVMS ユーザ名かリソース識別名のどちらかを指定します。

7.4.2 入れ子グループのサポート

グループ内のグループは入れ子グループと呼ばれます。 WINBIND が提供する入れ子グループ機能を使用すると，以下のようなユーザおよびグループを CIFS ローカル・グループのメンバーとして追加できます。

1. CIFS Server がメンバーとなっているドメインに属するユーザおよびドメイン・グローバル・グループ
2. CIFS Server がメンバーとなっているドメインによって信頼されている ドメインに属するユーザおよびドメイン・グローバル・グループ
3. CIFS Server が PDC あるいは BDC の場合，信頼されているドメインに属する ユーザおよびドメイン・グローバル・グループ
4. CIFS サーバー・データベースのユーザおよびローカル・グループ

入れ子グループの機能により，CIFS ローカル・グループに基づいたファイル・セキュリティを確立することができます。 自動マッピング機能が有効でない場合も， WINBIND は入れ子グループをサポートします。

7.5 WINBIND を無効にする

Linux/UNIX 版の Samba とは異なり，HP CIFS for OpenVMS では，Windbind 機能は SMBD プロセスに統合されています。 そのため，独立した winbind デーモン・プロセスは作成されません。

WINBIND 機能はすべての HP CIFS 構成に必要なわけではありません。 CIFS をスタンドアロン・サーバーとして構成する場合は，winbind を構成し有効にすることは必須ではありません。 HP CIFS で winbind を無効にするには，次の論理名を定義してください。

```
$ DEFINE/SYSTEM WINBINDD_DONT_ENV 1
```

SMB.CONF に idmap UID および idmap GID パラメータが含まれない場合も winbind は無効となります。

7.6 WINBIND を使用した HP CIFS Server の構成

winbind 機能のサポートを使用するには，HP CIFS Server のセットアップと構成を行う必要があります。

7.6.1 WINBIND の構成パラメータ

表 7-1 に，winbind の動作を制御するために使われる新しいグローバルパラメータを示します。 これらのパラメータは，SAMBA$ROOT:[LIB]SMB.CONF ファイルの [global] セクションに設定されます。 詳細は，SMB.CONF マンページを参照してください。

表 7-1 windind 関連のグローバルパラメータ

パラメータ	説明
security	WINBIND は Windows ドメイン認証を必要とします。 security = domain あるいは security = ads
winbind separator	この文字列型の変数には，ドメイン名とユーザ名のセパレータ (区切り文字) を指定します。例: winbind separator = \
idmap uid	この変数には，ドメインユーザの UID 範囲を指定します。 例: idmap uid = 5000-6000
idmap gid	この変数には，ドメイングループの GID 範囲を指定します。 例: idmap gid = 5000-6000
idmap backend	この文字列型の変数には，使用する idmap バックエンドのタイプを指定します。構文は次のようになります。 • idmap backend = これがデフォルトで，ローカルな idmap tdb ファイルが使用されます。 • idmap backend = ldap:ldap://*<LDAP server name>*[:389] ID マッピングデータは，共通の LDAP ディレクトリサーバー・バックエンドに格納されます。 例: idmap backend = ldap:ldap://ldapserverA.hp.com
winbind cache time	この整変数は，Windows NT サーバーが再度照会する前に winbind がユーザおよびグループ情報をキャッシュする秒数を指定します。デフォルト値は 300 です。

7.6.1.1 SMB.CONF の例

SMB.CONF ファイルの例を以下に示します。

```
[global]
 # Doamin name
 workgroup = DomainA
 security = domain

 # Winbindd section
 idmap uid = 5000-6000
 idmap gid = 5000-6000
 idmap backend = idmap_tdb
 winbind cache time = 300
 winbind separator = \
```

7.7 LDAP バックエンドのサポート

複数の CIFS Server が Windows NT または Windows ADS ドメインに存在しており，これらが winbind を使用する場合，複数の CIFS Server が LDAP ディレクトリに ID マップを格納するように構成できます。 LDAP サーバーを使用し，SMB.CONF で idmap backend パラメータを指定して CIFS サーバーを構成すると，すべての UID および GID がドメイン内でユニークとなるように設定することができます。

7.8 wbinfo ユーティリティ

wbinfo ツールを使用すると，winbind から情報を取得できます。 このツールについての詳細は11.1.2 項「wbinfo」を参照してください。

第8章 ユーザ，グループ，アカウント・ポリシー，信頼関係の管理

この章では以下の内容について説明します。

- 8.2 項「ユーザの管理」
- 8.3 項「グループの管理」
- 8.4 項「アカウント・ポリシーの管理」
- 8.5 項「信頼関係の管理」

8.1 概要

CIFS Server 管理ユーティリティ SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM を使用して，HP CIFS Server データベースのユーザおよびグループ，アカウント・ポリシー，信頼関係の管理を行うことができます。

8.2 ユーザの管理

HP CIFS Server データベースのユーザの管理には，HP CIFS Server 管理ユーティリティ SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM あるいは pdbedit コマンド行ユーティリティが使用できます。

- 8.2.1 項「CIFS Server 管理ユーティリティによるユーザの管理」では，SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM を使用して CIFS Server ユーザを追加，修正，削除する方法について説明します。
- 8.2.2 項「pdbedit ユーティリティによるユーザの管理」では， pdbedit ユーティリティで同様の作業を実行する方法について説明します。

8.2.1 CIFS Server 管理ユーティリティによるユーザの管理

SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM ユーティリティは， HP CIFS Server アカウント・データベースからの情報をもとに ユーザの一覧表示，追加，修正，あるいは削除をメニュー・オプションを選択して実行することができます。

CIFS Server 管理ユーティリティの起動方法は以下のとおりです。

```
$ @SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM
```

あるいは，次のコマンドを実行します。

```
$ @SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS
$ SMBMANAGE
```

HP OpenVMS CIFS Server Management のメイン・メニューが表示されたら オプション 3 の Manage Users を選択して， 以下のユーザ管理メニューを表示させます。

```
HP CIFS Server User Management Menu

                  1  - List users
                  2  - List a user
                  3  - Add user
                  4  - Modify user
                  5  - Remove user
                 [E] - Exit
Enter CIFS user management option:
```

8.2.1.1 ユーザの一覧表示

オプション 1 の List users を使用すると，以下の例のように CIFS Server アカウント・データベースに存在するすべてのユーザとマシン・アカウントを一覧表示できます。

```
Enumerating users in the domain PIANODOM.
  Please wait...

User name             Comment
---------------------------------------
sso                   Generic account for SSO team
ganga
cifsadmin
tunga                 Account for user Tunga

Press Enter to continue:
```

8.2.1.2 ユーザに関する詳細情報の表示

オプション 2 の List a user を使用すると，HP CIFS Server アカウント・データベースに存在するユーザあるいはマシン・アカウントの詳細情報を表示できます。アカウント名を入力するためのプロンプトが表示され，以下のように出力が表示されます。

```
 This option displays full information for the specified user.

Enter the username: tunga

OpenVMS username:     tunga
NT username:
Account Flags:         [U          ]
User SID:              S-1-5-21-4210255526-1716153954-2929367854-1005
Primary Group SID:     S-1-5-21-4210255526-1716153954-2929367854-513
Full Name:
Home Directory:        \\piano\tunga
HomeDir Drive:
Logon Script:
Profile Path:
Domain:                PIANODOM
Account desc:          Account for user Tunga
Workstations:
Munged dial:
Logon time:            0
Logoff time:           never
Kickoff time:          never
Password last set:     Mon, 03 May 2010 13:18:48 PDT
Password can change:   Mon, 03 May 2010 13:18:48 PDT
Password must change: never
Last bad password   :  0
Bad password count  :  0
Logon hours         :  FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

Press Enter to continue:
```

8.2.1.3 ユーザの追加

オプション 3 の Add user を使用すると，CIFS Server アカウント・データベースにユーザあるいはマシン・アカウントを追加することができます。

CIFS Server が PDC あるいは BDC の場合，以下のようなメニューが表示されます。

```
HP CIFS Server User Account Creation Menu

                1. User name (*):
                2. Full name:
```

```
                3. Description:
                4. Home drive:
                5. Logon script:
                6. Profile path:

                * = required field

Enter item number or press Enter to accept current values [Done]:
```

CIFS Server がメンバーサーバーあるいはスタンドアロン・サーバーの場合， 以下のようなメニューが表示されます。

```
HP CIFS Server User Account Creation Menu

                1. User name (*):
                2. Full name:
                3. Description:

                * = required field

Enter item number or press Enter to accept current values [Done]:
```

選択したオプションに対して値を入力すると，ユーティリティは次のようにアカウントを修正するためのメニューを表示します。

```
HP CIFS Server User Account Flags Menu

                1. Disable Account: no
                2. Password not required: no
                3. Password does not expire: yes
                4. Automatic locking: no
                5. Account Type: user
Enter item number or press Enter to accept current values [Done]:
```

これらの各オプションについて，以下の項で詳しく説明します。

注記: オプション 5. Account Type: user は， CIFS Server が PDC あるいは BDC の場合のみ表示されます。

8.2.1.3.1 ユーザ名

User name オプションでは，追加するアカウント名を指定します。このフィールドは必須フィールドです。指定するユーザ名は，管理対象のドメインあるいはサーバーに同じユーザ名あるいはグループ名が存在しないことが必要です。 CIFS Server は，CIFS Server データベースで作成されるユーザ・アカウントごとに対応する OpenVMS ユーザ名を必要とします。 ユーザ名を指定する際は，以下のガイドラインを満たすようにしてください。

- 使用可能な文字は，英数字，ドル記号 ($)，アンダースコア (_) のみです。
- 数字で開始することはできません。
- 文字数は 12 文字を超えることはできません。

ユーザ・アカウントを作成する際，指定したユーザ名が SYSUAF データベースに存在しない場合，管理ユーティリティは SYSUAF にそのユーザ名を作成するかどうかのオプションを提示します。 オプションに従ってユーザ名を作成する場合は，その OpenVMS グループの UIC を生成するためにグループ ID 番号を指定する必要があります。

8.2.1.3.2 フルネーム

Full name オプションでは，そのユーザの完全な名前を指定します。 フルネームの指定は任意です。 文字数は 256 を超えることはできません。 入力する際，フルネームを引用符で囲む必要はありません。

8.2.1.3.3 説明

Description オプションでは， そのユーザ・アカウントに関する説明を記述した文字列を指定します。 このオプションの指定は任意です。

8.2.1.3.4 ホーム・ドライブ

Home drive オプションでは， そのユーザのホーム・ディレクトリが共有ネットワーク・ディレクトリの場合に， ホーム・ディレクトリへの接続に使用するドライブ文字を指定します。 ホーム・ドライブの指定は任意です。 ドライブ文字として，D ~ Z の文字が使用可能です。 ユーザ・アカウントに対して指定したホーム・ドライブが Samba 構成ファイルのグローバル・セクションに存在する場合， ユーザ・アカウントに対して指定されたホーム・ドライブの方が， SMB.CONF パラメータ logon drive よりも優先されます。

8.2.1.3.5 ログオン・スクリプト

Logon script オプションでは，ユーザ・ログオン時に実行するログオン・スクリプトの名前を指定します。 ログオン・スクリプトの指定は任意です。 ログオン・スクリプトは，バッチ・ファイル (拡張子.BAT あるいは .CMD) でも， 実行プログラム (ファイル拡張子 .EXE) でもかまいません。 1 つのログオン・スクリプトを複数のユーザ・アカウントで使用することも可能です。 ユーザがログインする際，ログイン要求を認証するサーバーは， ユーザが指定したサーバー・ログオン・スクリプトのパスに従ってスクリプトを探します。

このスクリプトは [netlogon] 共有に対する相対パスでなければなりません。 [netlogon] 共有が /SAMBA$ROOT/NETLOGON/ としてパス指定され， ログオン・スクリプトが SCRIPTS/STARTUP.BAT として指定されている場合， ダウンロードされるファイルは次のようになります。

```
SAMBA$ROOT/NETLOGON/SCRIPTS/STARTUP.BAT
```

ユーザ・アカウントに対して指定されたログオン・スクリプトは， Samba 構成ユーティリティのグローバル・セクションに存在する SMB.CONF パラメータ logon script よりも優先されます。

8.2.1.3.6 プロファイル・パス

Profile path オプションには， ユーザのローミング・プロファイル (Desktop，NTuser.dat など) が保管されるディレクトリを指定します。プロファイル・パスの指定は任意です。 指定したディレクトリには Application Data，desktop，start menu，network neighborhood，programs フォルダあるいはその他のフォルダとそれらの内容が保管され，Windows クライアントに表示されます。 \\%L\profiles\%U のようにプロファイル共有に対する相対パスで プロファイルを指定することができます。 この場合，%L は CIFS Server NetBIOS 名で置き換え， %U はセッション・ユーザ名で置き換えます。

ユーザ・アカウントに対して指定したプロファイル・パスは， Samba 構成ファイルのグローバル・セクションに存在する SMB.CONF パラメータ logon path より優先します。 ユーザのプロファイル・パスと SMB.CONF パラメータ logon path がともに空文字の場合，そのユーザに対するローミング・プロファイルは無効になります。

8.2.1.3.7 アカウント・フラグ・メニュー

User Account Flags メニューでは， アカウントを無効にしたり， 規定の回数を超える不正なパスワード入力が発生した時に自動ロックを有効にしたり，パスワードが必要ないことを指示したり，あるいは，アカウントの期限切れフラグを設定あるいはクリアするためのオプションを提供します。また，CIFS Server が PDC あるいは BDC の場合，アカウント・タイプが設定されます。

8.2.1.3.8 アカウントを無効にする

Disable account フラグを yes に設定することにより， ユーザ・アカウントを無効にすることができます。

8.2.1.3.9 パスワード無しに設定

Password not required フラグを yes に設定することにより，ユーザは指定されたユーザ・アカウントにパスワード無しでログインできます。

8.2.1.3.10 パスワードの期限切れを設定しない

デフォルトでは，ユーザ・アカウントは Password does not expire フラグを設定せずに作成されます。このため，アカウントのパスワードはパスワード期限アカウント・ポリシーに依存します。 Password does not expire フラグが yes に設定されていると，パスワード期限アカウント・ポリシーの設定に関係なく，指定されたユーザ・アカウントのパスワードは期限切れになりません。

8.2.1.3.11 自動ロックの設定

Automatic locking オプションは，サーバー・アカウント・ポリシーによって制御される自動ロック機能をそのアカウントに適用するかどうかを指定するのに使用します。この機能が有効な場合，bad password count アカウント・ポリシーの規定回数を超えて不正なパスワードを入力すると，アカウントが自動的にロックされます。

8.2.1.3.12 アカウント・タイプの指定

Account Type オプションでは，アカウントが通常のユーザ・アカウントであるか，ワークステーション信頼アカウントであるか，サーバー信頼アカウントであるか，あるいはドメイン信頼アカウントであるかを指定します。 CIFS Server 管理ユーティリティは，2 種類のアカウント・タイプの作成のみが可能です。

- Normal user account (デフォルト)

  標準のユーザ・アカウント

- Workstation trust account

  HP CIFS サーバーが PDC あるいは BDC の場合のみ有効。ワークステーション (クライアント) システムに対してドメインに参加可能なマシン・アカウントを作成します。

ユーザ・アカウントの作成には U を指定し，ワークステーション信頼アカウントの作成には W を指定します。

8.2.1.4 ユーザの変更

CIFS Server アカウント・データベースのユーザあるいはマシン・アカウントを変更するには，オプション 4 の Modify user を使用します。このオプションを選択すると，変更するアカウント名の入力を促すプロンプトが表示されます。

CIFS Server が PDC あるいは BDC の場合，以下のようなメニューが表示されます。

```
HP CIFS Server User Account Modification Menu


        1. User name (*): cifsadmin
        2. Full name: CIFS Administrator
        3. Description: CIFS Server administrator account
        4. Home drive: H:
        5. Logon script:
        6. Profile path:
        7. Reset logon hours: no
        8. Reset bad password count: no

        * = required field

Enter item number or press Enter to accept current values [Done]:
```

CIFS Server がメンバーサーバーあるいはスタンドアロン・サーバーの場合は，次のようなメニューが表示されます。

```
 HP CIFS Server User Account Modification Menu


                1. User name (*): cifsadmin
                2. Full name: CIFS Administrator
                3. Description: CIFS Server administrator account
                4. Reset logon hours: no
                5. Reset bad password count: no

                * = required field

Enter item number or press Enter to accept current values [Done]:
```

HP CIFS Server User Account Modification Menu には Reset logon hours および Reset bad password count の 2 つのオプションが追加されていますが，それ以外は HP CIFS Server User Account Creation Menu と同じです。 User name を除き， HP CIFS Server User Account Modification Menu のどのオプションも変更できます。

選択したオプションの値を変更すると，ユーティリティはアカウント・フラグを変更するためのメニューを表示します。 このメニューは，ユーザ・アカウントの作成時に表示される HP CIFS Server User Account Flags Menu に似ています。 CIFS Server が PDC あるいは BDC の場合，Account type を除くどのフラグも変更できます。

この項では，Reset logon hours および Reset bad password count について説明します。 HP CIFS Server User Account Modification Menu および HP CIFS Server User Account Flags Menu の残りのオプションについては， 8.2.1.3 項「ユーザの追加」 を参照してください。

8.2.1.4.1 ログオン時間のリセット

必要に応じて Reset logon hours オプションを使用することにより，ユーザのログオン時間をリセットできます。

8.2.1.4.2 不正パスワード回数のリセット

必要に応じて Reset bad password count オプションを使用することにより，bad password count の値を 0 回にリセットできます。

8.2.1.5 ユーザの削除

CIFS Server アカウント・データベースからのユーザあるいはマシン・アカウントの削除には，オプション 5 の Remove user を使用します。 次のように削除するアカウント名の入力を促すプロンプトが表示されます。

```
Enter the username to remove: tunga

Username tunga deleted.
```

8.2.2 pdbedit ユーティリティによるユーザの管理

この項では，pdbedit ユーティリティを使用して CIFS Server アカウント・データベースのユーザ・アカウントを管理する方法について説明します。

8.2.2.1 ユーザ・アカウントの追加

CIFS Server データベースにユーザ・アカウントを追加する手順は以下のとおりです。

1. CIFS Server データベースにユーザ・アカウントを追加するには，ユニークな UIC が割り当てられた同じ名前の OpenVMS ユーザ・アカウントが必要です。 アカウントがユニークな UIC 識別子を持っているかどうかを確認する手順は，以下のとおりです。
   a. 次のコマンドで，SYSUAF データベースにユーザ・アカウントが存在するかどうかを確認します。

      MC AUTHORIZE SHOW *ユーザ名*

たとえば次のように実行します。

```
$ MC AUTHORIZE SHOW GANGA
```

アカウントが存在する場合，次のコマンドでユニークなUIC識別子が割り当てられているかどうか確認します。

`MCR AUTHORIZE SHOW /IDENTIFIER` ***ユーザ名***

次に例を示します。

```
$ MCR AUTHORIZE SHOW /IDENTIFIER GANGA
```

アカウントが存在しない場合は，OpenVMSアカウントを作成してユニークなUICを割り当てます。 次に例を示します。

```
$ MCR AUTHORIZE COPY SAMBA$TMPLT GANGA/UIC=[500,1]
```

アカウントは存在するがユニークなUIC識別子が割り当てられていない (すなわちUICを他のアカウントと共有している) 場合，そのアカウントではCIFSサーバーにアクセスできません。

これを修正する方法としては，以下の方法があります。

- アカウントにユニークなUICを割り当てた後，そのアカウントに対するUIC識別子を作成します。 以下に例を示します。

  ```
  $ MCR AUTHORIZE MODIFY GANGA/UIC=[500,1]/NOMODIFY_IDENTIFIER
  $ MCR AUTHORIZE ADD/IDENTIFIER/USER=GANGA
  ```

- 他のアカウントにユニークなUICを割り当てた後，UIC識別子を持っていないアカウントに対し，UIC識別子を作成します。
- 複数のアカウントでUISは共用し続けますが，UICに関連付けられた既存のUIC識別子は削除し，そのUICに対して新しい識別子を作成します。 なお，新しい識別子の名前は，CIFS Serverへのアクセスが必要なユーザのアカウント名と一致していなければなりません。

b. `SYSUAF`データベースの既存のユーザ・アカウントが適切でない場合は，`SYSUAF`データベースに新たにユーザ・アカウントを追加します。SYSUAFデータベースにユーザ・アカウントを追加する場合は，ユニークな`UIC (/uic=[<uic value>]`と/ADD_IDENTIFIERおよび/flags= NODISUSER修飾子を指定するか，次のようにデフォルトのユーザ・アカウント・テンプレート`SAMBA$TMPLT`を使用します。

```
$ MC AUTHORIZE COPY SAMBA$TMPLT GANGA /UIC=[500,500]
```

2. 次のコマンドでHP CIFS Serverアカウント・データベースにユーザ・アカウントを追加します。

   `pdbedit -a` ***ユーザ名***

   以下に例を示します。

   ```
   $ pdbedit -a GANGA
   new password:
   retype new password:
   ```

8.2.2.2 ユーザ・アカウントの変更

CIFS Serverデータベースのユーザ・アカウントは次のコマンドで変更します。

- `pdbedit -r` ***ユーザ名 オプション***

  以下に例を示します。

  — ユーザのアカウントの説明を変更するには，次のようなコマンドを実行します。

```
$ pdbedit -r ganga --account-desc=User account for Ganga Roy
```

— ユーザのフルネームを変更するには，次のようなコマンドを実行します。

```
$ pdbedit -r ganga --fullname=Ganga Roy
```

— ユーザ・アカウントに対する不正パスワード回数をリセットするには，次のようなコマンドを実行します。

```
$ pdbedit -r ganga --bad-password-count-reset
```

— ユーザ・アカウントのログイン時間をリセットするには，次のようなコマンドを実行します。

```
$ pdbedit -r ganga --logon-hours-reset
```

— いずれかのアカウント制御フラグを変更するには，次のようなコマンドを実行します。

```
pdbedit -r ganga --account-control=[<flags>]
```

<flags> には以下の値のいずれか，あるいは複数の値を指定します。

- N: パスワード不要
- D: アカウント無効
- L: 自動ロッキング
- X: パスワードは期限切れにならない

たとえば，GANGA アカウントで automatic locking フラグを設定し，その他の修正可能なフラグをクリアする場合は，次のようなコマンドを実行します。

```
$ pdbedit -r ganga --account-control="[L]"
```

注記: ここでは，すでに前の項で説明済みのオプションについては説明していません。それらのオプションについては，8.2.1.3 項「ユーザの追加」を参照してください。

1 つのコマンド行で複数のオプションを指定することも可能です。

8.2.2.3 ユーザ・アカウントの削除

CIFS Server データベースのアカウントの削除には次のコマンドを使用します。

```
pdbedit -x ユーザ名
```

たとえば，ユーザ・アカウント GANGA を削除する場合は，次のコマンドを実行します。

```
$ pdbedit -x ganga
```

8.2.2.4 ユーザの一覧表示

CIFS Server アカウント・データベースにあるすべてのユーザを一覧表示するには，次のコマンドを実行します。

```
pdbedit --list
```

あるいは

```
net sam list users
```

8.2.2.5 アカウントの詳細情報の表示

アカウントの詳細情報を表示するには，次のコマンドを実行します。

```
pdbedit --list --verbose ユーザ名
```

たとえば，ユーザ・アカウント GANGA についての詳細を表示するには，次のコマンドを実行します。

```
$ pdbedit --list --verbose ganga
```

8.2.3 ユーザ・アカウント・パスワードの変更

OpenVMS では，管理者だけが HP CIFS Server ユーザのパスワードを変更できます。パスワードの変更には smbpasswd ユーティリティを使用します。

```
$ SMBPASSWD USER1
New SMB password:
Retype new SMB password:
```

別の方法として，HP CIFS ユーザのパスワードは Windows クライアントで **Ctrl+Alt+Delete** キーを押した後に表示されるダイアログ・ボックスで Change Password をクリックする方法でも変更可能です。

8.3 グループの管理

HP CIFS Server データベースのグループは，HP CIFS Server 管理ユーティリティ SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM あるいは NET コマンド行ユーティリティを使用して管理できます。

- 8.3.1 項「CIFS Server 管理ユーティリティによるグループの管理」で，SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM を使用して CIFS Server グループを追加，修正，削除する方法について説明します。
- 8.3.2 項「NET コマンドによるグループの管理」で，NET コマンドを使用して同様の処理を行う方法について説明します。

8.3.1 CIFS Server 管理ユーティリティによるグループの管理

SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM ユーティリティは，CIFS Server アカウント・データベースに登録されているグループの一覧表示，追加，修正，削除に使用できます。

CIFS Server 管理ユーティリティを起動するには，次のコマンドを実行します。

```
$ @SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM
```

あるいは，次のコマンドを実行します。

```
$ @SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS
$ SMBMANAGE
```

これにより，HP OpenVMS CIFS Server Management メイン・メニューが表示されます。オプション 2 の Manage groups を選択すると，次のようなグループ管理メニューが表示されます。

```
        HP CIFS Server Group Management Menu

        Group Management Options:

                 1  - List groups
                 2  - Add group
                 3  - Remove group
                 4  - List group members
                 5  - Add group members
                 6  - Remove group members
                [E] - Exit
Enter group management option:
```

8.3.1.1 グループの一覧表示

オプション 1 の List groups を選択すると， CIFS Server アカウント・データベースに存在するすべてのグループ・アカウントが表示されます。 表示例を以下に示します。

```
Enumerating groups in the domain PIANODOM.
  Please wait...

Domain Admins
Domain Users
Domain Guests
Print Operators
Backup Operators
Replicator
RAS Servers
Pre-Windows 2000 Compatible Access
Administrators
Users
Guests
Power Users
Account Operators
Server Operators

Press Enter to continue
```

8.3.1.2 グループの追加

オプション 2 の Add group を選択すると，CIFS Server アカウント・データベースにグループ・アカウントを追加できます。 出力例を以下に示します。

```
        HP CIFS Server Group Account Creation Menu

                1. CIFS Server group name (*):
                2. OpenVMS resource identifier name (*):
                3. Group account description:
                4. Group Type (*): domain

                * = required field

        Enter item number or press Enter to accept current values [Done]:
```

注記: CIFS Server がメンバーサーバーあるいはスタンドアロン・サーバーの場合， 4. Group Type (*): domain は表示されません。

8.3.1.2.1 CIFS Server グループ名

CIFS Server group name オプションでは， 追加するグループのグループ名として，Windows のアカウント名として有効な 1 ～ 256 文字の名前を指定します。 指定するグループ名は，管理対象のドメインあるいはサーバー内の他のグループ名あるいはユーザ名と同じではいけません。 このグループ名の指定は必須です。

8.3.1.2.2 OpenVMS リソース識別子名

HP CIFS Server アカウント・データベースにグループ名を作成するには， まず，OpenVMS リソース識別子にマッピングする必要があります。 指定する OpenVMS リソース識別子は，既存のものあるいは存在しないもの，どちらでもかまいません。 指定する OpenVMS リソース識別子名は CIFS Server グループ名と同じにできますが，それは必須ではありません。

グループ・アカウントの作成の際，存在しない OpenVMS リソース識別子名が指定されていることをユーティリティが検知すると，その指定されたリソース識別子を OpenVMS RIGHTSLIST データベースに作成します。リソース識別子の指定は必須です。

8.3.1.2.3 グループ・アカウントの説明

グループ・アカウントの説明は，グループについての情報を記述するためのオプションのフィールドです。

8.3.1.2.4 グループ・アカウント・タイプ

グループ・アカウント・タイプは CIFS Server が PDC あるいは BDC の場合のみ適用されます。メンバーサーバーあるいはスタンドアロン・サーバーとして構成された CIFS Server では， すべてのグループ・アカウントは LOCAL タイプでなければなりません。 CIFS Server がメンバーサーバーあるいはスタンドアロン・サーバーの場合， ユーティリティは LOCAL タイプのグループ・アカウントを作成します。

CIFS Server が PDC あるいは BDC の場合，次の 2 種類のタイプのグループ・アカウントを CIFS Server データベースに作成することができます。

- LOCAL

  ローカル・グループは，セキュリティ・システムにローカルに作成されたグループです。ドメイン・コントローラに作成されたローカル・グループは，同じドメイン内のすべてのドメイン・コントローラで利用可能です。 ローカル・グループには CIFS サーバーで作成されたユーザおよびグローバル・グループを含めることができます。ローカル・グループには，信頼関係で受け渡すことにより，別のドメインのユーザおよびグローバル・グループも含めることができます。 ローカル・グループは信頼関係を横断することはできません。

- DOMAIN

  ドメインあるいはグローバル・グループには，1 つのグループ名でグループ化された CIFS Server ドメイン・グループのユーザ・アカウントを含めることができます。 グローバル・グループには，他のグローバル・グループあるいはローカル・グループをメンバーとして含めることはできません。グローバル・グループは，同じドメインあるいはそのドメインによって信頼されるドメインのどちらのローカル・グループのメンバーにも設定可能です。

8.3.1.3 グループ・アカウントの削除

CIFS Server アカウント・データベースからグループ・アカウントを削除するには オプション 3 の Remove group を選択します。 削除するグループ・アカウント名を入力するためのプロンプトが表示され， 以下のような出力が表示されます。

```
Enter the group name to delete: testgroup
  Deleting group testgroup. Please wait...
Sucessfully removed testgroup from the mapping db
```

8.3.1.4 グループ・メンバーの一覧表示

CIFS Server データベースに存在するグループ・アカウントのメンバーを一覧表示するには，オプション 4 の List group members を使用します。 以下のように，メンバーを一覧表示させるグループの名前を入力するためのプロンプトが表示されます。

```
Enter group name to list members: administrators

BUILTIN\administrators has 1 members
 PIANODOM\Domain Admins

Press Enter to continue:
```

8.3.1.5 グループ・メンバーの追加

オプション 5 の Add group members を使用して，グループのメンバー・リストにメンバーを追加することができます。 メンバーを追加するグループの名前を入力するためのプロンプトが表示されます。

CIFS Server がメンバーサーバーの場合は，以下のユーザおよびグループ・アカウントをメンバーとして追加できます。

- CIFS Server データベースに存在するユーザ・アカウントおよびグループ・アカウント
- CIFS Server がメンバーとなっているドメインに存在するユーザ・アカウントおよびドメイン・グローバル・グループ・アカウント
- CIFS Server がメンバーとなっているドメインによって信頼されたドメインに存在するユーザ・アカウントおよびドメイン・グローバル・グループ・アカウント

CIFS Server が PDC あるいは BDC の場合は， メンバーとして以下のユーザ・アカウントおよびグループ・アカウントを DOMAIN (あるいは GLOBAL) グループに追加できます。

- CIFS Server データベースに存在するユーザ・アカウント

CIFS Server が PDC あるいは BDC の場合は， 以下のユーザ・アカウントおよびグループ・アカウントを LOCAL グループに追加できます。

- CIFS Server データベースに存在するユーザ・アカウントおよびグループ・アカウント
- CIFS ドメインによって信頼されているドメインに存在するユーザ・アカウントおよびドメイン・グローバル・グループ・アカウント

CIFS Server がスタンドアロン・サーバーの場合は，以下のユーザ・アカウントおよびグループ・アカウントをメンバーとして追加できます。

- CIFS Server データベースに存在するユーザ・アカウントおよびグループ・アカウント

グループ・メンバー・アカウント名の指定には，以下の構文を使用します。

*<domain-name>**<group-member-name>*

- 追加するユーザ・アカウントあるいはグループ・アカウントが CIFS Server データベースに存在する場合は，ドメイン名の指定は省略できます。
- *<group-member-name>* は， メンバーとしてグループに追加するユーザあるいはグループの名前と置き換えてください。
- 追加するユーザあるいはグループ・アカウントが信頼されたドメインに存在する場合，*<domain-name>* は，信頼されているドメイン名と置き換えてください。
- HP CIFS Server がメンバーサーバーで， 追加するユーザあるいはグループ・アカウントがその HP CIFS Server がメンバーとなっているドメイン (たとえば WINDOM) に存在する場合，*<domain-name>* をドメイン名 WINDOM に置き換えます。

グループに対して，メンバーとして複数のアカウントを同時に追加することができます。これを可能にするために，ユーザがグループ・メンバー名を指定せずに Enter キーを押すまで，次のグループ・メンバー名を入力するためのプロンプトが表示されます。

次のような出力が表示されます。

```
Enter group name: cifsteam

Enter group member name: ganga
Added PIANODOM\ganga to PIANODOM\cifsteam

Enter next group member name: tunga
Added PIANODOM\tunga to PIANODOM\cifsteam

Enter next group member name: domain admins
Added PIANODOM\domain admins to PIANODOM\cifsteam

Enter next group member name:
```

8.3.1.6 グループ・メンバーの削除

オプション 6 の Remove group members を使用すると， 指定したメンバーをグループのメンバー・リストから削除できます。削除するべきグループ・メンバー・アカウント名を指定するためのプロンプトとは別に，そのメンバーを削除するグループ・アカウント名を入力するためのプロンプトが表示されます。

グループ・メンバー・アカウント名を指定するには，次のように入力します。

<domain-name>\<group-member-name>

- 削除するユーザあるいはグループ・アカウントが CIFS Server データベースに存在する場合は，*<domain-name>* の部分は省略できます。
- *<group-member-name>* には，メンバーとしてグループから削除されるべきユーザあるいはグループ・アカウント名を指定します。
- 削除するユーザあるいはグループ・アカウントが信頼されたドメインに存在する場合，*<domain-name>* には，信頼されているドメイン名を指定します。
- HP CIFS Server がメンバーサーバーで，削除するユーザあるいはグループ・アカウントがその HP CIFS Server がメンバーとなっているドメイン (たとえば WINDOW) に存在する場合，*<domain-name>* をドメイン名 WINDOW に置き換えます。

グループのメンバー・リストから同時に複数のアカウントを削除することができます。このため，グループ・メンバー名を指定せずにユーザが **Enter** キーを押すまで，次のグループ・メンバー名を入力するためのプロンプトを表示します。

次のような出力が表示されます。

```
Enter group name: cifsteam

Enter group member name to remove: ganga
Deleted PIANODOM\ganga from PIANODOM\cifsteam

Enter next group member name to remove: tunga
Deleted PIANODOM\tunga from PIANODOM\cifsteam

Enter next group member name to remove: domain admins
Deleted PIANODOM\domain admins from PIANODOM\cifsteam

Enter next group member name to remove:
```

