

Advanced Server for UNIX

コンセプトとプランニング・ガイド

Part Number: AA-R9P9B-TE

2002 年 11 月

ソフトウェア・バージョン: Advanced Server for UNIX バージョン 5.1B
オペレーティング・システム: Tru64 UNIX バージョン 5.1A 以降

本書では、Advanced Server for UNIX (ASU) ソフトウェアのプランニングと管理の考え方について説明します。

日本ヒューレット・パッカード株式会社

© 2002 Hewlett-Packard Company

本書の著作権は日本ヒューレット・パッカード株式会社が保有しており、本書中の解説および図、表は日本ヒューレット・パッカードの文書による許可なしに、その全体または一部を、いかなる場合にも再版あるいは複製することを禁じます。

日本ヒューレット・パッカードは、弊社または弊社の指定する会社から納入された機器以外の機器で対象ソフトウェアを使用した場合、その性能あるいは信頼性について一切責任を負いかねます。

本書に記載されている事項は、予告なく変更されることがありますので、あらかじめご承知おきください。万一、本書の記述に誤りがあった場合でも、弊社は一切その責任を負いかねます。

本書で解説するソフトウェア(対象ソフトウェア)は、所定のライセンス契約が締結された場合に限り、その使用あるいは複製が許可されます。

COMPAQ, Compaq ロゴ, Digital ロゴは U.S. Patent and Trademark Office に登録されています。Alpha, AlphaServer, NonStop, TruCluster, および Tru64 は米国 Compaq Computer Corporation の商標です。

Microsoft, Windows および Windows NT は米国 Microsoft 社の登録商標です。Intel は米国 Intel 社の登録商標です。Motif, OSF/1, UNIX, The Open Group および X/Open は、The Open Group の米国ならびに他の国における商標です。

このドキュメントに記載されているその他の会社名および製品名は、各社の商標または登録商標です。

目次

まえがき

1 ASU の概要

1.1	ASU サーバの概要	1-1
1.2	ASU サーバ・プロセス・モデル	1-3
1.3	ASU サーバ・アーキテクチャ	1-4
1.4	ASU サーバ管理インタフェース	1-5
1.4.1	ASU コマンド	1-6
1.4.2	net コマンド	1-6
1.4.3	Tru64 UNIX コマンドおよび GUI	1-6
1.4.4	Windows GUI	1-7

2 Advanced Server ドメイン

2.1	ドメイン・ロール	2-1
2.2	共通ドメイン・モデル	2-2
2.2.1	保護ドメイン・モデル	2-3
2.2.1.1	シングル・マスタ・ドメイン・モデル	2-3
2.2.1.2	マルチ・マスタ・ドメイン・モデル	2-5
2.2.2	シングル・ドメイン・モデル	2-7
2.3	コンピュータ・アカウント	2-8
2.4	ドメインへのログイン	2-8
2.4.1	対話形式のログオン認証	2-9
2.4.2	リモート・ログオン認証	2-10
2.4.3	キャッシュされたログオン情報	2-11
2.5	ドメインの管理	2-11

2.5.1	ディレクトリ・データベースの同期化	2-11
2.5.1.1	ディレクトリ・データベースの変更	2-12
2.5.1.2	完全同期化および部分同期化	2-12
2.5.2	コントローラの昇格および降格	2-13
2.5.3	ドメインのセキュリティの原則の管理	2-14
2.5.3.1	ドメイン・ユーザ・アカウントの原則	2-15
2.5.3.2	監査の原則	2-17
2.5.4	信頼関係の管理	2-18
2.5.4.1	信頼関係の確立	2-18
2.5.4.2	ドメイン ユーザー マネージャの制限	2-19

3 ドメイン・ユーザ・アカウントおよびグループ

3.1	ドメイン・ユーザ・アカウント	3-1
3.1.1	ログオン時間の指定	3-4
3.1.2	ログオン・スクリプト	3-5
3.1.2.1	ログオン・スクリプトの作成	3-5
3.1.2.2	ログオン・スクリプトの割り当て	3-6
3.1.3	ホーム・ディレクトリ	3-6
3.1.3.1	ホーム・ディレクトリの割り当て	3-7
3.1.4	ユーザ・プロファイル	3-8
3.1.4.1	ユーザ・プロファイルの作成	3-9
3.1.4.2	プロファイルの割り当て	3-10
3.1.5	ユーザ権利の原則の管理	3-10
3.1.5.1	ユーザ権利の割り当て	3-12
3.1.6	ビルトイン・ドメイン・ユーザ・アカウント	3-12
3.1.6.1	ビルトイン Administrator ユーザ・アカウント	3-12
3.1.6.2	ビルトイン Guest ユーザ・アカウント	3-13
3.1.6.2.1	Guest アカウントの有効化	3-14
3.2	Tru64 UNIX ユーザ・アカウント	3-14

3.2.1	ドメイン・ユーザ・アカウントの Tru64 UNIX ユーザ・アカウントへの関連付け	3-15
3.3	ドメイン・ユーザ・アカウントのグループ化	3-15
3.3.1	ローカル・グループ	3-16
3.3.2	グローバル・グループ	3-18
3.3.3	特殊グループ	3-20
3.3.4	グループを使用するための方策	3-21
3.3.5	グループの管理	3-23
4	ディスク共有	
4.1	ディスク共有のアクセス権	4-1
4.1.1	Windows NT のアクセス権	4-3
4.1.2	Windows NTFS のアクセス権	4-4
4.1.3	Tru64 UNIX のアクセス許可	4-7
4.1.4	ディスク共有のアクセス権に関する考慮事項	4-7
4.2	ディレクトリの複製	4-8
4.2.1	ディレクトリの複製の概要	4-9
4.2.2	ディレクトリの複製の構成	4-10
4.2.3	エクスポート・サブディレクトリの管理	4-11
4.2.4	インポート・サブディレクトリの管理	4-12
4.2.5	ログオン・スクリプトの複製	4-13
4.2.6	ディレクトリの複製の使用	4-14
4.2.7	複製に関する問題解決のヒント	4-14
4.2.7.1	アクセスの拒否	4-15
4.2.7.2	特定のコンピュータへのエクスポート	4-15
4.2.7.3	インポート・ディレクトリのアクセス権の喪失	4-16
4.2.7.4	WAN 接続を経由したドメイン名への複製	4-16
4.3	ディスク共有の使用管理	4-16
4.3.1	共有からのユーザの切断	4-17

4.3.2	ユーザへのメッセージ送信	4-18
5	ASU プリンタ共有	
5.1	印刷の操作についての計画	5-1
5.1.1	プリンタの選択	5-2
5.1.2	プリント・サーバにするコンピュータの選択	5-3
5.1.3	プリンタ共有へユーザがアクセスする方法の計画	5-3
5.1.4	プリンタ・ドライバ	5-4
5.2	プリンタ共有のプロパティ	5-5
5.2.1	区切りページ	5-5
5.2.2	プリント・プロセッサ・スクリプトの使用	5-6
5.2.3	スケジュールとスプールの設定	5-7
5.2.4	プリンタ共有へのアクセスの制御	5-7
5.2.5	プリンタ共有の監査	5-8
5.2.6	独自の印刷フォーム	5-9
5.2.7	デバイス固有のプロパティの設定	5-9
5.2.7.1	プリンタ・メモリの設定	5-10
5.2.7.2	印刷フォームの使用	5-10
5.2.7.3	フォントの種類の選択	5-11
5.2.8	ドキュメントの省略時の設定	5-12
6	イベントの監視	
6.1	イベントビューアの概要	6-2
6.2	監査の有効化	6-2
6.3	イベントのログ・オプション	6-3
6.4	イベントの解釈	6-4
6.4.1	イベントのヘッダ	6-4
6.4.2	イベントの説明	6-5
6.5	イベントビューアの使用	6-6

6.5.1	ログの選択	6-6
6.5.2	コンピュータの選択	6-7
6.5.3	表示の更新	6-7
6.5.4	フォントの変更	6-8
6.5.5	ログ・ファイルの保存	6-8
6.5.6	特定のイベントの表示	6-10
6.5.6.1	イベントの詳しい情報の表示	6-10
6.5.6.2	イベントのソート	6-10
6.5.6.3	イベントの選別	6-11
6.5.6.4	イベントの検索	6-12
6.6	イベント・ログによる問題解決	6-12

索引

図

1-1	ASU プロセス・モデル	1-4
1-2	ASU ネットワーク・アーキテクチャ	1-5
2-1	シングル・マスタ・ドメイン・モデル	2-4
2-2	マルチ・マスタ・ドメイン・モデル	2-6

表

1-1	ASU サービス	1-2
2-1	ドメイン・ユーザ・アカウントの原則のオプション	2-15
2-2	監査イベント	2-17
3-1	ドメイン・ユーザ・アカウントの要素	3-2
3-2	ドメイン・ユーザ・アカウントのパスワードのオプション ...	3-3
3-3	ログオン・スクリプトのパラメータ	3-6
3-4	ユーザ権利	3-11
3-5	ローカル・グループ	3-16

3-6	ビルトイン・ローカル・グループ	3-18
3-7	グローバル・グループ	3-19
3-8	特殊グループ	3-21
3-9	グループのガイドライン	3-23
4-1	Windows NT のアクセス権	4-3
4-2	NTFS の標準アクセス権	4-5
4-3	NTFS の個別アクセス権	4-5
4-4	ディスク共有の使用	4-16
5-1	サポートしていない印刷装置	5-5
5-2	プリント・プロセッサ・スクリプトの環境変数	5-6
5-3	スケジュールのオプション	5-7
5-4	プリンタ共有のアクセス権	5-8
5-5	プリンタ共有の監査オプション	5-9
5-6	一般的な設定	5-12
6-1	ディレクトリとファイルの監査	6-3
6-2	イベントのログ・オプション	6-4
6-3	イベントのヘッダ	6-5
6-4	イベントの種類	6-6
6-5	イベント・フィルタ	6-11

まえがき

本書では、Advanced Server for UNIX (ASU) ソフトウェアの計画および運用管理に関連するコンセプトについて説明しています。

対象読者

本書は、ASU ソフトウェアの設計、インストール、構成、および管理を行うすべてのユーザを対象としています。

本書の構成

本書の構成は、次のとおりです。

第 1 章	ASU ソフトウェアについて説明します。
第 2 章	ASU ドメイン環境について説明します。
第 3 章	ドメイン・ユーザ・アカウントおよびグループについて説明します。
第 4 章	ASU サーバで Tru64 UNIX ベースのファイル・システムを共有する方法について説明します。
第 5 章	ASU サーバで Tru64 UNIX ベースのプリンタを共有する方法について説明します。
第 6 章	ASU サーバを監視する方法について説明します。

関連資料

ASU ソフトウェアについては、次のマニュアルに詳しい説明があります。

- 『Advanced Server for UNIX インストレーション/管理ガイド』では、ASU ソフトウェアをインストール、構成、管理する方法について説明しています。
- 『Advanced Server for UNIX リリース・ノート』では、ASU ソフトウェアについて、最新情報を記載しています。

本書で使用する表記法

本書では、次の表記法を使用しています。

%

\$

パーセント記号は、C シェルのシステム・プロンプトを表します。ドル記号は、Bourne シェル、Korn シェル、および POSIX シェルの場合のシステム・プロンプトを表します。

#

番号記号は root としてログインした場合のシステム・プロンプトを表します。

file

イタリック体 (斜体) は、変数値、プレースホルダ、および関数の引数名を示します。

[|]

{ | }

構文定義では、大カッコはオプションの項目を示し、中カッコは必須項目を示します。大カッコまたは中カッコの中の項目を縦線で区切っている場合は、そこに併記されている項目の中から 1 つの項目を選択することを示します。

...

構文定義では、水平の反復記号は、前の項目を 1 回以上繰り返して使用できることを示します。

cat(1)

リファレンス・ページの参照には、該当するセクション番号をカッコ内に示します。たとえば、cat(1) は、cat コマンドについての情報が、リファレンス・ページのセクション 1 に記載されていることを示します。

Return

四角で囲まれたキー名はユーザがそのキーを押すことを示します。

Ctrl/x

この記号は、スラッシュの前に指定されているキーを押しながら、スラッシュの後のキーまたはマウス・ボタンを押すことを示します。例中では、この

ようなキーの組み合わせは、四角あるいは大カッコで囲まれて示されます(たとえば、`Ctrl/C`)。



ASU の概要

Advanced Server for UNIX (ASU) ソフトウェアは、Windows ユーザが UNIX ベースのファイル・システムとプリンタを共有として利用できるようにする、Tru64 UNIX のレイヤード・アプリケーションです。Windows ユーザは、ソフトウェアを変更しなくても共有に接続できます。一度接続すると、共有に関連付けられているファイル・システムとプリンタは、Windows ユーザのローカル・コンピューティング環境からは透過的な拡張のように見えます。

この章では、次の項目について説明します。

- ASU サーバ
- ASU サーバ・プロセス・モデル
- ASU サーバ・アーキテクチャ
- ASU サーバ管理インタフェース

1.1 ASU サーバの概要

システム上で ASU ソフトウェアをインストール、構成、および実行すると、それらのシステムは ASU サーバとして構成されます。ASU サーバは、Windows ユーザに対し、UNIX ファイル・システムにはディスク共有としてアクセスし、プリンタにはプリンタ共有としてアクセスする機能を提供します。

ASU サーバは、Windows NT セキュリティ・モデルだけで、または Tru64 UNIX セキュリティ・モデルと Windows NT セキュリティ・モデルを組み合わせでサポートすることにより、ディスクおよびプリンタ共有に柔軟性のあるセキュリティ機能を提供します。省略時の設定では、ASU サーバは両セキュリティ・モデルを組み合わせで使用します。このセキュリティ・モデルでは、Windows ユーザは次に示すユーザ・アカウントを持つ必要があります。

- ユーザが作成するドメイン・ユーザ・アカウント。ASU サーバは、このアカウントを使って Windows NT セキュリティを実現します。

- ドメイン・ユーザ・アカウントを作成する際に自動的に作成される Tru64 UNIX ユーザ・アカウント。Tru64 UNIX オペレーティング・システム・ソフトウェアでは、このアカウントを使って、Tru64 UNIX セキュリティ・ポリシを実現します。

ASU サーバは、プリエンブティブ・マルチタスキング、シンメトリック・マルチプロセッシングおよびタイムシェアリングなど、Tru64 UNIX オペレーティング・システムの諸機能との間での相互運用を提供します。Tru64 UNIX オペレーティング・システム・ソフトウェアと相互にやりとりする方法は、ASU レジストリと呼ばれるデータベースに格納されている値エントリに割り当てられている値によって決まります。

ASU サーバを、Windows ドメインで、プライマリ・ドメイン・コントローラ (PDC)、バックアップ・ドメイン・コントローラ (BDC) またはメンバーサーバとして構成すると、表 1-1 に示す、Windows NT Advanced Server Version 4.0 のサービスを、Windows ユーザ、クライアントおよびサーバに対して提供します。