8.3.2 NET コマンドによるグループの管理

この項では，CIFS Server グループの管理を手動で実行するための手順とコマンドについて説明します。

8.3.2.1 グループ・タイプ

NET コマンドでグループを作成する際， グループ・アカウント・タイプを指定することが重要です。メンバーサーバーあるいはスタンドアロン・サーバーとして構成された HP CIFS Server では，すべてのグループ・アカウントは LOCAL でなければなりません。

HP CIFS Server が PDC あるいは BDC の場合， CIFS Server データベースには 2 種類のタイプのグループ・アカウントを作成できます。

- LOCAL

  ローカル・グループはそれが作成されたセキュリティ・システムにローカルなグループです。 ドメイン・コントローラに作成されたローカル・グループは， 同じドメイン内のすべてのドメイン・コントローラで利用できます。 ローカル・グループには，CIFS Server に作成されたユーザおよびグローバル・グループを含めることができます。また，信頼関係が結ばれている別のドメインのユーザあるいはグローバル・グループも含めることができます。 ローカル・グループは信頼関係を横断することはできません。

- DOMAIN

  ドメインあるいはグローバル・グループには，CIFS Server ドメインからユーザ・アカウントを含めることができます。グローバル・グループには，別のグローバル・グループあるいはローカル・グループをメンバーとして含めることはできません。グローバル・グループは，同じドメインあるいは信頼されているドメインのローカル・グループのメンバーになることができます。

8.3.2.2 グループ・メンバー

グループ・アカウントを CIFS Server データベースに追加した後，それらのグループ・アカウントに複数のユーザあるいはグループ・アカウントをメンバーとして追加することができます。 メンバーとして追加可能なユーザおよびグループ・カウントは，CIFS Server の役割に依存します 。 CIFS Server がメンバーサーバーの場合，次のユーザおよびグループ・アカウントをメンバーとして追加できます。

- CIFS Server データベースに存在するユーザおよびグループ・アカウント
- CIFS Server がメンバーとなっているドメインのユーザおよびドメイン・グローバル・グループ・アカウント
- CIFS Server がメンバーとなっているドメインによって信頼されているドメインの ユーザおよびドメイン・グローバル・グループ・アカウント

CIFS Server が PDC あるいは BDC の場合， 以下のユーザおよびグループ・アカウントを DOMAIN (あるいは GLOBAL) タイプのグループ・アカウントにメンバーとして追加可能です。

- CIFS Server データベースに存在するユーザ・アカウント

HP CIFS Server が PDC あるいは BDC の場合， 以下のユーザおよびグループ・アカウントを LOCAL タイプのグループ・アカウントにメンバーとして追加可能です。

- CIFS Server データベースに存在するユーザおよびグループ・アカウント
- CIFS ドメインによって信頼されているドメインのユーザおよびドメイン・グローバル・グループ・アカウント

HP CIFS Server がスタンドアロン・サーバーの場合，以下のユーザおよびグループ・アカウントをメンバーとして追加可能です。

- CIFS Server データベースに存在するユーザおよびグループ・アカウント

8.3.2.3 HP CIFS Server グループの管理コマンド

HP CIFS Server グループの管理は以下の手順で行います。

1. OpenVMS システムにログインし，コマンドを定義します。
   1. OpenVMS システムにログインします。 たとえば，CIFS Server が構成されている OpenVMS システム (PIANO) に，十分な特権を持つ OpenVMS ユーザ・アカウント (たとえば SYSTEM) を使用してログインします。
   2. CIFS Server ユーティリティのためのシンボルを定義します。

      ```
      $ @SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS.COM
      ```

2. 特権を持つ CIFS ユーザを作成します。

   グループの管理には，管理者特権のあるアカウントが必要です。そのようなアカウントが無い場合は，作成する必要があります。 OpenVMS CIFS V1.2 以降，CIFS Server は，デフォルトで SYSUAF データベースに CIFSADMIN アカウントを作成します。
   1. OpenVMS ユーザ名を作成します。

      たとえば，ユーザ名 CIFSADMIN で作成する場合，次のように実行します。

      ```
      $ MCR AUTHORIZE COPY SAMBA$TMPLT CIFSADMIN/UIC=[600,600]/FLAG=NODISUSER
      ```

   2. 前の手順で作成した OpenVMS ユーザ名と同じ名前で，CIFS ユーザ・アカウントを作成します。

      ```
      $ PDBEDIT -a CIFSADMIN
      new password: any1willdo
      retype new password: any1willdo
      ```

   3. `admin users` パラメータを変更します。

      ユーザに管理者特権を与える場合は，サーバー構成ファイルの [global] セクションの `admin users` パラメータにそのユーザを追加する必要があります。

1. SAMBA$CONFIG.COM ユーティリティで HP CIFS Server が構成されている場合，インクルード構成ファイル SAMBA$ROOT:[LIB]ADMIN_USERS_SMB.CONF を編集して，admin users のリストにアカウント名を追加します。
2. HP CIFS Server が SAMBA$CONFIG.COM で構成されてない場合は， メイン構成ファイル SAMBA$ROOT:[LIB]SMB.CONF を変更します。 必要に応じて，[global] セクションに *admin users* パラメータを追加して，管理者特権を付与するアカウント名を指定します。

3. グループ・アカウントを追加します。

   CIFS Server データベースにグループ・アカウントを追加するには，そのグループ・アカウントに割り当てる OpenVMS リソース識別子を指定する必要があります。既存の OpenVMS リソース識別子にグループ・アカウントを割り当てることも，あるいは，RIGHTSLIST データベースに新しいリソース識別子を作成してそれにグループ・アカウントを割り当てることもできます。

   リソース識別子の作成

   RIGHTSLIST データベースにリソース識別子を作成するには，次のコマンドを実行します。

   MCR AUTHORIZE ADD/IDENTIFIER/ATTRIBUTE=RESOURCE *<OpenVMS-resource-id-name>*

   たとえば次のように実行します。

   ```
   $ MCR AUTHORIZE ADD/IDENTIFIER/ATTRIBUTE=RESOURCE CIFSUSERS
   ```

   グループ・アカウントの作成

   CIFS Server データベースに LOCAL タイプのグループ・アカウントを作成するには，次のコマンドを実行します。

   NET GROUPMAP ADD NTGROUP=*<CIFS Server group name>* UNIXGROUP=*<OpenVMS-resource-id-name>* TYPE=LOCAL

   たとえば，グループ・アカウント CIFSUSERS を作成するには次のようなコマンドを実行します。

   ```
   $ NET GROUPMAP ADD NTGROUP=CIFSUSERS UNIXGROUP=CIFSUSERS TYPE=LOCAL
   ```

   CIFS Server が PDC あるいは BDC の場合，CIFS Server データベースに DOMAIN タイプのグループ・アカウントも作成するには次のコマンドを実行します。

   NET GROUPMAP ADD NTGROUP=*<CIFS Server group name>* UNIXGROUP=*<OpenVMS-resource-id-name>* TYPE=DOMAIN

   たとえばグループ・アカウント DOMAINGROUP を作成するには，次のようなコマンドを実行します。

   ```
   $ NET GROUPMAP ADD NTGROUP=DOMAINGROUP UNIXGROUP=DOMAINGROUP TYPE=DOMAIN
   ```

注記: スペースを含むグループ名は，たとえば "Account Team" のように引用符で囲みます。

4. グループの表示

   マッピングされた OpenVMS リソース識別子を含め，CIFS Server データベースに存在するすべてのグループ・アカウントを表示するには，次のコマンドを実行します。

   ```
   $ NET GROUPMAP LIST
   ```

   グループのタイプに基づいてグループ・アカウントを表示するには， NET SAM LIST コマンドを使用します。

   すべての組み込みグループを表示するには，次のコマンドを実行します。

```
$ NET SAM LIST BUILTIN
```

ローカル・グループを表示するには，次のコマンドを実行します。

```
$ NET SAM LIST LOCALGROUPS
```

CIFS Server が PDC あるいは BDC の場合，ドメイン・グループを表示するには次のコマンドを実行します。

```
$ NET SAM LIST GROUPS
```

それらの説明も含め，すべてのグループ・アカウント (すべてのタイプの) を表示するには，NET RPC GROUP LIST コマンドを使用します。 ただしこのコマンドは，ユーザが管理者アカウントの認証情報を指定することが必要です。 次に例を示します。

```
$ net rpc group list --user cifsadmin
Password:
```

5. グループの削除

   グループ・アカウントを削除する前に，NET RPC GROUP DELMEM コマンドを使用してグループ・メンバーを削除してから，CIFS Server データベースからグループを削除することをお勧めします。

   CIFS Server データベースからグループ・アカウントを削除するには，NET RPC GROUP DELETE コマンドを使用します。

注記: このコマンドは管理者アカウントのユーザ固有の認証情報を必要とします。

次に例を示します。

```
$ net rpc group delete GROUP1 --user cifsadmin
Password:
```

あるいは，NET GROUPMAP DELETE コマンドを使用して，CIFS Server データベースからグループ・アカウントを削除します。次に例を示します。

```
$ net groupmap delete ntgroup=GROUP1
```

6. グループ・メンバーの追加

   グループ・メンバーの追加には NET RPC GROUP ADDMEM コマンドを使用します。

注記: このコマンドは管理者アカウントのユーザ固有の認証情報を必要とします。

たとえば，ドメイン PIANODOM のグループ PLAYERS を CIFS Server グループ CIFSUSERS に追加する場合，次のように実行します。

```
$ net rpc group addmem cifsusers pianodom\players --user cifsadmin
Password:
```

7. グループ・メンバーの削除

   グループからメンバーを削除するには，NET RPC GROUP DELMEM コマンドを使用します。

注記: このコマンドは管理者アカウントのユーザ固有の認証情報を必要とします。

たとえば，CIFS Server グループ CIFSUSERS から PIANODOM ドメインのグループ PLAYERS を削除する場合，次のように実行します。

```
$ net rpc group delmem cifsusers pianodom\players --user cifsadmin
Password:
```

8. グループ・メンバーの表示

   グループ・メンバーの表示には，NET RPC GROUP MEMBERS コマンドを使用します。なおこのコマンドは，ユーザが管理者アカウントの認証情報を指定する必要があります。たとえば，グループ CIFSUSERS のメンバーを一覧表示するには，次のようなコマンドを実行します。

```
$ net rpc group members cifsusers --user cifsadmin
Password:
```

8.4 アカウント・ポリシーの管理

HP CIFS Server のアカウント・ポリシーは，CIFS Server 管理ユーティリティ SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM あるいは NET コマンドを使用して管理できます。

- 8.4.1 項「CIFS Server 管理ユーティリティによるアカウント・ポリシーの管理」では，SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM ユーティリティを使用して CIFS Server アカウント・ポリシーを設定および表示する方法について説明しています。
- 8.4.2 項「NET コマンドによるアカウント・ポリシーの管理」では，NET コマンドを使用して同様の操作を行う方法について説明しています。

8.4.1 CIFS Server 管理ユーティリティによるアカウント・ポリシーの管理

SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM ユーティリティを使用すると，メニュー・オプションを使用して HP CIFS Server データベースのアカウント・ポリシーの表示および設定が可能です。

CIFS Server 管理ユーティリティは次のコマンドで起動します。

```
$ @SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM
```

あるいは次のコマンドを実行します。

```
$ @SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS
$ SMBMANAGE
```

これにより，HP OpenVMS CIFS Server Management Main Menu が表示されます。オプション 4 の Manage account policies を選択すると， アカウント・ポリシーの管理メニューが表示されます。

```
HP CIFS Server Account Policies Management Menu

                1  - List Account policies
                2  - Set Account policies
               [E] - Exit
Enter account policies menu option:
```

8.4.1.1 アカウント・ポリシーの表示

オプション 1 の List Account policies を選択すると， CIFS Server のアカウント・ポリシーを表示できます。 次のような表示が出力されます。

```
 Account Policy for domain "PIANODOM":

Account policy "min password length" value is: 5
Account policy "password history" value is: 0
Account policy "user must logon to change password" value is: 0
Account policy "maximum password age" value is: -1
Account policy "minimum password age" value is: 0
Account policy "lockout duration" value is: 30
Account policy "reset count minutes" value is: 30
```

```
Account policy "bad lockout attempt" value is: 3
Account policy "disconnect time" value is: -1
Account policy "refuse machine password change" value is: 0

Press Enter to continue:
```

8.4.1.2 アカウント・ポリシーの設定

オプション 1 の Set Account policies で，CIFS Server データベースのアカウント・ポリシーを設定できます。 次のような表示が出力されます。

```
    HP CIFS Server Set Account Policies Management Menu

                 1  - Minimum password length
                 2  - Password history
                 3  - User must logon to change password
                 4  - Maximum password age
                 5  - Minimum password age
                 6  - Lockout duration
                 7  - Reset count minutes
                 8  - Bad lockout attempt
                 9  - Disconnect time
                10 - Refuse machine password change
                [E] - Exit
Enter set account policies menu option:
```

この項の残りの部分で，アカウント・ポリシーを設定する際に利用できる各オプションについて詳しく説明します。パラメータの設定を変更するには，Enter set account policies menu option プロンプトでオプション番号を指定します。

8.4.1.2.1 パスワードの最短長

Minimum password length オプションは，パスワード長の下限を設定します。 このポリシーは，パスワードで必要とする最小文字数を指定し，0 ～ 4294967295 の値を指定できます。値 0 はパスワード無しを意味します。

8.4.1.2.2 パスワードの履歴

Password history オプションは，古いパスワードを再利用できるようになるまでに設定しなければならない新しいパスワードの数を指定します。 この値は，履歴として保持するパスワードの数で，0 ～ 4294967295 の範囲で指定します。

8.4.1.2.3 パスワードの変更にユーザ・ログオンが必要

"User must logon to change password" ポリシーを有効にすると，パスワードの変更の前にユーザによる CIFS Server へのログオンが必要になります。 ユーザ・アカウントのパスワードが期限切れになっている場合，そのユーザのアカウントは管理者のみが変更できます。 値 0 (ゼロ) はこのアカウント・ポリシーを無効にし，値 2 以上だとこのポリシーが有効になります。

8.4.1.2.4 パスワードの有効期限

Maximum password age オプションは，サーバーからの変更要求が発行されるまでの間，ユーザのパスワードが使用可能となる最大秒数を設定します。 この値は 0 ～ 4294967295 の範囲で指定できます。

8.4.1.2.5 パスワードが変更可能になるまでの最小期間

Minimum password age オプションは，パスワードが変更可能になるまでの間，そのユーザ・パスワードを使用しなければならない秒数を指定します。パスワード履歴値が設定されている場合，CIFS Server はパスワードをすぐに変更することを許可しません。 この値は 0 ～ 4294967295 の範囲で指定できます。

8.4.1.2.6 ロックアウト期間

Lockout duration オプションは，ロックアウトされたアカウントのロックが自動的に解除されるまでの値を分の単位で指定します。 この値は 0 ～ 4294967295 の範囲で指定できます。

8.4.1.2.7 ログイン失敗回数のリセット時間

Reset count minutes オプションは，最も近いログインの失敗が発生してからログイン失敗回数の値がゼロにリセットされるまでの期間を，分の単位で指定します。 たとえば，"reset count minutes" が 30 分に設定されている場合，ログインが最後に失敗してから 30 分が経過すると，ログイン失敗回数がゼロにリセットされます。 この値は 0 ～ 4294967295 の範囲で指定できます。

8.4.1.2.8 不正ログインのロックアウト

Bad lockout attempt オプションはログインの失敗回数を指定します。 指定した回数のログインの失敗が発生すると，そのアカウントはロックされます。 この値は 0 ～ 4294967295 の範囲で指定できます。 値 0 (ゼロ) はこのポリシーを無効にし， 0 より大きな値はこのポリシーを有効にします。

8.4.1.2.9 切断時間

Disconnect time オプションは，ユーザ・アカウントのログイン時間が所定の時間を越えた場合に，そのユーザのドメイン内のサーバーへの接続を強制的に切断するかどうかを制御します。このオプションは，各ユーザ・アカウントに対して定義されているログイン時間をもとに処理を行います。 この値は 0 ～ 4294967295 の範囲で指定できます。 値 0 (ゼロ) の場合はこのポリシーが有効で，ユーザの接続が切断されます。 このポリシーを無効にするには，値を 4294967295 に設定します。

8.4.1.2.10 マシン・パスワードの変更の禁止

Refuse machine password change オプションが設定されている場合は， マシン・アカウントのパスワードの変更が許可されません。 値 0 (ゼロ) の場合はこのポリシーが無効で， 0 よりも大きな値だとこのポリシーが有効になります。

8.4.2 NET コマンドによるアカウント・ポリシーの管理

CIFS Server は以下のアカウント・ポリシーをサポートします。

```
min password length
password history
user must logon to change password
maximum password age
minimum password age
lockout duration
reset count minutes
bad lockout attempt
disconnect time
refuse machine password change
```

これらのアカウント・ポリシーについては， 8.4.1.2 項「アカウント・ポリシーの設定」 を参照してください。

アカウント・ポリシーの値を表示するには，次のコマンドを使用します。

```
NET SAM POLICY SHOW "<account policy>"
```

たとえば，アカウント・ポリシー min password length の値を表示するには，次のようなコマンドを実行します。

```
$ NET SAM POLICY SHOW "min password length"
```

アカウント・ポリシーの値を変更するには，次のコマンドを使用します。

```
NET SAM POLICY SET "<account policy>" <value>
```

たとえば，アカウント・ポリシー password history の値を変更するには，次のようなコマンドを実行します。

```
$ NET SAM POLICY SET "password history" 3
```

8.5 信頼関係の管理

CIFS Server が CIFS ドメイン内の PDC の場合，HP CIFS Server は，他のドメイン (外部ドメイン) と信頼関係を確立できます。 信頼関係とは，あるドメインが別のドメインのユーザを信頼するような 2 つのドメイン間のリンクで，この関係が確立されている場合，他のドメインが自身のユーザに対して行ったログイン認証を受け入れます。 信頼されたドメインで定義されたユーザ・アカウントおよびグローバル・グループは，信頼するドメインとそのメンバー・システムの特権，リソース権限，ローカル・グループを，たとえ信頼するドメインのセキュリティ・データベースにそれらのアカウントが存在しなくても，認証することができます。ネットワーク内のすべてのドメイン間で適切な信頼関係が確立されている場合， ユーザが 1 つのドメインで持つ 1 つのユーザ・アカウントと 1 つのパスワードのみで，ネットワーク内の任意のリソースへのアクセスが可能となります。

信頼関係の確立には，2 つの異なるドメインで，まず最初のドメインでもう 1 つのドメインを許可し，次に 2 つめのドメインで最初のドメインの信頼を設定するという 2 段階の処理が必要になります。 双方向の信頼関係 (各ドメインが他ドメインを信頼する) の確立には，両方のドメインで上記の両方の処理を行う必要があります。

信頼関係は，CIFS Server 管理ユーティリティ SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM あるいは NET コマンド・ユーティリティを使用して管理できます。 8.5.1 項 「 CIFS Server 管理ユーティリティによる信頼の管理 」 では SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM による信頼関係の表示および確立について説明し，8.5.2 項 「NET コマンドによる信頼の管理」 では NET コマンドで同様の操作を行う方法について説明します。

8.5.1 CIFS Server 管理ユーティリティによる信頼の管理

SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM ユーティリティを使用すると，メニュー形式で信頼関係の表示と確立が可能です。

CIFS Server 管理ユーティリティは下記のコマンドで起動します。

```
$ @SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM
```

あるいは下記のコマンドを使用します。

```
$ @SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS
$ SMBMANAGE
```

これにより，HP OpenVMS CIFS Server Management Main Menu が表示されます。 オプション 5 の Manage trusts を選択すると，信頼関係の管理メニューが表示されます。

```
        HP CIFS Server Trust Relationship Management Menu

                1  - List trusts
                2  - Add in-coming trust
                3  - Remove in-coming trust
                4  - Add out-going trust
                5  - Remove out-going trust
                6  - Help
               [E] - Exit
Enter item number:
```

以降の各項で，信頼関係の管理メニューから利用できる各オプションについて説明します。 Enter item number: プロンプトに対して，オプションの番号を指定してください。

8.5.1.1 信頼関係の表示

list trusts オプションを選択すると， CIFS Server データベースに現在存在する， 信頼する関係 (入力方向の信頼)，および信頼される関係 (出力方向の信頼) が表示されます。 たとえば，次のような出力が表示されます。

```
Trusted domains list:

CIFSDOM             S-1-5-21-160935111-2493731623-2036278074

Trusting domains list:

CIFSDOM             S-1-5-21-3707034097-1477131719-1377839329

Press Enter to continue:
```

8.5.1.2 入力方向の信頼の追加

CIFS ドメインに属するユーザが外部ドメインのリソースにアクセスできるようにするために，CIFS ドメインが外部ドメインを信頼できるように設定する必要があります。 この処理は，次の 2 段階の処理で行います。

1. CIFS ドメインで，外部ドメインに対する入力方向の信頼アカウント (信頼するアカウント) を作成し，指定された信頼アカウント・パスワードを書き留めます。 入力方向の信頼アカウントの追加には，trust relationship management menu の Add in-coming trust オプションが使用できます。
2. 外部ドメインで，CIFS ドメインに対する出力方向の信頼アカウント (信頼されるアカウント) を作成します。 この処理の間，手順 1 で指定された信頼アカウント・パスワードを使用する必要があります。

   このユーティリティを使用して入力方向の信頼アカウントを追加する間，次のような項目を入力するためのプロンプトが表示されます。
   - 入力方向の信頼アカウントを追加する外部ドメイン名
   - CIFS ドメインの管理者の認証情報
   - OpenVMS ユーザ・アカウントのグループ ID (idmap uid および idmap gid パラメータが構成ファイル SMB.CONF に無い場合)
   - 信頼アカウント・パスワード。外部ドメインで手順 2 を実行した際に必要とされた，信頼アカウント・パスワードを憶えておく必要があります。

   CIFS Server データベースに入力方向の信頼アカウントを正しく追加するために，SYSUAF データベースに対応する OpenVMS アカウント名が存在しない場合，ユーティリティがこれを追加します。 外部ドメインに対する OpenVMS アカウント名は，外部ドメインの後ろにドル記号 ($) を添える形で SYSUAF データベースに追加されます。 たとえば，外部ドメイン名が WINDOM の場合，SYSUAF データベースに追加される OpenVMS アカウント名は，WINDOM$ になります。

注記:

- 外部ドメインが Windows ドメインの場合， CIFS ドメインと Windows ドメイン間の出力方向の信頼あるいは双方向の信頼を追加して手順 2 の処理を完了するには，8.5.2.9 項 「Windows ドメインでの信頼の確立」 を参照してください。
- OpenVMS のアカウント名の制約により，現在のところ，このユーティリティは 12 文字未満のドメイン名に対する入力方向の信頼アカウントの作成に限定されます。

8.5.1.3 入力方向の信頼の削除

入力方向の信頼アカウントの削除には， オプション Remove in-coming trust が使用できます。ドメインに対する入力方向の信頼を削除すると，CIFS ドメインから外部ドメインのリソースにアクセスするユーザの能力が削除されます。 入力方向の信頼アカウントを正しく削除するため

に，このユーティリティは，CIFS ドメインの管理者の認証情報を尋ねるプロンプトを表示します。

8.5.1.4 出力方向の信頼の追加

外部ドメインに属するユーザが CIFS ドメインのリソースにアクセスできるようにするには，外部ドメインと信頼を確立する必要があります。この処理は，次の 2 段階の処理で行います。

1. 外部ドメインで，CIFS ドメインに対する入力方向の信頼アカウントを作成し，指定された信頼アカウント・パスワードを書き留めます。
2. CIFS ドメインで，外部ドメインに対する出力方向の信頼 (信頼されたアカウント) を作成します。出力方向の信頼アカウントの追加にはオプション Add out-going trust が使用できます。外部ドメインとの出力方向の信頼は，上記の手順 1 でも説明したように，CIFS ドメインに対する入力方向の信頼アカウントが外部ドメインで作成された後でのみ正常に確立できます。

このユーティリティで出力方向の信頼アカウントを追加する際，次のような項目を入力するためのプロンプトが表示されます。

- 出力方向の信頼を確立する外部ドメイン名
- 信頼アカウント・パスワード。これは，手順 1 で，CIFS ドメインに対する入力方向の信頼アカウントを外部ドメインで作成した際に指定したのと同じパスワードでなければなりません。
- 外部ドメインの PDC エミュレータの完全修飾ドメイン名 (FQDN) FQDN で PDC エミュレータに到達できない場合，ユーティリティは，PDC エミュレータの IP アドレスを入力するためのプロンプトを表示します。

注記: 外部ドメインが Windows ドメインの場合，8.5.2.9 項「Windows ドメインでの信頼の確立」を参照して，CIFS ドメインおよび Windows ドメイン間で入力方向の信頼あるいは双方向の信頼を追加して手順 1 を完了してください。

8.5.1.5 出力方向の信頼の削除

出力方向の信頼関係の削除には Remove out-going trust オプションを使用できます。ドメインの出力方向の信頼関係を削除すると，外部ドメイン・ユーザは CIFS ドメインのリソースにアクセスできなくなります。出力方向の信頼を正しく削除するために，ユーティリティは，削除する出力方向の信頼名 (外部ドメイン) とともに CIFS ドメインの管理者の認証情報の入力を促すプロンプトを表示します。

8.5.2 NET コマンドによる信頼の管理

`NET RPC TRUSTDOM` コマンドを使用して，信頼関係を手動で表示，追加，および削除することができます。

8.5.2.1 信頼関係の表示

CIFS Server データベースの既存の信頼関係は次のコマンドで表示できます。

`NET RPC TRUSTDOM LIST -U <CIFS domain administrator user>`

たとえば，アカウント CIFSADMIN を使用した信頼関係を一覧表示するには，次のようなコマンドを実行します。

```
$ NET RPC TRUSTDOM LIST -U CIFSADMIN
Password:
```

プロンプトに対して，CIFS ドメインの管理者のパスワードを入力します。

8.5.2.2 入力方向の信頼の追加

CIFS Server PDC で外部ドメインに対して 入力方向の信頼 (信頼するアカウント) を追加する方法について以下に説明します。

1. 入力方向の信頼アカウント (信頼するアカウント) を作成する外部ドメインのドメイン名と一致する名前にドル記号 ($) を追加して OpenVMS アカウントを作成します。

   たとえば，外部ドメインの NetBIOS 名が trustingdom の場合，次のようなコマンドを実行します。

   ```
   $ MC AUTHORIZE COPY SAMBA$TMPLT TRUSTINGDOM$ /UIC=[1000,1]
   ```

2. NET コマンドを実行して入力方向の信頼アカウントを追加します。 コマンド構文は次のとおりです。

   NET RPC TRUSTDOM ADD *<foreign-domain-name>* *<trust-account-password>* -U*<CIFS domain administrator user>*

   たとえば，外部ドメインの NetBIOS 名が trustingdom で，CIFS ドメインの管理者名が CIFSADMIN の場合，次のようなコマンドを実行します。

   ```
   $ NET RPC TRUSTDOM ADD TRUSTINGDOM "TrustPwd1" -U CIFSADMIN
   Password:
   ```

   プロンプトに対して，CIFS ドメインの管理者のパスワードを入力します。

注記:

- 信頼関係を完成させるには，外部ドメイン (たとえば TRUSTINGDOM ドメイン) で， 上記の手順 2 で指定したものと同じ信頼アカウント・パスワードを使用して， CIFS ドメインに対する出力方向の信頼 (信頼されたドメイン・アカウント) を追加する必要があります。
- 外部ドメインが Windows ドメインの場合，8.5.2.9 項「Windows ドメインでの信頼の確立」 を参照して CIFS ドメインと Windows ドメイン間に出力方向の信頼あるいは双方向の信頼を追加してくださ。

8.5.2.3 入力方向の信頼の削除

外部ドメインに対する入力方向の信頼アカウント (信頼するアカウント) を削除するためのコマンド構文は，以下のとおりです。

NET RPC TRUSTDOM DEL *<foreign-domain-name>* -U *<CIFS domain administrator user>*

たとえば，外部ドメイン trustingdom に対する入力方向の信頼アカウントを削除するには，CIFS 管理者名が CIFSADMIN の場合，次のコマンドを実行します。

```
$ NET RPC TRUSTDOM DEL TRUSTINGDOM -U CIFSADMIN
Password:
```

プロンプトに対して CIFS ドメインの管理者のパスワードを入力します。

8.5.2.4 出力方向の信頼の追加

外部ドメインで CIFS ドメインに対する入力方向の信頼アカウント (信頼するアカウント) を追加した後，信頼関係の確立を完了させるには，外部ドメインに対する出力方向の信頼 (信頼されたドメイン関係) を確立しなければなりません。 この処理には，NET RPC TRUSTDOM コマンドで出力方向の信頼関係を確立するのとは別に，必要に応じて idmap domains パラメータ値を設定する作業も含まれます。

8.5.2.5 idmap domains パラメータの設定

信頼されたドメインのユーザが CIFS Server PDC のリソースにアクセスできるように，idmap domains パラメータ値を設定することができます。 この設定はオプションで，CIFS Server が OpenVMS ユーザ・アカウントおよびリソース識別子の作成とマッピングに WINBIND の自動マッピングを使用する場合のみ設定が必要です。 idmap domains パラメータはドメインのリストを定義し，WINBIND の SID/UID/GID テーブルを管理するためにそれぞれはバックエンドで構成されます。 このリストには，WINBIND のプライマリあるいは信頼されたドメイン全体の

ための短いドメイン名が含まれます。 idmap domains パラメータのデフォルト値はありません。

たとえば，外部ドメイン WINDOM に対して CIFS Server で出力方向の信頼を追加する場合，次のように設定します。

```
idmap domains = WINDOM
idmap alloc backend = tdb
```

ドメイン名をコンマで区切って，idmap domains に複数のドメイン名を指定することができます。

8.5.2.6 LMHOSTS. ファイルの更新

CIFS ドメインの CIFS Server PDC および外部ドメインの PDC エミュレータで 出力方向の信頼関係を確立する際に使用する名前解決の方法を決定します。 名前の解決に WINS Server を使用しない場合は，CIFS Server PDC の samba$root:[lib]lmhosts ファイルを外部ドメインのためのエントリで更新します

次の例は，ドメイン WINDOM の IP アドレス 10.20.20.40 の WINPDC という名前の Windows PDC Emulator に対して，CIFS Server PDC で必要となる lmhosts. ファイルのエントリです。

```
10.20.20.40 WINPDC
10.20.20.40 WINDOM#1B
10.20.20.40 WINDOM#1C
```

8.5.2.7 出力方向の信頼の確立

CIFS Server で外部ドメインに対して出力方向の信頼を確立するためのコマンド構文は，次のとおりです。

```
NET RPC TRUSTDOM ESTABLISH <foreign domain name>
```

プロンプトに対して入力するパスワードは，外部ドメインで CIFS ドメインに対して入力方向の信頼アカウント (信頼するアカウント) を追加する際に提供される信頼アカウント・パスワードと同じでなければなりません。

注記:

- 出力方向の信頼関係を CIFS Server の外部ドメインに追加する前に， 外部ドメインで CIFS ドメインに対して入力方法の信頼アカウント (信頼するアカウント) を追加しておかなければなりません。
- 外部ドメインが Windows ドメインの場合，CIFS ドメインと Windows ドメイン間で入力方向の信頼あるいは双方向の信頼を追加するには，8.5.2.9 項 「Windows ドメインでの信頼の確立」 を参照してください。

8.5.2.8 出力方向の信頼の削除

CIFS Server で外部ドメインに対する出力方向の信頼関係を削除するには，次のコマンドを使用します。

```
NET RPC TRUSTDOM REVOKE <foreign-domain-name> -U <CIFS domain
administrator user>
```

十分な特権を持った OpenVMS アカウント (たとえば SYSTEM) を使用して OpenVMS システムにログインした場合，次のコマンドが使用できます。

```
$ NET RPC TRUSTDOM REVOKE <foreign-doimain-name>
```

プロンプトが表示されたら，CIFS ドメインの管理者のパスワードを入力します。

8.5.2.9 Windows ドメインでの信頼の確立

CIFS ドメインと Windows ドメイン間で入力方向 (信頼する) と出力方向 (信頼される) の関係を完成させるには，CIFS ドメインと Windows ドメインで 双方向 (入力方向および出力方向) の信頼関係を確立する必要があります。 8.5.1 項「 CIFS Server 管理ユーティリティによる信頼の管理 」 および 8.5.2 項「NET コマンドによる信頼の管理」 では， HP CIFS Server で入力方向の信頼および出力方向の信頼を，自動化された手順あるいは手動でコマンドを実行して追加する方法を，それぞれ説明しています。 この項では，Windows システムで入力方向の信頼と出力方向の信頼を別々に追加する方法と，双方向の信頼関係を確立する方法を説明しています。

8.5.2.9.1 LMHOSTS. ファイルの更新

CIFS ドメインと Windows ドメイン間でいずれかのタイプの信頼関係を追加する前に， CIFS ドメインの CIFS Server PDC と Windows ドメインの PDC エミュレータが使用する名前解決方法を決定する必要があります。 Windows ドメインの PDC エミュレータが WINS Server を使用して CIFS ドメインの PDC 名を解決できない場合，Windows PDC エミュレータ上の lmhosts ファイルは CIFS ドメインの CIFS Server PDC のエントリで更新しなければなりません。

下記に示すのは，CIFS ドメイン PIANODOM にある IP アドレス 10.20.30.40 の PIANO という名前の CIFS Server PDC に対する Windows PDC エミュレータで必要となる lmhosts. ファイルのエントリの例です。

```
10.20.30.40 piano #PRE #DOM:pianodom
10.20.30.40 "pianodom       \0x1b" #PRE
10.20.30.40 "pianodom       \0x1c" #PRE
```

注記: 上記のエントリの引用符で囲まれた部分は，正確に 20 文字でなければなりません。ドメイン名はスペースを埋め込んで 15 文字とし，最後に \0x1b あるいは \0x1c を付けます。

8.5.2.9.2 双方向 trust の確立

Windows ドメインで入力方向の信頼と出力方向の信頼の両方を確立するには， Windows ドメインの PDC エミュレータで次のような手順を実行します。

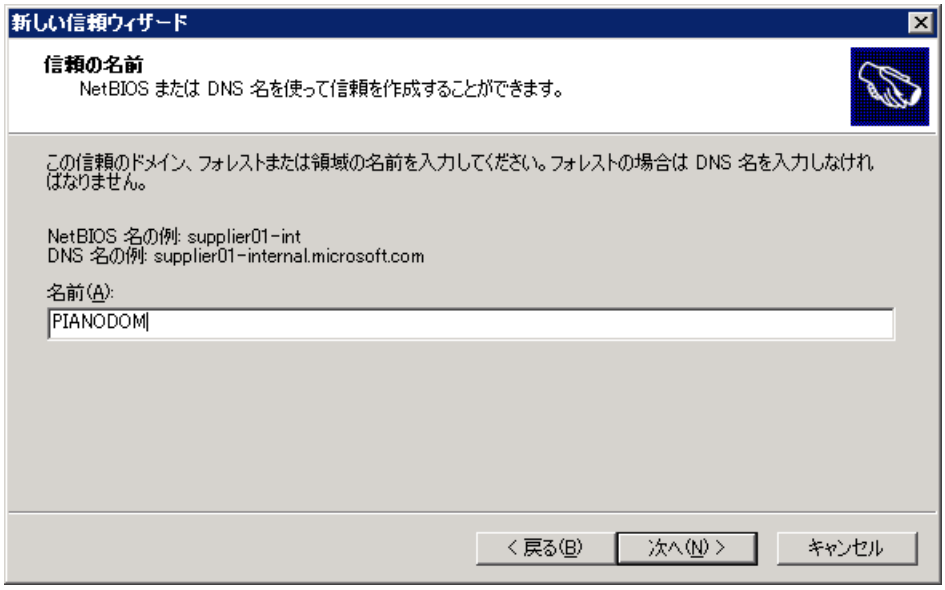
1. 「**新しい信頼ウィザード**」 をオープンします。

   このためには，Windows ドメイン名を Windows PDC エミュレータの Windows ドメイン名を選択し，「**プロパティ**」 を右クリックします。 その Windows ドメインに対して表示された「**プロパティ**」 ダイアログ・ボックスから，「**新しい信頼**」 をクリックします。

   「**新しい信頼ウィザード**」で「**次へ**」をクリックし，「**新しい信頼ウィザード**」の「**信頼の名前**」 ウィンドウをオープンします。

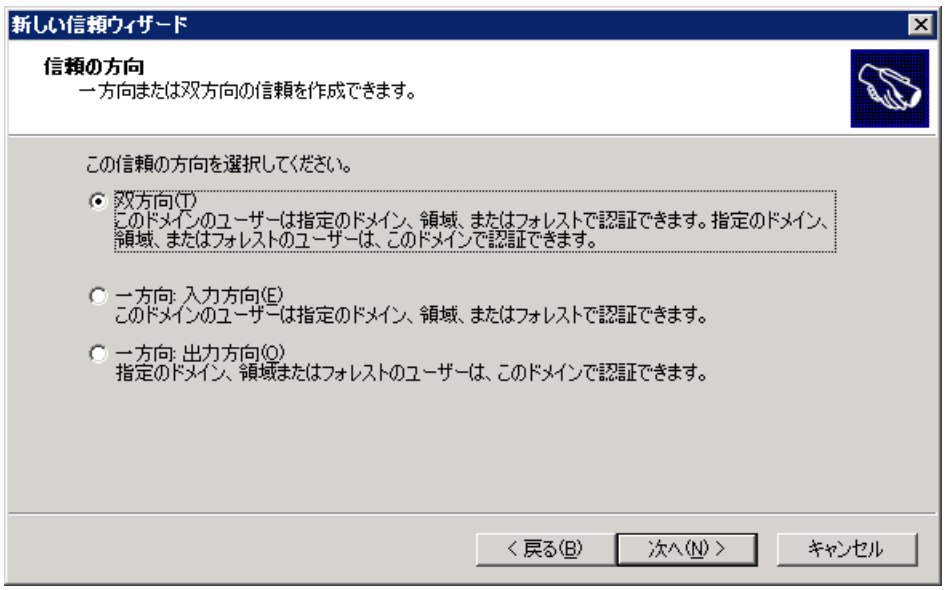
2. 「**名前**」 の下で，CIFS ドメインの NetBIOS 名をタイプします。 たとえば CIFS ドメイン名が pianodom の場合， 図 8-1 のように PIANODOM とタイプし，「**次へ**」 をクリックします。

図 8-1 CIFS ドメイン名の入力



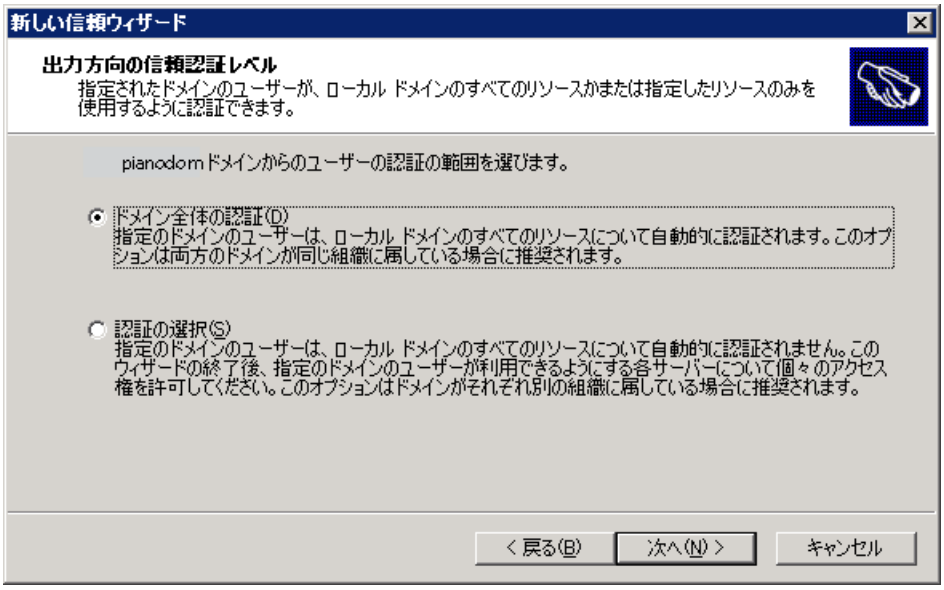
3. 入力方向の信頼と出力方向の信頼の両方を確立するために「**信頼の方向**」ウィンドウで「**双方向**」を選択し，「**次へ**」をクリックします。

図 8-2 信頼の方向の選択



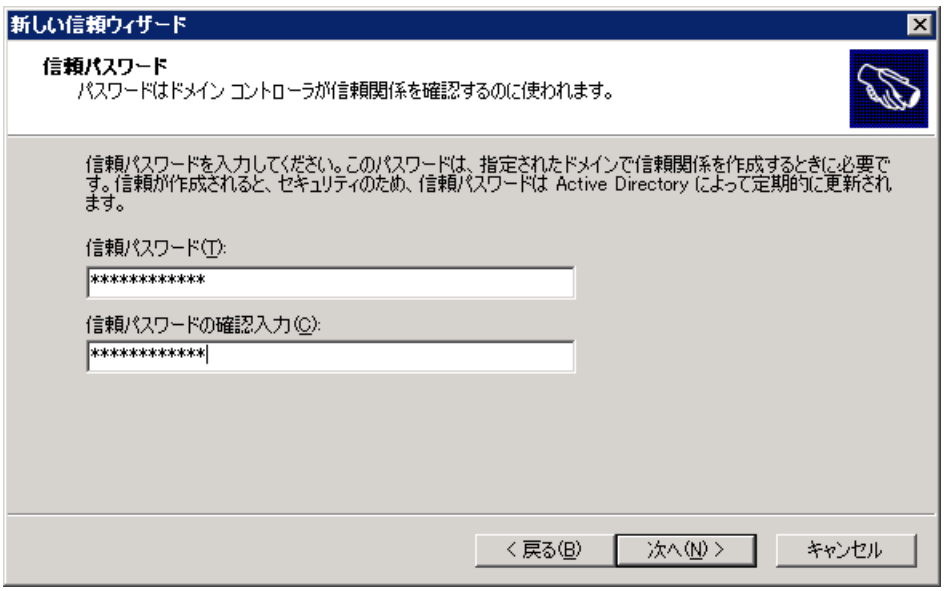
4. 「**出力方向の信頼認証レベル**」ウィンドウで「**ドメイン全体の認証**」オプションを選択し，「**次へ**」をクリックします。

図 8-3 認証レベルの選択



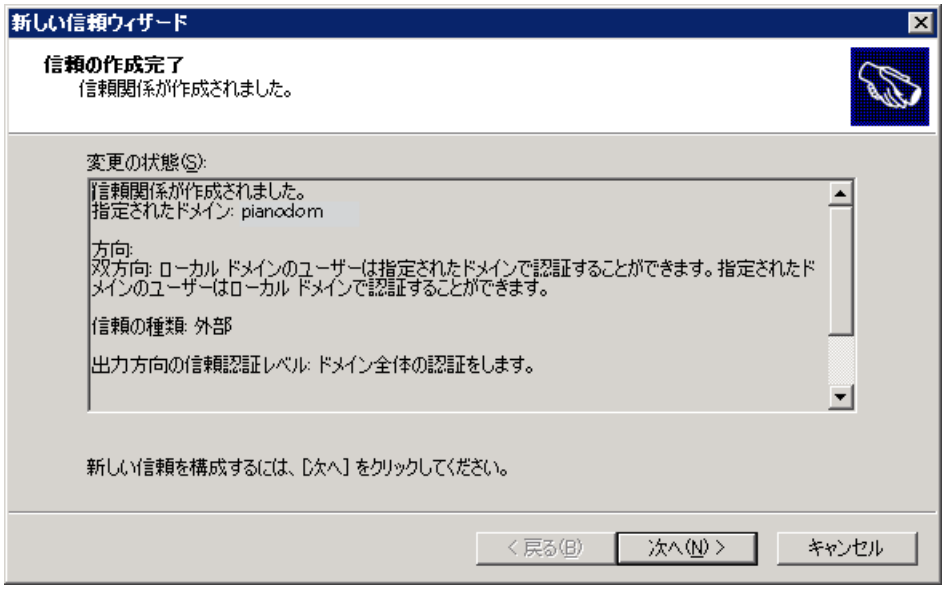
5. 「**新しい信頼ウィザード**」の「**信頼パスワード**」ウィンドウで信頼アカウントのパスワードを入力します。 CIFS ドメインの CIFS Server PDC で入力方向の信頼および出力方向の信頼を追加する際にそのパスワードが必要になるので，書き留めておいてください。「**次へ**」をクリックして「**信頼の選択の完了**」ウィンドウを表示します。

図 8-4 詳細セキュリティ設定ウィンドウ



6. 「**信頼の選択の完了**」ウィンドウに 追加される信頼のタイプに関する情報が表示され，その信頼の作成の準備ができていることを示すメッセージが表示されます。 このウィンドウで「**次へ**」をクリックします。 次に「**信頼の作成完了**」ウィンドウが表示されます。

図 8-5 詳細セキュリティ設定ウィンドウ



7. 正しく信頼が作成されたら，「**信頼の作成完了**」 ウィンドウが表示されます。「**次へ**」をクリックします。
8. 「**出力方向の信頼の確認**」ウィンドウで 確認しない を選択し，「**次へ**」をクリックします。
9. 「**入力方向の信頼の確認**」ウィンドウで 確認しない を選択し，「**次へ**」をクリックします。
10. 「**新しい信頼ウィザードの完了**」 ウィンドウで 「**完了**」 をクリックし，ウィザードを終了します。
11. 信頼関係を完成させるために，手順 5 で 「**新しい信頼ウィザード**」 の 「**信頼パスワード**」ウィンドウで入力したものと同じパスワードを指定して，CIFS ドメインの CIFS Server PDC で入力方向の信頼および出力方向の信頼を追加します。

8.5.2.9.3 入力方向の信頼の確立

CIFS ドメインと Windows ドメイン間で一方向のみの信頼を確立したいような場合があるかもしれません。 CIFS ドメインで Windows ドメインのリソースに対するユーザ・アクセスを可能にするには，Windows ドメインで CIFS ドメインに対する入力方向の信頼を確立します。 Windows ドメインの PDC エミュレータで入力方向の信頼を確立する手順は以下のとおりです。

1. 「**新しい信頼ウィザード**」 をオープンします。

   このためには，Windows PDC エミュレータの Windows ドメイン名を選択して，「**プロパティ**」 を右クリックします。 Windows ドメインに対して表示される 「**プロパティ**」 ダイアログ・ボックスから，「**新しい信頼**」 をクリックします。 「**新しい信頼ウィザード**」 が表示されたら，「**次へ**」 をクリックして 「**新しい信頼ウィザード**」 の 「**信頼の名前**」 ウインドウを表示しさせす。
2. 「**名前**」 の下に CIFS ドメインの NetBIOS 名を入力して 「**次へ**」 をクリックします。 たとえば，CIFS ドメイン名が pianodom であれば PIANODOM と入力します。
3. 入力方向の信頼を確立するために 「**信頼の方向**」 ウィンドウで 「**一方向: 入力方向**」 を選択し，「**次へ**」 をクリックします。
4. 「**新しい信頼ウィザード**」 の 「**信頼パスワード**」 ウィンドウで信頼アカウントのパスワードを入力します。 CIFS ドメインの CIFS Server PDC で出力方向の信頼を追加する際に必要となるため，そのパスワードは書き留めておきます。 その後 「**次へ**」 をクリックします。

5. 「**信頼の選択の完了**」ウィンドウには，追加されようとしている信頼のタイプに関する情報が表示されます。このウィンドウで「**次へ**」をクリックすると，その後「**信頼の作成完了**」ウィンドウが表示されれます。
6. 信頼が正しく作成されると，「**信頼の作成完了**」ウィンドウが表示されます。この後「**次へ**」をクリックします。
7. 「**入力方向の信頼の確認**」ウィンドウで 確認しない を選択し，「**次へ**」をクリックします。
8. 「**新しい信頼ウィザードの完了**」ウィンドウで「**完了**」をクリックして，ウィザードをクローズします。

8.5.2.9.4 入力方向の信頼の確立

CIFS ドメインのユーザが Windows ドメインのリソースにアクセスできるようにするためには，Windows ドメインで CIFS ドメインに対する入力方向の信頼を確立します。Windows ドメインの PDC エミュレータで入力方向の信頼を確立する手順は以下のとおりです。

1. 「**新しい信頼ウィザード**」をオープンします。

   このためには，Windows PDC エミュレータの「**Active Directory ドメインと信頼関係**」アプレットから Windows ドメイン名を選択し，「**プロパティ**」を右クリックそます。Windows ドメインに対して表示される「**プロパティ**」ダイアログ・ボックスから，「**新しい信頼**」をクリックします。表示された「**新しい信頼ウィザード**」で「**次へ**」をクリックして，「**新しい信頼ウィザード**」の「**信頼の名前**」ウィンドウを表示します。
2. 「**名前**」の下に CIFS ドメインの NetBIOS 名を入力し，「**次へ**」をクリックします。たとえば，CIFS ドメイン名が pianodom の場合は，PIANODOM と入力します。
3. 入力方向の信頼を確立するために「**信頼の方向**」ウィンドウで「**一方向: 入力方向**」を選択し，「**次へ**」をクリックします。
4. 「**新しい信頼ウィザード**」の「**信頼パスワード**」ウィンドウで信頼アカウント・パスワードを入力します。このパスワードは，CIFS ドメインの CIFS Server PDC で出力方向の信頼を追加する際に必要となるため，書き留めておきます。この後「**次へ**」をクリックします。
5. 「**信頼の選択の完了**」ウィンドウに，追加される信頼の対応についての情報が表示されます。このウィンドウで「**次へ**」をクリックすると，「**信頼の作成完了**」ウィンドウが表示されます。
6. 信頼が正しく作成されると「**信頼の作成完了**」ウィンドウが表示されます。「**次へ**」をクリックします。
7. 「**入力方向の信頼の確認**」で 確認しない を選択し，「**次へ**」をクリックします。
8. 「**新しい信頼ウィザードの完了**」で「**完了**」をクリックしてウィザードをクローズします。
9. 信頼関係を完成させるために，手順 4 の 新しい信頼ウィザード の 信頼パスワード ウィンドウで入力したのと同じ信頼アカウント・パスワードを指定して，CIFS ドメインの CIFS Server PDC で出力方向の信頼を追加します。

8.5.2.9.5 出力方向の信頼の確立

Windows ドメインのユーザが CIFS ドメインのリソースにアクセスできるようにするために，Windows ドメインで CIFS ドメインに対する出力方向の信頼を確立することができます。Windows ドメインで出力方向の信頼を確立する前に，CIFS ドメインの CIFS Server PDC で Windows ドメインに対する入力方向の信頼を追加し，信頼パスワードを書き留めます。信頼関係を完成させるために，Windows ドメインで CIFS ドメインに対して 出力方向の信頼を追加します。

Windows ドメインの PDC エミュレータで出力方向の信頼を確立する手順は，以下のとおりです。

1. 「**新しい信頼ウィザード**」をオープンします。

   Windows PDC エミュレータで「**Active Directory ドメインと信頼**」アプレットから Windows ドメイン名を選択し，「**プロパティ**」を右クリックします。Windows ドメインに対して表示される「**プロパティ**」ダイアログ・ボックスから，「**新しい信頼**」をクリックします。表示された「**新しい信頼ウィザード**」で「**次へ**」をクリックして，「**新しい信頼ウィザード**」の「**信頼の名前**」ウィンドウを表示します。
2. 「**名前**」の下に，CIFS ドメインの NetBIOS 名を入力して，「**次へ**」をクリックします。たとえば CIFS ドメイン名が pianodom であれば，PIANODOM と入力してください。
3. 入力方向の信頼を確立するために「**信頼の方向**」ウィンドウで「**一方向: 出力方向**」を選択し，「**次へ**」をクリックします。
4. 「**出力方向の信頼認証レベル**」ウィンドウで「**ドメイン全体の認証**」を選択して，「**次へ**」をクリックしてください。
5. 「**新しい信頼ウィザード**」の「**信頼パスワード**」ダイアログ・ボックスで信頼アカウントのパスワードを入力します。CIFS ドメインの CIFS Server PDC で出力方向の信頼を追加する際に必要となるため，そのパスワードは書き留めておきます。その後，「**次へ**」をクリックします。
6. 「**信頼の選択の完了**」ウィンドウには，追加される信頼のタイプに関する情報が表示されます。「**次へ**」をクリックします。

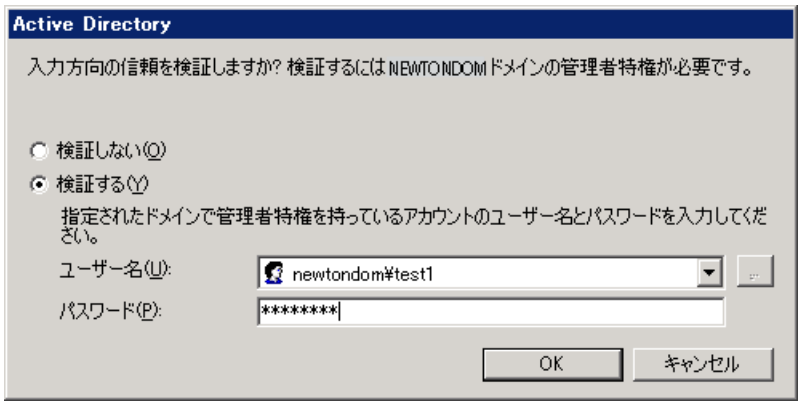
   「**信頼の作成完了**」ウィンドウが表示されます。
7. 「**次へ**」をクリックします。出力方向の信頼の確認ダイアログ・ボックスが表示されます。
8. 確認しない を選択，「**次へ**」をクリックします。
9. 「**新しい信頼ウィザードの完了**」で「**完了**」をクリックします。

8.5.3 信頼関係の確認

Windows PDC で信頼関係を確認する手順は以下のとおりです。

1. 「**Active Directory ドメインと信頼関係**」アプレットから Windows ドメイン名を選択して「**プロパティ**」を右クリックします。
2. Windows ドメインに対して表示された「**プロパティ**」ダイアログ・ボックスから，信頼関係を確認する CIFS ドメイン名を選択し，「**プロパティ**」をクリックします。
3. CIFS ドメインに対して表示された「**プロパティ**」ダイアログ・ボックスから，「**検証**」をクリックします。
4. 「**Active Directory**」ウィンドウで HP CIFS ユーザ名と `Password` を入力します。「**OK**」をクリックします。

図 8-6 Active Directory



`The trust has been validated. It is in place and active` というメッセージが表示されます。

第9章　共有の管理

この章では，以下の内容について説明します。

- 9.1 項「共有の管理」
- 9.2 項「プリンタの管理」

共有の管理では，ディスク (ディレクトリ) 共有とプリンタ共有に関する情報を提供します。プリンタの管理では，クライアントにおけるプリント・キューの追加，プリンタ・ドライバ・ファイルのアップロード，プリンタの追加について扱います。 第10章「ファイルとプリントのセキュリティ」で， ディレクトリ共有およびプリント共有におけるセキュリティの確立方法について説明します。

9.1 共有の管理

この節では，SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM ユーティリティを使用して，あるいは HP CIFS Server 構成ファイルを手動で編集して，ディスク (ディレクトリ) 共有およびプリント共有を管理する方法について情報を提供します。この節で説明する方法で，ディスク共有およびプリント共有を一覧表示，追加，修正，および削除することができます。

9.1.1 CIFS 共有の自動管理

SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM ユーティリティは， HP CIFS Server 構成ファイル SMB.CONF で定義されている共有を表示，追加，修正，あるいは削除するのに使用できます。

注記:　共有の修正および削除操作は，共有定義がメイン CIFS Server 構成ファイル SMB.CONF に存在する場合のみ使用できます。 INCLUDE ファイルのいずれかに存在する共有定義に対しては，SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM ユーティリティはその共有の修正操作あるいは削除操作を正しく実行できません。

HP CIFS Server 管理ユーティリティを起動するには，以下のコマンドを実行します。

```
$ @SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM
```

あるいは下記のコマンドを実行します。

```
$ @SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS
$ SMBMANAGE
```

これにより HP OpenVMS CIFS Server Management Main Menu が表示されます。 このメイン・メニューからオプション 1 の Manage Shares を選択すると， 次のような HP CIFS Server 共有管理メニューが表示されます。

```
HP CIFS Server Share Management Menu

        Share Management Options:

                  1  - List shares
                  2  - List a share detail
                  3  - Add share
                  4  - Modify share
                  5  - Delete share
                 [E] - Exit
Enter share management option:
```

9.1.1.1 共有の一覧表示

オプション 1 の List Shares を選択すると，隠されていない (browseable=yes と設定されている) すべてのディレクトリ共有およびプリント共有を表示できます。 たとえば，Enter share management option: プロンプトで 1 を選択すると，次のような出力が表示されます。

```
Enumerating shares available through the CIFS Server PIANO.
  Please wait...

Enumerating shared resources (exports) on remote server:


Share name   Type     Description
----------   ----     -----------
projects     Disk     Project Share
DCPS_PRINTER Print    Printer share
udfprint     Print
IPC$         IPC      IPC Service (Samba 3.0.28a running on piano (OpenVMS))

Press Enter to continue:
```

9.1.1.2 共有の詳細表示

オプション 2 の List a share detail を使用すると，特定の共有に設定された構成パラメータとそれらの値を表示できます。

```
This option displays CIFS Server configuration parameters and
   their values set for the specified share

Enter the share name: projects

Samba configuration details for the share:
[projects]
        comment = Project Share
        path = dka0:[projects]
        read only = No
        vms rms format = stream

Press Enter to continue:
```

このオプションは，隠された (browseable=no が設定された) 共有を表示するためにも使用できます。

9.1.1.3 共有の追加

SAMBA$MANAGE_CIFS.COM ユーティリティを使用して， 共有の追加および以下の構成パラメータの修正が可能です。

- path
- comment
- browseable
- read only
- valid users
- admin users
- guest ok
- inherit owner
- vms rms format
- vms inherit rms protections
- force create mode
- create mask

- directory create mask
- force directory create mode
- directory security mask
- force directory security mode
- store dos attributes
- printable
- printer name
- use client driver

オプション 3 の Add share を使用すると， SMB.CONF 構成ファイルに共有定義を追加することができます。この際，ユーティリティは，次のような共有タイプに関するプロンプトを表示します。

```
A share can be of 2 types:
   - Disk, for sharing directories and files on the disk
   - Printer, for sharing printers

  For adding a disk share, specify the share type as D
  and for printer share, specify the share type as P.

Enter the share type [D/P]: [D]
```

ディスク共有を追加する場合はデフォルトのオプション D を選択します。 プリント共有を追加する場合は P を入力します。 ディスク共有オプションが選択された場合，次のようなメニューが表示されます。

```
HP CIFS Server Menu for Adding a Disk Share

         1. Share name (*):
         2. Share path (*):
         3. Share comment:
         4. Valid users:
         5. Admin users:
         6. Hide share: no
         7. Enable guest access: no
         8. Inherit owner: no
         9. RMS file format: stream
        10. Allow write access: yes
        11. Inherit RMS protection: no
        12. Store DOS attributes: no

        * - required field

Enter item number or press Enter to accept current values [Done]:
```

Share name および Share path は必須フィールドで，それ以外のフィールドはすべてオプション・フィールドです。 オプション 11. Inherit RMS protection が no の場合は，Done を指定して表示された値を受け入れた後，マスク・パラメータとモード・パラメータを修正するためのメニューが表示されます。

```
HP CIFS Server Share Section Mask and Mode Parameters Menu

                1. Directory security mask: 07777
                2. Directory force security mode: 0
                3. File create mask: 07777
                4. File force create mode: 0
                5. Directory create mask: 07777
                6. Directory force create mode: 0
                H. Display help text
Enter item number or press Enter to accept current values [Done]:
```

プリント共有を追加している場合は，次のようなメニューが表示されます。

```
HP CIFS Server Share Section Mask and Mode Parameters Menu

                1. Directory security mask: 07777
                2. Directory force security mode: 0
                3. File create mask: 07777
                4. File force create mode: 0
                5. Directory create mask: 07777
                6. Directory force create mode: 0
                H. Display help text
Enter item number or press Enter to accept current values [Done]:
```

以下の各項で，ディレクトリ共有あるいはプリント共有を追加する際に利用できるオプションについて説明します。 パラメータの設定を変更するには，Enter item number プロンプトでオプション番号を指定します。 いずれかのオプションを選択して修正するには， 項目番号を入力するためのプロンプトで 共有追加メニューの項目番号を指定してください。

9.1.1.3.1 **共有名** (Share name)

共有名は，共有リソースを識別してアクセスする際に使用される名前を指定します。 ディスク共有を追加する際，その共有リソースはディスク上のディレクトリでなければなりません。 プリント共有を追加する場合，その共有名はOpenVMS プリンタ・キューの名前でなければなりません。 共有名は，HP CIFS Server 構成ファイルの [<share section name>] でマップングされます。

9.1.1.3.2 **共有パス** (Share path)

共有パスは，共有のユーザがアクセスの際に使用するディレクトリを指定します。 たとえば，ディレクトリ `DISK$DATA:[PROJECTS]` を共有したい場合は，共有パスのプロンプトで `DISK$DATA:[PROJECTS]` を指定します。

プリント共有の場合，CIFS Server は，印刷のためにプリント・キューに送信する前に，共有パス・ディレクトリにプリント・データをスプールします。 プリント共有に対しては，デフォルトの共有パスとしてディレクトリ `SAMBA$ROOT:[SPOOL]` を選択することができます。 このオプションは，共有セクションの Samba 構成パラメータ path にマッピングを行います。

共有パスは，UNIX パス形式でも OpenVMS パス形式でも入力できます。 ユーティリティが正しく共有パスを作成できるように，有効な共有パスを入力する必要があります。

9.1.1.3.3 **共有のコメント** (Share comment)

共有のコメントには，共有リソースについて説明した文字列を指定します。 このオプションは，共有セクション・パラメータの comment にマッピングを行います。

9.1.1.3.4 **有効なユーザ** (Valid users)

有効なユーザとは，共有リソースへのアクセスを許可するユーザのリストです。 プリント共有の場合，有効なユーザは，そのプリント共有への印刷を許可するユーザのリストです。 このオプションは，共有セクション・パラメータ valid users に対してマッピングを行います。

valid users の値がヌル (デフォルト値) の場合， その共有パスのセキュリティ設定がアクセスを許可していれば， 認証されたどのユーザも共有にアクセスできます。

有効なユーザを指定するためには，次のガイドラインを考慮する必要があります。

- 信頼されるドメインあるいは CIFS Server がメンバーサーバーとなっているドメインに属するユーザあるいはグループを指定する場合，ユーザ名あるいはグループ名の前に，バックスラッシュで区切ってドメイン名を指定する必要があります。 たとえば，CIFSDOM ドメインの ANITA ユーザを指定するには，CIFSDOM\ANITA と指定します。
- グループ名を指定するには，その前に @ 文字をつける必要があります。 たとえば，有効なユーザとして ENGPROJECT グループに属するすべてのユーザを指定するには，@ENGPROJECT と入力する必要があります。

- 有効なユーザとして複数の名前を入力できます。この場合，プロンプトに対して何も名前タイプせずにリターン・キーを押すまでの間，valid users プロンプトが表示し続けます。

9.1.1.3.5 **管理者** (Admin users)

管理者には，共有内のすべてのオブジェクトに対する管理特権を与えられたユーザのリストを指定します。 管理者として認識されるユーザは，その共有内のオブジェクトにアクセスする際，すべての特権が与えられた OpenVMS ユーザが持つすべての特権が与えられます。 両方の共有セクションで admin users 特権を持っていない限り， ある共有セクションの管理者が別の共有セクションの管理者にはなることはできません。このオプションは，共有セクション・パラメータ admin users にマッピングを行います。

管理者を指定する際は，以下のガイドラインに従います。

- 信頼されるドメインあるいは CIFS Server がメンバーサーバーとなっているドメインに属するユーザあるいはグループを指定する場合，ユーザ名あるいはグループ名の前に，バックスラッシュで区切ってドメイン名を指定する必要があります。 たとえば，CIFSDOM ドメインの ANITA ユーザを指定するには，CIFSDOM\ANITA と指定します。
- グループ名を指定するには，その前に @ 文字をつける必要があります。 たとえば，管理者として SHAREADMIN グループに属するすべてのユーザを指定するには，@SHAREADMIN と入力する必要があります。
- 管理者として複数の名前を入力できます。この場合，プロンプトに対して何も名前タイプせずにリターン・キーを押すまでの間，admin users プロンプトが表示し続けます。

9.1.1.3.6 **隠し共有** (Hide share)

隠し共有は，net view や Windows explorer ブラウザ・リストの利用可能な共有リストには表示されません。ディスク上のルート・ディレクトリをポイントする共有は， Windows explorer ブラウザ・リストに表示されないように隠すことができます。たとえば DISK$DATA:[000000] ディレクトリを共有している場合に， Windows explorer ブラウザ・リストに表示されないようにこの共有を隠すことができます。 このオプションは，共有セクション・パラメータ browseable にマッピングを行います。

9.1.1.3.7 **ゲストアクセスを可能にする** (Enable guest access)

共有に対するゲストアクセスが有効になっている場合，その共有に対するアクセスはゲスト・アカウント特権に基づいて与えられます。 ゲストとして接続するユーザは，HP CIFS Server 構成ファイルで guest account として指定されている OpenVMS アカウント (デフォルトでは SAMBA$GUEST) にマッピングされます。 ゲストユーザによるリソースへのアクセスを許可するには，そのオブジェクトで適切なプロテクションを設定してください。

CIFS Server に接続したユーザが CIFS プリント共有を使用して印刷できるように，プリント共有に対するゲストアクセスを可能にしておくと便利です。ゲストアクセスを可能にする別の例として，共有セキュリティ・モードを設定したスタンドアロン・サーバーとして HP CIFS Server が構成されている場合に，パスワードの指定無しで共有に接続できるようにユーザへのゲストアクセスを可能にすることが考えられます。

このオプションは，共有セクション・パラメータ guest ok のマッピングを行います。

9.1.1.3.8 **所有者の継承** (Inherit owner)

所有者の継承が yes に設定されている場合，CIFS Server は，新しく作成されたオブジェクトに親ディレクトリの所有者を設定します。 このオプションは，共有セクション・パラメータ inherit owner にマッピングを行います。 このオプションはディスク共有に対してのみ適用されます。

9.1.1.3.9 RMS **ファイル形式** (RMS file format)

RMS ファイル形式は，共有ディレクトリに作成されるファイルの OpenVMS RMS レコード形式を指定します。指定するレコード形式に関係なく，作成されたファイルは連続的に編成されます。

以下のいずれかのキーワードを使用してレコード形式を指定します。

表 9-1 レコード形式キーワード

レコード形式	説明
FIXED	共有ディレクトリに 512 バイト・レコードの RMS 順編成ファイルが作成されます。
STREAM	共有ディレクトリに RMS ストリーム形式のファイルが作成されます。 デフォルトのキーワードです。
STREAMLF	共有ディレクトリに RMS Stream_LF 形式のファイルが作成されます。
UNDEFINED	共有ディレクトリに作成されるファイルの RMS 形式を指定しません。 形式は，ファイルを作成するアプリケーションにより決まります。

RMS ファイル形式オプションは， 共有セクション・パラメータ vms rms format にマッピングを行います。このオプションは，ディスク共有に対してのみ適用されます。

9.1.1.3.10 書き込みアクセスを可能にする (Enable write access)

デフォルトでは，ファイル許可モードには関係なくすべての共有は読み取り専用です。 ユーザによるファイルの作成あるいは修正を可能にするには，書き込みアクセスが可能となっている必要があります。 このオプションは，共有パラメータ read-only および writeable にマッピングを行います。 このオプションは，ディスク共有に対してのみ適用されます。

9.1.1.3.11 RMS プロテクションを継承 (Inherit RMS protection)

このオプションが有効な場合，HP CIFS Server は次のように動作します。

- 新たに作成されたファイルおよびディレクトリの RMS プロテクションを親ディレクトリから継承します。
- 親ディレクトリの DEFAULT_PROTECTION ACE は無視します。
- SYSGEN パラメータ RMS_FILEPROT で指定された RMS プロテクション・マスクを無視します。
- その共有に対して指定されたマスクおよびモードのパラメータ値を無視します。