表 1-1: ASU サービス

サービス	説明
Alerter	使用中のコンピュータで発生した管理上の警告について、指定したユーザおよびコンピュータに通知するために、ASU サーバおよび他の ASU サービスによって使用される。
Browser	ドメインにあるコントローラの最新リストを維持管理し、要求があればリストを提供する。
EventLog	システム、セキュリティ、およびアプリケーション・イベントをイベント・ログに記録し、これらのログにリモート・アクセスできるようにする。
NetLogon	ドメインまたは ASU サーバにログインするユーザのドメイン・ユーザ名とパスワードを確認する。
Netrun	ユーザが、ワークステーションからサーバ上の UNIX システム・アプリケーションを実行できるようにする。
Replicator	ディレクトリやディレクトリ内のファイルを他のワークステーションに複製する。

表 1-1: ASU サービス (続き)

サービス	説明
Server	ファイル、プリント、名前付きパイプを共有できるようにし、リモート・プロシージャ・コールをサポートする。
TimeSource	ドメインのタイム・ソースとしてコントローラを識別する。他のコントローラは、クロックをタイム・サーバに同期させる。

1.2 ASU サーバ・プロセス・モデル

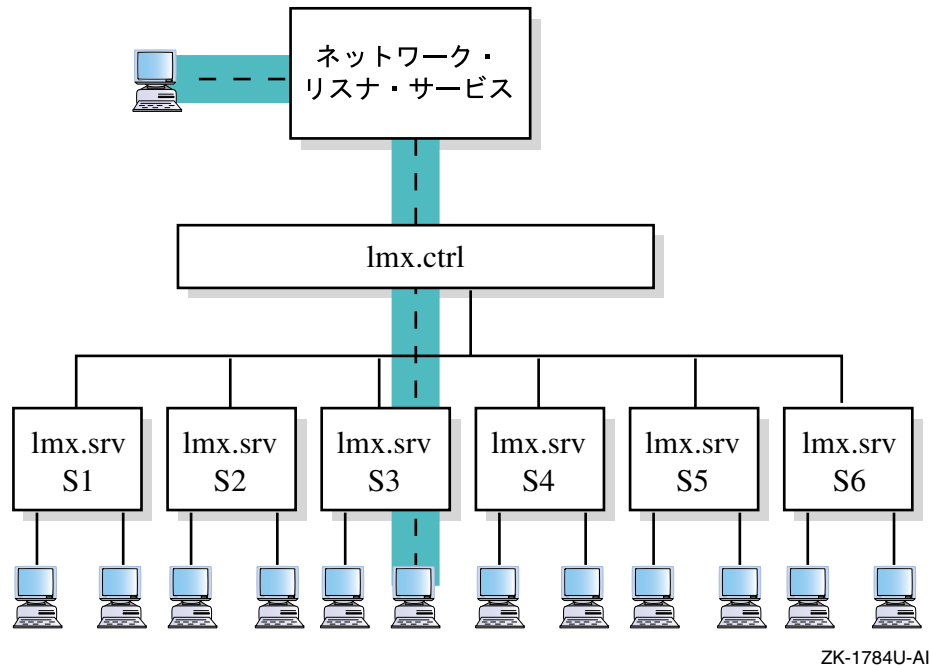
ASU サーバおよびクライアント・ワークステーションは、Microsoft Windows および OS/2 オペレーティング・システムのネイティブのファイル共有プロトコルであるサーバ・メッセージ・ブロック (SMB) プロトコルを使って通信します。

クライアントは、ASU サーバに SMB 要求を送信します。SMB を受信すると、ASU サーバは、リクエストを等価な Tru64 UNIX システムのセマンティクスにマップし、クライアントの意図を解釈し、Tru64 UNIX システム機能を実行して、クライアントの要求に応えます。トランスポートやハードウェアなどのネットワーク・アーキテクチャの各層によって、信頼性の高い SMB のやりとりが保証されます。

ASU サーバは、協調して動作するシステム・プロセスを組み合わせたものです。lmx.ctrl プロセスは、ASU の マスタ制御プロセスであり、必ず実行されていなければなりません。UNIX ネットワーク・リスナ・サービスは、新しい ASU クライアント接続要求またはセッションを lmx.ctrl プロセスに渡します。lmx.ctrl プロセスは、新しいクライアント・セッションを受け付け、それを lmx.srv プロセスに割り当てます。lmx.srv プロセスが、実際にクライアントのニーズに合ったサービスを提供します。

図 1-1 は、ネットワーク・リスナ・サービス、lmx.ctrl プロセス、lmx.srv プロセス、およびクライアントとの関係について示しています。

図 1-1: ASU プロセス・モデル



起動される `lmx.srv` プロセスの数は、クライアント・セッションの数によって異なります。ASU プロセス・モデルでは、複数のクライアント・セッションが 1 つの `lmx.srv` プロセスで処理できるようになっています。`lmx.ctrl` プロセスは、新しいクライアント・セッションを既存の `lmx.srv` プロセスでサービスするか、または新しい `lmx.srv` プロセスを起動するかを判断します。このようにクライアント・セッションを `lmx.srv` プロセスに割り振ることによって、複数のクライアントの要求が一度に処理できます。

1.3 ASU サーバ・アーキテクチャ

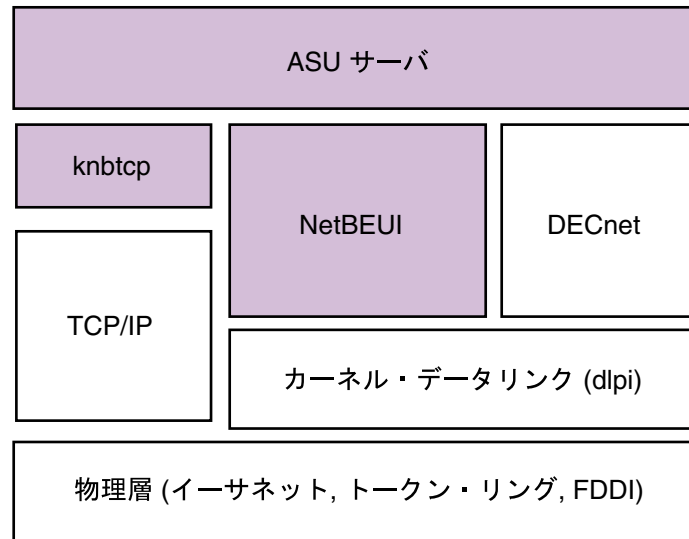
ASU サーバは、Tru64 UNIX オペレーティング・システム・ソフトウェアでサポートされる、イーサネット、FDDI、またはトークン・リング・ネットワーク・アダプタ上で NetBIOS プロトコルを使用して、ネットワークに SMB を送信します。NetBIOS プロトコルは、ネットワーク上にあるワークステーションの論理名の確立、ネットワーク上にあるワークステーションの論理名間でのセッションの確立、およびそれらの間における、信頼性の高いデータ転送のサポートを担当します。

ASU ソフトウェアでは、次のトランスポート機能に対して、NetBIOS プロトコルを提供するとともに使用します。

- ローカルおよびワイド・エリア・ネットワーキング用にシステムに実装されている TCP/IP トランスポート・ソフトウェアで使用する NetBIOS over TCP/IP (knbtcp)
- ローカル・エリア・ネットワーキングだけで使用される NetBEUI トランスポート

図 1-2 に、ASU アーキテクチャを示します。網掛け部分の構成要素は、ASU ソフトウェアから提供されます。

図 1-2: ASU ネットワーク・アーキテクチャ



ZK-1785U-AI

1.4 ASU サーバ管理インタフェース

ASU ソフトウェアの管理には、次のものが利用できます。

- ASU コマンド
- net コマンド
- Tru64 UNIX コマンドおよびグラフィカル・ユーザ・インタフェース (GUI)
- Windows GUI

注意

Windows 2000 ドメインで ASU サーバを構成する場合は、Windows 2000 インタフェースを使って ASU サーバを管理する必要があります。

1.4.1 ASU コマンド

ASU コマンドは Tru64 UNIX 形式のコマンドであり、ASU サーバおよびドメインに関する情報の表示、管理、および問題の対処を行うときに使用します。ASU ソフトウェアを実行しているシステム上で、Tru64 UNIX コマンド・プロンプトに対して ASU コマンドを小文字で入力します。ASU コマンドについての詳細は、『*Advanced Server for UNIX* インストレーション/管理ガイド』を参照してください。

1.4.2 net コマンド

net コマンドは Windows 形式のコマンドであり、ASU サーバの情報表示や、共有、ドメイン・ユーザ・アカウント、グループの作成および管理を行う際に使用します。

net コマンドを入力するときは、net の後にキーワードとオプションを指定します。ASU ソフトウェアを実行しているシステム上で、コマンド・プロンプトに対して次の形式で net コマンドを小文字で入力します。

```
# net keyword [/option]
```

net コマンドについての詳細は、『*Advanced Server for UNIX* インストレーション/管理ガイド』を参照してください。

1.4.3 Tru64 UNIX コマンドおよび GUI

Tru64 UNIX のユーザ・コマンドとファイル・システム・コマンドおよび GUI を使用すれば、追加の ASU 関連オプションを指定して、共有およびドメイン・ユーザ・アカウントの作成と管理を行うことができます。Tru64 UNIX コマンドと GUI を使用して ASU サーバを管理する方法については、『システム管理ガイド』を参照してください。

1.4.4 Windows GUI

次の Windows ベースの GUI を使用して、ASU サーバおよびドメインを管理できます。

- サーバー マネージャは、共有に関する情報の表示や、共有の作成および管理を行います。
- ドメイン ユーザー マネージャは、ドメイン・ユーザ・アカウントおよびグループに関する情報の表示や、ドメイン・ユーザ・アカウントおよびグループの作成と管理を行います。
- ポリシー エディタは、ASU レジストリに関する情報の表示や、ASU レジストリの管理を行います。
- イベント ビューアは、ASU 関連アプリケーション、セキュリティ、およびシステム・イベントを表示します。

Windows NT Server Version 4.0 および Windows 2000 Server で提供される Windows バージョンの GUI を使用して ASU サーバを管理することができます。別のタイプの Windows オペレーティング・システム・ソフトウェアを実行しているシステムについては、ASU ソフトウェアが提供する Windows バージョンの GUI をインストールする必要があります。Windows ベースの GUI のインストールについての詳細は、『*Advanced Server for UNIX* インストールレーション/管理ガイド』を参照してください。



Advanced Server ドメイン

各 ASU サーバは、Windows ドメインに属し、そのドメイン内で役割を果たします。Windows ドメインとは、ドメイン内のすべてのセキュリティ、ユーザ・アカウント、およびグループ情報が格納されている共通のディレクトリ・データベースを共有する Advanced Server のグループをいいます。Advanced Server には、ASU サーバ、Windows NT サーバまたは Windows 2000 サーバが使用できます。このディレクトリ・データベースは、他の Advanced Server および Windows NT のマニュアルでは、セキュリティ・アカウント・マネージャ (SAM) データベースと呼ぶことがあります。

この章では、次の項目について説明します。

- ドメイン・ロール
- 共通のドメイン・モデル
- コンピュータ・アカウント
- ドメインへのログイン
- ドメインの管理

ASU ソフトウェアをインストールする方法およびドメインに ASU サーバを構成する方法については、『*Advanced Server for UNIX* インストール／管理ガイド』を参照してください。

2.1 ドメイン・ロール

Advanced Server のドメイン・ロールは、どの Advanced Server がディレクトリ・データベースを維持管理し、どの Advanced Server がディレクトリ・データベースのコピーを受け取るかを決定します。各 Advanced Server は、ドメイン内で次のいずれかの役割を果たしています。

- プライマリ・ドメイン・コントローラ (PDC)

PDC は、ディレクトリ・データベースの格納と維持管理およびドメイン・ユーザのログイン要求の認証を行います。Advanced Server を PDC

として構成することにより、ドメインを作成します。PDC は各ドメインに 1 つだけ構成できます。

Windows 2000 ドメインでは ASU サーバを PDC として構成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・ユーザのログオン要求を認証するためにディレクトリ・データベースのコピーを受け取ります。このコピーは、一定の間隔で自動的に PDC と同期がとられます。BDC は 1 つのドメインに複数存在することができます。

Windows 2000 Server が混在モード用に構成されている場合に限り、ASU サーバを Windows 2000 Server ドメイン内に BDC として構成することができます。

- メンバ・サーバ

メンバ・サーバは、自分のローカル・ユーザ・アカウントのデータベースを維持管理し、ディレクトリ・データベースのコピーは受け取りません。したがって、ドメインのログイン要求は処理しません。メンバ・サーバは、ドメイン内で共有資源の提供に加わることができます。ただし、ユーザは、メンバ・サーバ上またはメンバ・サーバが信頼するドメイン内にユーザ・アカウントを持っている必要があります。信頼についての詳細は、2.2 節で説明しています。メンバ・サーバは 1 つのドメインに複数存在することができます。

Windows 2000 Server が混在モードまたはネイティブ・モード用に構成されている場合、ASU サーバを Windows 2000 Server ドメイン内にメンバ・サーバとして構成できます。

2.2 共通ドメイン・モデル

ドメインを適切に設計して構成すると、ネットワーク管理を簡略化できると同時に、ユーザがネットワーク全体の共有に接続できるようになります。ドメイン・モデルには次の 2 つのタイプがあります。

- 保護ドメイン・モデル

このドメイン・モデルでは、Advanced Server が複数のドメインで構成され、そのドメインが信頼関係を確立しています。信頼関係により、信頼する側のドメインは、信頼される側のドメイン内で認証されたユー

ザを信頼できるので、信頼される側のドメインのユーザは、共有へアクセスできるようになります。

- シングル・ドメイン・モデル

このモデルでは、各 Advanced Server は 1 つのドメインで構成されています。

2.2.1 保護ドメイン・モデル

信頼関係には次の 2 種類があります。

- 一方向の信頼関係 — 一方のドメインがもう一方のドメインを信頼する場合です。
- 双方向の信頼関係 — 2 つ以上のドメインが相互に信頼する場合です。

保護ドメイン・モデルには次の 2 種類があります。

- シングル・マスタ・ドメイン・モデル — 少数のユーザを持つ環境に適しています。
- マルチ・マスタ・ドメイン・モデル — 多数のユーザを持つ環境に適しています。