RMS プロテクションの継承オプションは，共有パラメータ inherit vms rms protection にマッピングを行います。 このオプションは，ディスク共有に対してのみ適用されます。

9.1.1.3.12 DOS 属性を保管 (Store DOS attributes)

このオプションが有効な場合，HP CIFS Server は，オブジェクトの HP CIFS Server ACE から DOS 属性 (SYSTEM，HIDDEN，ARCHIVE，あるいは READ-ONLY) を読み取ろうとします。 クライアントが DOS 属性を設定する際，それらはオブジェクトに存在する HP CIFS Server ACE に保管されます。 既存の HP CIFS Server ACE がない場合，これらの属性を保管した新しい HP CIFS Server ACE がオブジェクトに適用されます。 DOS 属性を使用する予定がある場合は，このオプションを有効にしておきます。 このオプションは，共有セクション・パラメータ store dos attributes にマッピングを行います。 このオプションは，ディスク共有に対してのみ適用できます。

9.1.1.3.13 マスクおよびモード・パラメータ (Mask and Mode parameters)

ディスク共有に適用されるファイルおよびディレクトリの種々のマスク・パラメータおよびモード・パラメータについては，10.1.5 項「 構成パラメータによる RMS 保護コードの制御 」 を参照してください。

9.1.1.3.14 クライアント・ドライバを使用 (Use client drivers)

CIFS サーバーに有効なプリンタ・ドライバを事前にアップロードせずに Windows クライアントに対してプリンタをサービスするには，クライアントにローカル・プリンタ・ドライバがインストールされている必要があります。 この場合，クライアントはプリンタを，ネットワーク・プリンタ接続ではなくローカル・プリンタとして扱います。 このため，特権のないユーザ

による OpenPrinterEx() 呼び出しは失敗し，クライアントはアクセス拒否エラーになります。プリンタに対してこのオプションが有効になっていると，OpenPrinterEx() 呼び出しが可能になる代わりに，PRINTER_ACCESS_ADMINISTER 権限によるプリンタのオープンが PRINTER_ACCESS_USE にマップングされます。 このパラメータは，CIFS Server に適切なプリント・ドライバがアップロードされているプリント共有では有効にすべきではありません。このオプションは，共有セクション・パラメータ use client drivers にマッピングを行います。 このオプションは，プリント共有に対してのみ適用可能です。

注記: プリント共有を追加する前に，OpenVMS プリント・キューが存在しているか，存在しない場合は作成しておく必要があります。プリント・キュー名とプリント共有名が同一でない場合，論理名を使用してこれらを関連付けておく必要があります。この論理名はプリント共有と同じ名前で，同時に，OpenVMS プリント・キューの名前を同じものと解釈するように定義されていなければなりません。 たとえば，既存のプリント・キュー名が HPLASERJET4100_PORTRAT で，プリンタ共有名が HP4100POR の場合，次のようなシステム論理名を定義してください。

```
$ define/system HP4100PORT HPLASERJET4100_PORTRAIT
```

プリント・キューを追加する手順については，9.2.1 項「プリンタ・キューの追加」 を参照してください。

9.1.1.4 共有の修正

共有を修正する場合はオプション 4 を選択します。 このオプションを選択すると，次のような共有名の入力のためのプロンプトが表示されます。

```
Enter the share name to modify:
```

修正する共有の名前を指定します。 たとえば，共有 PROJECTS を修正するには，共有名として PROJECTS を入力します。 共有名が入力されると，その共有に対する現在のパラメータを収集し，共有のタイプを識別します。ディレクトリ共有の修正のために，HP CIFS Server Menu for Adding a Disk Share と同じようなメニューが表示されます。 共有の追加メニューと修正メニューの違いは，修正メニューでは，それぞれのオプションの現在のパラメータ値が表示される点だけです。たとえば，共有 PROJECTS を修正しようとしている場合，次のようなメニューが表示されます。

```
HP CIFS Server Menu for Modifying a Disk Share

         1. Share name (*): projects
         2. Share path (*): dka0:[projects]
         3. Share comment: project share
         4. Valid users:
         5. Admin users:
         6. Hide share: no
         7. Enable guest access: no
         8. Inherit owner: no
         9. RMS file format: stream
        10. Allow write access: yes
        11. Inherit RMS protection: no
        12. Store DOS attributes: no

        * - required field

Enter item number or press Enter to accept current values [Done]:
```

オプション 1 の Share name を除き，どのオプションも修正可能です。

9.1.1.5 共有の削除

共有を削除するには，オプション 5 を選択します。 次のような，共有名を入力するためのプロンプトが表示されます。

```
Enter the share name to delete:
```

指定した共有名が HP CIFS Server 構成ファイル SMB.CONF に存在する場合，その共有名が削除されます。

9.1.2 CIFS 共有を手動で管理する

9.1.2.1 共有の一覧表示

HP CIFS Server 実行中に共有を一覧表示するには，次のコマンドを実行します。

```
$ @SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS.COM
$ net rpc share --long --user=""%
```

1 つの共有に関して Samba 構成ファイルの詳細を表示するには，次のコマンドを表示します。

```
$ @SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS.COM
$ testparm --suppress-prompt --section-name=<sharename>
```

9.1.2.2 ディスク共有およびプリント共有の追加

1. ディスク共有を追加するには，SAMBA$ROOT:[LIB]SMB.CONF ファイルを編集して，次のような形式でディスク共有エントリを追加します。

```
[<DISK_SHARE_NAME>]
path = <OpenVMS Directory name that must be shared>
comment = <Directory Share description>
read only = no
```

注記:

- ディスク共有の構成パラメータの要件に基づいて，共有セクション・パラメータのいずれかを上記のディスク共有定義に追加することができます。
- HP CIFS Server 構成における共有パスが検索リスト論理名の場合， Advanced Server での動作と同じように検索リストの最初の論理名を使用します。
- TESTPARM ユーティリティは， *"path"* パラメータとして指定されているすべての論理名を最大 20 レベルまで解決します。

2. プリンタ共有を追加するには，SAMBA$ROOT:[LIB]SMB.CONF ファイルを編集して，次の形式でプリント共有エントリを追加します。

```
[<PRINT_SHARE_NAME>]
printer name = <Same as PRINT_SHARE_NAME>
path = samba$root:[spool]
comment = <Print Share description>
printable = yes
read only = yes
guest ok = yes
```

注記:

- プリント共有を追加する前に，OpenVMS プリント・キューが存在するか確認し，無ければ作成しておく必要があります。プリント・キュー名とプリント共有名が同一でない場合，論理名を使用してそれらを関連付ける必要があります。この論理名はプリント共有と同じ名前で，同時に，OpenVMS プリント・キューの名前を同じものと解釈するように定義されていなければなりません。たとえば，既存のプリント・キューが HPLASERJET4100_PORTRAT で，プリント共有名が HP4100POR の場合，次のようにシステム論理名を定義してください。

  ```
  $ define/system HP4100PORT HPLASERJET4100_PORTRAIT
  ```

  プリント・キューを追加する手順については，9.2.1 項「プリンタ・キューの追加」を参照してください。
- プリント共有の構成パラメータの要件に基づいて，任意の共有セクション・パラメータを上記のプリント共有定義に追加することができます。

9.1.2.3 ディスク共有とプリント共有の管理

ディスク共有あるいはプリント共有を修正するには，共有定義が存在する HP CIFS Server 構成ファイルを編集します。たとえば，HP CIFS Server 構成ファイル SAMBA$ROOT:[LIB]SMB.CONF に存在するディスク共有 PROJECTS を修正するには， このファイルをオープンして共有定義 [PROJECTS] が始まる行に移動し，必要な共有パラメータの修正を行い，ファイルを保管します。

9.1.2.4 ディスク共有とプリント共有の削除

ディスク共有あるいはプリント共有を削除するには，共有定義が存在する HP CIFS Server 構成ファイルを編集し，共有セクションを削除して，ファイルを保管します。

9.2 プリンタの管理

プリンタの管理作業としては，プリンタ共有の設定，プリント・キューの設定，ドライバ・ファイルのアップロード，クライアントへのネットワーク・プリンタあるいはローカル・プリンタの追加，などがあります。 プリンタ共有の一覧表示，追加，修正，および削除については，9.1 項「共有の管理」 で説明しています。 プリンタ共有を追加するためには，まずプリンタ・キューの設定が必要です。

9.2.1 プリンタ・キューの追加

プリンタ共有を追加するための第一の要件は，プリンタ・キューの設定です。 この項では，HP CIFS がサポートするいくつかの異なる OpenVMS キューの設定について，それぞれ下記の項で説明します。

- 9.2.1.1 項「DCPS プリント・キュー」
- 9.2.1.2 項「TCPIP$TELNETSYM プリント・キュー」
- 9.2.1.3 項「LPD プリント・キュー」

9.2.1.1 DCPS プリント・キュー

DCPS プリント・キューを追加するには，SYS$STARTUP:DCPS$STARTUP.COM を編集して，DCPS プリント・キューに関する次のような行を追加します。

```
$ @SYS$STARTUP:DCPS$EXECUTION_QUEUE -
<print-queue-name> -                          ! P1 - Execution queue name
"ip_rawtcp/<printer-ip-address>:9100" -       ! P2 - Interconnect protocol
DCPS_LIB -                                    ! P3 - Logical name for libraries
"DATA=<data-type>" -                          ! P4 - Default queue parameters
```

```
"/SEPARATE=(NOBURST,NOFLAG,NOTRAIL)" -          ! P5 - Default queue qualifiers
""-                                             ! P6 - Communication speed(serial
- ! devices only)
""-                                             ! P7 - Device characteristics
""                                              ! P8 - Verify on/off
```

1. P1 を，作成する DCPS 実行キュー名と置き換えます。
2. P2 の "ip_rawtcp" により，DCPS による "Raw TCP" 印刷のサポートが可能になります。
3. DCPS IP_LPD 印刷を使用したい場合は， P2 を "IP_LPD/<*printer-ip-address*>" で置き換えます。 HP OpenVMS CIFS は，DCPS IP_LPD プリント・キューとでもテストされています。ただし，DCPS IP_LPD 印刷を使用する際にプリンタ・ドライバで必要となる論理名 "DCPS$_<*print-queuename*>_PRODUCT_NAME" を定義しておく必要があります。たとえば 8150 PS driver を使用するには， DCPS$_<*print-queuename*>_PRODUCT_NAME を次のように定義します。

   ```
   $ define/system DCPS$_<print-queuename>_PRODUCT_NAME - "HP LaserJet
   8150 Series PS
   ```

4. P2 パラメータの "9100" は，raw TCP プリンタのポートです。
5. P4 パラメータに対して次のように指定します。
   - 印刷に PS ドライバを指定する場合は "DATA=POSTSCRIPT" を指定します。
   - 印刷に PCL ドライバを使用する場合は，DATA=PCL" を指定します。
6. プリンタが PCL のみをサポートする場合，DCPS キューは使用されません。

詳細は，DCPS$STARTUP.COM に記述されているコメントを参照してください。
DCPS$STARTUP.COM を編集したら，次のコマンド・プロシージャを実行してキューを作成します。

```
$ @SYS$STARTUP:DCPS$STARTUP
```

上記のコマンドをサイト固有のシステム・スタートアップ・プロシージャに追加して， システム・ブートの際にこのプリント・キューが作成されるようにしてください。

次のコマンドを実行して，新しく作成されたプリント・キューを確認します。

```
$ show queue
```

論理名 DCPS_LIB が定義されていることを確認します。

```
$ show logical DCPS_LIB
```

論理名 DCPS_LIB が存在しない場合，SYS$STARTUP:DCPS$STARTUP.COM ファイルの次の行からコメントを取り除きます。

```
$ DEFINE /EXECUTIVE_MODE /SYSTEM DCPS_LIB  DCPS$DEVCTL
```

9.2.1.2 TCPIP$TELNETSYM プリント・キュー

HP CIFS Server ソフトウェアには，コマンド・プロシージャ SAMBA$PRINT_QSETUP.COM が含まれています (このコマンド・プロシージャは SAMBA$ROOT:[BIN] にインストールされます)。 このコマンド・プロシージャを使用して，TCPIP$TELNETSYM プリント・キューを設定することができます。 次に例を示します。

```
$ @SAMBA$ROOT:[BIN]SAMBA$PRINT_QSETUP.COM
Enter unique number for print form: 3974
The print queue name entered here must match with printer name in SMB.CONF
Enter VMS print queue name: HPLASER
Enter Ip address of printer: 16.138.22.23
Enter printer port: 9100
Enter print form name: xyx
```

TCPIP$TELNSYM プリント・キューを使用する場合は，以下の論理名を定義しておくと便利です。

```
DEFINE/SYSTEM TCPIP$TELNETSYM_RAW_TCP 1
DEFINE/SYSTEM TCPIP$TELNETSYM_SUPPRESS_FORMFEEDS 35
```

システム・ブート時にこれらの論理名が定義されるように，サイト固有のシステム・スタートアップ・プロシージャに上記の定義を追加してください。TCPIP$TELNETSYM プリント・キューについての詳細は，『HP TCP/IP Services for OpenVMS Management Guide』 を参照してください。

9.2.1.3 LPD プリント・キュー

前提条件

LPD プリント・キューには以下の前提条件があります。

- HP TCP/IP Services for OpenVMS が実行中であることを確認します。詳細は，『HP TCP/IP Services for OpenVMS インストレーション/コンフィギュレーション・ガイド』 を参照してください。
- LPD サービスが有効になっていることを確認します。詳細は，ご使用のサーバーにインストールされている TCP/IP 製品のドキュメントを参照してください。
  - HP TCP/IP Services for OpenVMS Version 4.0 あるいはそれ以前のバージョンを実行している場合は，次のコマンドを実行してください。

    ```
    $ RUN SYS$MANAGER:UCX$CONFIG.COM
    ```

  - HP TCP/IP Services for OpenVMS Version 5.0 あるいはそれ以降のバージョンを実行している場合は，次のコマンドを実行してください。

    ```
    $ RUN SYS$MANAGER:TCPIP$CONFIG.COM
    ```

- TCP/IP ローカル・ホスト・テーブルにリモート・プリンタ・サーバー (IP=10.0.0.1) のエントリを追加します (LPD キュー設定の `'rm'` パラメータの名前を使用します)。 次に例を示します。

  ```
  $ TCPIP SET HOST LPDSRV1/ADDRESS=10.0.0.1/ALIAS="ldpsrv1"
  ```

9.2.1.3.1 LPD プリント・キューの設定

OpenVMS LPD プリント・キューを設定するには，次のように TCPIP Printcap データベース・ユーティリティ・プログラムを実行して，リモート・プリンタを追加します。

```
$ RUN SYS$SYSTEM:TCPIP$LPRSETUP
TCPIP Printer Setup Program
Command < add delete view help exit >: add
Adding printer entry, type ? for help.
Enter printer name to add : HPLASER (The printer share mentioned in smb.conf)
Enter the FULL name of one of the following printer types:
remote local : remote
Enter printer synonym: HPLASER
Enter printer synonym:
Enter full file specification for spool directory
SPOOLER DIRECTORY sd : [TCPIP$LPD_ROOT:[HPLASER]] ? SAMBA$ROOT:[VAR.SPOOL]
Set LPD PrintServer extensions flag ps [] ?
Set remote system name rm [] ? lpdsrv1
Set remote system printer name rp [] ? Text
Set printer error log file lf [/TCPIP$LPD_ROOT/000000/HPLASER.LOG] ?
Enter the name of the printcap symbol you wish to modify. Other
valid entry is :
q to quit (no more changes)
The names of the printcap symbols are:
sd for the printer spool directory
```

```
lf for the printer error log file
lp for the name of the local printer
ps for the LPD PrintServer extensions flag
rm for the name of the remote host
rp for the name of the remote printer
fm for the printer form field
pa for the /PASSALL flag
Queue Setup 79
nd for the /NODELETE flag
cr for the cr flag
sn for the setup NoLF flag
p1-p8 for the /PARAMETER=(p1,...,p8) field
Enter symbol name: q
Symbol type value
------ ---- -----
Error log file : lf STR /TCPIP$LPD_ROOT/000000/HPLASER.LOG
Printer Queue : lp STR HPLASER
PS extensions flag: ps STR
Remote Host : rm STR lpdsrv1
Remote Printer : rp STR Text
Spool Directory : sd STR /SAMBA$ROOT/VAR/SPOOL
Are these the final values for printer HPLASER ? [y] y
Adding comments to printcap file for new printer, type ? for help.
Do you want to add comments to the printcap file [n] ? : n
Do you want the queue to default to print flag pages [y] : n
Do you want this procedure to start the queue [y] : y
Creating execution queue: HPLASER
Updating TCPIP$LPD_SYSTARTUP.COM
Updating TCPIP$LPD_SYSHUTDOWN.COM
**********************************************
* TCPIP$LPD_SYSTARTUP.COM, the printcap file *
* and TCPIP$LPD_SYSHUTDOWN.COM *
* have been updated for this printer *
* *
* Set up activity is complete for this printer *
**********************************************
```

9.2.2 プリンタ・ドライバのアップロード

CIFS プリント共有は，ネットワーク・プリンタあるいはクライアント上のローカル・プリンタとして追加することができます。 ネットワーク・プリンタとしてプリンタを追加したい場合は，最初に HP CIFS Server にプリンタ・ドライバをアップロードしておくことをお勧めします。 これにより，クライアントのネットワーク・プリンタとしてプリンタが追加された場合に，必要なドライバが HP CIFS Server から自動的にダウンロードされます。 プリンタ・ドライバのアップロードは，各クライアント・オペレーティング・システムごとに 1 回だけ必要です。

たとえば，Windows XP および Windows Vista クライアントで CIFS プリンタ HP_LASER_PRINTER を構成したい場合は，Windows XP と Windows Vista 用のドライバをそれぞれ 1 回だけアップロードする必要があります。ドライバ・ファイルをアップロードするこのオプションは，プリント・ドライバを手動でインストールせずに，Windows ユーザが自動的に CIFS プリンタを追加できるようにしたい場合に便利です。

Windows システムにローカル・プリンタを追加する場合は， ドライバ・ファイルをクライアント自身にインストールすることができ， HP CIFS Server にプリンタ・ドライバ・ファイルをアップロードする必要はありません。 この方法では，クライアントにプリンタを追加する際に，各クライアントにプリンタ・ドライバを手動でインストールすることが必要です。

9.2.2.1 PRINT$ 共有の作成

プリンタ・ドライバをアップロードする前に，Windows クライアントがプリンタ・ドライブのダウンロードの際に自動的に接続する PRINT$ という名前の共有を作成します。 HP OpenVMS CIFS V1.2 以降では，Samba 構成ユーティリティ SAMBA$CONFIG.COM を 1 度でも使用していれば，PRINT$ 共有は自動的に追加されています。 HP CIFS Server 構成ファイルに PRINT$ 共有が存在するかどうか確認するには，SAMBA$MANAGE_CIFS.COM を実行して共有の詳細情報を表示させるか，あるいは以下のコマンドを実行します。

```
$ @SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS.COM
$ testparm --suppress-prompt --section-name=print$
```

PRINT$ 共有セクションが存在しない場合は，SAMBA$ROOT:[LIB]SMB.CONF ファイルを編集して，次のように PRINT$ 共有を追加します。

```
[print$]
        comment = Printer Driver Download Area
        path = /samba$root/print_drivers/
        guest ok = yes
        read only = yes
        browseable = no
        vms path names = no
        write list = @Administrators, "@Print Operators", cifsadmin
```

注記:

- コンマで区切ってさらに追加のユーザあるいはグループの名前を write list に追加することができます。 グループ名を指定する際は，名前の前に @ を付けてください。
- write list で指定されているユーザ，あるいは，ここで指定されたグループに属するユーザは，プリンタ共有のためのプリンタ・ドライバ・ファイルをアップロードすることが可能です。
- ユーザが管理特権なしでプリンタ・ドライバ・ファイルをアップロードできるようにするために，そのユーザを HP CIFS Server Print Operators の組み込みグループのメンバーにすることができます。
- HP OpenVMS CIFS キットをインストールすると， デフォルトで samba$root:[print_drivers] ディレクトリが作成されます。

9.2.2.2 ドライバのアップロード

Windows のプリンタ・ドライバを PRINT$ 共有にアップロードするには，次の手順で行います。

1. 管理者あるいは適切な特権を持つユーザとして (すなわち PRINT$ 共有に対する write list で指定されているいずれかのユーザ名を使用して)，Windows クライアントから HP CIFS Server に接続します (**Start** -> **Run** -> **\\servername**)。
2. 「**Printers and Faxes**」フォルダをオープンします。
3. ドライバをアップロードしたいプリンタを右クリックし，「**Properties**」を選択します。

注記: これにより，デフォルトの NULL ドライバが割り当てられたキューに対するプリンタとドライバ・プロパティを表示しようとします。この結果，次のようなエラー・メッセージが表示されます。

```
The printer driver is not installed on this computer. Some printer
properties will not be accessible unless you install the printer
driver. Do you want to install the driver now?"
```

このエラー・ダイアログでは Yes はクリックせず，**No** をクリックします。 選択したプリンタのプロパティ・ウィンドウが表示されます。

4. 「**Properties**」 ウィンドウで， 「**Advanced**」 タブを選択します。「**Advanced**」 ダイアログ・ボックスで「**New Drive**」 をクリックします。 これにより Add Printer Driver ウィザードが起動されます。
5. 「**Add Printer Driver** 」 ウィザードで 「**Next**」 をクリックします。
6. 「**Printer Driver Selection**」 ボックスで適切な製造者とプリンタ・ドライバを選択します。 たとえば，プリンタが HP プリンタの場合，製造者として HP を選択します。 「**Printers**」ドロップダウン・リストから，適切なプリンタ・ドライブを選択します。 「**Printer**」 ドロップ・ボックスの下にドライバがリストされていない場合は，「**Have**

Disk」をクリックして ディスク上でプリンタ・ドライバの位置を選択します。 製造者とプリンタを選択したら，「**Next**」 をクリックします。

7. 「**Finish**」 をクリックしてプリンタ・ドライバのアップロードを開始します。
8. プリンタ・ドライバがアップロードされたら，「**Apply**」 をクリックします。 プリンタの名前が，インストールしたプリンタ・ドライバに変更されます。
9. プリンタ名を元の名前に変更するには，「**General**」 タブをクリックします。 ドライバ名を元のプリンタ名 (プリンタ・アイコンの反対側) に変更して，「**OK**」 をクリックします。
10. 別のバージョンの Windows オペレーティング・システムのためにさらに別のドライバをアップロードするには，プリンタ・プロパティの 「**Sharing**」 タブで 「**Additional Drivers**」 をクリックして，「**Additional Drivers**」 ダイアログ・ボックスを表示します。 追加でドライバをアップロードしたいオペレーティング・システムを選択したら，「**OK**」 をクリックします。 表示された 「**Printer drivers**」 ダイアログ・ボックスを使用して，ディスク上に存在する，選択したオペレーティング・システムのためのドライバ・ファイルをコピーすることができます。

9.2.3 クライアントでネットワーク・プリンタを追加

1. Windows クライアントから CIFS サーバーに接続します。
2. 「**Printers and Faxes**」 フォルダをオープンしてプリンタを選択します。 右クリックして，「**Open**」 あるいは 「**Connect**」 を選択します。 必要に応じて，CIFS サーバーからプリンタ・ドライバがダウンロードされます。 CIFS プリント共有のための新しいプリンタのアイコンが，クライアント・システムの 「**Printer and Faxes**」 フォルダに表示されます。

注記: CIFS プリンタをネットワーク・プリンタとして構成するには，最初に HP CIFS Server へプリンタ・ドライバ・ファイルをアップロードしておく必要があります。

9.2.4 クライアントでのローカル・プリンタの追加

1. Windows を実行しているシステムで「**Start**」 から 「**Settings**」を選択し，「**プリンタと FAX**」をクリックします。
2. 「**Printers and Faxes**」 フォルダで右クリックし，「**Add Printer**」 を選択します。
3. 「**Next**」 をクリックします。
4. 「**Local printer**」 をクリックし，「**Automatically detect and install my Plug and Play printer**」チェック・ボックスをクリックしてクリアし，その後「**Next**」をクリックします。
5. 「**Create a new port**」 をクリックして，「**Type of Port**」 の隣のドロップ・ダウンから「 **Local Port**」 を選択します。
6. 「**Port Name**」 ダイアログ・ボックスで， 次のような構文でプリンタのパスをタイプします。

   \\<*cifs server name*>\<*printer share name*>

7. 「**Next**」 をクリックします。
8. 「**Install Printer Software**」ページで，「**Manufacturer**」パネルの下の正しい製造者をクリックし，ご使用のプリンタと同じプリンタ・エミュレーションをサポートするプリンタの名前をクリックし，「**Next**」 をクリックして， 最後に 「**Finish**」 をクリックします。

第10章　ファイルとプリントのセキュリティ

ファイルやプリントのサービスにおいて重要なものに，ファイルのセキュリティがあります。OpenVMS のファイル・セキュリティに加えて NT ACL のファイル・セキュリティを提供する Advanced Server for OpenVMS とは異なり，HP CIFS Server は，OpenVMS のファイル・セキュリティのみを Windows クライアントに提供します。 つまり，ファイルおよびディレクトリに適用される Windows セキュリティを OpenVMS ファイル・セキュリティにマッピングします。 ファイル・セキュリティは，どの CIFS ドメイン・ユーザあるいはグループにも設定できます。 CIFS はファイルおよびディレクトリ監査機能を提供しませんが，OpenVMS 標準の監査機能がこの目的に使用できます。 CIFS のファイル・セキュリティは，次の 2 つの手順で構成されます。

1. ユーザとグループのマッピング
2. アクセス許可のマッピング

この章では，以下の内容について説明します。

- 10.1 項「ファイル・アクセス許可のマッピング」
- 10.2 項「DOS 属性の保管」
- 10.3 項「CIFS ファイル・セキュリティを適用する際の ACL の順序」
- 10.4 項「ファイル・セキュリティ・マッピングに起因する制限事項」
- 10.5 項「ファイル・セキュリティの設定に必要なアクセス許可と特権」
- 10.6 項「ファイルのセキュリティ」
- 10.7 項「重要なデータベース・ファイル」
- 10.8 項「プリント・セキュリティ」

第6章 「ユーザとグループのマッピング 」 および 第7章 「WINBIND のサポート」 で，CIFS のファイル・セキュリティの概要と，CIFS ドメイン・ユーザおよびグループの OpenVMS ユーザ名およびリソース識別子へのマッピングについて説明しています。 第10章では，CIFS Server がリソースへのアクセスを管理する方法に加え，Windows のアクセス許可を OpenVMS ファイル・セキュリティにマッピングする方法について説明します。

HP CIFS Server はプリンタ・オブジェクトでアクセス制御リスト (ACL) もサポートしており，これについては 10.8 項「プリント・セキュリティ」 で説明しています。

10.1 ファイル・アクセス許可のマッピング

Windows から OpenVMS へのファイル・アクセス許可のマッピングでは，Windows ファイル・アクセス許可の OpenVMS ファイル・セキュリティへのマッピングが行なわれます。 この章では，HP CIFS Server の構成パラメータによって，新しいファイルおよびディレクトリで OpenVMS の RMS アクセス許可コードがどのように制御されるかについても説明しています。

10.1.1 Windows から OpenVMS へのアクセス許可のマッピング

OpenVMS では，ユーザがオブジェクトに対して，読み取り (R)，書き込み (W)，実行 (E)，削除 (D)，制御 (C)， あるいはこれら RWEDC の組み合わせでアクセス許可を指定することができます (後述の「注記」を参照)。 一方 Windows 標準のアクセス許可では，「**セキュリティ**」ダイアログ・ボックスを使用して，フルコントロール，変更，読み取りと実行，ファイルの内容の一覧表示 (ディレクトリのみ)，読み取り，および，書き込みなどの，一連のアクセス許可をオブジェクトに対して設定できます。 また Windows では，「**プロパティ**」ページの「**セキュリティ**」タブの「**詳細設定**」ボタンにより，特別なアクセス許可を設定する機能が提供されます。

表 10-1 に，CIFS によって Windows のアクセス許可がどの OpenVMS アクセス許可にマッピングされるかを示します。カッコで囲んで詳細設定と記述しているアクセス許可は，そのアクセス許可が Windows の「**セキュリティの詳細設定**」ダイアログ・ボックスでのみ提供されることを示します。フルコントロールと読み取りのアクセス許可に関しては，詳細設定ダイアロ

グ・ボックスで表示される特別なアクセス許可だけでなく標準のアクセス許可にも含まれます。

表 10-1 Windows アクセス許可と OpenVMS アクセス許可のマッピング

Windows アクセス許可	OpenVMS アクセス許可
フルコントロール	RWEDC
変更	RWED
読み取りと実行	RE
読み取り	R
書き込み	W
フルコントロール (詳細設定)	RWEDC
フォルダのスキャン/ファイルの実行 (詳細設定)	E
フォルダー一覧/データの読み取り (詳細設定)	R
属性の読み取り (詳細設定)	R
拡張属性の読み取り (詳細設定)	R
フォルダの作成/データの書き込み (詳細設定)	W
フォルダの作成/データの追加 (詳細設定)	W
属性の書き込み (詳細設定)	W
拡張属性の書き込み (詳細設定)	W
サブフォルダとファイルの削除 (詳細設定)	サポートされない
削除 (詳細設定)	D
アクセス許可の読み取り (詳細設定)	R
アクセス許可の変更 (詳細設定)	C
所有権の取得 (詳細設定)	C

注記: オブジェクトに ACCESS=NONE アクセス制御指示子が存在する場合はこれも考慮されますが，HP CIFS Server は，Windows からアクセス許可を設定する場合に使用可能な DENY アクセス許可オプションをサポートしません。

10.1.2 Windows から OpenVMS への継承値のマッピング

Windows システムでは，ディレクトリでアクセス許可を設定する場合，そのディレクトリにのみ設定するか，その下のサブディレクトリおよびファイルに設定するか，あるいはそれらを組み合わせて設定するかを指定することができます。

同様に OpenVMS では，ディレクトの ACE によってディレクトリへのアクセスが制御される一方で，そのディレクトリの下に作成されるサブディレクトリとファイルに対してのみ適用される DEFAULT ACL を提供します。

たとえば，OpenVMS で親ディレクトリが以下のようなセキュリティに設定されているとします。

```
PROJECTS.DIR;1          [SYSTEM]                        (RWE,RWE,E,E)
DEFAULT_PROTECTION,SYSTEM:RWED,OWNER:RWED,GROUP:,WORLD:)
IDENTIFIER=ADMIN_USER,ACCESS=READ+WRITE+EXECUTE+DELETE)
IDENTIFIER=ADMIN_USER,OPTIONS=DEFAULT,ACCESS=READ+WRITE+EXECUTE+DELETE)
```

通常の OpenVMS 特権を持っているユーザに対しては，PROJECTS.DIR ディレクトリへのアクセスは ACE （IDENTIFIER=ADMIN_USER,ACCESS=READ+WRITE+EXECUTE+DELETE）で制御されます。

親ディレクトリ PROJECTS.DIR に新たに作成されたすべてのファイルおよびディレクトリに対しては ACE
（IDENTIFIER=ADMIN_USER,OPTIONS=DEFAULT,ACCESS=READ+WRITE+EXECUTE+DELETE）
が適用されます。

表 10-2 に， CIFS によって Windows から OpenVMS へ継承されるマッピングを示します。

表 10-2 Windows から OpenVMS へ継承されるマップング値

Windows の継承値	OpenVMS への継承マッピング
このフォルダのみ	ACCESS ACE にマッピング
このフォルダ，サブフォルダ，およびファイル	ACCESS ACE と OPTIONS=DEFAULT ACE の両方にマッピング
このフォルダとサブフォルダ	ACCESS ACE にマッピング
このフォルダとファイル	ACCESS ACE にマッピング
サブフォルダとファイルのみ	このディレクトリに OPTIONS=DEFAULT ACE にマッピング
サブフォルダのみ	サポートされません。無視されます。
ファイルのみ	サポートされません。無視されます。

10.1.3 Windows アクセス許可への OpenVMS RMS 保護コードのマッピング

OpenVMS の RMS 保護コードは，システム，所有者，グループ，ワールドの 4 つのユーザ・カテゴリに対する，読み取り許可，書き込み許可，実行許可，および削除許可で構成されます。 典型的な RMS 保護コードは (S:RWED,O:RWED,G:RE,W) で，これは，システムおよび所有者カテゴリのメンバーは読み取り，書き込み，実行，および削除アクセスが可能で， グループ・カテゴリのメンバーは読み取りおよび実行アクセスのみが可能で，ワールド・カテゴリのメンバーは何もアクセス権を持たないことを示しています。 すべてのオブジェクトは，作成時に RMS 保護コードを取得します。 RMS 保護マスクを割り当てる OpenVMS のセキュリティ・ルールは本書の対象外で，『HP OpenVMS システム・セキュリティ・ガイド』で詳しく説明しています。

ただし，一般に新しいディレクトリは RMS 保護コードを親ディレクトリから継承します。 新しいファイルに適用される RMS 保護コードは，実質的にそのファイルを作成するプロセスの RMS 保護マスクをベースにします。 デフォルトの RMS 保護マスクは，SYSGEN パラメータ RMS_FILEPROT によって制御されます (ただし SET PROTECTION/DEFAULT コマンドで変更できます)。 RMS_FILEPROT のデフォルト値は，(S:RWED,O:RWED,G:RE,W) の RMS 保護マスクになります。

さらに OpenVMS は，DEFAULT_PROTECTION ACE を提供します。 この ACE は，ディレクトリ上に存在する場合，(新しいディレクトリに対してではなく) ディレクトリに作成された新しいファイルに対して適用される RMS 保護コードを決定します。 DEFAULT_PROTECTION ACE は，ディレクトリ内に作成された新しいディレクトリのアクセス制御リストに伝えられますが，それらの新しいディレクトリに適用される RMS 保護マスクに影響することはありません。

Windows にはこれと同様の保護コードの概念はありませんが，ある程度似た機能を提供します。 Windows は，OpenVMS と同じようにオブジェクトの所有者を管理します。 Windows は， OpenVMS の RMS 保護コードのワールド・カテゴリと同じような概念の Everyone と呼ばれる特別なグループを持っています。 ディレクトリに対しては，Windows は CREATOR OWNER および CREATOR GROUP に対するアクセス許可も管理します。 CREATOR OWNER と CREATOR GROUP は，それぞれ，ファイル所有者の新しいオブジェクトに適用されるアクセス許可，お

よびファイル所有者のプライマリ・グループに関する新しいオブジェクトに適用されるアクセス許可を表します。

表 10-3 に，RMS 保護コード・カテゴリと Windows のセキュリティ概念について示します。

表 10-3 OpenVMS RMS 保護コードと Windows セキュリティのマッピング

RMS 保護コード・カテゴリ	Windows マッピング
所有者および SYSTEM	所有者
グループ	Unix のグループとして表示される
ワールド	Everyone
DEFAULT_PROTECTION_ACE における所有者	そのディレクトリ上で CREATOR OWNER
DEFAULT_PROTECTION_ACE におけるグループ	そのディレクトリ上で CREATOR GROUP
DEFAULT_PROTECTION_ACE におけるワールド	サブフォルダおよびファイルに対して Everyone

10.1.4 CREATOR OWNER および CREATOR GROUP への RMS 保護マスク RMS_FILEPROT のマッピング

Windows は，ディレクトリに CREATOR OWNER アクセス許可が存在していることを必要とします。 Windows システムからディレクトリのアクセス許可を表示および設定する際，DEFAULT_PROTECTION ACE がディレクトリに存在しない場合，CIFS Server は，表 10-4 に示すように，CREATOR OWNER および CREATOR GROUP に OpenVMS の SYSGEN パラメータ RMS_FILEPROT の保護マスクをマップングします。

表 10-4 RMS 保護マスク RMS_FILEPROT の Windows へのマッピング

RMS 保護マスク RMS_FILEPROT	Windows マッピング
RMS_FILEPROT の所有者	そのディレクトリ上の CREATOR OWNER
RMS_FILEPROT のグループ	そのディレクトリ上の CREATOR GROUP
RMS_FILEPROT のワールド	サブフォルダおよびファイルに対して Everyone

10.1.5 構成パラメータによる RMS 保護コードの制御

HP CIFS Server は，新しいオブジェクトの作成あるいは Windows アクセス許可の設定の際に適用される RMS 保護コードに影響を与えるのに使用可能な，いくつかの構成パラメータを提供します。 パラメータの名前は Samba 管理者にとってはお馴染みのものですが，その実装は (もともとは UNIX のセキュリティ・モデルをベースにした) オープンソース版の Samba とは大きく異なります。

デフォルトでは，HP CIFS Server は，OpenVMS の標準のセキュリティ・ルールに基づいて新しいオブジェクトのセキュリティ・プロファイルを決定します。 構成パラメータにデフォルト値以外が指定されている場合，HP CIFS Server はセキュリティを調整します。

注記: HP CIFS Server は，新しいディレクトリの所有者に削除アクセスを与えます。 これにより，作成者が新しいフォルダの名前変更および削除することが可能な Windows の標準の動作と同じになります (OpenVMS の標準の動作では，ディレクトリが親ディレクトリから RMS 保護マスクを継承する場合，すべての削除アクセスは削除されます)。

以下の構成パラメータを使用して，OpenVMS が適用するセキュリティを修正できます。

- *inherit owner*

  デフォルト値は no です。 yes が設定されている場合，HP CIFS Server は，新しいオブジェクトの RMS 所有者に親ディレクトリの所有者を設定します。

注記: `inherit owner = no` と設定されており，親ディレクトリがリソース識別子により所有されている場合， このディレクトリへの WRITE アクセスを持たない特権のないユーザが新しいファイルを作成すると，HP CIFS Server は，リソース識別子ではなく，そのファイルを作成したユーザの UIC をその所有者に設定します。 OpenVMS の動作を残すには (すなわち，リソース識別子を所有者として設定するには)， `SMB.CONF` ファイルの適切な [share] セクションに `inherit owner = yes` を追加します。

- *`inherit vms rms protections`*

  これは新しいパラメータで，デフォルト値は no です。 yes が設定されている場合，HP CIFS Server は次のように動作します。
  - RMS 保護コードを親ディレクトリのものに設定します。
  - DEFAULT_PROTECTION ACE が存在する場合これを無視します。
  - SYSGEN パラメータ *`RMS_FILEPROT`* によって指定された RMS 保護マスクを無視します。
  - `SMB.CONF` ファイルで指定されたマスクおよびモードのパラメータ値を無視します。
- 表 10-5 に示すのは，HP CIFS Server がサポートするマスクおよびモード・パラメータ値です。

表 10-5 マスクおよびモード・パラメータ

パラメータ名	RMS 保護コードに作用するタイミング
create mask	新しいファイルの作成時
force create mode	新しいファイルの作成時
directory mask	新しいディレクトリの作成時
directory security mask	Windows のユーザおよびアプリケーションがそのディレクトリでセキュリティを変更した時
force directory security mode	Windows のユーザおよびアプリケーションがそのディレクトリでセキュリティを変更した時

注記:

- CIFS for OpenVMS は，Windows のユーザおよびアプリケーションがファイルのセキュリティを変更する際に，構成パラメータ *`security mask`* および *`force security mode`* を使用しません。
- *`create mode`* パラメータは *`create mask`* と同じ意味です。 混乱を避けるため，*`create mask`* を使用することをお勧めします。

10.1.5.1 変更できない構成パラメータ

表 10-6 に示す構成パラメータの値はデフォルト値から変更できません (変更は無視されます)。

表 10-6 変更できない構成パラメータ

inherit acls	デフォルトは yes です。 ACL の継承は無効にできません。
inherit permissions	inherit vms rms protections パラメータで置き換えられます。
security mask	サポートされません
force security mode	サポートされません

10.1.5.2 マスクおよびモードのパラメータ値

HP CIFS Server で導入された重要なファイル・セキュリティの変更の 1 つに，新しいオブジェクトの RMS 保護コードでの削除アクセスの付与に関するものがあります。 以前は，種々のマスクおよびモード・パラメータが削除アクセスを書き込みビットと結び付けていました。 つまり，書き込みアクセスを有効にすると，削除アクセスを有効にすることにもなりました。 しかし，削除および書き込みアクセス許可は以下のように区別されます。

マスクおよびモード・パラメータの値は次のような意味を待ちます。

<mask or mode parameter name>= 0dogw

0= 値が 8 進数であることを示します。

d = RMS 保護コードのすべてのカテゴリに対する削除アクセスの付与を制御します。(「DELETE」を参照)

o = RMS 保護コードの所有者カテゴリに対する読み取り，書き込み，および実行アクセスの付与を制御します。

g = RMS 保護コードのグループ・カテゴリに対する読み取り，書き込み，および実行アクセスの付与を制御します。

w = RMS 保護コードのワールド・カテゴリに対する読み取り，書き込み，および実行アクセスの付与を制御します。

注記: RMS 保護コードのシステム・カテゴリは，所有者カテゴリと同じアクセス許可を受け取ります。この動作を変更するためのオプションはありません。

削除アクセスは次のような値のビットマスクを使用して示されます。

4 — RMS 保護コードの所有者カテゴリに削除アクセスを付与します。

2 — RMS 保護コードのグループ・カテゴリに削除アクセスを付与します。

1 — RMS 保護コードのワールド・カテゴリに削除アクセスを付与します。

所有者，グループ，およびワールド・アクセス値は，以下のアクセスを示すビットマスクでもあります。

4 — READ アクセスを付与します。

2 — 書き込みアクセスを付与します。

1 — EXECUTE アクセスを付与します。

また，マスクおよびモード・パラメータのデフォルト値は，OpenVMS が自身に適用するセキュリティを (明記したものを除き) これらのパラメータが調整しないように変更されています。

結果として得られる RMS 保護コードを生成するための AND & OR 操作を実行するために，以下のマスクとモード・パラメータが関連付けられています。

- *create mask* と *force create mode*
- *directory mask* と *force directory mode*
- *directory security mask* と *force directory security mode*

適切な *mask* パラメータの値が，OpenVMS が提供する RMS 保護コードの結果と AND 処理されます。 その後この結果が，適切な *mode* パラメータの値と OR 処理されます。

mask パラメータのデフォルト値は 07777 で， *mode* パラメータのデフォルト値は 00000 です。 ただし，*force directory mode* は例外です。 HP CIFS V1.2 以降，*force directory mode* のデフォルト値は 04000 です。 これは，新しいディレクトリを作成した場合に，保護コードの所有者カテゴリに対する削除アクセスを許可するためです。

10.2 DOS 属性の保管

HP CIFS Server は，ファイルの DOS 属性 SYSTEM，HIDDEN，ARCHIVE，あるいは READ-ONLY を保管する機能をサポートします。 デフォルトでは，この機能は無効になっています。 DOS 属性の保管を有効にするには，以下のように指定します。

```
store dos attributes = yes
```

store dos attributes パラメータは共有レベルのパラメータで，個々の共有ごとに設定できます。

RMS 保護コードで DOS 属性の保管をマッピングした以下の構成パラメータは，サポートされません。

- *map system*
- *map hidden*
- *map archive*
- *map readonly*

10.3 CIFS ファイル・セキュリティを適用する際の ACL の順序

OpenVMS システムでは，Windows と比べると，ACL における ACE の順序がアクセスを判断する際の重要な要素となります。これらはファイルとディレクトリに対して適用され，Windows システムがそれらを保持しないのに比べると，非常に重要です。

Windows と OpenVMS との間で対照的な ACL 処理の違いがあるため， オブジェクトにセキュリティを設定する際に HP CIFS Server が適用する ACE の順序を理解しておくことが重要になります。 オブジェクトに OpenVMS ACE を適用する際，HP CIFS Server は既存の OpenVMS 固有の ACE を，(理想的には元の順序で) 保管しておく必要があります (後述の「注記」を参照)。 Windows システムからオブジェクトのセキュリティを適用する場合，HP CIFS Server により以下のような設計で実現されます。

1. アクセス許可リストに新しいエントリが追加される場合，対応する ACE は ACL の最上位に置かれます。
2. 既存のアクセス許可リスト・エントリが変更される場合，ACL の順序は影響を受けません。
3. OpenVMS 固有のすべての ACE は，既存の順序のまま残されます。

注記: OpenVMS 固有の ACE には，保護された ACE あるいは 隠された ACE の他，Audit ACE，Alarm ACE， IDENTIFIER=* を含む ACE があります。このような ACE は，WIndows システムを使用して表示，変更，あるいは削除することはできません。

10.4 ファイル・セキュリティ・マッピングに起因する制限事項

本章のはじめの項で，Windows ファイル・セキュリティが OpenVMS ファイル・セキュリティにどのようにマッピングされるかを説明しています。Windows システムと OpenVMS システムとでは，オブジェクトへのアクセス付与のためのオブジェクトの ACL 処理方法が大きく異なるため，このマッピング・メカニズムは制限事項が無いわけではありません。HP CIFS Server が提供するファイル・セキュリティ・マッピングの制限事項としては，以下のようなものがあります。

- 10.4.1 項「オブジェクト・アクセスの制限事項」
- 10.4.2 項「継承されない OpenVMS ACE に関する制限事項 (ファイルのみ)」
- 10.4.3 項「組み込み管理者グループの制限事項」
- 10.4.4 項「Windows の継承値のマッピングに関する制限事項」
- 10.4.5 項「Windows の特別なアクセス許可に関する制限事項」
- 10.4.6 項「ディレクトリあるいは共有に対するアクセス許可を表示する際の制限事項」

10.4.1 オブジェクト・アクセスの制限事項

ユーザが特に権限を持っていない場合，Windows システムは，そのオブジェクトに対する累積したアクセス許可をもとにオブジェクトへのアクセスを許可します。たとえば，あるユーザが，あるオブジェクトに対する読み取り許可のみを持つグループのメンバーであると同時に，書き込み許可のみを持つグループのメンバーである場合，そのユーザは，読み取りおよび書き込みの両方のアクセス許可を持つことになります。このため，ACL の順序は，Windows では関係なくなります (DENY アクセス許可は例外です)。

OpenVMS システムでは，オブジェクトで ACL が現れる順序は非常に重要です。ユーザが特に特権を持っていたりファイルの所有者であったりしなければ，OpenVMS は，ACE リストの上位から最初に一致する ACE を基に，オブジェクトにアクセスを付与します。

この動作は，予想外のアクセスエラーになることがあります。たとえば，あるユーザが，あるオブジェクトに対する読み取り許可のみを持つグループのメンバーであると同時に，書き込み許可のみを持つグループのメンバーである場合，そのユーザは，読み取りおよび書き込みのどちらかのアクセスを許可されます。 両方ではありません。ユーザが読み取りと書き込みのどちらのアクセス許可を受け取るかは，どちらのアクセス許可エントリが最初にリストされているかによって決まります。 このような状況あるいはその他の状況では，Windows ではなく SET SECURITY などの OpenVMS コマンドを使用して，『HP OpenVMS システム・セキュリティ・ガイド』の推奨事項に従って，付与するアクセス数の多い ACE が少ないものよりリストの上位に置かれるように管理理者がオブジェクトのセキュリティを管理する必要がある場合があります。 Windows システムからアクセス許可を設定した場合に同じ結果が得られるように，管理者は，上から下へ表示したときにエントリがアクセス数の多いものから少ないものの順に並ぶように管理しなければなりません。 このようにするために，既存のすべてのエントリを削除して，新しいエントリをリストに追加する際に再度追加する必要があるかも知れません。

10.4.2 継承されない OpenVMS ACE に関する制限事項 (ファイルのみ)

ファイルの ACL が明示的かつ単独に (親ディレクトリで OPTIONS=DEFAULT ACE から継承されたのではなく) 追加された OpenVMS 固有の ACE (Audit，Alarm，Protected あるいは Hidden ACE など) を含む場合，このファイルが変更されると HP CIFS Server はこれらの OpenVMS 固有の ACE を残しません。この制限事項はディレクトリ・ファイルには適用されません。

たとえば，対応する継承可能な ACE を親ディレクトリに設定せずに，単一のファイルに対して明示的に Audit ACE を設定した場合を考えます。ユーザがこのファイルを変更した場合，このファイルに対して明示的に設定された Audit ACE は，ファイルをクローズしたときに失われる場合があります。 この状況は，Microsoft Office アプリケーションを使用してファイルを変更した場合に特に発生します。このようなファイルで OpenVMS 固有の ACE が失われる可能性を排除するために，ディレクトリ内で作成された新しいファイルに OpenVMS 固有 ACE が適用されるように， 継承可能な OPTIONS=DEFAULT ACE を親ディレクトリに適用します。ただし，この設定では，その ACE はそのディレクトリで作成されるすべての新しいファイルに適用されます。

10.4.3 組み込み管理者グループの制限事項

HP CIFS V1.1 ECO1 よりも前のバージョンでは，組み込みローカル Administrators グループのすべてのメンバーに 2 つの特別な OpenVMS 特権，BYPASS および SYSPRV が付与されました。これによりローカルの管理者は，ファイルのセキュリティ管理という本来の目的ために Windows クライアントからすべての共有のすべてのファイルにアクセスすることが可能でした。ただしこの動作は，明示的に許可されているリソースにのみ管理者がアクセスできるという Windows の標準の動作とは矛盾します。

本バージョンでは，Administrators グループのメンバーに BYPASS および SYSPRV 特権は付与されません。この結果，ローカルの Administrators グループのメンバーは引き続きその他の管理業務は行えますが，権限を付与されるまではファイルおよびフォルダのセキュリティを設定することはできません。特権の設定に必要なアクセス許可については，10.5 項を参照してください。

10.4.4 Windows の継承値のマッピングに関する制限事項

Windows システムからディレクトリのアクセス許可を設定する場合，Windows はアクセス許可の伝搬を制御するための複数のオプションを提供します。HP CIFS Server は，サブフォルダのみのオプションだけでなく，ファイルのみのオプションもサポートしません。HP CIFS Server が他のオプションを処理する方法については，表 10-2を参照してください。

10.4.5 Windows の特別なアクセス許可に関する制限事項

HP CIFS Server は，Windows の特別なアクセス許可 Delete Subfolders and Files をサポートしません。このオプションを設定すると，アクセス拒否エラーが発生する場合があります。

10.4.6 ディレクトリあるいは共有に対するアクセス許可を表示する際の制限事項

Windows システムからディレクトリあるいは共有のアクセス許可を表示する場合，「**Security**」ダイアログ・ボックスに表示されるアクセス許可はそのオブジェクトに設定されているアクセス許可が正しく反映されていない場合があるため，「**Advanced Security Settings**」ウィンドウを使用する必要があります。 この制限事項はファイルには適用されません。

Security プロパティ・ ダイアログ・ウィンドウで「**Advanced**」 ボタンをクリックして，「**Advanced Security Settings**」ウィンドウをオープンします。

10.5 ファイル・セキュリティの設定に必要なアクセス許可と特権

Windows からファイル・セキュリティを設定するには，そのユーザは一定のアクセス許可あるいは特権を持っている必要があります。この項では，これらのアクセス許可および特権について説明します。

10.5.1 Windows からのファイルに対する管理者アクセスの提供

管理者は，以下のいずれか 1 つの条件に当てはならない限り，Windows システムからファイル・アクセス許可を設定することはできません。

- そのファイルへのアクセスが許可されているローカルの Administrators グループにメンバーとして属している。 このローカルの Administrators グループは HP CIFS Server により作成され，OpenVMS リソース識別子 CIFS$ADMINISTRATORS にマッピングされる。 Grant the CIFS$ADMINISTRATORS 識別子に対し，少なくともそのディレクトリおよびファイルに対して読み取りアクセスが付与されている。この方法により，ファイルごとにアクセスが制御されます。
- admin user 構成パラメータにそのユーザがリストされている。 この方法は，共有ごと，すなわちすべての共有か個々の共有のどちらかで実現され，その共有内のすべてのファイルに適用される (詳しくは後述します)。
- OpenVMS アカウントがマッピングされたユーザが，BYPASS，GRPPRV，READALL，あるいは SYSPRV などの OpenVMS の特別なデフォルト特権を持っている。この場合，アクセスはそのユーザがアクセスするすべての共有のすべてのファイルに適用される。

10.5.2 admin user 構成パラメータ

サーバー・ワイドあるいは共有ごとのどちらかでユーザに Administrator アクセスを与えるための別の方法として，構成ファイル・パラメータ *admin users* を使用する方法があります。*admin users* は共有レベルのパラメータで，リストされたユーザに対してフルアクセス権を与えるために個々の共有セクションで指定される一方，すべての共有のすべてのファイルに対してフルアクセスを与えるとともにそのユーザがユーザ，グループ，共有を管理できるように完全な管理者権限を与えるためには [global] セクションで指定されます。

注記: このパラメータにリストされているユーザあるいはグループの構文は，そのサーバーの役割に依存します。あるドメイン内のメンバーサーバーの場合，そのドメインの名前がユーザ名あるいはグループ名の一部として含まれていなければなりません。サーバーの役割がそれ以外の場合は，ユーザあるいはグループが，信頼されているドメインからのものである場合のみ，ドメイン名が必要になります。

たとえば，OPERS ドメインを信頼する CORPDOM ドメイン内のメンバーサーバーで，ローカル・ユーザ CIFSADMIN，CORPDOM ドメインのユーザの ANITA，および OPERS グループの "Domain Admins" を PROJECTS 共有の管理者として指定したい場合，HP CIFS Server 構成ファイルの [PROJECTS] セクションに次のような行を追加します。

```
admin users = CIFSADMIN, CORPDOM\ANITA, OPERS\"DOMAIN ADMINS"
```

10.5.3 Windows の Change Permissions および Take Ownership アクセス許可

Windows の Change Permissions アクセス許可と Take Ownership アクセス許可は，どちらも OpenVMS の Control アクセスにマッピングされます。このため，Change Permissions あるいは Take Ownership のどちらかが付与されたユーザは，アクセス許可の変更と所有権の取得が可能です。

10.6 ファイルのセキュリティ

この項では，Windows システムあるいは OpenVMS システムからファイルのアクセス許可を設定する手順の概要を説明します。例に上げるユーザおよびグループ・アカウントがシステムに存在するものと仮定して説明します。

10.6.1 Windows システムからのファイル・セキュリティの変更

Windows 2003 システムからファイル・アクセス許可の表示および管理を行うには，以下のガイドラインに従います (他のバージョンの Windows システムでは手順が多少異なります)。

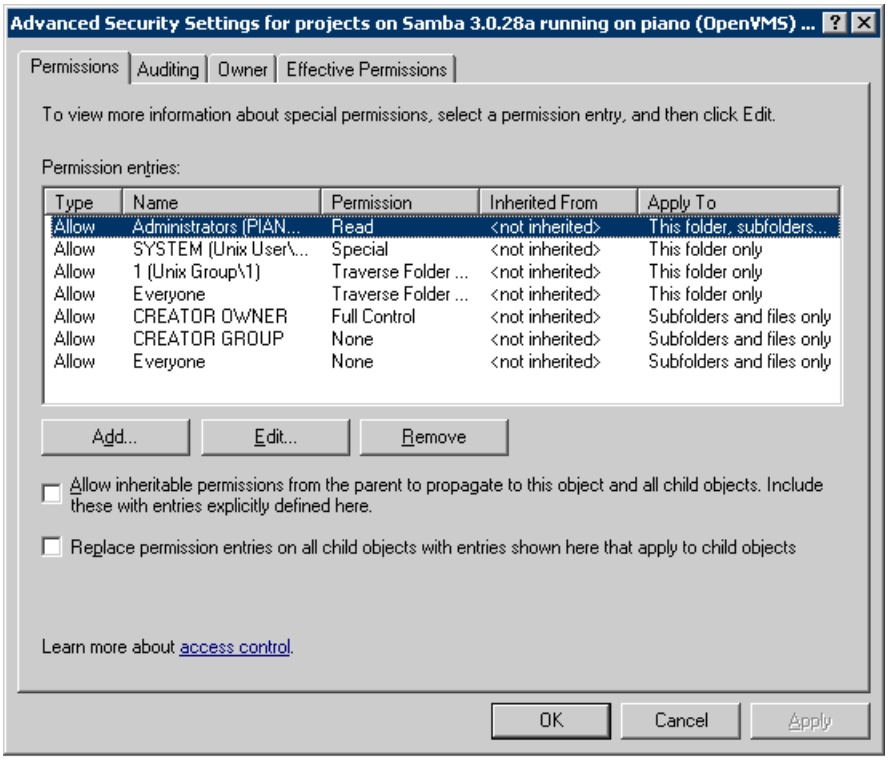
10.6.1.1 既存のアクセス許可の表示

オブジェクトに対するアクセス許可の既存の設定を表示するには，以下の手順に従います。

1. 接続を確立します。

   オブジェクトの変更アクセス許可を変更する権限を持つユーザとして認識されている HP CIFS Server に接続します。 たとえば，その HP CIFS Server で管理者特権を持つユーザとしてドメインにログインしている場合，「Start」から「Run」をクリックしてサーバー名を入力します。 利用できる共有ディレクトリの一覧が表示されます。 ただし，その HP CIFS Server で管理者特権を持つユーザとしてドメインにログインしていない場合，Connect As 機能を使用して管理者アクセス許可を持つユーザを指定して HP CIFS Server に対する新しいセッションを確立します。その後，「Start」から「Run」をクリックして，共有フォルダの一覧を取得するために サーバー名を入力します。
2. フォルダを選択するか，目的のフォルダまで移動してフォルダまたはファイルを選択します。
3. オブジェクトで右クリックし，「**Properties**」を選択します。
4. 「**Properties**」ウィンドウで「Security」タブを選択します。
5. 「**Security**」ウィンドウで「**Advanced**」ボタンをクリックして「**Advanced Security Settings**」ウィンドウをオープンします。

図 10-1 Advanced Security Settings ウィンドウ



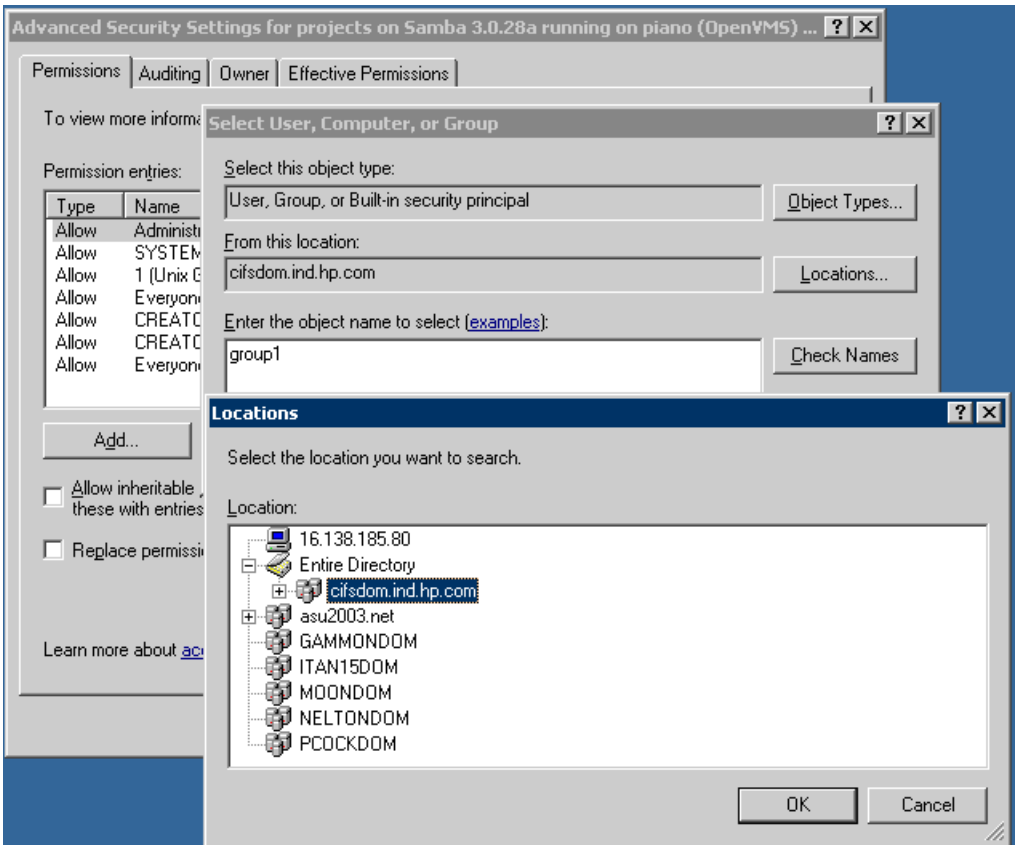
10.6.1.2 アクセス許可の管理

以下の手順で，ディレクトリ/フォルダのアクセス許可の設定および管理を行います。

アクセス許可の追加

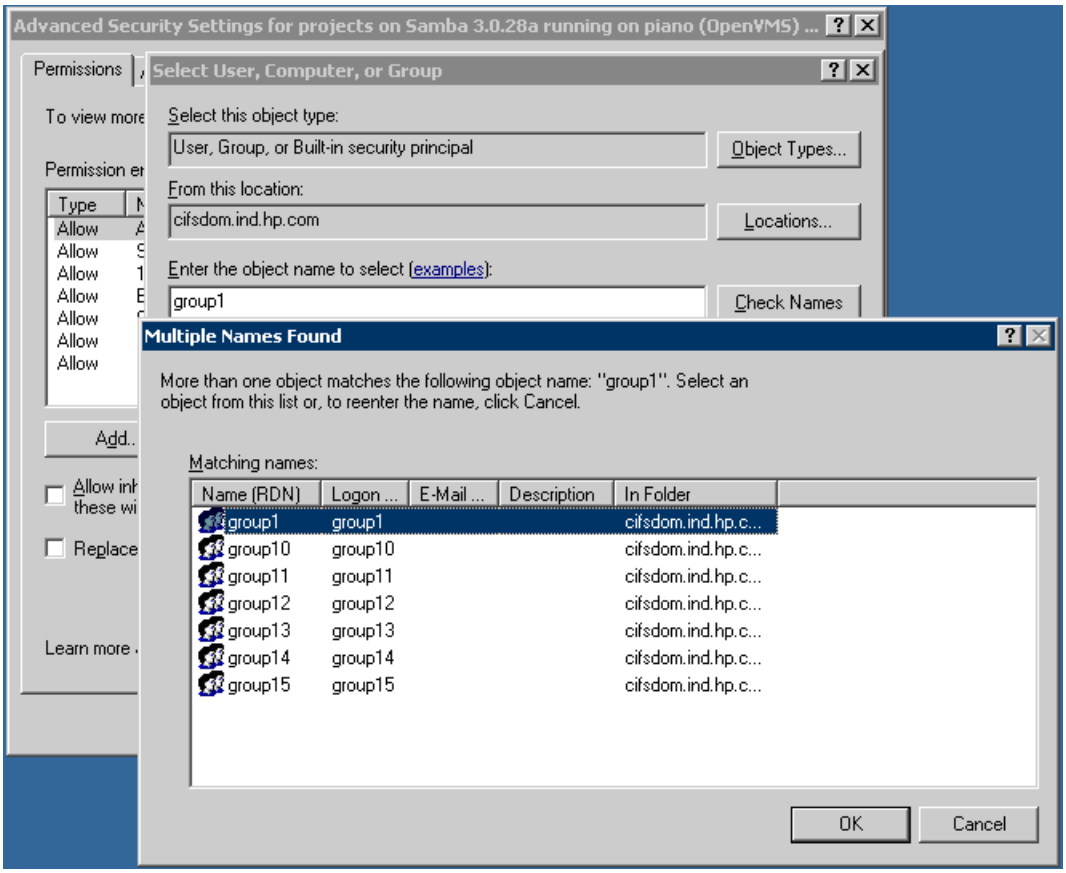
1. **Add** ボタンを追加して「**Select User, Computer, or Group**」ダイアログ・ボックスを表示します。
2. 必要であれば，「**Locations**」ボタンをクリックし， 適切なアカウントの場所を選択します。

図 10-2 アクセス許可の追加



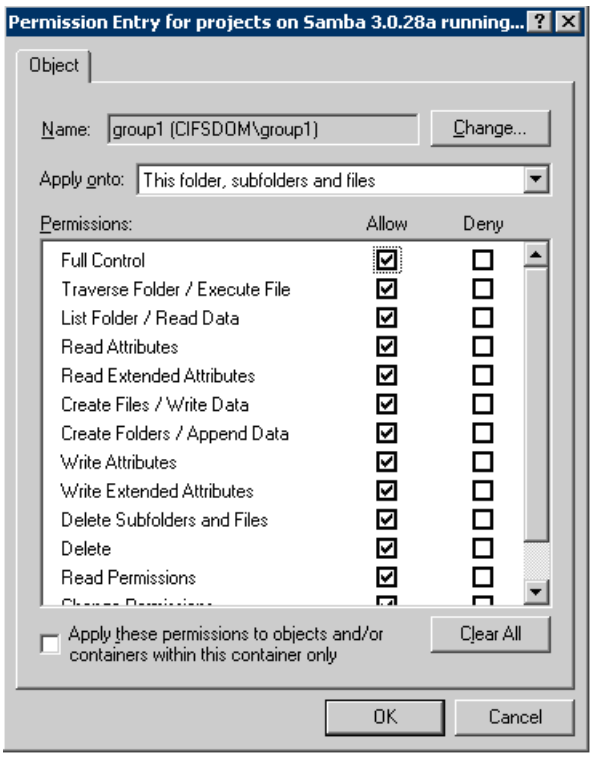
3. 「**Enter the object name to select**」のセクションにユーザあるいはグループ名を指定して，「**Check Names**」ボタンをクリックします。
4. 「**Multiple Names Found** 」ウィンドウが表示されたら，ユーザあるいはグループを選択して，「**OK**」をクリックして「**Select User, Computer, or Group**」ダイアログ・ボックスに戻ります。

図 10-3 ユーザあるいはグループの選択



5. 「**OK**」をクリックします。 Windows はそのオブジェクトに対する 「Permission Entry」ウィンドウを表示します。 必要な Allow アクセス許可を選択します。

図 10-4 アクセス許可



6. フォルダを選択した場合，適切であれば「Apply these permissions to objects and/or containers within this container only」 オプションを選択します。
7. 「**OK**」をクリックして「Advanced Security Settings」 ウィンドウへ戻ります。
8. 変更をすぐに保管してアクセス許可の変更を続けるには，「Apply」 をクリックします。そうでない場合は，「OK」 をクリックして「Properties」 ダイアログボックスへ戻り，操作を確定します。
9. 「**OK**」をクリックし「Properties」ウィンドウを終了させます。

既存のアクセス許可の変更

1. 「Advanced Security Settings」ウィンドウにあるアクセス許可エントリ・リストからエントリを選択し，「Edit」 をクリックします。
2. オブジェクトに対して表示される「permission Entry」 ウィンドウから，目的とするアクセス許可に変更します。
3. そのオブジェクトがフォルダの場合，それが適切であれば「Apply these permissions to objects and/or containers within this container only」 オプションを選択します。
4. 「**OK**」をクリックして「Advanced Security Settings」 ウィンドウへ戻ります。
5. 「**Apply**」をクリックして変更をすぐに保管し，アクセス許可の変更を続けます。そうでない場合は，「**OK**」 をクリックして「Properties」 ダイアログボックスに戻り，操作を確定します。
6. 「**Properties**」 ウィンドウで「**OK**」をクリックし，終了します。