これらの各ドメイン・モデルでは、次の 2 種類のドメインを作成できます。

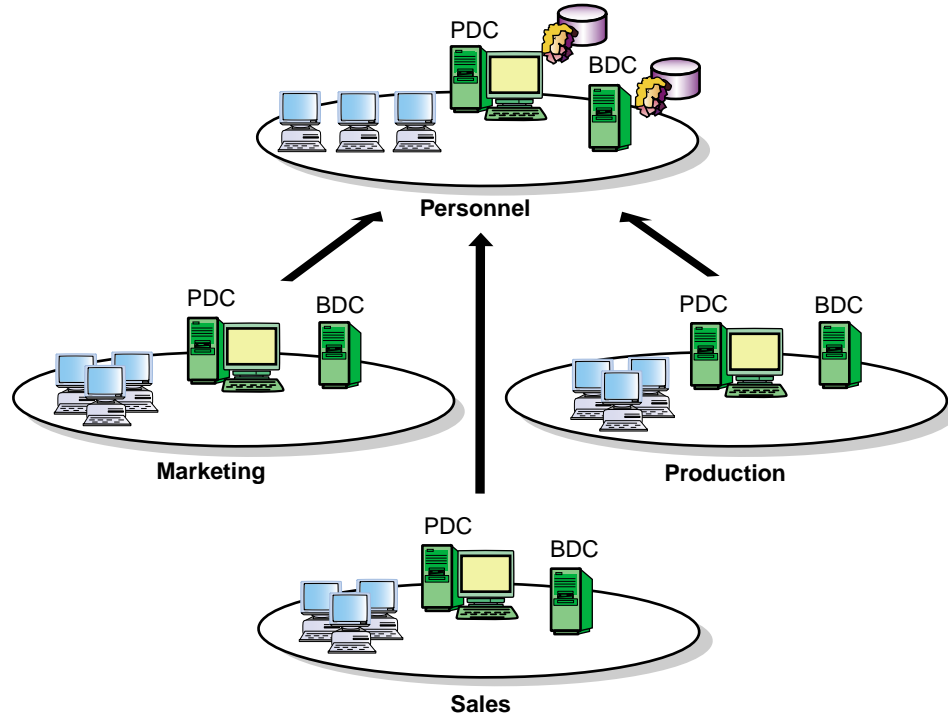
- マスタ・ドメイン — このドメインには、ドメイン・ユーザ・アカウントを作成します。
- 資源ドメイン — このドメインには、ディスク共有とプリンタ共有を作成します。

資源ドメインからマスタ・ドメインへの一方向の信頼関係を作成します。ユーザはマスタ・ドメインにログオンすると、一方向の信頼関係があるため、アクセスが許可されたリソース・ドメイン内にある、すべてのディスク共有およびプリンタ共有にアクセスできます。

2.2.1.1 シングル・マスタ・ドメイン・モデル

図 2-1 はシングル・マスタ・ドメイン・モデルで、すべてのユーザ・アカウントが Personnel (人事部) というマスタ・ドメイン内に作成されています。すべての共有は、Marketing (マーケティング部)、Sales (販売部)、および Production (製造部) という資源ドメイン内に作成されています。

図 2-1: シングル・マスタ・ドメイン・モデル



ZK-1782U-AI

すべてのドメイン・ユーザ・アカウントがマスタ・ドメインにあり、各資源ドメインはマスタ・ドメインを信頼するので、すべてのユーザ・アカウントはアクセスが許可された、どの資源ドメイン内の共有も使用できます。

シングル・マスタ・ドメイン・モデルには、次の機能があります。

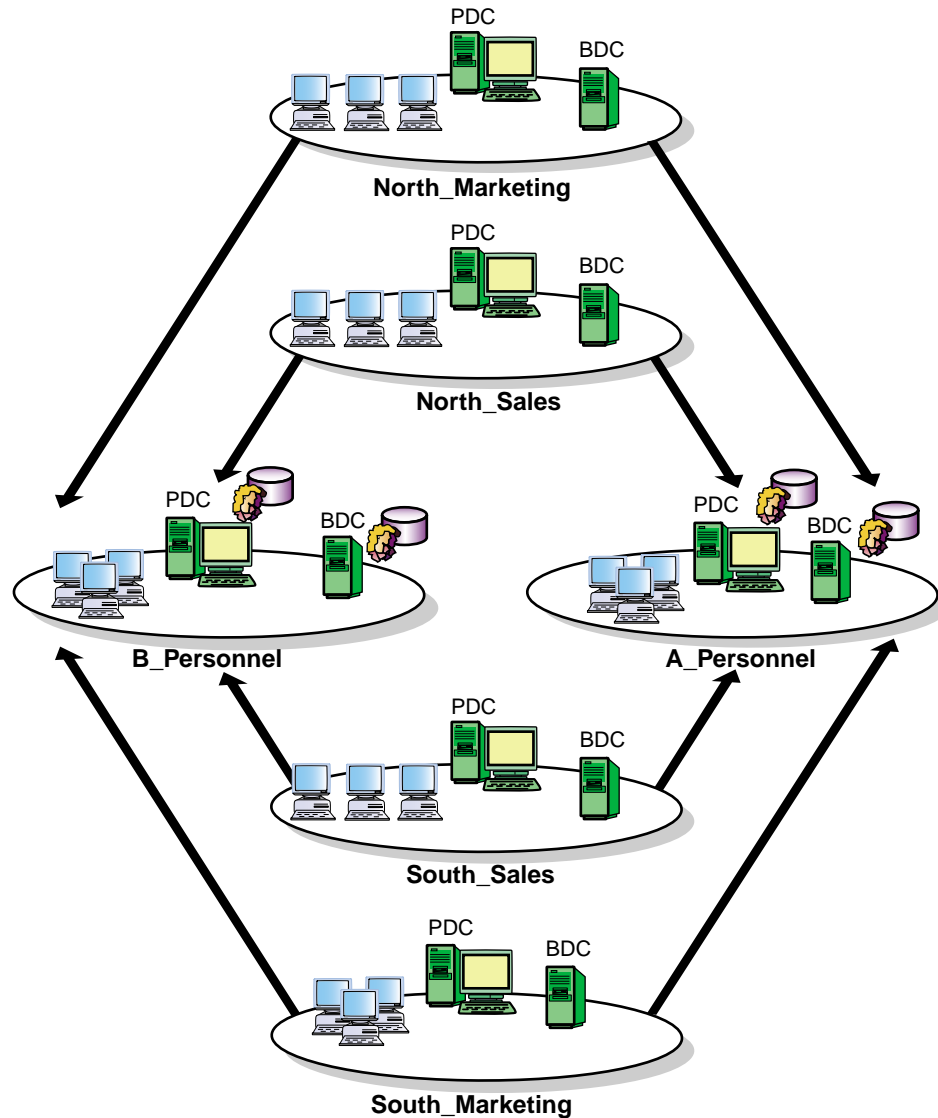
- ドメイン・ユーザ・アカウントの集中管理。1つのドメインにすべてのドメイン・ユーザ・アカウントを作成し、ドメイン間に一方向の信頼関係を確立することで、ユーザ・アカウントの管理を集約し、ユーザ・アカウント・データベースを個別に管理する手間を省くことができます。その結果、ユーザはどのドメインの共有も1つのドメイン・ユーザ・アカウントだけで使用できるようになります。
- 資源の分散管理 (ローカルでのシステム管理機能)。各部門のドメインで、その部門の資源を管理する独自の管理者を設けることができます。
- ローカル・ドメインに対応させて、資源を論理的にグループ化することができます。

2.2.1.2 マルチ・マスタ・ドメイン・モデル

マルチ・マスタ・ドメイン・モデルではシングル・ドメイン・モデルと同様に、マスタ・ドメインにドメイン・ユーザ・アカウントを作成し、資源ドメインには共有を作成します。このモデルでは、名前が示すように、複数のマスタ・ドメインが作成されます。

図 2-2 は、すべてのドメイン・ユーザ・アカウントが A_Personnel および B_Personnel という 2 つのマスタ・ドメインに作成されたマルチ・マスタ・ドメイン・モデルを示しています。すべての共有は、South_Sales, South_Marketing, North_Sales, および North_Marketing という資源ドメインに作成されています。

図 2-2: マルチ・マスタ・ドメイン・モデル



ZK-1783U-AI

ドメイン・ユーザ・アカウントがいずれかのマスタ・ドメインにあり、資源ドメインがこのマスタ・ドメインを信頼するので、すべてのユーザ・アカウントはアクセスが許可されたすべての資源ドメイン内の資源を使用することができます。

マルチ・マスタ・ドメイン・モデルは、シングル・マスタ・ドメイン・モデルのすべての機能を組み込み、さらに次のような機能にも対応しています。

- どのようなユーザ数のネットワークにもスケーラブルに対応可能。
- ユーザはネットワーク上のどこからでもログオン可能。
- 集中管理または分散管理を提供。

2.2.2 シングル・ドメイン・モデル

ドメイン・ユーザ・アカウントと共有が同じドメインに作成されているドメイン・モデルを作成できます。つまり、ドメイン・ユーザ・アカウントと共有が同じドメイン内にあるため、信頼関係を確立する必要がない、ということです。ドメイン・ユーザが他のドメインにある共有にアクセスする必要がある場合には、各ドメインで同じユーザ名およびパスワードを持つドメイン・ユーザを作成します。ユーザ名とパスワードが一致すると、ユーザがログオンしているドメインに関係なくアクセス権が与えられます。

この規則の例外は、信頼関係が成立している場合です。2つのドメイン間で信頼関係が確立されている場合、たとえ両方の名前とパスワードがそれぞれ同じであっても、信頼する側のドメインは、信頼される側のドメインにあるユーザと、ローカル・ドメインにあるユーザとを区別できます。

3つのドメイン (Athens, Berlin, Cairo) があるとします。各ドメインに同じパスワードを持つユーザ・アカウント、Peter があります。Athens ドメインは Berlin ドメインを信頼していますが、これ以外の信頼関係は確立されていません。下表は、Peter が各ドメインにログオンしたときの様子を示しています。

ログオンしたドメイン	アクセス可能なドメイン	アクセス不可能なドメイン
Athens	Athens, Berlin, Cairo	
Berlin	Berlin, Cairo	Athens
Cairo	Athens, Berlin, Cairo	

Athens と Berlin 間の信頼関係が各ドメインへのアクセスを制限しているように見えます。実際、信頼関係のおかげでアクセスの制御が容易になっています。Athens ドメインは現在、ユーザ Athens¥Peter とユーザ Berlin¥Peter とを区別できるため、それに応じてアクセス権を与えることができます。

2.3 コンピュータ・アカウント

コンピュータ・アカウントは、ドメインに参加する各 BDC に対してディレクトリ・データベース内に自動的に作成されます。コンピュータ・アカウントは、安全な通信セッションを確立するために使用されます。

安全な通信セッションが確立されるのは、ある接続で通信しているシステムが、相手コンピュータが自分自身を正しく識別したことを確認したときです。システムは自分のコンピュータ・アカウントを使って自分を確認します。安全な通信セッションが確立されると、2 台のコンピュータ間でセッションが開始されます。

安全な通信セッションでは、次のようなことが行われます。

- BDC は PDC と安全な通信セッションを確立して、マスタ・ディレクトリ・データベースのコピーと更新を受け取ります。
- 信頼する側のドメインにある PDC と BDC は、安全な通信セッションを確立して、信頼される側の PDC にユーザ認証情報を渡します。
- ドメイン内のメンバ・サーバとして動作している Windows NT Workstation または Windows NT Server システムは、ドメイン内の PDC または BDC と安全な通信セッションを確立して、ユーザ認証情報を渡します。

2.4 ドメインへのログイン

ドメインにログインするには、ユーザはドメイン内または信頼される側のドメインにドメイン・ユーザ・アカウントを持っていなければなりません。管理者は、ユーザ名とパスワードをアカウントに割り当て、ユーザ識別データを指定し、ドメインにユーザの権利を定義することで、ドメイン・ユーザ・アカウントを作成します。Advanced Server は次に、一意のセキュリティ識別子 (SID) を新しいアカウントに割り当てます。ドメイン・ユーザ・アカウントの作成についての詳細は、第 3 章を参照してください。

ユーザは、次の方法でドメインにログオンできます。

- ユーザがコンピュータのオペレーティング・システムから表示される [ログオン情報] ダイアログ・ボックスに情報を入力すると、対話形式のログオンが行われます。ユーザは、ユーザ・アカウントがどこで定義されているかに応じて、ドメインの名前、またはログオンに使用しているコンピュータ名を [ドメイン] ボックスで選択します。

- すでにユーザがドメインにログオンしていて、別のコンピュータにネットワーク接続するときは、リモート・ログオンします。たとえば、ユーザが [ネットワーク ドライブの割り当て] ダイアログ・ボックスを使用して別のコンピュータに接続する場合などがあります。

Windows コンピュータのユーザがドメインにログインしようとする、コンピュータ上の NetLogon は、ユーザを認証できるドメイン・コントローラ上の NetLogon サービスとの間で安全な通信チャネルを探して確立します。ASU サーバが起動すると、NetLogon サービスは自動的に開始します。これらの安全な通信チャネルは、コンピュータの NetLogon サービス間でユーザ識別データを交換するのに使用されます。PDC と BDC 上の NetLogon サービスも同様に、すべての信頼される側のドメインで探そうとします。ユーザを認証できるドメイン・コントローラが見つかり、そのドメイン・コントローラが以降のユーザ・アカウント認証に使用されます。

2.4.1 対話形式のログオン認証

ユーザのローカル・システム上で、[ログオン情報] ダイアログ・ボックスから、ユーザ名、パスワード、およびドメイン名またはコンピュータ名を入力するよう要求されます。

ユーザは、[ユーザー名] フィールドおよび [パスワード] フィールドにそれぞれユーザ名とパスワードを入力します。ユーザは、ドメイン・リストからドメインまたはコンピュータ名を選択します。ドメイン・リストの内容は、コンピュータがドメインに参加しているかどうかによって異なります。リストの内容は次のようになります。

- ワークグループのメンバとして参加している場合は、リストにはローカルのコンピュータ名が含まれる。
- ドメインに参加している場合は、リストにはコンピュータ名およびユーザ・アカウントが認証できる、すべてのドメイン (信頼される側のドメインを含む) が含まれる。

ローカルのコンピュータにログオンするときには、ユーザはローカルのコンピュータ名を選択します。コンピュータは、ローカルのディレクトリ・データベースをチェックして、指定したユーザ名およびパスワードの有無を調べます。一致する場合、ログオンは許可されます。一致しない場合には、ログオンは失敗します。

ドメインにログインするには、ユーザはドメイン名を選択します。コンピュータはドメイン名、ユーザ名、およびパスワードを、選択したドメインのドメイン・コントローラに送信します。ドメイン・コントローラはドメイン名をチェックし、次に、ユーザ名とパスワードをドメインのディレクトリ・データベースと照合して、要求を次のように処理します。

- ドメイン名が正しく、ユーザ名とパスワードがディレクトリ・データベースにあるエントリと一致する場合には、ドメイン・コントローラはログオンが許可されたことをコンピュータに通知します。
- ドメイン名が信頼される側のドメインと認識されると、ドメイン・コントローラは認証のため、ユーザ名とパスワード情報を信頼される側のドメイン・コントローラに渡します。信頼される側のドメイン・コントローラがそのアカウントを認証すると、ログオン情報は最初のドメイン・コントローラに送り返されて、ユーザはログオンできます。アカウントが認証されない(すなわち信頼される側のドメインのディレクトリ・データベースに定義されていない)場合には、ログオンは失敗します。
- ドメイン・コントローラがドメイン名を認識しないか、ユーザに対するエントリがディレクトリ・データベースに存在しない場合には、ログオンは失敗します。

2.4.2 リモート・ログオン認証

コンピュータまたはドメインにすでにログオンしているユーザが別のコンピュータにネットワーク接続を行う場合、リモート・ログオンが行われます。ユーザが [ネットワーク ドライブの割り当て] ダイアログ・ボックスの [名前を指定して接続] ボックスに別のドメイン名またはコンピュータ名およびユーザ名を入力してアカウント情報を上書きして無効にしない限り、対話形式のログオンで使用されたアカウント情報がリモート・ログオンでも使用されます。

ユーザが、ドメイン・ユーザ・アカウントが定義されているドメインにあるコンピュータとネットワーク接続を行う場合、ログオンはユーザがリモート・コンピュータ上のアカウントを使用して接続しているのと同じように進行します。リモート・コンピュータは、ログオン・クレデンシャルをそのディレクトリ・データベースと照合して認証します。アカウントがディレクトリ・データベースに定義されていない場合でも、パスワードなしの Guest アカウントが有効になっている場合には、ユーザは Guest 特権でログオンし

ます。Guest アカウントが有効でない場合、ログオンは失敗します。Guest アカウントについての詳細は、第 3 章を参照してください。

別のユーザと区別するためにドメイン・ユーザ・アカウントを作成していた場合は、ドメイン ユーザー マネージャなどの管理画面上では、ユーザ名の前にドメイン名を付けることをお勧めします。たとえば、Sales ドメインのユーザ JohnL は、Sales¥JohnL として表します。この名前により、Engineering¥JohnL など別のドメインにいる別の JohnL と区別できます。

2.4.3 キャッシュされたログオン情報

ユーザがある特定のコンピュータから初めてドメイン・アカウントにログオンすると、ドメイン・コントローラは、認証済みのログオン情報を(ディレクトリ・データベースから)コンピュータにダウンロードします。このダウンロード情報は、コンピュータのキャッシュに書き込まれます。以降のログオンでは、ドメイン・コントローラが利用できないとき、ユーザはキャッシュに書き込まれたログオン情報を使用してドメインにログオンできます。

Windows NT Server および Windows NT Workstation が動作しているコンピュータでは、対話形式でログオンした最近のユーザ(省略時の設定では 10 人)を認証するために使用した情報が格納されます。ローカル・コンピュータにログオンするユーザのアカウント情報も、そのコンピュータのローカルなディレクトリ・データベースに格納されます。

2.5 ドメインの管理

ドメインの管理には次の処理が含まれます。

- PDC と BDC 間のディレクトリ・データベースの同期化
- コントローラの昇格と降格
- ドメイン・アカウントの原則と監査の原則の管理
- 信頼関係の管理

2.5.1 ディレクトリ・データベースの同期化

PDC は自動的に、一定の間隔で BDC に対し PDC からのディレクトリ・データベースの変更内容を要求するように通知を送信します。この通知時間はずらしてあるため、すべての BDC は必ずしも同時に変更内容を要求するわけではありません。BDC が変更内容を要求する場合、BDC が最後に受

け取った変更内容を PDC に通知します。このため、PDC はどの BDC が変更を必要としているかを常に把握しています。BDC が最新である場合には、BDC は変更を要求しません。

2.5.1.1 ディレクトリ・データベースの変更

ディレクトリ・データベースの変更には、新規パスワードの設定や既存のパスワードの変更、またはユーザ・アカウントとグループの新規作成と変更、およびグループのメンバシップとユーザ権利の変更があります。

ディレクトリ・データベースの変更内容は、変更ログに記録されます。変更ログは約 2000 の変更内容を保持しています。保持可能な変更数は、変更ログのサイズによって決まります。ログがいっぱいになると、新しい変更が追加されると、最も古い変更が削除されます。BDC が変更内容を要求すると、最後に同期がとられた時点以降の変更内容が BDC にコピーされます。BDC が一定の間隔で変更内容を要求しなければ、ディレクトリ・データベース全体を BDC にコピーしなければなりません。たとえば、BDC が長期間オフラインになっていた場合、その期間の変更数が、変更ログに格納できる量を超えてしまうことがあります。

2.5.1.2 完全同期化および部分同期化

ディレクトリ・データベース全体を BDC に複製することを、完全同期化と呼びます。完全同期化は、新しい BDC がドメインに追加された場合か、複製が行われる前に変更内容が変更ログから削除された場合に自動的に実行されます。NetLogon サービスの省略時の更新のタイミングおよび変更ログのサイズでは、ほとんどの動作条件で完全同期化が必要になることはありません。

BDC に対して、最後に同期がとられた時点以降に生じたディレクトリ・データベースの変更内容だけを複製することを、部分同期化と呼びます。すべての BDC または特定の BDC に部分同期化を強制的に実行することができます。たとえば、ドメインに新しいユーザを追加した場合や、ユーザのパスワードを変更する場合には、部分同期化を実行して、すべての BDC 上のディレクトリ・データベースに新しいユーザ・アカウントやパスワード変更を速やかに複製することができます。

サーバー マネージャ GUI の [コンピュータ] メニューを使用して、ディレクトリ・データベースとの同期をとることができます。使用可能なオプションは、次に示すように選択しているコンピュータの種類によって異なります。

- PDC を選択すると、[ドメイン全体を同期] オプションが使用可能です。このコマンドは、ディレクトリ・データベースの最新の変更を PDC からドメインのすべての BDC にコピーします。[ドメイン全体を同期] は、現在処理中の同期化の終了を待たずに、すべての BDC の同期化を開始します。
- BDC を選択すると、[プライマリ ドメイン コントローラと同期] オプションが使用可能です。このコマンドは、データベースの最新の変更内容を、選択した BDC だけにコピーします。

ドメイン・コントローラを同期化する方法については、サーバー マネージャのヘルプの「バックアップ ドメイン コントローラをプライマリ ドメイン コントローラと同期させる」および「ドメインのすべてのバックアップ ドメイン コントローラを同期させる」を参照してください。

2.5.2 コントローラの昇格および降格

ソフトウェアのアップグレードや他の保守操作などの理由で PDC が使用できない場合があります。

ドメインが 1 つの PDC だけで構成される場合、それが使用不能になると、ユーザはログインできません。ドメインが 1 つの PDC と複数の BDC から構成されている場合は、PDC が使用不能になっても、ユーザはドメインにログインできます。ただし、ユーザは PDC 上にある資源にアクセスできず、また、ユーザ・アカウントを作成したり変更したりすることはできません。これは、マスタ・ディレクトリ・データベースが PDC 上だけにあるためです。

PDC が使用不能になっても、ドメインに BDC が 1 つ存在する場合は、BDC を PDC に昇格できます。BDC を PDC に昇格させると、ドメインのディレクトリ・データベースの最新コピーは、古い PDC から新しい PDC に複製され、古い PDC は BDC に降格されます。

BDC を PDC に昇格させて、以前の PDC のサービスが復旧した場合、以前の PDC を BDC に降格させなければなりません。以前の PDC が BDC に降格するまで、NetLogon サービスを実行したりユーザ・ログオンの認証に参加したりすることはできなくなり、[サーバー マネージャ] ウィンドウのアイコンは選択不可になります。

BDC を昇格してはじめて、PDC を別のドメインに移動できます。ASU サーバを別のドメインに移動するには、`joindomain` コマンドを使用します。詳細については、`joindomain(8)` を参照してください。

注意

通常、BDC が PDC に昇格すると、システムは自動的に以前の PDC を BDC に降格します。しかし、サーバー マネージャが PDC を見つけることができない場合には、PDC は降格されず、ユーザはこの状態を示すメッセージを受け取ります。この場合、PDC を降格させずに作業を進めるか、PDC が降格されるまで待機するかのいずれかを選択できます。

詳細は、サーバー マネージャのヘルプの「バックアップ ドメイン コントローラをプライマリ ドメイン コントローラに昇格させる」および「プライマリ ドメイン コントローラをバックアップ ドメイン コントローラに降格させる」を参照してください。

2.5.3 ドメインのセキュリティの原則の管理

ASU のセキュリティの原則の設定によって、ドメイン・コントローラ上、ワークステーション上、およびメンバ・サーバ上のドメイン・ユーザ・アクションにさまざまなレベルのセキュリティを設定できます。ドメインを設計する際には、ドメインのセキュリティの原則を検討しておく必要があります。

ドメインを管理する場合、セキュリティの原則はドメイン内の PDC と BDC に適用されます (同じセキュリティの原則を共有します)。メンバ・サーバとして動作しているコンピュータを管理する場合、セキュリティの原則はそのコンピュータだけに適用されます。

次のセキュリティの原則を定義できます。

- ドメイン・ユーザ・アカウントの原則では、ドメイン・ユーザ・アカウントによるパスワードの使い方を定義します。
- 監査の原則では、イベント・ログに記録されるイベントの種類を定義します。

2.5.3.1 ドメイン・ユーザ・アカウントの原則

ドメイン・ユーザ・アカウントの原則では、コンピュータやドメインのすべてのユーザ・アカウントで、パスワードを使用する方法を制御するとともに、アカウント・ロックアウトの原則を決定します。アカウントの原則への変更は、コンピュータまたはドメイン上のすべてのドメイン・ユーザ・アカウントに対して、次のログオン時から有効になります。表 2-1 は、設定できるドメイン・ユーザ・アカウントの原則のオプションを説明しています。

表 2-1: ドメイン・ユーザ・アカウントの原則のオプション

オプション	説明
パスワードの有効期間	システムから変更を要求されるまで、ユーザがパスワードを使用できる期間。
パスワードの変更禁止期間	変更が許可されるまで、ユーザが同じパスワードを使用しなければならない期間。
パスワードの長さ	パスワードの最小文字数。
パスワードの一意性	以前使用していたパスワードが再使用できるようになるまでに、ユーザ・アカウントで使用しなければならない新しいパスワードの数。
ログオン失敗--回後にロックアウトする	アカウントをロックさせる不正なログオンの試みの回数。範囲は 1 ~ 999。 ロックされたアカウントは、管理者がロックを解除するまで、または [ロックアウト期間] オプションによって指定された時間が過ぎるまでロックされたままになる。
カウンタを--分後にリセットする	任意の 2 度の不正なログオンの試みを発生させることができる最大間隔 (分単位)。範囲は 1 ~ 99999。 たとえば、[ログオン失敗--回後にロックアウトする] の指定が 5 回、[カウンタを--分後にリセットする] の指定が 30 分になっている場合、29 分ずつの間隔で 5 回不正なログオンを試みると、アカウントはロックアウトされる。

表 2-1: ドメイン・ユーザ・アカウントの原則のオプション (続き)

オプション	説明
ロックアウト期間	[無期限] を選択した場合は、管理者がロックを解除するまでアカウントはロックされ、[期間] を選択した場合は、指定した時間 (分単位)、アカウントはロックされる。
ログオン時間を超過したリモート ユーザーを強制的に切断	[ログオン時間] オプションで設定されたログオン時間を超過したユーザ・アカウントは、ドメイン内のすべてのコントローラから切断される。ユーザはログオン時間が切れる数分前に警告メッセージを受け取る。 このオプションを使用しない場合、ログオン時間を過ぎても接続は切断されない。ただし、新たに接続することはできなくなり、5 分ごとに警告メッセージを受け取る。 ログオン期間の設定については、3.1.1 項を参照。
パスワード変更にはログオンが必要	パスワードの有効期間が切れたときに、ユーザは自分でパスワードを変更できない。 このオプションを無効にしておくと、パスワードの有効期限が切れても、ユーザは管理者の助けなしに自分でパスワードを変更できる。

次の方法でドメイン・ユーザ・アカウントの原則のオプションを設定できます。

- `net account` コマンドを使用します。`net account` コマンドの詳細な説明を表示するには、次のコマンドを入力してください。

```
# net help accounts /options | more
```

- ドメイン ユーザー マネージャを使用して [原則] メニューから [アカウント] オプションを選択します。

詳細については、ドメイン ユーザー マネージャのヘルプの「アカウントの原則を管理するには」を参照してください。

2.5.3.2 監査の原則

監査を行うと、ドメイン・ユーザ・アカウントの特定の操作をイベント・ログ・ファイルに記録できます。監査の原則はドメイン内のすべての PDC および BDC に適用されます。

ASU サーバでは、ユーザ・ログオンなどのシステム全体にわたるイベントから、特定のユーザによる特定のファイルの読み取りなど、さまざまなイベントを監査したり記録したりできます。イベントの実行は、成功も失敗も監査および記録ができます。表 2-2 に、監査および記録できるイベントを示します。

表 2-2: 監査イベント

イベント	説明
ログオンとログオフ	ユーザのログオンまたはログオフ、あるいはネットワークへの接続。
ファイルとオブジェクトへのアクセス	ファイル マネージャで監査対象として設定されたディレクトリまたはファイルのオープン、あるいはプリント マネージャで監査対象として設定されたプリンタへのプリント・ジョブの送信。
ユーザー権利の使用	ユーザ権利 (ログオンとログオフに関連する権利を除く) の使用。
ユーザーとグループの管理	ユーザまたはグループの作成、変更、あるいは削除。ユーザ・アカウントの名前の変更、無効化、または有効化。あるいはパスワードの設定または変更。
セキュリティ原則の変更	ユーザ権利、監査、または信頼関係の原則の変更。

イベント・ログのサイズは限られているため、ログに使用するディスク容量を検討した上、監査の対象とするイベントを慎重に選択してください。ログの最大サイズを定義するにはイベント ビューアを使用します。

次の操作によって監査の原則を設定できます。

- `net auditing` コマンドを使用します。`net auditing` の詳しい説明を表示するには、次のコマンドを入力してください。

```
# net help auditing /options | more
```
- ドメイン ユーザー マネージャを使用して [原則] メニューから [監査] オプションを選択します。

詳しい説明は、ドメイン ユーザー マネージャのヘルプの「監査の原則を管理するには」を参照してください。

次の操作によってログを表示させることができます。

- ASU サーバが動作しているシステム上で `elfread` コマンドを使用します。詳しい説明は、`elfread(8)` を参照してください。
- Windows システム上でイベント ビューアを使用します。詳細については、第 6 章を参照してください。

2.5.4 信頼関係の管理

信頼関係は、集中管理の利便性をドメイン・レベルからネットワーク・レベルに拡大します。ネットワーク上のドメイン間に信頼関係を確立すると、ドメイン・ユーザ・アカウントは、アカウントが作成されたドメイン以外のドメインでも使用できるようになります。各ドメイン・ユーザ・アカウントの作成が一度だけですみ、その信頼関係を通して、そのアカウントを使って 1 つのドメイン内のコンピュータだけでなく、ネットワーク上の任意のコンピュータにアクセスできるようになります。