アクセス許可の削除

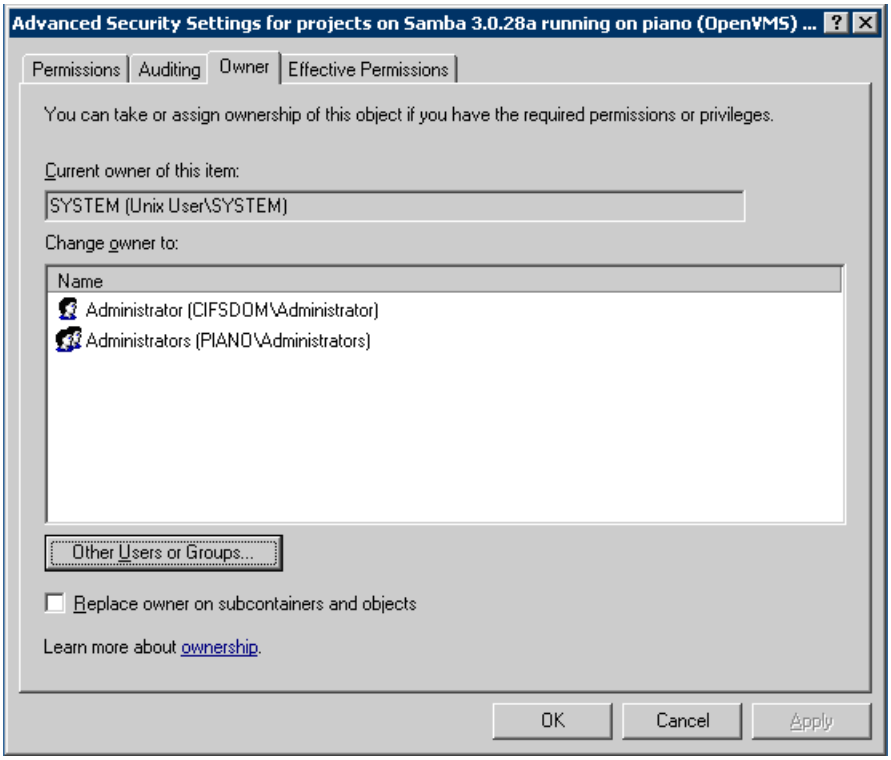
1. リストからエントリを選択し，「Remove」 ボタンをクリックします。
2. 「**Apply**」をクリックして変更をすぐに保管し，アクセス許可の変更を続けます。そうでない場合は，「**OK**」 をクリックして「Properties」 ダイアログボックスに戻り，操作を確定します。
3. 「**Properties**」 ウィンドウで「**OK**」をクリックし，終了します。

10.6.2 所有権の取得と割り当て

場合によっては，オブジェクトの所有者の変更が必要になる場合があります。 デフォルトでは，オブジェクトに対する Take Ownership 特権を持つ非管理者ユーザが，そのオブジェクトの所有者として割り当てることができるのは自分自身のみです。 管理者とバックアップ・オペレータは，他のユーザおよびグループに対して所有権を割り当てることができます。Windows 2003 システムからオブジェクトの所有権を割り当てるには，以下の手順で行います (この手順は使用する Windows のバージョンによってわずかに異なります)。

1. オブジェクト上で右クリックし，「**Properties**」 を選択します。
2. 「**Properties**」 ウィンドウから，「**Security**」 タブを選択します。
3. 「**Advanced**」 ボタンをクリックします。
4. 「**Owner**」タブを選択します。

図 10-5 Owner タブ



5. 「**Change owner to**」セクションにユーザあるいはグループの名前がリストされている場合は，ユーザを選択します。リストされない場合，「**Other Users or Groups**」ボタンをクリックして名前を指定し，「**OK**」をクリックします。
6. 「**Multiple Names Found**」ウィンドウが表示されたら，リストから名前を選択し，「**OK**をクリックします。
7. 「**Apply**」をクリックして変更内容をすぐに保管します。
8. 「**OK**」をクリックして「**Properties**」ウィンドウへ戻ります。
9. 「**OK**」をクリックして終了します。

10.6.3 OpenVMS ホストからのファイル・セキュリティの変更

この項では，OpenVMS ホストからファイル・セキュリティを設定する方法について簡単に説明します。

1. アクセスを認める OpenVMS アカウントあるいはリソース識別子の名前を確認します。マップピングされた OpenVMS アカウントあるいはリソース識別子がわからない場合は，WBINFO を使用して，ドメイン名と アクセス許可を付与する Windows アカウント名あるいはグループ名を指定します。アカウントあるいはグループが CIFS サーバーにローカルに存在する場合，ドメイン名は無視します (後述の注意を参照)。

   たとえば，CORPDOM ドメインの ACCTNG グループにマッピングされた OpenVMS リソース識別子の名前を確認するには，次のコマンドを実行します。

```
$ @SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS
$ WBINFO --DOMAINNAME-TO-HOSTNAME=CORPDOM\ACCTNG
```

注記:

- WBINFO ユーティリティの実行には SYSPRV 特権が必要です。
- ユーザあるいはグループが HP CIFS Server のローカル・データベースに存在する場合，Administrators，Domain Admins などの BUILTIN グループを除き，ドメイン名は無視されます。組み込みグループを指定するには，グループ名の前に BUILTIN\ を付けます。たとえば，Administrators グループにマッピングされた OpenVMS リソース識別子の名前を確認するには，次のコマンドを実行します。

```
$ WBINFO --DOMAINNAME-TO-HOSTNAME=BUILTIN\ADMINISTRATORS
```

2. OpenVMS アカウントあるいはリソース識別子の名前が認識できたら，DCL コマンド SET SECURITY を使用してオブジェクトのセキュリティを変更します。オブジェクトへのアクセスの管理と SET SECURITY コマンドについての詳細は，『HP OpenVMS システム・セキュリティ・ガイド』 および DCL のマニュアルを参照してください。

10.7 重要なデータベース・ファイル

デフォルトでは，HP CIFS Server はサーバー・データをいくつかのデータベース・ファイルに保管します。これらのファイルのいくつかは失うとセキュリティ上深刻な事態になるので，定期的にバックアップを取っておくことが必要です。ファイルが正しくリストアできるように，バックアップの際はそれらのデータベースをオープンすべきではありません。このため，バックアップ時には HP CIFS Server をシャットダウンする必要があります。複数のクラスタ・メンバーが同じ SAMBA$ROOT: ディレクトリ・ツリーを共有する場合，データベース・ファイルも共有します。 このため，バックアップ時には，関連するすべてのクラスタ・メンバーで HP CIFS Server をシャットダウンする必要があります。表 10-7 に，これらのデータベース・ファイルの名前，デフォルトの場所，目的を示します。

表 10-7 重要なデータベース・ファイル

名前	場所	目的
WINBINDD_IDMAP.TDB	SAMBA$ROOT:[VAR.LOCKS]	WINBIND 自動マッピング機能が有効な場合に使用します。ドメイン SID を idmap UID/GID 値に割り当てます。
GROUP_MAPPING.TDB	SAMBA$ROOT:[VAR.LOCKS]	グループ・アカウント，それらのメンバー，および OpenVMS リソース識別子のマッピングを保管します。
PASSDB.TDB	SAMBA$ROOT:[PRIVATE]	ユーザ・アカウントおよびマシン・アカウントを保管します (PDBEDIT で作成されます)。
SECRETS.TDB	SAMBA$ROOT:[PRIVATE]	マシン・アカウント・パスワード，信頼アカウント・パスワード， ldap admin 識別名およびパスワードなど，安全のために残さなければならない情報を保管します。
ACCOUNT_POLICY.TDB	SAMBA$ROOT:[VAR.LOCKS]	最大パスワード期限，最短パスワード長，パスワード履歴などの，アカウント・ポリシーの設定を保管します。
SHARE_INFO.TDB	SAMBA$ROOT:[VAR.LOCKS]	共有 ACL を保管します (共有レベルのアクセス許可)。
NTDRIVERS.TDB	SAMBA$ROOT:[VAR.LOCKS]	インストールされているプリンタ・ドライバの情報を保管します。

表 10-7 重要なデータベース・ファイル (続き)

名前	場所	目的
NTFORMS.TDB	SAMBA$ROOT:[VAR.LOCKS]	インストールされているプリンタ・フォームの情報を保管します。
NTPRINTERS.TDB	SAMBA$ROOT:[VAR.LOCKS]	プリンタのアクセス許可など，インストール済のプリンタについての情報を保管します。

10.8 プリント・セキュリティ

プリンタのセキュリティを提供するために，Windows セキュリティと OpenVMS セキュリティの両方が使用されます。

プリンタのセキュリティを制御するのに Windows のアクセス許可を使用すると，Windows クライアントにプリンタが接続されたときに，サーバーに保管されたプリンタ・ドライバ・ファイルを自動的にダウンロードできるようにしておく場合に便利です。 Windows のアクセス許可がプリンタに適用された場合，それらのアクセス許可はデータベース・ファイル SAMBA$ROOT:[VAR.LOCKS]NTPRINTERS.TDB に保管されます。プリント・キューに設定された OpenVMS セキュリティには影響を与えません。

注記: Windows 形式のプリンタ・セキュリティを確立する場合は，あらかじめサーバーにプリント・ドライバをアップロードしておく必要があります。

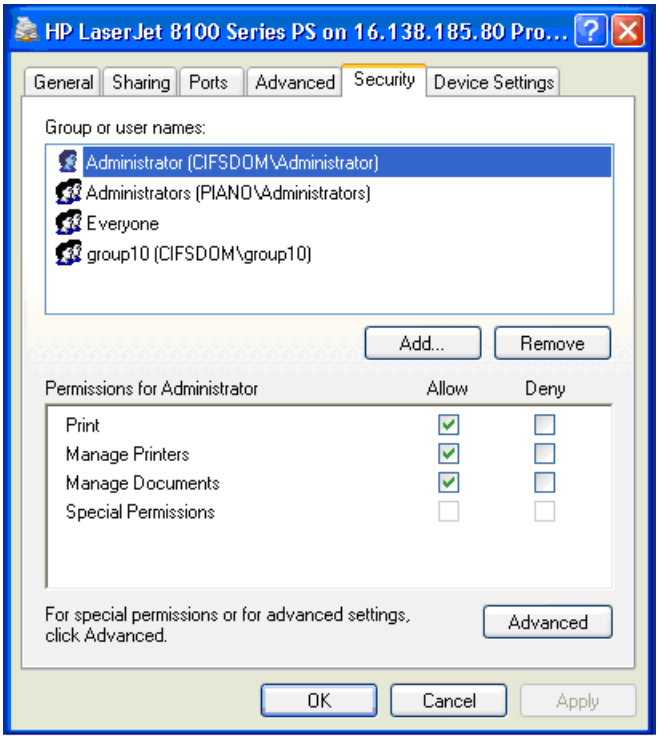
OpenVMS プリント・キューにおけるアクセス制御は，OpenVMS セキュリティを単独で，あるいは WIndows セキュリティを組み合わせて行なわれます。 この方法によるセキュリティ設定は，HP CIFS Server のプリント共有を Windows クライアント上のローカル・プリンタとして構成する場合に便利です。

10.8.1 Windows 形式のプリンタ・セキュリティの設定

Windows 形式のプリンタ・セキュリティを設定する手順は，以下のとおりです。

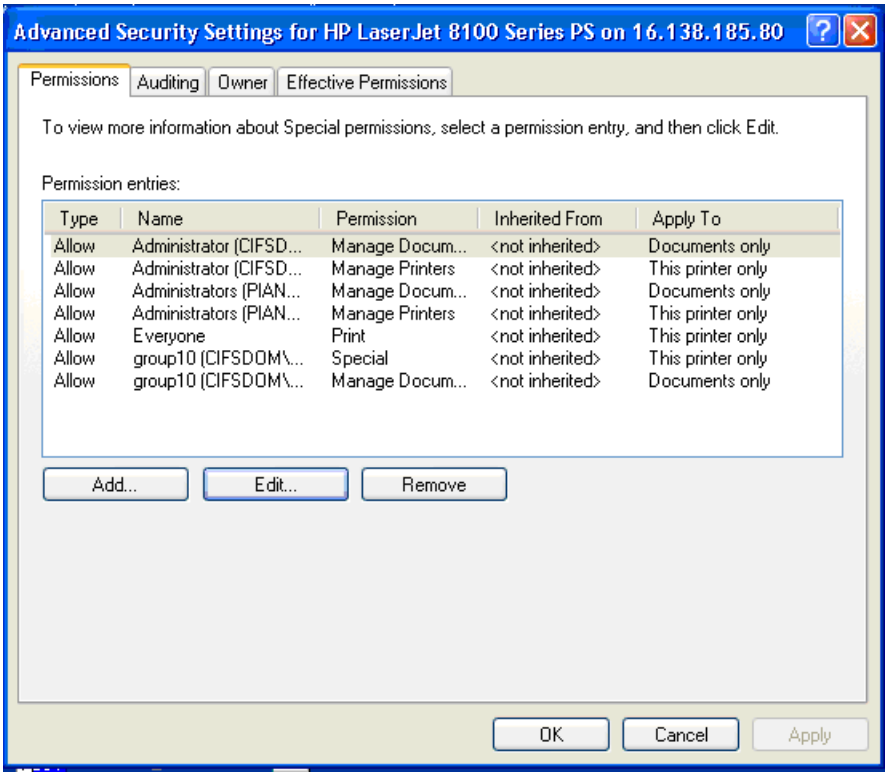
1. プリンタ・セキュリティを変更するための特権を持つアカウントを使用して HP CIFS Server にアクセスします。
2. 「**Printers and Faxes**」 フォルダをオープンします。
3. プリンタ上で右クリックし，「**Properties**」を選択します。
4. 「**Printer Properties**」ダイアログ・ボックスから，「**Security**」 タブを選択します。

図 10-6 Security タブ



5. 「**Advanced**」ボタンをクリックして，「**Advanced Security Settings**」ダイアログ・ボックスを表示させます。このダイアログ・ボックスにより，アクセス許可の追加，変更(編集)，あるいは削除が可能です。

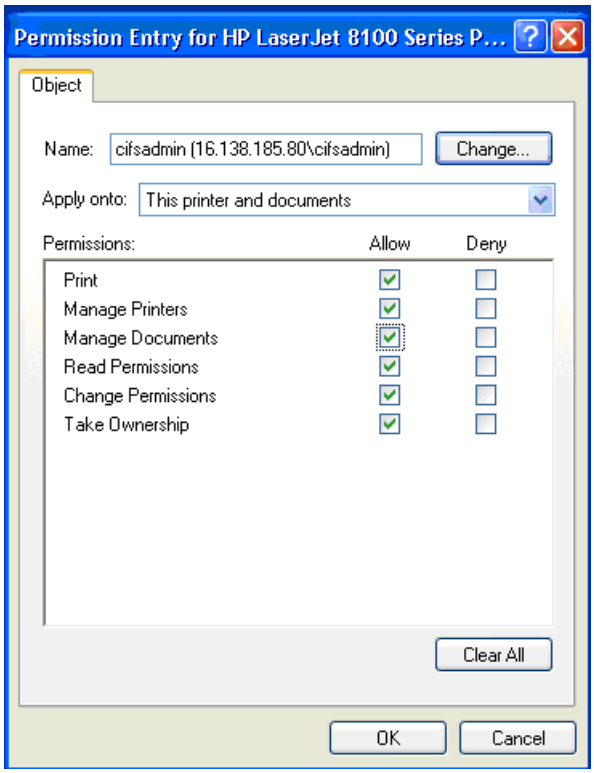
図 10-7 Permissions タブ



アクセス許可の追加

1. アクセス許可を追加するには，「**Add...**」 ボタンをクリックして「**Select User or Group**」ダイアログ・ボックスを表示させます。必要であれば，適切なアカウントの場所を選択します。
2. 「**Enter the object name to select**」 ボックスでユーザ名あるいはグループ名を入力して，「**Check Names**」 ボタンをクリックします。
3. 複数の名前がある場合は，必要な名前を選択し，「**OK**」をクリックします。
4. 「**Select Users, Computers, and Groups**」ダイアログ・ボックスで「**OK**」をクリックし，オブジェクトの「**Permission Entry**」ダイアログ・ボックスを表示させます。

図 10-8 プリンタのアクセス許可



5. 必要なアクセス許可を選択します。
6. 「**Apply onto:**」ドロップダウン・リストから目的のエントリを選択し，「**OK**」をクリックします。
7. 「**Advanced Security Settings**」ダイアログ・ボックスで「**OK**」あるいは「**Apply**」をクリックします。

アクセス許可の変更

1. ユーザあるいはグループ・アカウントを選択して 「**Edit...**」 ボタンをクリックし，「**Permission Entry**」 ダイアログ・ボックスを表示させます。
2. アクセス許可の変更
3. 「**Apply onto:**」ドロップダウン・リストから目的のエントリを選択し，「**OK**」をクリックします。
4. 「**Advanced Security Settings**」ダイアログ・ボックスで「**OK**」あるいは「**Apply**」をクリックします。

アクセス許可の削除

- アクセス許可を削除するには，ユーザあるいはグループ・アカウントを選択して「**Remove**」をクリックし，「**Apply**」 をクリックします。

6. 「**OK**」をクリックして「**Advanced Security Setting**」ダイアログ・ボックスでの操作を終了します。

7. 「**OK**」をクリックして，そのプリンタ共有の「**Properties**」ダイアログ・ボックスでの操作を終了します。

10.8.2 OpenVMS プリント・キュー・セキュリティ

プリンタのアクセス制御には OpenVMS セキュリティが使用できます。ただし，Windows のユーザおよびグループ名ではなく，それらにマッピングされ，アクセス権が付与された，OpenVMS アカウントおよびリソース識別子名を使用してセキュリティが設定されます。

マップピングされた OpenVMS アカウントあるいはリソース識別子がわからない場合は，WBINFO を使用して，ドメイン名と アクセス許可を付与する Windows アカウント名あるいはグループ名を指定します。アカウントあるいはグループが CIFS サーバーにローカルに存在する場合，ドメイン名は無視します (下記の注意を参照). たとえば，CORPDOM ドメインの ACCTNG グループにマッピングされた OpenVMS リソース識別子の名前を確認するには，次のコマンドを実行します。

```
$ @SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS
$ WBINFO --DOMAINNAME-TO-HOSTNAME=CORPDOM\ACCTNG
```

注記:

- WBINFO ユーティリティの実行には SYSPRV 特権が必要です。
- ユーザあるいはグループが HP CIFS Server のローカル・データベースに存在する場合，Administrators，Users などの BUILTIN グループを除き，ドメイン名は無視されます。組み込みグループを指定するには，グループ名の前に BUILTIN\ を付けます。たとえば，Administrators グループにマッピングされた OpenVMS リソース識別子の名前を確認するには，次のコマンドを実行します。

  ```
  $ WBINFO --DOMAINNAME-TO-HOSTNAME=BUILTIN\ADMINISTRATORS
  ```

OpenVMS アカウントあるいはリソース識別子の名前が認識できたら，DCL コマンド SET SECURITY を使用して適切なプリント・キューのセキュリティを変更します。オブジェクトへのアクセスの管理と SET SECURITY コマンドについての詳細は，『HP OpenVMS システム・セキュリティ・ガイド』 および 『HP OpenVMS DCL ディクショナリ』 を参照してください。

第11章　管理ツールのコマンド・リファレンス

この章では，pdbedit や smbclient などの多くの Samba ユーティリティも含め，OpenVMS CIFS に含まれている管理ツールについて説明します。 SMBSHOW などのツールは, HP OpenVMS CIFS 固有のツールです。 Samba ユーティリティについての詳細は下記の Samba の web サイトを参照してください。

http://samba.org

この章では次の内容について説明しています。

- 11.1 項「HP CIFS 管理ツール」
- 11.2 項「ODS-2 から ODS-5 へのエンコードされたファイル名の変換」
- 11.3 項「VAR あるいは VFC ファイルのヒント値のアップデート」

11.1 HP CIFS 管理ツール

HP CIFS の管理のために，多数の HP CIFS Server ツールが用意されています。 ここでは以下の HP CIFS 管理ツールについて説明します。

smbpasswd
HP CIFS の暗号化されたパスワードデータベースの管理用ツールです。 smbpasswd コマンドを使用してユーザ・アカウント・パスワードを変更する方法については，8.2.3 項「ユーザ・アカウント・パスワードの変更」 を参照してください。

pdbedit
SAM データベース (Samba ユーザアカウントのデータベース) の管理用ツールです。 pdbedit ユーティリティを使用してユーザを管理する方法については， 8.2.2 項「pdbedit ユーティリティによるユーザの管理」 を参照してください。

net
HP CIFS とリモート CIFS サーバーの管理用ツールです。

wbinfo
winbind 情報を取得するためのツールです。

smbclient
サーバー上の SMB/CIFS リソースにアクセスするための FTP に似たクライアントです。

smbstatus
HP CIFS Server への現在の接続についての情報にアクセスするためのツールです。

nmblookup
OpenVMS ホストから NetBIOS 名を問い合わせるためのツールです。

smbshow
実行中のすべての HP CIFS Server プロセスについての情報を入手するためのツールです。

smbversion
HP CISF Server の一部として使用されている種々のイメージについての情報を入手するためのツールです。

SAMBA$DEFINE_COMMANDS.COM
すべての HP CIFS ユーティリティのためのシンボルを定義するためのコマンド・プロシージャです。

SAMBA$GATHER_INFO.COM
情報およびデータ・ファイルを収集するためのツールです。

testparm
testparm ユーティリティは，SMB.CONF ファイルの内容が正しいかどうか評価するための重要なツールです。

tdbbackup
samba.tdb ファイルのバックアップを取り，整合性を確認するためのツールです。

tdbdump
TDB ファイルの内容を出力するためのツールです。

smbcontrol
smbd あるいは nmbd プロセスにメッセージを送信するためのツールです。

delete_ace
HP CIFS Server APPLICATION ACE とともに，PATHWORKS および Advanced Server の ACE を削除するためのツールです。

tdb_convert
CONVERT.FDL ファイルを使用して永続的な TBD ファイルを変換するためのツールです。

ods2_convert
ファイル名からエスケープでエンコードされた文字を取り除き，ファイル名を ISO-8859-1 文字に変更します。

SAMBA$CONFIG.COM
HP CIFS Server を様々な役割に構成するためのツールです。 このユーティリティの使用方法については，第2章「HP CIFS Server のインストールおよび構成」を参照してください。

SAMBA$MANAGE_CIFS.COM
HP CIFS Server で共有，ユーザ，グループ，アカウント・ポリシー，および信頼を管理するためのツールです。 このユーティリティの使用方法の詳細については 第8章「ユーザ，グループ，アカウント・ポリシー，信頼関係の管理」 および 第9章 「共有の管理」 を参照してください。

SAMBA$UPDATEFILEHINTVALUE.COM
ファイルの ODS-5 ファイル・ヘッダに保管されているファイル長ヒント値を Variable Length あるいは VFC レコード形式でアップデートするためのツールです。

これらの管理ツールは SAMBA$ROOT:[BIN] ディレクトリで提供されており，次のコマンドの実行により定義されます。

```
@SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS
```

11.1.1 net

このツールは，CIFS とリモート CIFS サーバーの管理のために使用します。CIFS の `net` ユーティリティには，Windows や DOS の `net` ユーティリティと同様の機能があります。`net` ユーティリティの最初の引き数は，`net` コマンドを実行するときに使われるプロトコルを指定するために使用します。引き数は，ADS，RAP，RPC のいずれかです。ADS は Windows Active Directory で使用し，RAP は旧 Windows クライアント (Win9x/NT3) で使用し，RPC は DCE-RPC で使用します。

SMB.CONF の `passdb backend` パラメータに `ldapsam:ldap://<LDAP server name>` を設定した場合には，`net` ツールの操作対象は LDAP ディレクトリになります。

多くの `net` コマンドがあります。この項では，利用できるコマンドの一部について説明します。ここでは，CIFS ユーザアカウントの管理で使用することができる `net rpc user` コマンドの構文だけを説明します。

net コマンドの使用方法と構文の詳細な説明については，SWAT の `net` のヘルプ，または『The Official Samba HOWTO and Reference Guide』を参照してください。

11.1.1.1 net コマンド

以下に，`net` コマンドについて，一部を説明します。

特定のコマンドとその構文についての詳細は，`net help <command_option>` を使用してください。

`net time`
時刻情報を表示/設定します。

`net lookup`
指定したホストの IP アドレスまたはホスト名を検索します。

`net cache`
TDB (Trivial Database) ファイルのキャッシュを操作します。

`net changesecretpw`
このコマンドを使用すると，CIFS マシンアカウントのパスワードに，外部アプリケーションを使って，Windows Active Directory に存在しているマシンアカウントのパスワードを設定できます。必要がない場合は，このコマンドは使用しないでください。このコマンドでは，強制フラグ (`-f`) を指定する必要があります。コマンドからはプロンプトは表示されません。stdin から入力した情報が，そのまま文字どおりにマシンパスワードとして格納されます。このコマンドは有効なマシンパスワードを警告なしに上書きするので，十分注意して使用してください。

`net status`
ローカルサーバーのマシンアカウントのステータスを表示します。

11.1.1.2 net lookup の構文

このセクションでは `net lookup` コマンドの構文のみ示します。

net lookup [*<host>*] HOSTNAME[*#<type>*]	指定したホスト名およびタイプの IP アドレスを検索します。
net lookup ldap [*<domain>*]	指定したドメインの LDAP サーバーの IP アドレスを提示します。
net lookup kdc [*<realm>*]	指定したレルムの KDC の IP アドレスを提示します。
net lookup dc [*<domain>*]	指定したドメインのドメインコントローラの IP アドレスを提示します。
net lookup master [*<domain|workgroup>*]	指定したドメインあるいはワークグループのマスターブラウザの IP アドレスを提示します。

net lookup name [*<name>*]	SID(およびアカウント・タイプ)を表示します。
net lookup sid [*<sid>*]	SID の名前とタイプを提示します。

11.1.1.2.1 実行例

指定したドメインのドメインコントローラの IP アドレスを調べるには，次のコマンドを実行します。

```
$ net lookup dc cifsdom
```

sydney という名前のグループアカウントの SID とアカウント・タイプをリストするには，次のコマンドを実行します。

```
$ net lookup name sydney
```

11.1.2 wbinfo

winbind 情報の入手には wbinfo ツールを使用します。

wbinfo ユーティリティは，ユーザ名，グループ名，あるいは，ドメイン・ユーザ/グループ名と OpenVMS ユーザ/リソース識別子名との間のマッピングなどの，詳細なドメイン情報を取得するのに使用できます。

11.1.2.1 構文

wbinfo [*option*]

option の部分には，以下のオプションを指定することができます。

-u, --domain-users	すべてのドメインユーザをリストします。
-g, --domain-groups	すべてのドメイングループをリストします。
-h, --domainname-to-hostname=NAME	ドメイン名をホスト名に変換します。
-H, --hostname-to-domainname=HOSTNAME	ホスト名をドメイン名にマップします。
-o, --hostgroups-to-domaingroups	すべての CIFS ホストグループをドメイングループにマップします。
-O, --hostusers-to-domainusers	すべての CIFS ホストユーザをドメインユーザにマップします。
-D, --domain-info=STRING	ドメインについての情報を表示します。
-r, --user-groups=USER	ユーザグループを取得します。
--user-domgroups=SID	ユーザドメイングループを取得します。
-a, --authenticate=user%password	ユーザを認証します。
--getdcname=domainname	外部ドメインの DC 名を取得します。
-p, --ping	WINBINDD が動作しているかどうか確認します。
-K, --krb5auth=user%password	Kerberos でユーザを認証します。

注記: **--hostusers-to-domainusers**，**--hostgroups-to-domaingroups** および **--hostname-to-domainname** の各オプションは，WINBIND が無効 (WIBINDD_DONT_ENV を 1 に定義することにより設定) かどうかには関係なく使用できます。残りのオプションは WINBIND が有効な場合のみ使用できます。

ヘルプ・オプション

-?, --help	ヘルプメッセージを表示します。
--usage	簡単な使用方法を表示します

共通の CIFS オプション

-V, --version	プログラムのバージョン番号を出力します。

このツールの使用方法の詳細については，/opt/samba/man/man1/wbinfo.1 を参照してください。

11.1.2.2 実行例

wbinfo -u コマンドを使ったときの出力例を，次に示します。

```
$ wbinfo -u
DOMAIN_DOM\johnb
DOMAIN_DOM\user1
DOMAIN_DOM\user2
DOMAIN_DOM\user3
DOMAIN_DOM\user4
DOMAIN_DOM\Guest
DOMAIN_DOM\user5
DOMAIN_DOM\ntuser
DOMAIN_DOM\root
DOMAIN_DOM\pcuser
DOMAIN_DOM\winusr
DOMAIN_DOM\maryw
```

wbinfo -g コマンドを使ったときの出力例を，次に示します。

```
$ wbinfo -g
DOMAIN_DOM\Domain Admins
DOMAIN_DOM\Domain Guests
DOMAIN_DOM\Domain Users
DOMAIN_DOM\Domain Computers
DOMAIN_DOM\Domain Controllers
DOMAIN_DOM\Schema Admins
DOMAIN_DOM\Enterprise Admins
DOMAIN_DOM\Cert Publishers
DOMAIN_DOM\Account Operators
DOMAIN_DOM\Print Operators
DOMAIN_DOM\Group Policy Creator Owners
```

WBINFO --domainname-to-hostname オプションの実行例

CIFS ドメイン・ユーザあるいはグループ・アカウントに対してマッピングされた OpenVMS ユーザ・アカウントあるいはリソース識別子名を見つけるには，次のコマンドを実行します。

```
wbinfo --domainname-to-hostname=<CIFS domain_account>
```

パラメータの意味は次のとおりです。

<CIFS domain_account> には，HP CIFS Server アカウント・データベースのユーザあるいはグループ・アカウント， HP CIFS Server がメンバーサーバーとなっているドメインのユーザあるいはグローバル・グループ・アカウント， あるいは HP CIFS Server の役割には関係なく信頼されたドメインのユーザあるいはグローバル・グループ・アカウントを指定します。

HP CIFS Server アカウント・データベースに存在するアカウントを除き， *<CIFS domain_account>* は <domain_name>\<account_name> の形式でなければなりません。

たとえば， CIFS Server がメンバーサーバーになっている CIFSDOM ドメインに存在するユーザ Administrator に対してマッピングされた OpenVMS ユーザ・アカウントを見つけるには，次のコマンドを実行します。

```
$ wbinfo --domainname-to-hostname=CIFSDOM\Administrator
CIFS$3E8
```

ユーザあるいはグループが HP CIFS Server のローカル・データベースに存在する場合，Administrators および Users などの BUILTIN グループを除き，ドメイン名は省略されます。 組み込みグループを指定するには，グループ名の前に BUILTIN\ を付けて指定します。

たとえば，Administrators グループにマッピングされている OpenVMS リソース識別子の名前を確認するには，次のコマンドを実行します。

```
$ wbinfo --domainname-to-hostname=BUILTIN\Administrators
CIFS$ADMINISTRATORS
```

WBINFO --hostusers-to-domainusers オプションの実行例

--hostusers-to-domainusers オプションは，次のように CIFS ドメイン・ユーザとそれにマップされている OpenVMS ユーザ名を表示します。

```
$ wbinfo --hostusers-to-domainusers
CIFSADMIN                                PIANO\cifsadmin
GANGA                                    PIANO\ganga
CIFS$3E8                                 CIFSDOM\Administrator

3 VMS users are currently mapped to CIFS domain users
```

WBINFO --hostgroups-to-domaingroups オプションの実行例

--hostgroups-to-domaingroups オプションは，CIFS ドメイン・グループとそれらがマップされている OpenVMS リソース識別子を表示します。

```
$ wbinfo --hostgroups-to-domaingroups
CIFSUSERS                                PIANO\cifsusers
PLAYERS                                  PIANO\players
CIFS$GRP1388                             CIFSDOM\Domain Users
CIFS$GRP1389                             CIFSDOM\Enterprise Admins
CIFS$GRP138A                             CIFSDOM\Domain Admins
CIFS$GRP138B                             CIFSDOM\Group Policy Creator Owners
CIFS$GRP138C                             CIFSDOM\Schema Admins
CIFS$GRP138D                             CIFSDOM\test_grp
CIFS$PRINTOPERATORS                BUILTIN\Print Operators
CIFS$GUESTS                              BUILTIN\Guests
CIFS$USERS                               BUILTIN\Users
CIFS$ADMINISTRATORS               BUILTIN\Administrators

12 VMS resource identifiers are currently mapped to CIFS domain groups.
```

WBINFO --hostname-to-domainname オプションの実行例

OpenVMS ユーザ・アカウントあるいはリソース識別子にマッピングされた CIFS ドメイン・ユーザあるいはグループ・アカウントを確認するには，次のコマンドを実行します。

wbinfo --hostname-to-domainname=<*OpenVMS-identifier*>

パラメータの意味は次のとおりです。

<OpenVMS-identifier> には，OpenVMS ユーザ・アカウント名かリソース識別子名のどちらかを指定します。

たとえば次のように実行します。

```
$ wbinfo --hostname-to-domainname=CIFS$3E8
CIFSDOM\Administrator   - USER

$ wbinfo --hostname-to-domainname=CIFS$GRP1388
CIFSDOM\Domain Users    - GROUP
```

WBINFO --domain-info オプションの実行例

ドメインについての情報を確認するには，次のコマンドを実行します。

wbinfo --domain-info

```
$ wbinfo --domain-info=cifsdom
Name                 : CIFSDOM
Alt_Name            : cifsdom.ind.hp.com
SID                  : S-1-5-21-160935111-2493731623-2036278074
Active Directory  : Yes
Native              : No
Primary              : Yes
Sequence            : 53966
```

11.1.3 smbclient

`smbclient` は，SMB/CIFS サーバーと通信するクライアントです。 FTP プログラムと同じようなインタフェースを提供します。サーバーからローカル・マシンへのファイルの設定，ローカル・マシンからサーバーへのファイルの転送，サーバーのディレクトリ情報の検索などの操作が可能です。

11.1.3.1 構文

`SAMBA$SMBCLIENT.EXE service <options>`

options としては，次のものが使用できます。

-R, --name-resolve=NAME-RESOLVE-ORDER
指定した名前解決のみを使用します。

-M, --message=HOST
このオプションを指定すると，WinPopup プロトコルを使用して別のコンピューターへのメッセージの送信が可能になります。

-I, --ip-address=IP
接続するサーバーの IP アドレスを指定します。

-E, --stderr
stdout ではなく stderr にメッセージを出力します。

-L, --list=HOST
ホストで利用できる共有のリストを取得します。

-t, --terminal=CODE
端末の I/O コードを指定します。{sjis|euc|jis7|jis8|junet|hex}

-m, --max-protocol=LEVEL
最大プロトコル・レベルを設定します。

-T, --tar=<c|x>IXFqgbNan
このオプションは，SMB/CIFS 共有上のすべてのファイルの tar 互換のバックアップを作成する場合に使用します。

-D, --directory=DIR
開始する前に初期ディレクトリを変更します。

-c, --command=STRING
セミコロンで区切ったコマンドを実行します。

-b, --send-buffer=BYTES
このオプションは転送/送信バッファ・サイズを変更します。

-p, --port=PORT
サーバーへの接続に使用する TCP ポート番号を指定します。

-g, --grepable
grep 可能な出力を生成します。

ヘルプ・オプション

-?, --help	ヘルプメッセージを表示します。
--usage	簡単な使用方法を表示します。

共通の CIFS オプション

共通の CIFS オプションを以下に示します。

-d, --debuglevel=DEBUGLEVEL
0 から 10 の整数でデバッグレベルを指定します。このパラメータを省略した場合のデフォルト値はゼロです。