2.5.4.1 信頼関係の確立

2つのドメイン間に信頼関係が確立されると、信頼される側のドメインとの安全な通信が確立するので、コンピュータ・アカウントは、信頼する側のドメイン内のコンピュータで 사용할 ことができます。

信頼する側のドメインと信頼される側のドメインは双方とも、次の手順に従って信頼関係を確立する必要があります。

1. 信頼される側のドメインで、そのドメインを信頼する側のドメインのリストに、信頼される側のドメインの名前を追加し、この信頼関係のためのパスワードを割り当てます。
2. 信頼する側のドメインで、信頼される側のドメインのリストに、信頼される側となるドメインの名前を追加します。この操作を行うにはステップ 1 のパスワードが必要です。

注意

信頼関係に割り当てられたパスワードが信頼される側または信頼する側のドメインで変更された場合には、信頼関係は機能し

ません。パスワードが信頼される側または信頼する側で変更されると、信頼関係は両方とも解消および再確立されなければなりません。信頼関係を再確立した場合、信頼する側のドメインと信頼される側のドメインで一致したパスワードを再度割り当てる必要があります。

次の操作を行って、信頼関係を確立したり解除したりできます。

- `net trust` コマンドを使用します。`net trust` コマンドの詳しい説明を表示するには、次のコマンドを入力してください。

```
# net help trust /options | more
```

- ドメイン ユーザー マネージャを使用して [原則] メニューから [信頼関係] オプションを選択します。

詳細については、ドメイン ユーザー マネージャのヘルプの「信頼関係」を参照してください。

2.5.4.2 ドメイン ユーザー マネージャの制限

Windows 95 コンピュータ用の Windows NT Server Tools プログラム・グループに含まれているドメイン ユーザー マネージャには、信頼される側のドメインの管理に影響する制限があります。

[信頼関係] ダイアログ・ボックスを使用して別のドメインを信頼し、[ユーザーとグループの追加] ダイアログ・ボックスを使用して、信頼される側のドメイン内のユーザとグループに特権を付与するには、次のうち少なくとも 1 つの条件を満たしている必要があります。

- 他のドメインによって、すでにドメインが信頼されている。
- ログオンするドメイン・ユーザ・アカウントの名前とパスワードが、他のドメイン内のドメイン・ユーザ・アカウントと同じである。
- 他のドメインが Guest アカウントを有効にしており、ログオンするドメイン・ユーザ・アカウントは、他のドメイン内のどのドメイン・ユーザ・アカウントとも名前が異なる。

さらに、Windows NT Server Tools プログラム・グループに含まれているドメイン ユーザー マネージャは、ドメイン間の信頼関係を検証できません。信頼関係のための正しいパスワードを確実に入力してください。Windows NT

Server Tools からこの手順を実行している場合は、信頼関係が検証されないことを示すメッセージを受け取ります。

ドメイン・ユーザ・アカウントおよびグループ

省略時の設定では、Windows NT および Tru64 UNIX のセキュリティの原則によって認証されてからでなければ、ユーザは共有へのアクセスを要求できません。したがって、共有にアクセスするユーザには、次のものがが必要です。

- ユーザが作成するドメイン・ユーザ・アカウント。ASU サーバはこのアカウントを使用して、共有のために設定された Windows NT のセキュリティの原則をユーザが実行することを認証します。
- ドメイン・ユーザ・アカウントを作成する場合に自動的に作成される Tru64 UNIX ユーザ・アカウント。Tru64 UNIX オペレーティング・システム・ソフトウェアはこのアカウントを使用して、共有に関連付けられたファイル・システムまたはプリンタに対して設定された Tru64 UNIX のセキュリティの原則をユーザが実行することを認証します。

ドメイン・ユーザ・アカウントおよび Tru64 UNIX ユーザ・アカウントには、名前、パスワード、およびセキュリティ・システムがユーザ認証に使用する情報など、ユーザに関する情報が含まれています。

この章では、次の項目について説明しています。

- ドメイン・ユーザ・アカウント
- Tru64 UNIX ユーザ・アカウント
- ドメイン・ユーザ・アカウントのグループ化

ドメイン・ユーザ・アカウントおよびグループの作成については、『*Advanced Server for UNIX* インストレーション/管理ガイド』を参照してください。

3.1 ドメイン・ユーザ・アカウント

ドメイン・ユーザ・アカウントには、Advanced Server ドメイン内に存在するユーザを定義する情報が含まれています。

表 3-1 は、ドメイン・ユーザ・アカウントの要素について説明しています。

表 3-1: ドメイン・ユーザ・アカウントの要素

アカウントの要素	説明
ユーザー名	ログオン時にユーザが入力する一意の名前。
フル ネーム	ユーザのフル・ネーム。
説明	ユーザまたはユーザ・アカウントに関する説明
パスワード	ユーザのパスワード。パスワードのオプションの設定については、表 3-2 を参照。
ログオン時間	ユーザがドメインにログオンできる時間。ログオン時間の設定についての詳細は、3.1.1 項を参照。 ユーザのログオン時間が過ぎた場合に、ユーザが強制的にログオフさせられるかどうかは、ドメインのアカウントのセキュリティの原則の [ログオン時間を超過したリモート ユーザーを強制的に切断] オプションによって定義される。ドメインのアカウントのセキュリティの原則の設定についての詳細は、2.5.3.1 項を参照。
ログオンできるワークステーション	ユーザがドメインにログインできるワークステーションのコンピュータ名。省略時の設定では、ユーザは任意のワークステーションにログインできる。
アカウントの有効期限	アカウントが自動的に無効になる日付。臨時の従業員や学生のアカウントが、不必要に使用可能なままの状態にならないようにするには便利である。
ログオン スクリプト	ユーザのログオン時に、自動的に実行されるバッチ・ファイルまたは実行可能ファイル。詳細については、3.1.2 項を参照。
ホーム ディレクトリ	ユーザに固有なディレクトリ。詳細については、3.1.3 項を参照。
プロファイル	プログラム・グループ、ネットワーク接続、および画面の色など、ユーザのデスクトップ環境を再現するための情報を含んだフォルダへのパス。詳細については 3.1.4 項を参照。
アカウントの種類	アカウントの種類は、グローバルまたはローカルのいずれかである。ほとんどの場合、グローバル・アカウントを作成することになる。

3-2 ドメイン・ユーザ・アカウントおよびグループ

表 3-2 は、ユーザのパスワードの管理に使用できるオプションを示しています。

表 3-2: ドメイン・ユーザ・アカウントのパスワードのオプション

オプション	説明
ユーザは次回ログオン時にパスワード変更が必要	チェック・ボックスがオンになっている場合、ユーザは、次回ドメインにログインする際にパスワードを変更しなければならない。 このオプションは、ドメイン・アカウントのセキュリティの原則にある [パスワードの変更禁止期間] オプションによって定義されている。ドメイン・アカウントのセキュリティの原則の設定についての詳細は、2.5.3.1 項を参照。
ユーザはパスワードを変更できない	チェック・ボックスがオンになっている場合、ユーザは、自分のパスワードを変更できない。この制限は、共有アカウントの場合に便利である。この制限は、管理者には適用されない。
パスワードを無期限にする	チェック・ボックスがオンになっている場合、ユーザのパスワードの有効期間は無期限となる。このオプションは、Replicator (複製) サービスなどのサービスを割り当てられたアカウントに使用する。
アカウントを無効にする	チェック・ボックスがオンになっている場合、アカウントは無効となり、このアカウントではログオンできなくなる。アカウントはディレクトリ・データベースから削除されないが、アカウントが有効になるまでユーザはそのドメインにログインできない。

ドメイン・ユーザ・アカウントには、そのアカウントを識別する一意の番号であるセキュリティ識別子 (SID) が含まれています。アカウントが作成されるときに、ネットワーク上のすべてのアカウントに対し一意の SID が発行されます。内部プロセスは、アカウントのユーザ名ではなくアカウントの SID を参照します。一度作成したアカウントを削除し、次に同じ名前でアカウントを作成しても、異なる SID 番号をもっているため、新しいアカウントは、古いアカウントに与えられていた権利またはアクセス権を持つことはできません。ユーザ・アカウントの名前を変更しても、SID は保持されます。

3.1.1 ログオン時間の指定

省略時の設定では、ユーザは時間を制限されことなく ASU サーバに接続できます。ただし、アクセスできる時間を制限することもできます。

ユーザがコントローラに接続している間にログオン時間が過ぎた場合、ユーザは、[ログオン時間を超過したリモート ユーザーを強制的に切断] オプションの設定によって、すべてのサーバ接続から切断されるか、または既存の接続は維持されるものの、新しい接続は拒否されるかのいずれかになります。このオプションの設定についての詳細は、2.5.3.1 項を参照してください。

次の手順によりユーザのログオン時間を指定します。

- `net user /TIMES:{times | ALL}` コマンド。 `net user` コマンドの詳細い説明を表示するには、次のコマンドを入力してください。

```
# net help user /options | more
```

- ドメイン ユーザー マネージャを使用して指定したユーザのプロパティを表示し、[ユーザのプロパティ] ダイアログ・ボックスの [時間] を選択します。

[ログオン時間] ダイアログ・ボックスが表示されます。[ログオン時間] ダイアログ・ボックスには 1 週間分のカレンダーが表示され、ログオン時間は曜日ごとに 1 時間刻みで表示されます。各ボックスは 1 時間を表します。たとえば、各行の最初のボックスは深夜午前 0 時 00 分から午前 0 時 59 分までの時間を、各行の最後のボックスは午後 11 時 00 分から午後 11 時 59 分までの時間をそれぞれ表します。塗りつぶされているボックスは、ユーザがコントローラへの接続を許可されていることを示します。空のボックスは、ユーザがコントローラへの接続を許可されていないことを示します。

注意

ログオン時間は、ユーザがログオンまたは接続しているワークステーションまたはサーバのタイム・ゾーンではなく、PDC のタイム・ゾーンの時間で示されます。

3.1.2 ログオン・スクリプト

ログオン・スクリプトは、ASU サーバを実行しているシステムにログオンするたびに、自動的に実行されるコマンドからなる実行可能ファイルまたはバッチ・ファイルです。ログオン・スクリプトは、ネットワークの接続およびアプリケーションの起動など、ユーザの作業環境を自動的に構成するために使用されます。

ログオン・スクリプトをいつでも使用できるようにするには、Replicator サービスを利用するのが最もよい方法です。Replicator サービスは、複数のコントローラ上にあるディレクトリ・ツリーと全く同じ複製物(コピー)を維持管理します。ツリー (エクスポート・サーバにある) のマスタ・コピー内のファイルに変更を加えると、Replicator サービスは変更内容をインポート・コントローラに自動的にコピーします。

3.1.2.1 ログオン・スクリプトの作成

ログオン・スクリプトは、テキスト・エディタで作成できます。Replicator サービスを使用して、ログオン・スクリプトをドメイン・コントローラに配布できます。

Replicator サービスを使用する場合、ASU サーバは、インポート・サーバ上の `/usr/net/servers/lanman/shares/asu/repl/import/scripts` ディレクトリおよびエクスポート・サーバ上の `/usr/net/servers/lanman/shares/asu/repl/export/scripts` ディレクトリでログオン・スクリプトを探します。Replicator サービスを使用しない場合には、コントローラはどれでもログオン要求を認証できるため、ログオン・スクリプトが各コントローラ上の同じディレクトリにあることを確認し、その後でログオン・スクリプトを実行する必要があります。ディレクトリの複製についての詳細は、4.2 節を参照してください。

表 3-3 に、ログオン・スクリプトを作成する場合に使用できる特殊なパラメータを示します。

表 3-3: ログオン・スクリプトのパラメータ

パラメータ	説明
%HOMEDRIVE%	ユーザのホーム・ディレクトリに接続されているユーザのローカル・ワークステーションのドライブ名
%HOMEPATH%	ユーザのホーム・ディレクトリの絶対パス名
%HOMESHARE%	ユーザのホーム・ディレクトリがある共有名
%OS%	ユーザのワークステーションのオペレーティング・システム
%PROCESSOR_ARCHITECTURE%	ユーザのワークステーションのプロセッサのタイプ
%PROCESSOR_LEVEL%	ユーザのワークステーションのプロセッサ・レベル
%USERDOMAIN%	ユーザのアカウントがあるドメイン
%USERNAME%	ドメインのユーザ名

3.1.2.2 ログオン・スクリプトの割り当て

ログオン・スクリプトをドメイン・ユーザ・アカウントに割り当てるには、次の操作を行います。

- `net user username /scriptpath:[pathname]` コマンドを使用します。`net user` コマンドの詳しい説明を表示するには、以下のコマンドを入力してください。

`# net help user /options | more`
- ドメイン ユーザー マネージャを使用します。ユーザのプロパティを選択し、[プロファイル] ボタンをクリックして、「ログオン スクリプト名」ボックスにログオン・スクリプトのパスを入力します。

3.1.3 ホーム・ディレクトリ

ユーザのホーム・ディレクトリとは、そのユーザがアクセス可能で、そのユーザのファイルおよびプログラムが含まれているディレクトリのことです。ユーザがワークステーションにログインすると、そのユーザのホーム・ディレクトリに自動的に接続されます。つまり、[開く] および [名前を付けて保存] のダイアログ・ボックス、コマンド・プロンプト、および作業ディレクトリが定義されていないすべてのアプリケーションに対して、そのユーザの省略時

のディレクトリになります。省略時の設定では、ドメイン・ユーザ・アカウントを作成すると、ASU サーバは、Tru64 UNIX アカウント名を使用して、`/usr/users` ディレクトリにユーザのホーム・ディレクトリを作成します。

ホーム・ディレクトリを指定しない場合、省略時のホーム・ディレクトリはユーザのローカル・ドライブの `¥USERS¥DEFAULT` です。

ホーム・ディレクトリを使用することにより、ユーザ・ファイルを一か所に集めることができるため、管理者はユーザ・ファイルのバックアップやユーザ・アカウントの削除が容易にできるようになります。

3.1.3.1 ホーム・ディレクトリの割り当て

次の操作を行い、ホーム・ディレクトリをユーザ・アカウントに割り当てます。

- `net user username /homedir:pathname` コマンドを使用します。
`net user` コマンドの詳しい説明を表示するには、以下のコマンドを入力してください。

`# net help user /options | more`
- ドメイン ユーザー マネージャを使用します。ユーザのプロパティを選択し、[プロファイル] ボタンをクリックして、[ホーム ディレクトリ] ボックスにホーム・ディレクトリのパスを入力します。

コントローラ上のホーム・ディレクトリを指定すると、そのディレクトリが存在しない場合には、作成されます。ユーザのローカル・システム上のディレクトリを指定すると、そのディレクトリが存在しなくても作成されません。