-l, --log-basename=LOGFILEBASE
ログファイルのベース名を指定します。拡張子 ".progname" が追加されます (たとえば `log.smbclient`, `log.smbd` など)。

-s, --configfile=CONFIGFILE
代替 CIFS 構成ファイルを指定します。

-V, --version
プログラムのバージョン番号を出力します。

接続オプション

-O, --socket-options=SOCKETOPTIONS
クライアントソケットで設定する TCP ソケットオプションを指定します。

-n, --netbiosname=NETBIOSNAME
プライマリ NetBIOS 名を指定します。

-W, --workgroup=WORKGROUP
ワークグループ名を設定します。

-i, --scope=SCOPE
NetBIOS 名を収集する際に `nmblookup` が通信に使用する NetBIOS スコープを指定します。

認証オプション

-U, --user=USERNAME	ネットワーク・ユーザ名を設定します。
-N, --no-pass	パスワードのプロンプトを表示しません。
-k, --kerberos	kerberos で認証を試みます。Active Directory 環境でのみ有用です。
-A, --authentication-file=FILE	ファイルから認証情報を取得します。
-S, --signing=on|off|required	クライアント署名状態を設定します。
-P, --machine-pass	保管されているマシンアカウント・パスワードを使用します。

11.1.3.2 実行例

```
$ smbclient --list mtabca --user mtabca\dynac
  Password:
  Anonymous login successful
  Domain=[CIFSDOM] OS=[Unix] Server=[Samba 3.0.24]
  Sharename       Type      Comment
  ---------       ----      -------
  IPC$            IPC       IPC Service (CIFS for OpenVMS 3.0.24)
  Anonymous login successful
  Domain=[CIFSDOM] OS=[Unix] Server=[Samba 3.0.24]
  Server               Comment
  ---------            -------
  CIFSCLUSTER          CIFS for OpenVMS 3.0.24
  HOMERJ               CIFS for OpenVMS 3.0.24
  HOMERJ_ALIAS         CIFS for OpenVMS 3.0.24

  Workgroup            Master
  ---------            -------
  CIFSDOM
```

11.1.4 smbstatus

smbstatus は，現在の Samba 接続をリストする簡単なプログラムです。

11.1.4.1 構文

smbstatus <*options*>

options には次のオプションを指定できます。

-p, --processes	プロセスのリストを出力します。
-v, --verbose	冗長モードで出力します。
-L, --locks	smbstatus にロックのみをリストさせます。
-S, --shares	smbstatus に共有接続のみをリストさせます。
-u, --user=STRING	指定したユーザ名と関係する情報のみを選択します。
-b, --brief	要約モードで出力します。
-P, --profile	Samba がプロファイリング・オプション付きでコンパイルされている場合，プロファイリング共有メモリ領域の内容のみを出力します。
-B, --byterange	バイト範囲ロックを含めます。
-n, --numeric	数値の UID/GID

ヘルプ・オプション

-?, --help	ヘルプメッセージを表示します。
--usage	簡単な使用方法を表示します。

共通の CIFS オプション

共通の CIFS オプションを以下に示します。

-d, --debuglevel=DEBUGLEVEL
0 から 10 の整数でデバッグレベルを指定します。このパラメータを省略した場合のデフォルト値はゼロです。

-l, --log-basename=LOGFILEBASE
ログファイルのベース名を指定します。 拡張子 ".progname" が追加されます (たとえば log.smbclient，log.smbd など)。

-s, --configfile=CONFIGFILE
代替 CIFS 構成ファイルを指定します。

-V, --version
プログラムのバージョン番号を出力します。

11.1.4.2 実行例

現在の Samba 接続をリストするには，次のコマンドを実行してください。

```
$ smbstatus
Samba version 3.0.28a
PID        Username      Group         Machine
-------------------------------------------------------------------
00000430   TEST1         TELNETS       test01(16.91.77.23)

Service      pid         machine       Connected at
-------------------------------------------------------
IPC$         00000430   test01     Thu Apr 24 17:13:01 2008
```

11.1.5 nmblookup

nmblookup は，NetBIOS over TCP/IP クエリを使用するネットワークで NetBIOS 名を調べ，それらに IP アドレスをマップするのに使用されます。

11.1.5.1 構文

nmblookup <*options*>

options には次のオプションを指定できます。

-B, --broadcast=BROADCAST-ADDRESS	ブロードキャストに使用するアドレスを指定します。
-f, --flags	戻された NMB フラグをリストします。
-U, --unicast=STRING	ユニキャストに使用するアドレスを指定します。
-M, --master-browser	マスターブラウザを検索します。
-R, --recursion	パケット中の再帰検索フラグを設定する。
-S, --status	名前の検索で IP アドレスが返されたら，ノードステータスの問い合わせも行う。
-T, --translate	IP アドレスを名前に変換する。
-r, --root-port	root ポート 137 を使用する (Windows 95 のみに適用)。
-A, --lookup-by-ip	<name> を IP アドレスとして解釈し，このアドレスでノードステータスの問い合わせを行う。
-?, --help	ヘルプメッセージを表示します。
--usage	簡単な使用方法を表示します。
-d, --debuglevel=DEBUGLEVEL	デバッグ・レベルを設定する。
-s, --configfile=CONFIGFILE	代替構成ファイルを使用する。
-l, --log-basename=LOGFILEBASE	ログファイルのベース名を指定する。
-V, --version	プログラムのバージョン番号を出力します。
-O, --socket-options=SOCKETOPTIONS	クライアントソケットで設定する TCP ソケットオプションを指定します。
-n, --netbiosname=NETBIOSNAME	プライマリ NetBIOS 名を指定します。
-W, --workgroup=WORKGROUP	ワークグループ名を設定する。
-i, --scope=SCOPE	NetBIOS 名を収集する際に nmblookup が通信に使用する NetBIOS スコープを指定します。

ヘルプ・オプション

-?, --help	ヘルプメッセージを表示します。
--usage	簡単な使用方法を表示します。

共通の CIFS オプション

共通の CIFS オプションを以下に示します。

-d, --debuglevel=DEBUGLEVEL	0～10 の整数でデバッグレベルを指定します。このパラメータを省略した場合のデフォルト値はゼロです。
-l, --log-basename=LOGFILEBASE	ログファイルのベース名を指定します。拡張子 ".progname" が追加されます (たとえば `log.smbclient`, `log.smbd`)。

-s, --configfile=CONFIGFILE 代替 CIFS 構成ファイルを指定する。

-V, --version プログラムのバージョン番号を出力します。

接続オプション

-O, --socket-options=SOCKETOPTIONS クライアントソケットで設定する TCP ソケットオプションを指定します。

-n, --netbiosname=NETBIOSNAME プライマリ NetBIOS 名を指定します。

-W, --workgroup=WORKGROUP ワークグループ名を設定します。

-i, --scope=SCOPE NetBIOS 名を収集する際に nmblookup が通信に使用する NetBIOS スコープを指定します。

11.1.5.2 実行例

NetBIOS ノードステータス問い合わせを指定した IP アドレスに送るには，次のコマンドを実行します。 成功すると，システムに登録されている NetBIOS 名が表示されます。

```
$ nmblookup --lookup-by-ip 16.105.15.72 -d0
Looking up status of 16.105.15.72
   SYDNEY    <00> -     B <ACTIVE>
   SYDNEY    <03> -     B <ACTIVE>
   SYDNEY    <20> -     B <ACTIVE>
   CIFSDOM   <1e> -<GROUP> B <ACTIVE>
   CIFSDOM   <00> -<GROUP> B <ACTIVE>

   MAC Address = 00-00-00-00-00-00
```

名前'Syndney'の IP アドレスを確認し，返される IP アドレスに NetBIOS ノードステータス要求を送るには次のコマンドを実行します。

```
$ nmblookup --status sydney
querying sydney on 16.105.15.72
16.105.15.72 sydney<00>
Looking up status of 16.138.185.72
   SYDNEY    <00> -     B <ACTIVE>
   SYDNEY    <03> -     B <ACTIVE>
   SYDNEY    <20> -     B <ACTIVE>
   CIFSDOM   <1e> -<GROUP> B <ACTIVE>
   CIFSDOM   <00> -<GROUP> B <ACTIVE>

   MAC Address = 00-00-00-00-00-00
```

11.1.6 smbshow

このツールは，すべての HP CIFS Server のプロセスについてのシステム情報を表示するのに使用します。 HP CIFS Server を起動すると，NMBD プロセスが作成されます。 各クライアントがサーバーとセッションを確立すると，新しい SMBD プロセスが作成されます。

11.1.6.1 実行例

次の例は，クライアント・セッションがオープンされていない場合にすべてのプロセスの情報を入手した場合の例です。

```
NELTON\SYSTEM> smbshow
20203D7E NMBD            LEF      6   421150   0 00:00:23.51       714    916
```

次の例は，クライアント・セッションがオープンされている場合にすべてのプロセスの情報を入手した場合の例です。

```
NELTON\SYSTEM> smbshow
20203D7E NMBD            LEF      5   421976   0 00:00:23.59       714    916
20203E61 SMBD445_BG19299 LEF      8     2151   0 00:00:00.56      1643   1788  N
```

11.1.7 smbversion

このツールは，HP CIFS Server に含まれている種々のイメージについての情報を入手する場合に使用します。

11.1.7.1 実行例

```
$ smbversion

Information on ANDICE for OpenVMS images installed on this system:

Image Name                     Image Version    Link date           Linker ID
------------------------------ ---------------- -----------------   -------------
SAMBA$ADD_DSKSHARE             V1.2-000         17-MAY-2010 19:48   A13-03
SAMBA$ADD_PRNFORM              V1.2-000         17-MAY-2010 19:48   A13-03
SAMBA$ADD_PRNQUEUE             V1.2-000         17-MAY-2010 19:48   A13-03
SAMBA$ADD_PRNSHARE             V1.2-000         17-MAY-2010 19:48   A13-03
SAMBA$DELETE_ACE               V1.2-000         17-MAY-2010 19:48   A13-03
SAMBA$IMPORTPWD                V1.2-000         17-MAY-2010 19:48   A13-03
SAMBA$NET                      V1.2-000         17-MAY-2010 19:47   A13-03
SAMBA$NMBD                     V1.2-000         17-MAY-2010 19:47   A13-03
SAMBA$NMBLOOKUP                V1.2-000         17-MAY-2010 19:48   A13-03
SAMBA$NTLMAUTH                 V1.2-000         17-MAY-2010 19:47   A13-03
SAMBA$ODS2_CONVERT             V1.2-PS003       14-JUN-2011 03:22   A13-03
SAMBA$PDBEDIT                  V1.2-000         17-MAY-2010 19:48   A13-03
SAMBA$PROFILES                 V1.2-000         17-MAY-2010 19:48   A13-03
SAMBA$RPCCLIENT                V1.2-000         17-MAY-2010 19:48   A13-03
SAMBA$SHARESEC                 V1.2-000         17-MAY-2010 19:48   A13-03
SAMBA$SHR                      V1.2-PS003       14-JUN-2011 03:21   A13-03
SAMBA$SMBCACLS                 V1.2-000         17-MAY-2010 19:48   A13-03
SAMBA$SMBCLIENT                V1.2-000         17-MAY-2010 19:47   A13-03
SAMBA$SMBCONTROL               V1.2-000         17-MAY-2010 19:48   A13-03
SAMBA$SMBCQUOTAS               V1.2-000         17-MAY-2010 19:48   A13-03
SAMBA$SMBD                     V1.2-000         17-MAY-2010 19:47   A13-03
SAMBA$SMBPASSWD                V1.2-000         17-MAY-2010 19:48   A13-03
SAMBA$SMBSPOOL                 V1.2-000         17-MAY-2010 19:48   A13-03
SAMBA$SMBSTATUS                V1.2-000         17-MAY-2010 19:48   A13-03
SAMBA$SMBTREE                  V1.2-000         17-MAY-2010 19:48   A13-03
SAMBA$SWAT                     V1.2-000         17-MAY-2010 19:48   A13-03
SAMBA$TDBBACKUP                V1.2-000         17-MAY-2010 19:48   A13-03
SAMBA$TDBDUMP                  V1.2-000         17-MAY-2010 19:48   A13-03
SAMBA$TDBTOOL                  V1.2-000         17-MAY-2010 19:48   A13-03
SAMBA$TDB_CONVERT              V1.2-000         17-MAY-2010 19:48   A13-03
SAMBA$TDB_MIGRATION            V1.2-000         17-MAY-2010 19:48   A13-03
SAMBA$TESTPARM                 V1.2-000         17-MAY-2010 19:47   A13-03
SAMBA$WBINFO                   V1.2-000         17-MAY-2010 19:48   A13-03
SAMBA$WINBINDD                 V1.2-000         17-MAY-2010 19:48   A13-03
SAMBA$ODS2                     V1.2-PS003       14-JUN-2011 03:22   A13-03
```

```
SAMBA$VARVFC                    V1.2-PS003      14-JUN-2011 03:23  A13-03
SAMBA$VTF                       V1.2-000        17-MAY-2010 19:49  A13-03
```

11.1.8 SAMBA$DEFINE_COMMANDS.COM

このコマンドプロシージャーは，HP CIFS ユーティリティのためのすべてのシンボルを定義します。 SMBSTART，SMBSTOP，SMBSHOW，および SMBVERSION などのシンボルも定義します。

シンボルを定義するには次のようにこのコマンド・プロシージャを実行します。

```
$ @SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS.COM
```

11.1.9 SAMBA$GATHER_INFO.COM

このコマンドプロシージャは，問題のレポートのために情報ファイルおよびデータファイルを収集し，バックアップ・セーブセット・ファイルを作成します。 作成したセーブセットからは，デバッグのために，すべてのログファイル，構成ファイル，lmhosts ファイル，ユーザマッピング・ファイル，パスワードの tbd ファイル，およびその他のマッピング関連の tbd を取り出すことができます。

11.1.10 testparm

testparm は，SMB.CONF ファイルの内容をテストするためのプログラムです。 SMB.CONF ファイルを変更した場合は，testparm ユーティリティを実行してください。testparm は，SMB.CONF ファイルの構文エラーを確認し，システムで有効なサービスの一覧とともに結果を報告します。

注記: SMB.CONF ファイルを変更した場合は，testparm ユーティリティを必ず実行してください。

11.1.10.1 構文

testparm <*options*>

options には次のオプションを指定できます。

-s, --suppress-prompt
このオプションを省略すると，testparm はサービス名を表示した後，サービス定義をダンプするための改行プロンプトを表示します。

-v, --verbose
冗長モードで出力します。

--show-all-parameters
パラメータ，タイプ，および使用できる値を表示します。

--parameter-name=STRING
指定したパラメータのみを testparm で処理します。

--section-name=STRING
指定したセクションのみを testparm で処理します。

ヘルプ・オプション

-?, --help ヘルプメッセージを表示します。

--usage 簡単な使用方法を表示します。

共通の CIFS オプション

-V, --version プログラムのバージョン番号を出力します。

11.1.10.2 実行例

```
NELTON\SYSTEM> testparm
Load smb config files from /SAMBA$ROOT/LIB/SMB.CONF
Processing section "[homes]"
Processing section "[streamlf]"
Processing section "[vfc]"
Processing section "[shared]"
creating default valid table
Loaded services file OK.
Server role: ROLE_DOMAIN_MEMBER
Press enter to see a dump of your service definitions

[global]
     workgroup = CIFSDOM
     server string = Samba %v running on %h (OpenVMS)
     security = DOMAIN
     client schannel = Yes
     server schannel = Yes
     username map = samba$root:[lib]usermap.map
     log level = 10
     log file = /samba$root/var/log_%h.%m
     name resolve order = lmhosts wins bcast
```

```
        add user script = @samba$root:[bin]useradd %u
        wins server = 16.138.16.104
        idmap uid = 2000-20000
        idmap gid = 5000-15000
        admin users = system
        create mask = 0755
        vms path names = No

    [homes]
        comment = Home Directories
        read only = No
        create mask = 0750
        browseable = No
```

11.1.11 tdbbackup

tdbbackup は HP CIFS .tdb ファイルのバックアップを取るためのツールです。 このツールは，HP CIFS のスタートアップ前あるいは運用中に，.tdb ファイルの整合性を確認するためにも使用できます。ファイルの損傷を発見した場合，以前のバックアップも発見した場合はそのバックアップがリストアされます。

tdbbackup ユーティリティは，任意のタイミングで安全に実行できます。 HP CIFS の運用中であっても，任意のタイミングで tbd ファイルの整合性を確認できるようにデザインされています。 このコマンドの典型的な使用例は以下のとおりです。

```
tdbbackup [-s suffix] *.tdb
```

HP CIFS Server を再起動する前に，次のコマンドを実行することで.tbd ファイルのチェックができます。

```
tdbbackup -v [-s suffix] *.tdb
```

11.1.11.1 構文

tdbbackup <*options*>

options には次のオプションを使用できます。

-h	ヘルプ情報を表示します。
-s suffix	管理者がファイルバックアップの拡張子を指定する場合に使用します。
-v	このオプションを指定するとデータベースに損傷(データの損傷)がないかチェックします。ダメージを検出した場合は，バックアップをリストアします。
-n	バックアップのための新しいハッシュサイズを設定します。

11.1.11.2 実行例

samba$root:[private] ディレクトリで すべての TDB ファイルをバックアップするには以下のコマンドを実行します。

```
$ tdbbackup samba$root:[private]*.tdb
The backup of the TDB file samba$root:[private]passdb.tdb is samba$root:[private]passdb.tdb_bak
The backup of the TDB file samba$root:[private]secrets.tdb is samba$root:[private]secrets.tdb_bak
```

デフォルトでは，tdbbackup ユーティリティは TDB ファイル名の最後に _BAK を付けて TDB バックアップ・ファイルを作成します。 **-s** オプションを使用すると，別の接尾辞で TDB バックアップ・ファイルを作成できます。 たとえば次の例では，_OLD の接尾辞で TDB バックアップ・ファイルを作成しています。

```
$ tdbbackup -s _old samba$root:[private]*.tdb
The backup of the TDB file samba$root:[private]passdb.tdb is samba$root:[private]passdb.tdb_old
The backup of the TDB file samba$root:[private]secrets.tdb is samba$root:[private]secrets.tdb_old
```

TDB ファイルの有効性は次のコマンドで確認します。

```
$ tdbbackup -v samba$root:[private]passdb.tdb
samba$root:[private]passdb.tdb : 5 records
```

11.1.12 tdbdump

tdbdump は，TDB (Trivial DataBase) ファイルの内容を人が読めるフォーマットで標準出力にダンプするための大変簡単なユーティリティです。このツールは，TDB ファイルに関する問題をデバッグする際に利用できます。

11.1.12.1 構文

tdbdump <*options*>

options には次のオプションを指定できます。

-h	ヘルプ情報を表示します。
-k keyname	keyname の値をダンプします。

11.1.13 smbcontrol

`smbcontrol` は NMBD あるいは SMBD プロセスにメッセージを送信します。

11.1.13.1 構文

`smbcontrol` [*OPTION*]... <*destination*> <*message-type*> <*parameters*>

options には次のオプションを指定できます。

-t, --timeout=TIMEOUT タイムアウト値を秒数で設定します。

ヘルプ・オプション

-?, --help ヘルプメッセージを表示します。

--usage 簡単な使用方法を表示します。

共通の CIFS オプション

共通の CIFS オプションを以下に示します。

-l, --log-basename=LOGFILEBASE ログファイルのベース名を指定します。拡張子 ".progname" が追加されます (たとえば `log.smbclient`, `log.smbd` など)。

<*destination*> にはターゲット・プロセスのプロセス ID (PID) を指定します。

メッセージタイプ

次のメッセージタイプを使用できます。

close-share 指定した共有へのクライアント接続をクローズすることを smbd に指示します。

注記: 他の共有へのクライアント接続には影響を与えません。 このメッセージタイプは，クライアント接続をクローズする共有名あるいは * を引数として取ります。 * 文字は，現在オープンしているすべての共有への接続をクローズすることを示します。 このメッセージタイプは共有へのアクセス制御を変更した場合に便利です。 このメッセージは smbd へのみ送信できます。

debug パラメータとして指定した値にデバッグレベルを設定します。 送信先 (<*destination*>) はどちらでも可能です。

force-election このメッセージは nmbd に新しいマスターブラウザを選択させます。

ping 指定した数の ping メッセージを送信し，同じ数の応答メッセージが届くのを待ちます。 送信先 (<*destination*>) はどちらでも可能です。

profile パラメータに従ってデーモンのプロファイルの設定を変更します。パラメータとして `on` を指定すると profile stats の収集が可能になります。 `off` を指定すると profile stats の収集が無効になります。 `count` を指定すると count stats の収集が有効になります (time stats は無効)。 `flush` を指定すると現在の profile stats がゼロになります。

debuglevel デーモンのデバッグレベルを要求し，stdout に出力します。

profilelevel デーモンのプロファイルレベルを要求し，stdout に出力します。

printnotify プリンタに接続している Windows NT クライアントに対してプリンタ通知メッセージを送信するよう smbd に指示します。 以下の引数が使用できます。

queuepause printername
指定したプリンタに queue pause change notify メッセージを送信します。

queueresume printername
指定したプリンタに queue resume change notify メッセージを送信します。

jobpause printername unixjobid
指定したプリンタおよび UNIX の jobid に job pause change notify メッセージを送信します。

jobresume printername unixjobid
指定したプリンタおよび UNIX の jobid に job resume change notify メッセージを送信します。

jobdelete printername unixjobid
指定したプリンタおよび UNIX の jobid に job delete change notify メッセージを送信します。

注記: このメッセージはイベントが発生したことを通知するだけです。実際にイベントを実行するわけではありません。このメッセージは smbd にのみ送信することができます。

shutdown	指定したデーモンをシャットダウンします。このメッセージは smdb と nmbd の両方に送信することができます。
drvupgrade	特定のドライバを使用しているプリンターのクライアントに対し，ドライバをアップデートさせます。このメッセージは smbd にのみ送信することができます。
reload-config	デーモンに smb.conf 構成ファイルをリロードさせます。

11.1.13.2 実行例

```
$ smbshow
0004E32D NMBD             LEF      6      747   0 00:00:00.15       826    1063
0004E334 SMBD445_BG1309   LEF      7     2366   0 00:00:00.79      1408  1762  N

$ smbcontrol SMBD445_BG1309 ping
PONG from pid 320308

$ smbcontrol 0004E334 ping
PONG from pid 320308
```

プロセスのログ (デバッグ) レベルを 5 に増やすには次のように実行します。

```
$ smbcontrol SMBD445_BG1309 debug 5
```

プロセスの現在のログ (デバッグ) レベルは次のように確認します。

```
$ smbcontrol SMBD445_BG1309 debuglevel -d0
PID 320308: all:5 tdb:5 printdrivers:5 lanman:5 smb:5
rpc_parse:5 rpc_srv:5 rpc_cli:5 passdb:5
sam:5 auth:5 winbind:5 vfs:5 idmap:5 quota:5 acls:5 locking:5 msdfs:5 dmapi:5
```

CIFS Server 構成ファイルのリロードは次のように行ないます。

```
$ smbcontrol SMBD445_BG1309 reload-config
```

CIFS Server プロセスのシャットダウンは次のように行ないます。

```
$ smbcontrol SMBD445_BG1309 shutdown
```

11.2 ODS-2 から ODS-5 へのエンコードされたファイル名の変換

既存の HP OpenVMS CIFS 共有を ODS-2 から ODS-5 へ変換すると，OpenVMS の EFS (Extended File Specifications) の機能を利用することができます。 HP OpenVMS CIFS ソフトウェアは，ODS-2 から変換された ODS-5 デバイス上に存在する ODS-2 エンコードされたファイル名を変換するためのユーティリティを提供します。この変換ユーティリティは，ファイル名に含まれるエスケープ・エンコード文字を取り除き，ファイル名を ISO-8859-1 文字に変更します。

たとえば，ODS-2 ディスクで作成されたファイル名に小文字のウムラウト () を表現するための文字エンコーディング・シーケンス _ _*E4*, が含まれる場合，変換ユーティリティはこのエンコーディングを取り除き 文字と置き換えます。

ODS-2 ファイル名から ODS-5 ファイル名への変換は，以下の作業を完了した後に実行できます。

- HP OpenVMS CIFS のインストールおよび構成
- エスケープ・エンコーディングされたファイル名を含むディスク・デバイスの ODS-2 から ODS-5 へのボリューム構造の変換。 ODS-5 へのディスク・デバイスの変換については，『OpenVMS Extended File Specifications の手引』を参照してください。

注記: HP OpenVMS CIFS が提供する変換ユーティリティは，変換後の文字が ASCII あるいは拡張 ASCII 文字のいずれかになる場合のみ，ファイル名に含まれているエスケープ・エンコードされた文字を変換することができます。

11.2.1 ファイル名変換ユーティリティの使用

ODS-2 ファイル・システム用のエンコーディングから ISO-8859-1 ファイル名へのファイル名の変換には，次のファイル名変換ユーティリティを使用します。

SAMBA$ROOT:[BIN.<*ARCH_TYPE*>]SAMBA$ODS2_CONVERT.EXE

ARCH_NAME には，ご使用の OpenVMS システムのアーキテクチャによって ALPHA あるいは IA64 のどちらかを指定します。

Samba コマンドが定義されている場合は，ODS2_CONVERT システム管理コマンドを使用してファイル名変換ユーティリティを起動することができます。

ODS2_CONVERT コマンドを手動で定義するには，次の DCL コマンドを実行してください。

```
$ ODS2_CONVERT :==  SAMBA$ROOT:[BIN.<ARCH_NAME>]SAMBA$ODS2_CONVERT.EXE
```

ARCH_NAME には，ご使用の OpenVMS システムのアーキテクチャによって ALPHA あるいは IA64 のどちらかを指定します。

11.2.2 ODS2_CONVERT

ODS2_CONVERT ユーティリティは，エンコードされたファイル名文字の ASCII および 拡張 ASCII 文字への変換をサポートします。

11.2.2.1 構文

ODS2_CONVERT *qualifiers file-spec*

以下とおりパラメータを指定します。

- *qualifiers* の指定はオプションです。表 11-1 「ODS2_CONVERT 修飾子」 に示す修飾子を指定します。いずれの修飾子も指定しなかった場合，デフォルトの設定が使用されます。
- *file-spec* 引数の指定は必須で，デバイス名，ディレクトリ名，およびファイル名を指定します。
  - ディスク・デバイスのみを指定した場合，変換ユーティリティはエンコーディングされているファイル名が無いかデバイス全体を走査し，必要に応じて変換を行ないます。

— ディスク・デバイスとディレクトリを指定した場合，変換ユーティリティは指定されたディレクトリのすべてのファイルを走査し，必要に応じて変換を行ないます。ディレクトリ名およびファイル名にワイルドカード文字を使用することもできます。
— ディスク・デバイス，ディレクトリ，および単一のファイル名を指定した場合，そのファイルのみ変換が行なわれます。
— ファイル指定無しで ODS2_CONVERT コマンドを実行した場合，ファイル指定のためのプロンプトが表示されます。

以下に例を示します。

```
$ ODS2_CONVERT
FILENAME:
```

FILENAME プロンプトで，変換するデバイスの名前，さらに必要であればディレクトリとファイル名を指定します。 ここで修飾子を指定することもできます。

表 11-1 ODS2_CONVERT 修飾子

修飾子	説明	デフォルト
/DISABLE=*keyword*	指定されたキーワードに従って変換ユーティリティの機能を無効にします。キーワードとしては，変換ユーティリティがチェックしないファイル・システム・タイプとして STRUCTURE_LEVEL (ODS-2 あるいは ODS-5) を指定します。	/NODISABLE
/LOG=*log-filespecification*	変換したファイル名を含むログファイルを作成します。この修飾子を使用してログファイルの場所の名前を指定できます。	/NOLOG (情報は表示されますがログファイルは作成されません。)
/VERBOSE	変換時に走査したすべてのファイル名が表示されます。	/NOVERBOSE
/NOLIST	変換したファイル名の表示を行ないません。エラー・メッセージのみ表示されます。	/LIST

11.2.2.2 実行例

エンコードされた 1 つのファイル名の変換の例

ここで示すのは，DISKA 上に Windows クライアントによって作成された A FILE.TXT というファイルが A__20FILE.TXT とエンコードされている場合の例です。 デバイス DISKA のボリューム構造は ODS-2 から ODS-5 へ変換されています。 OpenVMS システムでは，このファイルは下記のように表示されます。

```
$ DIRECTORY DISKA:[FILES]
Directory DISKA:[FILES]
.
.
.
A__0FILE.TXT
$
```

ODS2_CONVERT コマンドを使用してこのファイルを変換します。

```
$ ODS2_CONVERT/VERBOSE DISKA:[FILES]A__20FILE.TXT
```

ODS2_CONVERT ユーティリティは，エンコードされているファイル名文字の ASCII 文字および拡張 ASCII 文字への変換をサポートします。

```
Scanning file - DISKA:[FILES]A__20FILE.TXT;1
Renamed A__20FILE.TXT to A FILE.TXT
```

```
Convert Utility Complete
$
```

エンコードされたすべてのファイル名の変換の例

ディスク・デバイスおよびディレクトリ上にあるエンコードされたすべてのファイル名を変換するには，ファイル名は指定せずにディスク・デバイスとディレクトリを指定して ODS2_CONVERT コマンドを実行します。 たとえば，デバイス DISK$USER1 上でエンコードされているすべてのファイル名を変換するには，次のようなコマンドを実行します。

```
$ ODS2_CONVERT/VERBOSE DISKA:[FILES]A__20FILE.TXT
```

ODS2_CONVERT ユーティリティは，エンコードされているファイル名文字の ASCII 文字および拡張 ASCII 文字への変換をサポートします。

```
FILENAME: DISK$USER1:
Renamed A__20FILE.TXT to A FILE.TXT
.
.
.
Convert Utility Complete
```

11.2.2.3 delete_ace ユーティリティ

delete_ace ユーティリティは， HP CIFS Server によって適用された APPLICATION ACE に加えて，PATHWORKS あるいは Advanced Server for OpenVMS の ACL をすべて削除します。この際，ファイルの修正日時は変更されません。

このユーティリティを使用するには，次のようにシンボルを定義してくださいい。

```
delete_ace :== $SAMBA$EXE:SAMBA$DELETE_ACE.EXE
```

あるいは以下のコマンドを実行します。

```
@SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS.COM
```

PATHWORK あるいは SAMBA ACE を削除するには，次のように実行します。

```
delete_pwrkace <p1 parameter> <p2 parameter>
```

<*p1 parameter*> には，以下のように 有効なほとんどの OpenVMS ファイル指定形式が使用可能です。

```
dka100:[test...]
dka100:[test.testing]temp.doc
dka100:[test]*.*,dka200:[temp]*.*
dka100:[test...]*.*;*
dka100:[test.testing]temp.doc,tester.doc
```

<*p2 parameter*> には以下のいずれかを指定できます。

- pwrk — PATHWORKS および Advanced Server の ACE を削除する (デフォルト)。
- samba — HP CIFS Server ACE を削除する。

注記: このユーティリティは，PATHWORKS および Advanced Server の ACE を永久に削除します。 このユーティリティは，他のクラスタ・ノードで PATHWORKS あるいは Advanced Server を実行し続けているような OpenVMS クラスタ，あるいは，PATHWORKS または Advanced Server から HP CIFS Server へ移行した環境では注意して使用します。

delete_ace の実行例

特定のディレクトリのすべてのファイルの PATHWORKS および Advanced Server ACE を削除するには，次のコマンドを実行してください。

```
$ delete_ace dka100:[test]*.* pwrk
```

特定のファイルの CIFS Server (SAMBA) ACE を削除すえには，次のコマンドを実行します。

```
$ delete_ace dka100:[test.testing]temp.doc samba
```

11.2.2.4 tdb_convert ユーティリティ

tdb_convert ユーティリティは，samba$root:[lib]convert.fdl ファイルにある値を使用して既存の永続的な TDB ファイルを変換します。 CONVERT.FDL ファイルは，最適化された FDL 値を含むように変更できます。

注記: CONVERT.FDL ファイルに正しくない値が含まれる状態で変換を行うと，変換後，TDB ファイルが使用できなくなるため，CONVERT.FDL ファイルの変更は注意して行なう必要があります。

SAMBA$CONFIG.COM ファイルを使用して，HP CIFS Server がデフォルトの設定で構成されている場合，構成処理の一部として，HP CIFS Server によって SAMBA$ROOT:[LIB]CONVERT.FDL ファイルが作成されます。 SAMBA$ROOT:[LIB] ディレクトリに CONVERT.FDL ファイルが存在しない場合は， SAMBA$ROOT:[LIB]CONVERT.FDL ファイルを編集して 下記のように記述してください。

```
SYSTEM
        SOURCE                  "OpenVMS"

FILE
        ORGANIZATION             indexed
        PROTECTION               (system:RWD, owner:RWD, group:, world:)
        GLOBAL_BUFFER_COUNT       0
        GLBUFF_CNT_V83           200
        GLBUFF_FLAGS_V83        none

RECORD
        CARRIAGE_CONTROL         carriage_return
        FORMAT                   variable
        SIZE                     0

AREA 0
        ALLOCATION                240
        BEST_TRY_CONTIGUOUS          yes
        BUCKET_SIZE               4
        EXTENSION                 80

AREA 1
        ALLOCATION                48
        BEST_TRY_CONTIGUOUS          yes
        BUCKET_SIZE               4
        EXTENSION                 48

KEY 0
        CHANGES                   no
        DATA_AREA                 0
        DATA_FILL                 100
        DATA_KEY_COMPRESSION         no
        DATA_RECORD_COMPRESSION      yes
        DUPLICATES                no
        INDEX_AREA                1
        INDEX_COMPRESSION          no
        INDEX_FILL                100
        LEVEL1_INDEX_AREA           1
        NAME                      "TDBHASH.1/16"
        PROLOG                    3
        SEG0_LENGTH                16
```

```
SEG0_POSITION                   0
TYPE                            string
```