[ホーム ディレクトリ] ボックスで、パスの最後のエントリを `%USERNAME%` に置き換えることができます。`%USERNAME%` は、システムによって、後でドメイン・ユーザ・アカウントのユーザ名に置き換えられます。この置き換えは、複数のドメイン・ユーザ・アカウントを選択する場合に便利です。たとえば、8つのドメイン・ユーザ・アカウントを選択しているとします。[ホーム ディレクトリ] ボックスで[ドライブ]を選択し、ドライブ文字として `K` を指定して [パス] ボックスを選択し、`¥¥SALES¥home¥%username%` と入力します。[OK] を選択して、ユーザー環境プロファイルを保存すると、各 `%USERNAME%` は実際のユーザ名に置き換えられます。

ドメイン・ユーザ・アカウントがコピーされると、ホーム・ディレクトリは次の2つの方法のいずれかによってコピーされます。

- コピー元のユーザ・アカウントのホーム・ディレクトリ・パスの最後のサブディレクトリがユーザ名の場合、新しいアカウントには、ホーム・ディレクトリ・パスにある新しいユーザ名が与えられます。たとえば、もとのドメイン・ユーザ・アカウントのユーザ名が PETER でホーム・ディレクトリが ¥¥SETTER¥USERS¥PETER の場合、ユーザ名 EVAN というコピーされた (新しい) ドメイン・ユーザ・アカウントのホーム・ディレクトリは ¥¥SETTER¥USERS¥EVAN となります。
- コピー元のユーザ・アカウントのホーム・ディレクトリ・パスの最後のサブディレクトリがユーザ名でない場合、ホーム・ディレクトリ・パスはそのままコピーされます。たとえば、もとのドメイン・ユーザ・アカウントのユーザ名が PETER でホーム・ディレクトリが ¥¥HOUND¥USERS¥HOME の場合、ユーザ名 EVAN というコピーされた (新しい) ドメイン・ユーザ・アカウントのホーム・ディレクトリは、同じ ¥¥HOUND¥USERS¥HOME となります。

3.1.4 ユーザ・プロフィール

ユーザ・プロフィールは、ユーザがログインしたときに設定する作業環境の設定項目を定義します。この設定には、使用できるコントロール・パネルのオプション、画面の色、共有の接続、マウスの設定、ショートカット、ウィンドウ・サイズと位置など、Windows 環境のユーザ固有の設定がすべて含まれます。

ユーザ・プロフィールには次のタイプがあります。

- ローカル・ユーザ・プロフィールは、Windows オペレーティング・システムが動作しているコンピュータにユーザが初めてログオンしたとき、そのコンピュータ上に自動的に作成されます。それ以降、ユーザがそのコンピュータにログオンするたびに、ユーザごとのユーザ・プロフィールが利用可能になります。
- 移動ユーザ・プロフィールは、ASU サーバまたは Windows オペレーティング・システムが動作しているコンピュータ上で利用できます。移動ユーザ・プロフィールを使用できるようにするには、管理者がユーザ・アカウントにユーザ・プロフィールのパスを入力します。その後最初にログオフしたとき、ローカル・ユーザ・プロフィールがそのユーザ・プロフィールのロケーションにコピーされます。以降、ユーザがログオンするたびに、ユーザ・プロフィールのサーバ・コピーがダウンロードされます (サーバ・コピーがローカル・コピーよりも新しい

場合)。ローカル・コピーとサーバ・コピーは両方とも、ユーザがログオフするたびに更新されます。

- 固定ユーザ・プロファイルは、ユーザ用に作成された移動プロファイルですが、ユーザはそのファイルを変更できません。ユーザがログオフしても、ローカル・ユーザ・プロファイルは保存されず、ローカル・ユーザ・プロファイルはサーバにコピーされません。

ユーザ・プロファイルは、Windows 95 が動作しているコンピュータで利用可能です。ただし、ユーザ・プロファイルがこのシステムに格納されている場合でも、ASU サーバまたは Windows NT が動作しているコンピュータ上のユーザは、Windows 95 上で作成されたユーザ・プロファイルを利用できません。

3.1.4.1 ユーザ・プロファイルの作成

システム ポリシー エディタを使用して、ユーザ・プロファイルを作成できます。システム ポリシー エディタは Windows ベースのインタフェースで、このツールを使用すれば、ドメインにログインして、特定の Windows コンピュータ、ユーザまたはグループの環境を定義するポリシーを表示させて管理することができます。

システム ポリシー エディタを使用すると、次のポリシーが設定できます。

- 各ドメイン・ユーザ・アカウントまたはグループに適用されるユーザ固有のポリシー。多くのポリシーがユーザ固有です。
- Windows システム上のすべてのユーザに適用され、ユーザごとには変わらないマシン固有のポリシー。ユーザがさまざまなシステム間を移動しても、ユーザには対応しません。

システム ポリシー エディタは、ポリシー (.POL) ファイルに設定を保存します。ユーザがログインすると、ポリシー・ダウンローダというプログラムが起動します。ポリシー・ダウンローダは、すべての Windows クライアントにインストールされています。ポリシー・ダウンローダは、ネットワーク上にポリシー・ファイルがないかどうかを調べたり、ポリシー・ファイルをオープンしたり、ローカルのコンピュータ名やユーザ名を使ったエントリを探したり、ポリシー・ファイルに定義された、管理者のレジストリ設定をローカル・レジストリにマージしたりします。ダウンローダがポリシー・ファイルにローカルのコンピュータ名またはユーザ名を持つエントリを見つけられない場合は、DEFAULT USER または DEFAULT COMPUTER のエントリを探し、これらのレジストリ設定をマージ用に使用します。特定の

ユーザまたはコンピュータのエントリがなく省略時のエントリも存在しない場合、マージは行われません。

システム ポリシー エディタについての詳細は、『*Advanced Server for UNIX* インストール/管理ガイド』を参照してください。

3.1.4.2 プロファイルの割り当て

ドメイン・ユーザ・アカウントにプロファイルを割り当てるには、次の操作を行います。

- `net user username /profilepath:[pathname]` コマンドを使用します。`net user` コマンドの詳細な説明を表示するには、次のコマンドを入力してください。

```
# net help user /options | more
```
- ドメイン ユーザー マネージャを使用します。ユーザのプロパティを選択し、[プロファイル] ボタンをクリックして、[ユーザー プロファイルのパス] ボックスにプロファイルのパスを入力します。

3.1.5 ユーザ権利の原則の管理

権利とは、ファイルやディレクトリのバックアップ、コンピュータへの対話形式のログオン、システムのシャットダウンなど、コンピュータ・システム上で特定の操作の実行をユーザに許可することをいいます。権利は、ドメイン・レベルでは、ドメイン・コントローラを使用する能力であり、ローカル・レベルでは、ワークステーションまたはメンバ・サーバを使用する能力です。権利は、ドメイン・ユーザ・アカウントまたはグループに与えることができます。

ドメイン・ユーザ・アカウントにログオンするユーザ、または操作を実行するために適切な権利が与えられたグループに属するユーザは、操作を実行できます。ユーザが操作を実行するために適切な権利をもっていない場合、その操作を実行しようとすると、ASU サーバによってブロックされます。

権利は、システム全体に適用されるもので、特定のオブジェクトに適用されるアクセス権とは異なります。アクセス権とは、オブジェクト（通常、ディレクトリ、ファイル、またはプリンタ）に関連付けられた規則のことで、そのオブジェクトにアクセスできるユーザと、そのアクセス方法を制御します。ほとんどの場合、オブジェクトの作成者や所有者が、そのオブジェクトのアクセス権を設定します。しかし、すべての権利が特定のオブ

ジェクトに関連付けられているわけではなく、ドメイン (ドメイン・コントローラ) レベルまたはローカル (ワークステーションあるいはメンバ・サーバ) レベルで適用されるため、オブジェクトに対して設定されたアクセス権を無効にする場合があります。たとえば、Backup Operators グループのメンバであるドメイン・アカウントにログオンしているユーザは、ドメインのすべてのサーバに対してバックアップ作業を実行する権利を持っています。バックアップ作業を実行するには、サーバ上のすべてのファイルを読み取る能力が必要になります。しかし、ファイルによっては、所有者がアクセス権を明示的に設定して Backup Operators グループのメンバを含む、すべてのユーザのアクセスを拒否する設定になっている場合があります。この場合、バックアップを実行する権利は、すべてのファイルおよびディレクトリへのアクセス権よりも優先されます。

表 3-4 は、各種のユーザ権利を説明しています。アクセス権についての詳細は、4.1 節を参照してください。

表 3-4: ユーザ権利

ユーザ権利	実行できる操作
ネットワーク経由でコンピュータへアクセス	ネットワークを経由してコントローラに接続する。この権利は管理者のローカル・グループから取り消せない。
ドメインにワークステーションを追加	ドメインにワークステーションを追加する。その結果、ワークステーションはドメインおよび信頼される側のドメインのユーザ・アカウントとグローバル・グループを認識できる。
ファイルとディレクトリのバックアップ	ファイルとディレクトリをバックアップし、すべてのファイルを読み取る。この権利は、ファイルやディレクトリのアクセス権よりも優先され、レジストリにも適用される。
システム時刻の変更	コントローラの内部時計の時刻を設定する。
リモートコンピュータからの強制シャットダウン	この権利は現在、実装されていない。将来の使用のために予約されている。
デバイスドライバのロードとアンロード	デバイス・ドライバのインストールと削除を行う。
ローカル ログオン	コントローラにローカルでログオンする。
監査とセキュリティログの管理	どんな種類の共有へのアクセス (ファイル・アクセスなど) を監査するかを指定する。セキュリティ・ログの表示とクリアを行う。ユーザがこの権利を持っていてもシステム監査を設定することはできない。この機能は Administrators グループだけが有する。

表 3-4: ユーザ権利 (続き)

ユーザ権利	実行できる操作
ファイルとディレクトリの復元	ファイルとディレクトリの復元 (書き込み) を行う。 この権利は、ファイルとディレクトリのアクセス権より優先され、レジストリにも適用される。
システムのシャットダウン	コントローラをシャットダウンする。
ファイルとその他のオブジェクトの所有権の取得	コントローラ上のファイル、ディレクトリ、およびその他のオブジェクトの所有権を取得する。

3.1.5.1 ユーザ権利の割り当て

ドメイン ユーザー マネージャを使用し、[原則]、次に [ユーザーの権利] を選択することにより、ドメイン・ユーザ・アカウントに権利を割り当てます。

ドメインにユーザ権利を割り当てると、それらの権利はすべてのコントローラに適用されます。ワークステーションまたはメンバ・サーバ上で管理されるユーザ権利は、ワークステーションまたはメンバ・サーバにだけ適用されます。

3.1.6 ビルトイン・ドメイン・ユーザ・アカウント

ASU ソフトウェアをインストールすると、次の 2 つのビルトイン・ユーザ・アカウントが自動的に作成されます。

- Administrator アカウント
- Guest アカウント

3.1.6.1 ビルトイン Administrator ユーザ・アカウント

ビルトイン Administrator アカウントには、ドメインに属する、コントローラ、ワークステーション、またはメンバ・サーバ上でドメイン管理作業を実行する権利が与えられます。

ASU ソフトウェアをインストールすると、ビルトイン Administrator アカウントにパスワードの入力が指示されます。このパスワードは、十分注意を払って保護する必要があります。パスワードを忘れてしまったり、パスワードを知っている人間がいなくなったりすると、ビルトイン Administrator アカウントが使用できなくなるためです。パスワードの変更は可能で、有効期限はありません。

3-12 ドメイン・ユーザ・アカウントおよびグループ

ビルトイン Administrator アカウントは、削除することも無効にすることもできません。この特長は、ビルトイン Administrator アカウントが Administrators ローカル・グループの他のメンバと異なる点です。

ASU ソフトウェアのインストールに続いて、管理者レベルの機能を持つ管理アカウントをもう 1 つ作成し、ビルトイン Administrator アカウントを緊急時用のアカウントとして確保しておくことをお勧めします。管理特権を持つユーザに個別のアカウントを作成すれば、これらのユーザ操作をビルトイン Administrator アカウントではなく、個々のユーザ・アカウントによって監査できます。

ASU ソフトウェアのインストールについては、『*Advanced Server for UNIX* インストレーション/管理ガイド』を参照してください。監査については、第 6 章を参照してください。

3.1.6.2 ビルトイン Guest ユーザ・アカウント

ビルトイン Guest アカウントは、ドメインまたは信頼される側のドメインに、ドメイン・ユーザ・アカウントを持たないユーザがログオンする場合に使用します。アカウントが無効になっている (ただし削除されていない) ユーザも Guest アカウントを使用できます。

Guest アカウントは、省略時の設定では無効になっています。Guest アカウントはパスワードを必要とせず、ドメイン上ではあらかじめ定義されている権利やアクセス権はありませんが、他のドメイン・ユーザ・アカウントと同じように、パスワード、権利およびアクセス権を設定できます。

ゲスト・ログオンには次の 2 種類があります。

- ローカル・ゲスト・ログオン。ローカル・ゲスト・ログオンでは、Windows ソフトウェアが動作しているコンピュータにユーザが対話形式でログオンするとき、[ログオン情報] ダイアログ・ボックスでユーザ名に Guest を指定します。(ドメイン・コントローラではなく) コンピュータ上の Guest アカウントにはローカルにログオンできる組み込み済みの権利があるので、ゲスト・ユーザはそのコンピュータで (Guest アカウントに与えられた権利とアクセス権の範囲内で) 作業を行い、ネットワークにアクセスできます。
- ネットワーク・ゲスト・ログオン。ユーザがコントローラにネットワーク接続するとき、そのコントローラがユーザ名、ドメイン名、およびパスワードを認識しない場合にネットワーク・ゲスト・ログオンになり

ます。ネットワーク・ゲスト・ログオンは、接続先のコントローラで Guest アカウントが有効になっており、パスワードが設定されていない場合に限り、承認されます。その場合、ゲスト・ユーザは、ユーザ名として Guest を指定しなくても、コントローラ上で Guest アカウントに与えられている、すべての権利、アクセス権、およびグループ・メンバーシップを持つことになります。

3.1.6.2.1 Guest アカウントの有効化

次の操作を行い、各コントローラの Guest アカウントを有効にします。

- `net user Guest /active:yes` コマンドを使用します。`net user` コマンドの詳しい説明を表示するには、以下のコマンドを入力してください。

```
# net help user /options | more
```

- ドメイン ユーザー マネージャを使用し、Guest ユーザを選択して、[アカウントを無効にする]の隣にあるボックスをクリックしてチェック・マークをはずします。

3.2 Tru64 UNIX ユーザ・アカウント

省略時の設定では、Tru64 UNIX オペレーティング・システム・ソフトウェアは、共有に関連付けられたファイル・システムまたはプリンタにユーザがアクセスする前にユーザを認証します。

省略時の設定では、ドメイン・ユーザ・アカウントを作成したときに、同じ名前を持つ Tru64 UNIX ユーザ・アカウントが存在しなければ、ローカルの `/etc/passwd` ファイルに自動的に作成されます。Tru64 UNIX オペレーティング・システム・ソフトウェアはこのアカウントを使用して、ユーザを認証します。なお、認証要求をネットワーク情報サービス (NIS)、Windows 2000 Server、または Windows NT Server Version 4.0 に送付するように、Tru64 UNIX オペレーティング・システム・ソフトウェアを構成することもできます。NIS、Windows 2000 Server、または Windows NT Server Version 4.0 は、ユーザ・アカウント・データベースの情報を使用し、Tru64 UNIX オペレーティング・システム・ソフトウェアに代わってユーザを認証して、その結果を返送します。これは、NIS、Windows 2000 Server 上にユーザ・アカウント・データベースがあって、Tru64 UNIX システム上にユーザ・アカウント・データベースを作成したくない場合に便利です。

ユーザ・アカウント認証の設定についての詳細は、『*Advanced Server for UNIX* インストレーション/管理ガイド』を参照してください。

3.2.1 ドメイン・ユーザ・アカウントの Tru64 UNIX ユーザ・アカウントへの関連付け

省略時の設定では、ドメイン・ユーザ・アカウントは Tru64 UNIX ユーザ・アカウントに関連付けられています。この関連付けにより、Tru64 UNIX ファイルは、Tru64 UNIX システム・ユーザ・アカウントによって所有され、ドメイン・ユーザ・アカウントによってアクセス可能になります。特定のユーザ・アカウントにマップされていないドメイン・ユーザ・アカウントは、省略時の設定では `lmworld` Tru64 UNIX ユーザ・アカウントにマップされます。

ドメイン・ユーザ・アカウントに割り当てられる Tru64 UNIX ユーザ・アカウント名は、ドメイン・ユーザ・アカウント名と同じか、それとよく似たものになります。ユーザ・アカウント名が長い、重複しているか、または特殊文字を使用している場合には差異が生じます。ドメイン・ユーザ・アカウント・ユーザが、存在しない Tru64 UNIX ユーザ・アカウントに関連付けられているか、またはそのユーザの Tru64 UNIX ユーザ・アカウントが削除されている場合、ユーザはどの共有にもアクセスできません。

`mapuname` コマンドを使用して、ドメイン・ユーザ・アカウントの Tru64 UNIX ユーザ・アカウントへの関連付けを制御できます。ドメイン・ユーザ・アカウントと Tru64 UNIX ユーザ・アカウントとの省略時の関係は、ASU レジストリのユーザ関連レジストリ値エントリに割り当てられた値によって制御されます。

ASU レジストリについての詳細は、『*Advanced Server for UNIX* インストレーション/管理ガイド』を参照してください。

3.3 ドメイン・ユーザ・アカウントのグループ化

管理を簡略化するために、ドメイン・ユーザ・アカウントをグループ化し、グループを一単位として管理できます。グループに追加されたドメイン・ユーザ・アカウントは、そのグループのメンバになり、グループに与えられた権利とアクセス権を直ちに取得できます。グループに行った変更は、各メンバに影響を与えます。グループ・メンバシップとすることで、多数のユーザに共通的な機能を簡単に与えることができます。

グループには次の 3 つのタイプがあります。

- ローカル・グループ
- グローバル・グループ
- 特殊グループ

3.3.1 ローカル・グループ

ローカル・グループには、ローカル・ドメインおよびそれを信頼する側のドメインのドメイン・ユーザ・アカウントとグローバル・グループが含まれています。ローカル・グループには他のローカル・グループを入れることはできません。表 3-5 は、ビルトイン・ローカル・グループについて説明しています。

表 3-5: ローカル・グループ

グループ	説明
Administrators	メンバには自動的に、ドメインとコントローラを管理するための、すべての組み込み済みの権利と能力が与えられる。 省略時の設定では、Domain Admins グローバル・グループは Administrators ローカル・グループのメンバになる。
Users	メンバは、ドメインへの通常のユーザ・アクセス権と能力を持っている。 省略時の設定では、Domain Users グローバル・グループは、Users ローカル・グループのメンバになる。
Guests	メンバは、コントローラ上では何の権利も持っていない。しかし、個々のワークステーションで特定の権利を持っている。 省略時の設定では、Domain Guests グローバル・グループは Guests ローカル・グループのメンバになる。

表 3-5: ローカル・グループ (続き)

グループ	説明
Account Operators	メンバは、ほとんどのドメイン・ユーザ・アカウントとグループの作成、変更、および削除、ドメイン・コントローラのログオンとシャットダウン、さらにドメインへのコントローラまたはメンバ・サーバの追加を行うことができる。 メンバは、セキュリティの原則を管理することはできない。また、Domain Admins グローバル・グループを変更または削除することもできない。さらに、Administrators、Account Operators、Backup Operators、Print Operators または Server Operators の各ローカル・グループとこれらのローカル・グループに属するグローバル・グループを変更または削除することはできない。これらのグループ・メンバのアカウントを変更および削除することもできない。
Backup Operators	メンバは、PDC および BDC 上のファイルのバックアップおよび復元を行うことができる。
Print Operators	メンバは、ドメインのコントローラ上のプリンタ共有の作成、削除、および管理を行うことができる。コントローラをシャットダウンすることもできる。
Server Operators	メンバは、共有の作成、削除および管理と、システム時刻の変更を行うことができる。
Replicator	メンバは、ドメイン内の PDC および BDC の Replicator サービスを管理することができる。ディレクトリの複製については、第 4 章を参照。

すべてのビルトイン・ローカル・グループが ASU サーバ、Windows NT サーバ、Windows NT ワークステーション、およびメンバ・サーバ上に存在するわけではありません。表 3-6 は、どのビルトイン・ローカル・グループが ASU サーバ、Windows NT サーバ、Windows NT ワークステーション、およびメンバ・サーバ上に存在するかについて説明しています。

表 3-6: ビルトイン・ローカル・グループ

ASU サーバおよび Windows NT サーバ	Windows NT ワークステーション およびメンバ・サーバ
Administrators	Administrators
Users	Users
Guests	Guests
Account Operators	Backup Operators
Backup Operators	Replicator
Print Operators	Power Users
Server Operators	
Replicator	

3.3.2 グローバル・グループ

グローバル・グループには、作成されたドメインのドメイン・ユーザ・アカウントが含まれています。グローバル・グループにはローカル・グループ、他のグローバル・グループ、または他のドメインのドメイン・ユーザ・アカウントを入れることはできません。グローバル・グループは、同じドメインおよびそのドメインを信頼する側のドメインに追加することができます。また、同じドメインおよびそのドメインを信頼する側のドメインにあるメンバ・サーバや Windows NT Workstation が動作しているコンピュータにグローバル・グループを追加することもできます。グローバル・グループに対しては、アクセス権と権利を、そのドメイン内、ワークステーションまたはメンバ・サーバ上、あるいは信頼する側のドメイン内で与えることができます。Windows NT Workstation が動作するコンピュータまたはメンバ・サーバとして動作するコンピュータ上にはグローバル・グループを作成できません。

表 3-7 は、ビルトイン・グローバル・グループについて説明しています。これらのグループは削除できません。

表 3-7: グローバル・グループ

グループ	説明
Domain Admins	<p>メンバは、ドメイン、ドメインのコントローラとワークステーション、および信頼する側のドメインを管理できる。ただし、この信頼する側のドメインには、あらかじめこのドメインの Domain Admins グローバル・グループを、Administrators ローカル・グループに追加しているものとする。Administrators ローカル・グループだけが Domain Admins グローバル・グループを変更できる。</p> <p>ビルトイン Administrator ユーザ・アカウントは、Domain Admins グローバル・グループのメンバである。Domain Admins グローバル・グループは Administrators ローカル・グループのメンバである。ドメイン・ユーザ・アカウントに管理者レベルの能力を与えるには、そのアカウントを Domain Admins グローバル・グループに追加する。</p>

表 3-7: グローバル・グループ (続き)

グループ	説明
Domain Users	<p>メンバは、そのドメインおよびドメイン内の Windows NT ワークステーションと、メンバ・サーバとして動作している Windows NT サーバに対して、通常のユーザ・アクセス権と能力を有する。Administrators と Account Operators だけが Domain Users グローバル・グループを変更できる。</p> <p>ビルトイン Administrator ユーザ・アカウントは、Domain Users グローバル・グループのメンバである。省略時の設定では、すべての新しいドメイン・ユーザ・アカウントは、特に削除しない限り、Domain Users グループに追加される。</p> <p>Domain Users グローバル・グループは、そのドメインの Users ローカル・グループのメンバであり、ドメイン内で Windows NT Workstation が動作しているすべてのコンピュータと Windows NT Server が動作しているメンバ・サーバの Users ローカル・グループのメンバである。</p>
Domain Guests	<p>メンバは、コントローラに対してはどんな権利も持っていない。</p> <p>ビルトイン Guests ユーザ・アカウントは、Domain Guests グローバル・グループのメンバである。Domain Guests グローバル・グループは、Guests ローカル・グループのメンバである。</p> <p>ユーザ・アカウントを追加する場合、そのアカウントの権利とアクセス権を一般的なドメイン・ユーザ・アカウントよりも厳しく制限するには、ユーザ・アカウントを Domain Guests グループに追加し、Domain Users グループからは削除する。Administrators と Account Operators だけが Domain Guests グローバル・グループを変更できる。</p>

3.3.3 特殊グループ

表 3-8 は、特殊な目的に使用されるその他のグループを示しています。これらのグループのメンバシップは変更できないため、ドメイン ユーザー マネージャにはリストされません。

ASU サーバを管理するときに、これらの特殊グループがグループのリストに時々表示されます。たとえば、共有およびファイルにアクセス権を割り当てるときに表示されることがあります。

表 3-8: 特殊グループ

グループ	説明
Everyone	メンバには、すべてのローカル・ユーザおよびリモート・ユーザ (Interactive グループと Network グループを組み合わせたもの) が含まれる。 ドメインでは、メンバはネットワークへのアクセス、ディスク共有およびプリンタ共有への接続が可能。
Interactive	メンバには、ローカルでコンピュータを使用している任意のユーザが含まれる。
Network	メンバには、ネットワークを介してコンピュータに接続されているユーザが含まれる。
System	メンバにはオペレーティング・システムが含まれる。
Creator Owner	メンバには、サブディレクトリ、ファイル、またはプリント・ジョブの作成者が含まれる。ディレクトリに対して、Creator Owner グループにアクセス権が与えられている場合、サブディレクトリまたはファイル作成者にはそのサブディレクトリまたはファイルに対するアクセス権が与えられる。プリンタに対しては、Creator Owner グループにアクセス権が与えられている場合、プリント・ジョブの作成者に、そのプリント・ジョブに対するアクセス権が与えられる。

3.3.4 グループを使用するための方策

権利の中には、特定のグループのメンバであるユーザにしか与えられないものがあります。たとえば、ユーザがドメイン・ユーザ・アカウントを作成できるようにする唯一の方法は、ドメイン上の Administrators または Account Operators ローカル・グループにその人のドメイン・ユーザ・アカウントを追加することです。

複数のビルトイン・グループにユーザを追加することができます。たとえば、Print Operators と Backup Operators グループの両方のユーザには、Print Operators に与えられたすべての権利と、Backup Operators に与えられたすべての権利が与えられます。

1 つのドメインで、権利をドメイン・レベルで与えたり、制限したりすることができます。グループがドメインの中に権利をもっている場合、そのメンバはドメイン内のすべてのコントローラに対して権利を持ちます。メンバ・サーバでは、与えられた権利はそのコンピュータにだけ適用されます。

複数のドメインが設定されている場合、信頼する側のドメインのローカル・グループにユーザを追加する方法として、グローバル・グループを利用する方法があります。ユーザの権利とアクセス権を他のドメイン上の資源に拡張する場合、ドメインのグローバル・グループにアカウントを追加し、信頼する側のドメインのローカル・グループにそのグローバル・グループを追加します。

単一のドメインを維持管理する場合でも、今後ドメインが追加されるかもしれないことに留意してください。すべての権利とアクセス権を与える方法として、グローバル・グループをローカル・グループに追加する方法があります。後で別のドメインが作成された場合は、信頼関係を確立して、新しいドメインのグローバル・グループをローカル・グループに追加すれば、ローカル・グループに割り当てられていた権利とアクセス権を、新しいドメインのユーザにまで拡張できます。同様に、新しいドメインが現在のドメインを信頼する場合、現在のグローバル・グループを新しいドメインのローカル・グループに追加できます。

ドメインのグローバル・グループは、Windows NT Workstation が動作するコンピュータ上または Windows NT Server が動作するメンバ・サーバ上で管理目的に使用することも可能です。たとえば、Domain Admins グローバル・グループは、省略時の設定では、既存のドメインに参加している各ワークステーションまたはメンバ・サーバ上の Administrators ビルトイン・ローカル・グループに追加されます。ワークステーションまたはメンバ・サーバの Administrators ローカル・グループのメンバシップを使用することにより、ネットワーク管理者はプログラム・グループの作成、ソフトウェアのインストール、コンピュータの問題解決を行って、そのコンピュータをリモートから管理できます。

ネットワーク管理者には通常 2 つの役割があります。つまり、ネットワークの管理者とユーザの役割です。安全性の点で、ネットワーク管理者は 2 つのドメイン・ユーザ・アカウントを使用する方が有理です。これらのアカウントのうち 1 つは Domain Admins グローバル・グループに属し、ネットワークの管理作業に使用します。もう 1 つのアカウントは Domain Users グローバル・グループに属し、管理以外のすべての作業に使用します。通常のユーザとしてログオンしていれば、管理者だけが変更できるネットワーク関連を不用意に変更してしまうことはありません。管理者がうっかりウィルスを持ち込んで、そのプログラムに管理者の権利がなければ、オペレーティング・システムが変更されてしまうような事態は避けられます。

表 3-9 は、グローバル・グループとローカル・グループの使用方法的ガイドラインを示しています。

表 3-9: グループのガイドライン

グループの目的	種類	説明
他のドメインまたはユーザのワークステーションで使えるように、ドメインのユーザを 1 つにグループ化する。	グローバル	グローバル・グループは、ローカル・グループに入れて、他のドメインのアクセス権と権利を直接与えることができる。
1 つのドメインだけでアクセス権と権利を必要とするユーザをグループ化する。	ローカル	ローカル・グループには、このドメインと他のドメインのユーザとグローバル・グループを入れることができる。
Windows NT Workstation が動作しているコンピュータ、またはメンバ・サーバ上でアクセス権を必要とするユーザをグループ化する。	グローバル	ドメインのグローバル・グループには、これらのコンピュータ上のアクセス権を与えることができるが、ドメインのローカル・グループには与えることができない。
他のグループを入れる。	ローカル	ローカル・グループにはグローバル・グループとユーザを入れることができるが、他のローカル・グループを入れることはできない。
複数のドメインのユーザをグループ化する。	ローカル	ローカル・グループは、それが作成されたドメイン内だけで使用できる。このローカル・グループのアクセス権を複数のドメインに与える必要がある場合は、必要とするすべてのドメインにローカル・グループを作成しなければならない。