TDB を変換する手順は以下のとおりです。

1. `samba$root:[lib]convert.fdl` ファイルを編集して，必要となる値の変更を行ない，内容を保管します。

   たとえば，HP CIFS Server が使用するグローバル・セクション数を減らすために GLBUFF_CNT_V83 の値を 50 に減らす場合， `samba$root:[lib]convert.fdl` ファイルの GLBUFF_CNT_V83 の値を 50 に変更します。

2. 次のコマンドを実行します。

   ```
   $ @SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS.COM
   $ TDB_CONVERT SAMBA$ROOT:[<subdir>]<TDB-File-Name>
   ```

   パラメータには下記の値を指定します。

   - *<subdir>* — PRIVATE あるいは VAR.LOCKS
   - *<TDB-File-Name>* — いずれかの永続的 TDB のファイル名

   たとえば， `samba$root:[private]` ディレクトリに存在する `passdb.tdb` を変換するには，次のようにします。

   ```
   $ TDB_CONVERT SAMBA$ROOT:[PRIVATE]PASSDB.TDB
   ```

   永続的 TDB ファイルについての詳細は， 第10章「ファイルとプリントのセキュリティ」を参照してください。

11.3 VAR あるいは VFC ファイルのヒント値のアップデート

OpenVMS では，ODS-5 ディスク上のシーケンシャルな VAR および VFC ファイル (印刷属性付きの VFC ファイルを除く) に対してファイルの実データとレコード数を示すために，ファイル長の値を提供します。 この機能により，SMBD プロセスはファイル・サイズの計算のためにファイル全体を読み取る必要が無くヒント値を読み取るだけで良いので，この機能はファイルを一覧表示する際に便利です。 ヒント値の不便な点は，値が不正確になる場合があることです。 SMBD プロセスがこれらのファイルを一覧表示しようとした時にヒント値が正しくない場合，実際のファイル・サイズを計算するためにファイル内容全体の読み取りを行なう必要があります。 この処理は，VAR および VFC ファイルに対する SMBD プロセスの性能を低下させる可能性があります。

HP CIFS for OpenVMS のソフトウェア・キットには，VAR ファイルおよび VFC ファイルのヒント値をアップデートするための `SAMBA$UPDATEFILEHINTVALUE.COM` というユーティリティが含まれています。

このユーティリティは，ODS-5 ディスク上に存在するファイル共有パス (`SMB.CONF` に記述されている) の各ファイルを読み取り，それらがシーケンシャル VAR および VFC フォーマットであるかどうか識別することができます。 ファイルがシーケンシャル VAR および VFC フォーマットで，それらのファイル長ヒント値が正しくない場合，このユーティリティは `analyze/rms/update_header` コマンドを呼び出し，そのファイルのファイル長ヒント値をアップデートします。

注記: `SAMBA$UPDATEFILEHINTVALUE.COM` スクリプトは，ファイル・サイズを調べるために SAMBA がファイル内容全体を読み取る必要がないように，対話形式でも，一定間隔でヒント値をアップデートできるようにバッチ形式でも，どちらでも実行できます。

このユーティリティが存在する場所は `SAMBA$ROOT:[BIN]SAMBA$UPDATEFILEHINTVALUE.COM` です。

構文

```
@SAMBA$ROOT:[BIN]SAMBA$UPDATEFILEHINTVALUE.COM
```

得られた結果は以下のファイルに保管されます。

samba$root:[var]FileHintUpdate.output
: analyze コマンドの詳細な出力が含まれます。

samba$root:[var]FileHintUpdatefile.list
: 正しいヒント値でアップデートされた VAR および VFC ファイルのファイル名の一覧が含まれます。

SAMBA$UPDATEFILEHINTVALUE.COM を使用して VAR および VFC ファイルのヒント値をアップデートする実行例を次に示します。

例 11-1 VAR および VFC ファイルのファイル・ヒント値のアップデート

```
$ @SAMBA$UPDATEFILEHINTVALUE.COM

****************************************
Script to update the File Hint Value of the VAR  &  VFC files
****************************************
Following are the share pathes found in smb.conf
        path = DKA100:[SAMBA.523]
        path = DKA100:[SAMBA.510]
        path = DKA100:[SAMBA.511]

****************************************
Analysing each share path
****************************************
Results
****************************************
Following  VAR  & VFC  files have been updated
----------------------------------------
DKA100:[SAMBA.523]OUTFILE_ VFC .TXT;1
DKA100:[SAMBA.523.VAR]SAMBA$INFO.TXT;3
DKA100:[SAMBA.523.VAR]SAMBA$NMBD_AQUILA.LOG;35
DKA100:[SAMBA.523.VAR]SAMBA$SMBD_STARTUP.LOG;4458
DKA100:[SAMBA.510]OUTFILE_ VFC1 .TXT;1
DKA100:[SAMBA.511]OUTFILE_ VFC2 .TXT;1

----------------------------------------
****************************************
Please find the detailed log in samba$root:[var]FileHintUpdate.output.
```

第12章　性能に関する注意事項とトラブルシューティング

この章では以下のような項目について説明します。

12.1 システム・ディスク以外での SAMBA$ROOT ディレクトリのホスティング

SAMBA$ROOT ディレクトリ・ツリーをシステム・ディスクでホスティングした場合，オペレーティング・システムがシステム・ディスクの使用状況が高負荷になると HP CIFS Server の性能が低下する場合があります。このため，PRODUCT INSTALL コマンドの /DESTINATION 修飾子を使用して，システム・ディスク以外に HP CIFS Server をインストールすることをお勧めします。SAMBA$ROOT: ディレクトリ・ツリーがすでにシステム・ディスクでホスティングされている場合は，2.8 項「SAMBA$ROOT ディレクトリの移動」で説明する手順に従ってください。

12.2 ディレクトリの一覧表示性能

ディレクトリの一覧表示性能に最も大きな影響を与えるのは，共有レベルの構成パラメータ *vms path names* の設定です。このパラメータが有効 (デフォルト) になっている場合，ODS-2 および ODS-5 のどちらのボリュームの場合も，HP CIFS Server はディレクトリの一覧表示で性能が改善されます。HP が推奨する場合を除き，*vms path names* パラメータは無効にしないでください。

12.3 ディスク・ボリュームのチューニング

1. 書き込み性能を改善するには，次の方法でボリューム・ハイウォータ・マーキングを無効にします。
   a. ボリュームを初期化する際に /NOHIGHWATER_MARKING 修飾子を指定してください。
   b. すでにボリュームが初期化されている場合は，次のようなコマンドを実行してボリュームにハイウォータ・マーキングを設定します。

      ```
      SET VOLUME /NOHIGHWATER_MARKING <volumename>
      ```

      この設定はボリュームを再マウントするまで有効にはなりません。
2. ディスク・クラスタ・サイズを 16 の倍数に設定します。この処理は，ディスクを初期化する際に INITIALIZE コマンドの /CLUSTER_SIZE 修飾子を使用することで実行できます。
3. SAMBA$ROOT:[BIN]SAMBA$SMBD_STARTUP.COM ファイルに次の行を追加します。

   ```
   SET RMS_DEFAULT -/EXTEND_QUANTITY=10240/BLOCK_COUNT=n/BUFFER_COUNT=8
   ```

   n には次の値を指定します。

- EVA の場合は 124
- XP の場合は 96
- その他のディスクの場合は 127

注記: `EXTEND_QUANTITY` の値は 16 ブロックの倍数で指定します。

4. OSD-2 ではなく ODS-5 ボリュームを使用します。

   ODS-5 ボリューム上の可変長あるいは VFC レコード形式 のファイルのファイル・ヘッダには，HP CIFS Server がファイルのデータ・バイト数を認識するのに使用可能な付加的なファイル長ヒント値が含まれています。

   ファイル長ヒント値が存在しない，あるいは有効でない場合，HP CIFS Server は，Windows クライアント上に表示するサイズを確認するためにファイル全体を読み取る必要があります。

12.4 ファイル長ヒント値のアップデート

可変長レコード・フォーマットのファイルのファイル長ヒント値をアップデートするために，定期的に次のコマンドを実行してください。.

```
@SAMBA$ROOT:[BIN]SAMBA$UPDATEFILEHINTVALUE.COM
```

詳細は，11.3 項「VAR あるいは VFC ファイルのヒント値のアップデート」を参照してください。

12.5 CIFS Server ACE

HP CIFS Server V1.2 以降，HP CIFS Server は，`Stream` あるいは `Stream_LF` 以外のレコード・フォーマットのファイルのサイズを，そのファイルに保管されているアプリケーション ACE に保管します。有効なファイル長ヒント値を持つ可変長レコード・フォーマットのファイルの場合を除き，このようなファイルを最初に読み取ったときに，HP CIFS Server はファイルの内容全体を読み取ってファイル・サイズを計算します。計算されたファイル・サイズは HP CIFS Server ACE に保管され，ファイルに適用されます。このファイルが変更されなければ，HP CIFS Server はそのファイル上に存在する HP CIFS Server ACE からファイル・サイズを取得します。これにより性能が改善されます。ファイルが変更されるとファイル・サイズが再度計算され，ACE に保管されます。`DELETE_ACE` ユーティリティはファイル上の HP CIFS Server ACE を削除できますが，特にその必要がなければ，HP CIFS Server ACE を削除しないことをお勧めします。

注記: HP CIFS Server ACE が有効になっている場合，さらに DOS 属性を保管することもできます。

12.6 vms estimate file size パラメータ

特定の OpenVMS ファイル・フォーマットでは，HP CIFS Server は，ファイルのサイズを確認するためにファイルの内容全体を読み取る必要があります。この結果，そのようなファイルが含まれているディレクトリの一覧表示で，期待よりも出力が遅くなる場合があります。以下のファイル・フォーマットを除き，この動作の影響を受けます。

- Stream あるいは Stream_LF レコード・フォーマットの順編成ファイル (ODS-2 および ODS-5 のどちらのボリュームでも)
- 固定長レコード・フォーマットで，ファイル・サイズが偶数で，`None` あるいは `Carriage return carriage control` のレコード属性の順編成ファイル (ODS-2 および ODS-5 のどちらのボリュームでも)
- ヘッダに有効なファイル長ヒント値を含む ODS-5 ボリューム上の可変長あるいは VFC レコード・フォーマットの順編成ファイル (印刷属性付きの VFC ファイルを除く)

HP CIFS Server は，計算済のファイル・サイズが保管されたファイル上の APPLICATION ACE を適用するので，この性能の低下は一時的なものになります。それ以降，ファイル・サイズは APPLICATION ACE から取得され，クライアントがファイルを変更すると ACE が更新されます。

ただし，その後にこのファイルが HP CIFS Server 以外の OpenVMS アプリケーションにより変更されると，APPLICATION ACE は無効化され，ファイル・サイズの計算のために HP CIFS Server によるファイル全体の読み取りが再度必要になります。また，そのようなファイルを含むディレクトリの内容が頻繁に変更される場合は，APPLICATION ACE は期待するほどの性能の改善をもたらさない可能性があります。

この問題がいつまでも続く場合は，そのようなファイルのサイズを見積もるための共有を構成すると良いかもしれません。共有パラメータ `vms estimate file size` の設定が `YES` でこの機能が有効になっている場合，HP CIFS Server はファイル・ヘッダに含まれている値を使用してこれらのファイルのサイズを見積もり，ディレクトリ一覧表示の性能を大きく改善させます。`vms estimate file size` 共有パラメータは，個々の共有セクションに含まれるか，あるいは (共有セクションに明示的な `vms estimate file size` エントリを持たない) すべての共有に適用されるように構成ファイルの [GLOBAL] セクションに置かれます。

クライアントがディレクトリの内容を一覧表示させるときに，そのディレクトリにファイル・サイズの見積もりのために読み取りが必要になるサイズの非常に大きなファイルが 1 つあるいは複数含まれていると，HP CIFS Server がファイル・サイズを確認する間にクライアントがタイムアウトに場合があります。この場合，`vms estimate file size` を有効にすると，ディレクトリの一覧表示性能を改善させることができます。

⚠ **警告!** ファイル・ヘッダ・データから計算されたサイズは，HP CIFS Server がファイルの内容全体を読み取って計算したサイズよりも常に大きくなります。このため，`vms estimate file size` パラメータを有効にする場合は，これらのファイルにアクセスするクライアント・アプリケーションが問題なく機能するかどうかを確認するのが良いでしょう。クライアント・アプリケーションが悪影響を受ける場合は，ODS-5 ボリュームへファイルを移動するばど，他の選択肢を検討すべきです。

12.7 vms open file caching パラメータ

HP OpenVMS CIFS V1.2 以降，次のような HP CIFS Server 固有の 2 つの新しい共有構成パラメータが提供されます。

- `vms open file caching`
- `vms ofc time interval`

`vms open file caching` 共有パラメータは， HP CIFS Server が提供する Open File Caching (OFC) 機能を制御します。デフォルトでは，この機能は無効です。OFC が有効になっていると，立て続けにオープンとクローズが繰り返されるようなファイルを処理する場合に，HP CIFS の性能が大幅に改善されます。 たとえば，クライアントはログイン・スクリプトなどの DOS バッチ・ファイルをサーバーに保管します。このファイルにアクセスする最後のクライアントがファイルをクローズした後，ファイルは一定の期間サーバー上でオープンされたままになります。 このキャッシュは，Advanced Server for OpenVMS が使用する OFC に似ています。HP CIFS Server が提供する OFC 機能は，HP CIFS Server 構成ファイルの共有セクションに次のような行を追加することで有効にできます。

```
vms open file caching = yes
```

ファイルがキャッシュにオープンし続ける期間は，ミリ秒単位で指定される OFC タイムインターバルによって決まります。OFC タイムインターバルを制御する共有パラメータは `vms ofc time interval` です。このパラメータのデフォルト値は 5000 ミリ秒です。OFC タイムインターバルのデフォルト値は，HP CIFS Server 構成ファイルの共有セクションに次のような行を追加することで変更できます。たとえば，OFC タイムインターバルとして 1000 ミリ秒を指定する場合は，次のように指定します。

```
vms ofc time interval = 1000
```

12.8 Microsoft Distributed File System

Microsoft の Distributed File System (MS DFS) を利用していない場合は，SMB.CONF ファイルの [global] セクションに次のパラメータを追加して，HP CIFS Server における DFS サポートを無効にしてください。これにより，ネットワーク・トラフィックと DFS 関係のエラーの発生を低減できます。

```
host msdfs = no
```

注記: MS DFS を無効にした後，既に HP CIFS Server との接続を確立していたクライアントを再起動する必要があるかもしれません。

MS DFS を無効にしておくと，存在しない共有パスを使用してアクセスしようとしたときに発生するクライアント・システムのクラッシュ，あるいはアクセス許可がない場合に発生するクライアント・システムのクラッシュを回避することができます。

12.9 クライアント接続数の構成

サーバーが処理可能なクライアント接続の最大数は，サーバーがサポートするプロセスの最大数(プロセス・エントリ・スロット)によって制限されます。この値は次のコマンドで確認できます。

```
$ SHOW MEMORY/SLOT
```

Process Entry Slots パラメータ値の変更方法については，『HP OpenVMS システム管理者マニュアル』を参照してください。

12.10 不要なデータグラム・パケットの無視

HP CIFS Server の SMB.CONF グローバル・パラメータ *store dgpackets* が no (デフォルト) に設定されている場合，NMBD プロセスは不要なデータグラムを無視します。dgpackets = yes を設定すると，NMBD プロセスは不要なデータグラム・パケットを unexpected.tdb ファイルに書き込むためサイズが大きくなり，NMBD による CPU 消費量が増加する原因となります。HP が推奨する場合以外は，このパラメータの値は yes に設定しないでください。

12.11 TDB データベース・ファイルの最適化

HP CIFS Server は，ファイル名にファイル拡張子 .TDB を含むファイルにデータを保管します。これらのファイルは，一般に TDB ファイルと呼ばれています。HP CIFS Server は，RMS インデックス・ファイルを使用して TDB ファイルをエミュレートします。すべての RMS インデックス・ファイルと同様に，これらのデータベース・ファイルは定期的にメンテナンスや最適化を行なうと恩恵があります。FDL を使用して TDB データベースを分析および最適化する方法について，以降の項で説明します。

12.11.1 FDL ファイル名の処理

TDB ファイルを作成する際，HP CIFS Server は以下の順番で最初に見つけた FDL ファイルを使用します。

1. SAMBA$ROOT:[LIB]<*tdb-filename*>.FDL

   パラメータには以下の値を指定します。

   <*tdb-filename*> には TDB ファイルの名前を指定します。

   たとえば，LOCKING.TDB を作成する際， SAMBA$ROOT:[LIB]LOCKING.FDL ファイルが存在する場合は，HP CIFS Server はこの FDL ファイルを使用して新しい LOCKING.TDB を作成します。

2. SAMBA$ROOT:[LIB]]GENERIC_TDB.FDL

   このファイルは，HP CIFS Server が TDB ファイルを作成する際に TDB 固有の FDL ファイルが無い場合に使用します。

3. HP CIFS Server が TDB 固有の FDL ファイルも GENERIC_TDB.FDL ファイルも検出しなかった場合，デフォルトの FDL 値を使用します。

   FDL のデフォルト値の詳細ついては，12.11.3 項を参照してください。

12.11.2 最適化された FDL ファイルの作成

TDB ファイルの性能を改善するために，分析，FDL の最適化，新しい TDB ファイルの作成の 3 段階の手順を実行してください。データ・ファイルが存在する間この操作を定期的に実行することにより，最適に実行されるファイルが得られます。得られたファイルは，TDB 固有の FDL ファイルあるいは GENERIC_TDB.FDL ファイルとして使用できます。これにより，最適化された FDL 値を使用して HP CIFS Server が TDB ファイルを作成できます。 最適化された FDL ファイルの生成手順は以下のとおりです。

1. データファイルの分析

   ANALYZE/RMS_FILE/FDL コマンドを使用して，データファイルの現在の状態を反映した出力ファイル (*analysis-fdl-file*) を作成してください。分析 FDL ファイルを作成するためのコマンド構文は次のとおりです。

   ANALYZE/RMS_FILE/FDL/OUTPUT=<*analysis-fdl-file*> <*original-data-file*>

   出力ファイル <*analysis-fdl-file*> には，作成時の属性や，作成後のデータファイルの構造や内容に対する変更を反映した情報など，データファイルに関するすべての情報と統計値が含まれます。

   たとえば，LOCKING.TDB の分析 FDL ファイルを入手するには，次のコマンドを実行します。

   ```
   $ ANALYZE/RMS_FILE/FDL/OUTPUT=ANALYSIS_LOCKING.FDL SAMBA$ROOT:[VAR.LOCKS]LOCKING.TDB
   ```

   これにより，現在の作業ディレクトリに ANALYSIS_LOCKING.FDL が作成されます。

2. FDL の最適化

   Edit/FDL ユーティリティを使用して，最適化された FDL ファイル (*optimized-fdl-file*) を作成します。

   FDL ファイルの変更は，端末を使用して対話的に，あるいは Edit/FDL ユーティリティが分析レポートをもとに最適化された値を計算できるようにすることにより非対話的に行なうことができます。

   ファイルを対話的に最適化するには，次のように OPTIMIZE スクリプトを使用します。

   EDIT/FDL/ANALYSIS=<analysis-fdl-file>/SCRIPT=OPTIMIZE/OUTPUT=<*optimized-fdl-file*> <*analysis-fdl-file*>

   非対話的にファイルを最適化するには，次のように行ないます。

   EDIT/FDL/ANALYSIS=<*analysis-fdl-file*>/NOINTERACTIVE /OUTPUT=<*optimized-fdl-file*> <*analysis-fdl-file*>

   たとえば，ANALYSIS_LOCKING.FDL を非対話的に使用して最適化された FDL を生成するには，次のようなコマンドを実行します。

   ```
   $ EDIT/FDL/ANALYSIS=ANALYSIS_LOCKING.FDL/NOINTERACTIVE /OUTPUT=OPTIMIZED_LOCKING.FDL ANALYSIS_LOCKING.FDL
   ```

3. ファイルの変換

   変換とは，最適化された FDL ファイルを元のデータファイルに適用するする処理です。

   次のように Convert ユーティリティを使用します。

   CONVERT/FDL=<*optimized-fdl-file*> <*original-data-file*>[<*new-data-file*>]

たとえば，最適化された FDL ファイルを使用して新しいバージョンの LOCKING.TDB ファイルを入手するには，次のコマンドを実行します。

```
$ CONVERT/FDL=OPTIMIZED_LOCKING.FDL SAMBA$ROOT:[VAR.LOCKS]LOCKING.TDB
```

4. 最適化された FDL ファイルの値を確認した後，GENERIC_TDB.FDL あるいは *<tdb-datafile-name>.FDL* (すなわち LOCKING.TDB) に名前を変更し，SAMBA$ROOT:[LIB] ディレクトリにコピーします。

12.11.3 デフォルトの FDL 値

.TDB ファイルを作成する際， HP CIFS Server は次のデフォルト FDL 値を使用します。

```
SYSTEM
        SOURCE                      "OpenVMS"
FILE
        ORGANIZATION                indexed
        PROTECTION                  (system:RWD, owner:RWD, group:, world:)
        GLOBAL_BUFFER_COUNT         0
        GLBUFF_CNT_V83              200
        GLBUFF_FLAGS_V83             none
RECORD
        CARRIAGE_CONTROL            carriage_return
        FORMAT                      variable
        SIZE                        0
AREA 0
        ALLOCATION                  240
        BEST_TRY_CONTIGUOUS         yes
        BUCKET_SIZE                4
        EXTENSION                   80

AREA 1
        ALLOCATION                  48
        BEST_TRY_CONTIGUOUS         yes
        BUCKET_SIZE                 4
        EXTENSION                   48

KEY 0
        CHANGES                     no
        DATA_AREA                   0
        DATA_FILL                   100
        DATA_KEY_COMPRESSION        no
        DATA_RECORD_COMPRESSION     yes
        DUPLICATES                  no
        INDEX_AREA                  1
        INDEX_COMPRESSION           no
        INDEX_FILL                  100
        LEVEL1_INDEX_AREA           1
        NAME                        "TDBHASH.1/16"
        PROLOG                      3
        SEG0_LENGTH                 16
        SEG0_POSITION               0
        TYPE                        string
```

第13章　SMB.CONF パラメータ

この章では以下の項目について説明します。

13.1 概要

この章では，HP CIFS Server 構成パラメータについて， 変更可能なもの，変更できないもの，サポートされていないものを それぞれ説明します。 これらのパラメータの詳細は SWAT utility のヘルプページを参照してください。 この章では，HP CIFS Server 固有の構成パラメータについても説明します。

13.2 変更可能な構成パラメータ

```
- abort shutdown script
- add group script
- add machine script
- add share command
- add user script
- add user to group script
- addport command
- addprinter command
- admin users
- administrative share
- algorithmic rid base
- allocation roundup size
- allow trusted domains
- available
- bind interfaces only
- browse list
- browseable
- change share command
- check password script
- client NTLMv2 auth
- client lanman auth
- client plaintext auth
- client schannel
- client signing
- client use spnego
- cluster addresses
- comment
- create mask
- csc policy
- deadtime
- debug hires timestamp
- debug pid
- debug prefix timestamp
- debug timestamp
- debug uid
- default service
- delete group script
- delete readonly
- delete share command
- delete user from group script
- delete user script
```

- delete veto files
- deleteprinter command
- directory mask
- directory name cache size
- directory security mask
- disable netbios
- disable spoolss
- display charset
- domain logons
- domain master
- dont descend
- dos charset
- enable asu support
- enhanced browsing
- enumports command
- fake oplocks
- follow symlinks
- force create mode
- force directory mode
- force directory security mode
- force security mode
- force unknown acl user
- fstype
- guest account
- guest ok
- guest only
- hide unwriteable files
- host msdfs
- hostname lookups
- hosts allow
- hosts deny
- idmap alloc backend
- idmap backend
- idmap cache time
- idmap domains
- idmap gid
- idmap negative cache time
- idmap uid
- inherit owner
- inherit vms rms protections
- interfaces
- invalid users
- lanman auth
- large readwrite
- ldap admin dn
- ldap debug level
- ldap debug threshold
- ldap delete dn
- ldap group suffix
- ldap idmap suffix
- ldap machine suffix
- ldap page size
- ldap passwd sync
- ldap replication sleep
- ldap ssl
- ldap suffix
- ldap timeout
- ldap user suffix
- level2 oplocks
- lm announce
- lm interval
- local master
- lock directory
- lock spin time
- log file

- log level
- logon drive
- logon home
- logon path
- logon script
- lppause command
- lpq command
- lpresume command
- lprm command
- machine password timeout
- map to guest
- max connections
- max disk size
- max log size
- max open files
- max print jobs
- max protocol
- max reported print jobs
- max ttl
- max wins ttl
- max xmit
- message command
- min print space
- min protocol
- min wins ttl
- msdfs proxy
- msdfs root
- name cache timeout
- name resolve order
- netbios aliases
- netbios name
- netbios scope
- ntlm auth
- null passwords
- only user
- oplock break wait time
- oplock contention limit
- oplocks
- os level
- passdb backend
- password server
- path
- pid directory
- postexec
- preexec
- preexec close
- preferred master
- print command
- printable
- printer name
- private dir
- profile acls
- queuepause command
- queueresume command
- read list
- read only
- read raw
- realm
- remote announce
- remote browse sync
- rename user script
- require strongkey
- reset on zero vc
- restrict anonymous
- root postexec

- root preexec
- root preexec close
- security
- security mask
- server schannel
- server signing
- server string
- set primary group script
- show add printer wizard
- shutdown script
- smb ports
- socket options
- store dgpackets
- store dos attributes
- strict allocate
- strict sync
- svcctl list
- sync always
- template homedir
- time offset
- token sid limit
- unix charset
- unix extensions
- use client driver
- use kerberos keytab
- use spnego
- username map
- valid users
- veto files
- veto oplock files
- vfs objects
- vms asv domain
- vms estimate file size
- vms file flush
- vms ofc time interval
- vms open file caching
- vms path names
- vms rms format
- volume
- winbind cache time
- winbind nested groups
- winbind offline logon
- winbind refresh tickets
- winbind trusted domains only
- winbind use default domain
- wins server
- wins support
- workgroup
- write list
- write raw

13.3 変更できない構成パラメータ

以下のパラメータはデフォルト値に設定されており，サーバーの正しい動作のためには変更すべきではありません。

- acl check permissions
- acl map full control
- announce as
- announce version
- auth methods
- block size
- blocking locks
- case sensitive

- default case
- default devmode
- defer sharing violations
- dos filetimes
- enable core files
- enable privileges
- encrypt passwords
- getwd cache
- hide dot files
- inherit acls
- locking
- mangle prefix
- mangled map
- mangled names
- mangling char
- mangling method
- max mux
- nt acl support
- nt pipe support
- nt status support
- paranoid server security
- password level
- posix locking
- preserve case
- printing
- printjob username
- root directory
- set directory
- share modes
- short preserve case
- strict locking
- template shell
- update encrypted
- username level
- winbind separator
- wins proxy

13.4 HP CIFS Server 固有の構成パラメータ

HP CIFS Server 固有の以下の構成パラメータがサポートされています。グローバル・パラメータは構成ファイルの [GLOBAL] セクションでのみ使用できるパラメータで，共有パラメータは [GLOBAL] セクションおよび共有セクションの両方で使用できます。

グローバル・パラメータ

- store dgpackets
- require strongkey
- token sid limit
- vms asv domain

共有パラメータ

- vms rms format
- vms path names
- inherit vms rms protections
- vms estimate file size
- vms open file caching
- vms ofc time interval
- vms file flush

13.5 サポートされていない構成パラメータ

以下の構成パラメータはサポートされていないため，使用できません。

- acl compatibility
- acl group control
- afs share
- afs token lifetime
- afs username map
- aio read size
- aio write behind
- aio write size
- change notify
- config file
- cups options
- cups server
- dfree cache time
- dfree command
- dmapi support
- dns proxy
- dos filemode
- dos filetime resolution
- ea support
- eventlog list
- fake directory create time
- force group
- force printername
- force user
- get quota command
- hide files
- hide special files
- hide unreadable
- homedir map
- inherit permissions
- iprint server
- kernel change notify
- kernel oplocks
- load printers
- log nt token command
- magic output
- magic script
- map acl inherit
- map archive
- map hidden
- map readonly
- map system
- max smbd processes
- max stat cache size
- NIS homedir
- obey pam restrictions
- open files database hash size
- os2 driver map
- pam password change
- panic action
- passdb expand explicit
- passwd chat
- passwd chat debug
- passwd chat timeout
- passwd program
- preload
- preload modules
- printcap cache time
- printcap name
- printer admin
- read bmpx
- set quota command
- smb passwd file
- socket address

- stat cache
- syslog
- syslog only
- time server
- unix password sync
- use mmap
- username
- username map script
- use sendfile
- usershare allow guests
- usershare max shares
- usershare owner only
- usershare path
- usershare prefix allow list
- usershare prefix deny list
- usershare template share
- wide links
- winbind enum groups
- winbind enum users
- winbind normalize names
- winbind nss info
- wins hook
- write cache size

付録A インストレーションと削除の実行例

ここでは，HP CIFS Server ソフトウェアのインストールと削除の実行例を示します。

A.1 OpenVMS Integrity システムでのインストール実行例

```
$ PRODUCT INSTAL SAMBA /DESTINATION=PIANO$DKA0:[CIFS]

Performing product kit validation of signed kits ...

The following product has been selected:
    HP I64VMS SAMBA V1.2-ECO1              Layered Product

Do you want to continue? [YES]

Configuration phase starting ...

You will be asked to choose options, if any, for each selected product and for
any products that may be installed to satisfy software dependency requirements.

Configuring HP I64VMS SAMBA V1.2-ECO1: HP OpenVMS CIFS

    © Copyright 2010 Hewlett-Packard Development Company, L.P.

    HP OpenVMS CIFS is released under the terms of GNU Public License.

    This installation procedure requires that all the following
    conditions are satisfied:

    1.  This procedure is running on an Alpha or an IA64 processor.
    2.  The system is running OpenVMS V8.3 or later on both Alpha and
        IA64 system.
    3.  All required privileges are currently enabled.
    4.  No CIFS images are running on this node or anywhere in
        the cluster that make use of common samba$root installation
        directory.

    This procedure checks if the conditions are satisfied.
    If they are satisfied, the procedure continues.
    If not, the procedure stops.
Do you want to continue? [YES]

Do you want the defaults for all options? [YES]

Do you want to review the options? [NO]

Execution phase starting ...

The following product will be installed to destination:
    HP I64VMS SAMBA V1.2-ECO1              DISK$I6483:[VMS$COMMON.]

Portion done: 0%...30%...40%...60%...90%

   User Accounts and User Identification Codes (UICs)
   --------------------------------------------------

    The HP OpenVMS CIFS V1.2-ECO1 installation creates five OpenVMS
    accounts: SAMBA$SMBD, SAMBA$NMBD, SAMBA$GUEST, SAMBA$TMPLT
    and CIFSADMIN. The default UIC group number for these new
    accounts depends on the following:

    o If you are installing the server for the first time, the
      default is the first unused UIC group number, starting
      with 360.

    o If any of these account already exists, then the default
      UIC group number will not be used to change the UIC of
      any existing accounts.
```

```
    For more information about UIC group numbers, see the
    OpenVMS System Manager's Manual.

Enter default UIC group number for CIFS accounts
Group: [362]
Creating OpenVMS accounts required by CIFS
Created account SAMBA$SMBD
Created account SAMBA$NMBD
Created account SAMBA$GUEST
Created account SAMBA$TMPLT
Created account CIFSADMIN

   The release notes for HP OpenVMS CIFS, CIFS_REL_NOTES.TXT
   is available at SYS$COMMON:[SYSHLP].

   In a cluster, on all the nodes that are going to use common
   samba$root installation directory as the current node, copy
   the following file to SYS$STARTUP directory of each node:

        SYS$STARTUP:SAMBA$DEFINE_ROOT.COM

   To automatically define SAMBA$ROOT logical during system
   startup, add the following line in SYS$MANAGER:SYLOGICALS.COM:

        $ @SYS$STARTUP:SAMBA$DEFINE_ROOT.COM

   To automatically start HP OpenVMS CIFS during system startup,
   add following line to the file SYS$MANAGER:SYSTARTUP_VMS.COM
   after TCPIP startup command procedure:

        $ @SYS$STARTUP:SAMBA$STARTUP.COM

Press Enter to continue:

   To Configure HP OpenVMS CIFS on any of the nodes in OpenVMS
   cluster that will share the common samba$root installation
   directory as the current node, execute:

        $ @SYS$STARTUP:SAMBA$DEFINE_ROOT.COM
        $ @SAMBA$ROOT:[BIN]SAMBA$CONFIG.COM
...100%

The following product has been installed:
    HP I64VMS SAMBA V1.2-ECO1              Layered Product
$
```

A.2 OpenVMS Integrity システムでの削除の実行例

```
$ PRODUCT REMOVE SAMBA

The following product has been selected:
    HP I64VMS SAMBA V1.2-ECO1              Layered Product

Do you want to continue? [YES]

The following product will be removed from destination:
    HP I64VMS SAMBA V1.2-ECO1              DISK$I6483:[VMS$COMMON.]

Portion done: 0%...10%

Cleaning up temporary TDB files before initiating
HP OpenVMS CIFS product removal...

  This utility will remove all CIFS configuration files.

Save CIFS configuration files? [y/n]: [n]
```

```
  Some portions of CIFS may be useful even after CIFS is
  removed.

Save utility tools? [y/n]: [n]

Do you want to save CIFS release notes? [y/n]: [y]

  Files are present in CIFS source code directory
  SAMBA$ROOT:[SRC].

Save files under CIFS source code directory? [y/n]: [n]

Deleting CIFS files...

Completed deleting CIFS files.

  SAMBA$REMOVE_CONFIG.COM is present in the directory:
  SYS$COMMON:[SYSUPD.SAMBA$SAFETY].

  In an OpenVMS cluster, copy this file to each of the nodes
  that share the common samba$root installation directory as
  this node and execute it to remove CIFS system specific
  configuration on each of them.

CIFS Installation, configuration and data files have
been removed from $1$DKA0:[SYS0.SYSCOMMON.SAMBA]

...20%...30%...40%...50%...60%...70%...80%...90%...100%

The following product has been removed:
    HP I64VMS SAMBA V1.2-ECO1              Layered Product
```

索引

ひ

ふ

ほ

り