3.3.5 グループの管理

グループ名は管理されるドメインまたはコンピュータで一意でなければなりません。グローバル・グループ名は 20 文字以下とします。ローカル・グループ名は 256 文字以下とします。グループ名には、任意の大文字、小文字の英数字が使用できます。

グループ名を区別して表示する必要がある場合には、ASU サーバは、`DOMAINNAME¥groupname` または `COMPUTERNAME¥groupname` の形式でグループ名を表示して、グループのドメインまたはワークステーションを識別

します。たとえば、Engineering というドメインにある Managers というグループは、ENGINEERING¥Managers と表示されます。

グループはコピーしたり作成したりできます。コピーすると、新しいグループは元のグループと同じメンバを持ちます。ただし、元のグループのアクセス権と権利は新しいグループにはコピーされません。

グループには、グループを識別する一意の番号であるセキュリティ識別子 (SID) が含まれています。ネットワーク上のすべてのグループには、そのアカウントが初めて作成されたときに、一意の SID が発行されます。内部プロセスは、グループ名ではなくグループ SID を参照します。グループを作成し、そのグループを削除して、次に同じ名前で作成すると、新しいグループの SID が異なるため、新しいグループは古いグループに与えられていた権利またはアクセス権を持ちません。グループの名前を変更しても、SID は保持されます。作成したグループは削除できますが、ビルトイン・グループは削除できません。グループを削除すると、そのグループだけが削除されます。つまり、削除されたグループのメンバである、ドメイン・ユーザ・アカウントまたはグローバル・グループは削除されません。

ディスク共有

ASU サーバは、ディスク共有として UNIX ディレクトリの共有を可能にし、それらの共有がドメイン・ユーザ・アカウントとグループから使用できるようにします。たとえば、ディレクトリを共有すると、権限が与えられている Windows ユーザは自分のワークステーションから共有に接続し、そのファイルにアクセスできます。

ネットワークを経由してファイルにアクセスするための唯一の方法は、その親ディレクトリの 1 つをディスク共有として共有することです。ディレクトリを共有すると、Windows ユーザはそのディレクトリと、その中のファイル、およびすべてのサブディレクトリとファイルにアクセスできます。共有ディレクトリより下位のディレクトリ・ツリーにあるすべてのファイルが使用可能になります。Windows NT のアクセス権を使用して共有へのユーザ・アクセスを管理し、Windows NT ファイル・システム (NTFS) および Tru64 UNIX のアクセス権を使用して、共有内のファイルとディレクトリへのユーザ・アクセスを管理します。

この章では、次の項目について説明します。

- ディスク共有のアクセス権
- ディレクトリの複製
- ディスク共有の使用管理

ディスク共有の作成については、『*Advanced Server for UNIX* インストレーション/管理ガイド』を参照してください。

4.1 ディスク共有のアクセス権

すべてのファイルとディレクトリには所有者が存在します。所有者は、ファイルおよびディレクトリに対するアクセス権の設定を制御することも、他のユーザにアクセス権を与えることもできます。ファイルまたはディレクトリを作成すると、作成者は、自動的にその所有者になります。省略時の設定で

は、ディスク共有にあるファイルまたはディレクトリにアクセスする前に、次のセキュリティ・レベルをパスする必要があります。

- Windows NT 共有レベルのセキュリティ
- Windows NT File System (NTFS) のセキュリティ
- Tru64 UNIX ファイルおよびディレクトリのセキュリティ

ユーザがドライブをディスク共有にマッピングし、そのディスク共有にあるファイルへのアクセスを要求すると、次のような手順で、アクセス権がチェックされます。

1. Windows オペレーティング・システムが動作しているシステムから、ユーザがディスク共有に接続します。省略時の設定では、すべてのユーザは共有に接続するためのアクセス権を持っています。

ユーザの Windows システムは、ユーザ名、パスワード、およびセキュリティ ID などのユーザに関する認証情報を、ASU サーバに渡します。

2. ASU サーバは、ユーザ名とパスワードをディレクトリ・データベースで確認します。

ASU サーバがユーザの情報を認証すると、一意の ID がユーザの Windows システムに割り当てられます。ユーザが共有に対して、次回要求を行う際には、Windows システムはこの ID を提示する必要があります。

3. ユーザが共有内のファイルを開きます。

ASU の `lmx.srv` プロセスは、ユーザの要求に応答します。通常は、`lmx.srv` プロセスは Tru64 UNIX の最高の特権レベルである `root` として実行されます。

4. `lmx.srv` プロセスは、Windows NT 共有への適切なアクセス権を持っているかどうかを調べます。

アクセス権が不適切な場合には、`lmx.srv` は Windows システムにアクセス拒否エラーを返します。

5. `lmx.srv` プロセスは、ユーザが共有内のファイルにアクセスできる適切な NTFS アクセス権を持っているかどうかを調べます。

アクセス権が正しくない場合、`lmx.srv` プロセスは Windows システムにアクセス拒否エラーを返します。

- 6. `lmx.srv` プロセスは、ドメイン・ユーザ・アカウントと Tru64 UNIX ユーザ・アカウントとを照合して Tru64 UNIX のアクセス許可を調べます。
- 7. `lmx.srv` プロセスは、実効ユーザ ID を、`root` から対応する Tru64 UNIX アカウントの ID に変更して、ファイルを開きます。
- 8. Tru64 UNIX オペレーティング・システムは、ユーザが適切な Tru64 UNIX のアクセス許可を持っているかどうかを調べます。
アクセス許可が適切な場合、ファイルが開かれます。アクセス許可が不適切な場合、`lmx.srv` プロセスは Windows システムにアクセス拒否エラーを返します。

4.1.1 Windows NT のアクセス権

表 4-1 は、ディスク共有に対して設定できる Windows NT のアクセス権について説明しています。

表 4-1: Windows NT のアクセス権

アクセス権	意味
アクセス権なし	ユーザはディスク共有にアクセスできない。
読み取り	実行可能な操作： <ul style="list-style-type: none">ファイルとサブディレクトリ名の表示サブディレクトリへの移動ファイルのデータ表示アプリケーション・ファイルの実行

表 4-1: Windows NT のアクセス権 (続き)

アクセス権	意味
変更	「読み取り」で許可される操作に加えて、次の操作が可能： <ul style="list-style-type: none">ファイルとサブディレクトリの追加ファイルのデータ変更サブディレクトリとファイルの削除
フル コントロール	「読み取り」と「変更」で許可されるすべての操作に加えて、次の操作が可能： <ul style="list-style-type: none">Windows NT および NTFS のアクセス権の変更ファイルとサブディレクトリの所有権を取得するための、Windows NT および NTFS のアクセス権の設定 省略時の設定では、Everyone グループに対して新しいディスク共有への「フル コントロール」アクセス権を与える。

注意

アクセス権は累積されますが、「アクセス権なし」は他のアクセス権より優先します。たとえば、Coworkers グループはあるファイルに対して書き込みアクセス権を持っているが、Finance グループは読み取りアクセス権しか持っていないとします。John が両方のグループのメンバである場合、John には読み取りと書き込みのアクセス権が与えられます。そのファイルに対する Finance グループのアクセス権を「アクセス権なし」に変更すると、John がファイルに対して書き込みアクセス権を持つグループのメンバであっても、そのファイルを使用できません。

Windows NT のアクセス権の設定については、『*Advanced Server for UNIX* インストレーション/管理ガイド』を参照してください。

4.1.2 Windows NTFS のアクセス権

ユーザの必要に応じて、NTFS のアクセス権を設定またはカスタマイズできる NTFS アクセス権の標準セットがあります。表 4-2 は、設定可能な

Windows NTFS の標準アクセス権について説明しています。表 4-3 は、設定可能な Windows NTFS の個別アクセス権について説明しています。

表 4-2: NTFS の標準アクセス権

アクセス権	ファイルの場合	ディレクトリの場合
追加	現在のファイルの内容の読み取り、それらの変更、およびファイルの一覧を表示することはできない。	ファイルをディレクトリに追加できる。
追加と読み取り	ファイルの読み取りと実行はできるが、ファイルの変更はできない。	ディレクトリ内のファイルの読み取り、書き込み、および実行ができる。
変更	現在のファイルの内容を変更できる。	ファイルの読み取りと追加ができる。
フル コントロール	ファイルの読み取り、変更、新規ファイルの追加、ファイルのアクセス権の変更、およびファイルの所有権の取得ができる。	ディレクトリのアクセス権の変更と、ディレクトリの所有権の取得ができる。
アクセス権なし	適用されない。	ユーザが、ディレクトリへのアクセスが許可されているグループのメンバーであっても、このディレクトリにアクセスできない。
一覧	ファイルにアクセスできない。	このディレクトリ内にあるファイルとサブディレクトリの一覧表示と、このディレクトリのサブディレクトリへの移動ができる。
読み取り	ファイルの内容の読み取りおよびアプリケーションの実行ができる。	ファイルとサブディレクトリの名前を参照できる。

表 4-3: NTFS の個別アクセス権

アクセス権	ファイルの場合	ディレクトリの場合
アクセスの変更 (p)	ファイルのアクセス権を変更できる。	ディレクトリのアクセス権を変更できる。
削除 (d)	ファイルを削除できる。	ディレクトリを削除できる。
実行 (x)	ファイルがプログラムの場合に実行できる。	サブディレクトリに移動できる。

表 4-3: NTFS の個別アクセス権 (続き)

アクセス権	ファイルの場合	ディレクトリの場合
読み取り (r)	ファイルのデータを表示できる。	ファイルとサブディレクトリの名前を表示できる。
所有権の取得 (o)	ファイルの所有権を取得できる。	ディレクトリの所有権を取得できる。
書き込み (w)	ファイルのデータを変更できる。	ファイルとサブディレクトリを追加できる。

NTFS では、2 種類のアクセス権が表示されます。つまり、ディレクトリに設定されたアクセス権と、ディレクトリ内のファイルに設定されたアクセス権です。たとえば、peter というユーザに対し、ある共有に「追加と読み取り」アクセス権が設定されている場合には、次の出力が表示されます。(RWX) は、そのディレクトリに対して読み取り、書き込み、および実行のアクセス権を持っていることを示し、(RX) は、そのファイルに対して読み取りと実行のアクセス権を持っていることを示します。

```
Resource:      c:\usr\net\servers\lanman\shares\share1
Owner:         server1.dom\Administrators
Name:          Permissions:
-----
*Administrators      FullControl (All) (All)
*Everyone            Read (RX) (RX)
peter               AddRead (RWX) (RX)
```

ASU サーバでは、グループ名の前にアスタリスク (*) を付けてグループを表します。

ディレクトリ内のファイルに対する NTFS アクセス権は、「アクセス権の指定なし」に設定することができます。これは、そのディレクトリ内に存在するファイル、またはこのアクセス権を設定したのちに作成されたファイルに対して、省略時の設定により、そのユーザまたはグループにファイルに対する何のアクセス権も設定しないということです。アクセス権を付与しない限り、グループまたはユーザはそのディレクトリ内のファイルを使用することはできません。

ディレクトリにアクセス権を設定すると、CREATOR OWNER 特殊グループを使用して、ユーザがそのディレクトリ内に作成したサブディレクトリとファイルだけを制御できるようにすることができます。CREATOR OWNER に設定されたアクセス権は、ディレクトリ内にディレクトリまたはファイルを作成するユーザに転送されます。ディレクトリのアクセス権を変更するに

は、そのディレクトリの所有者になるか、または所有者によってそれを行うアクセス権を付与されている必要があります。

注意

Windows NTFS アクセス権の省略時の設定では、すべてのドメイン・ユーザ・アカウントが所属メンバとなる Everyone グループに読み取りおよび実行アクセス権が付与されます。ディスク共有にファイルの書き込みを行うドメイン・ユーザ・アカウントまたはグループに対しては、Windows NTFS 書き込みアクセス権を付与する必要があります。

Windows NTFS のアクセス権の設定については、『*Advanced Server for UNIX* インストレーション/管理ガイド』を参照してください。

4.1.3 Tru64 UNIX のアクセス許可

省略時の設定では、ディスク共有に作成されたサブディレクトリには、次の Tru64 UNIX のアクセス許可があります。

- 所有者 (Owner) は読み取りと書き込みのアクセス許可を持ちます。
- グループ (Group) は読み取りアクセス許可を持ちます。
- 他のユーザ (Other) は読み取りアクセス許可を持ちます。

省略時の設定では、ディスク共有に作成されたファイルには、次の Tru64 UNIX のアクセス許可があります。

- 所有者は読み取りと書き込みのアクセス許可を持ちます。
- グループは読み取りアクセス許可を持ちます。
- 他のユーザは読み取りアクセス許可を持ちます。

Tru64 UNIX のアクセス許可の設定方法については、『システム管理ガイド』を参照してください。

4.1.4 ディスク共有のアクセス権に関する考慮事項

ファイルまたはディレクトリを作成するユーザは、そのファイルまたはディレクトリの所有者です。ただし、Administrators グループのメンバであるユーザは常に、ファイルまたはディレクトリの所有権を取得できます。所有

者は、設定されているアクセス権を変更することにより、ファイルまたはディレクトリへのアクセスを制御できます。ディレクトリへのアクセス権を変更するときは、ディレクトリにあるすべてのファイルとサブディレクトリにその変更を適用するかどうかを決めます。ユーザは、使用するためのアクセス権が与えられているか、または使用するためのアクセス権を持つグループに所属していない限り、ディレクトリまたはファイルを使用できません。設定する各アクセス権は、グループまたはユーザがディレクトリまたはファイルに対して持つことができるアクセス権を指定します。たとえば、Coworkers グループに対して、MY_IDEAS.DOC というファイルに読み取りアクセス権を設定すると、Coworkers グループのユーザは、そのファイルのデータと属性を表示できますが、ファイルの内容を変更したり、ファイルを削除したりすることはできません。

セキュリティを管理する最も簡単な方法は、個々のユーザではなく、グループに対してアクセス権を設定することです。一般に、ユーザは多数のファイルにアクセスする必要があります。ユーザがファイルへのアクセス権を持つグループのメンバである場合、各ファイルのアクセス権を変更するのではなく、グループからユーザを削除することでユーザのアクセス権を終了させることができます。個々のユーザに対してアクセス権を設定しても、ユーザが所属するグループからユーザに与えられたアクセス権よりも優先されることはないことに留意してください。

ファイルまたはディレクトリをコピーすると、現在のセキュリティ・アクセス権、所有権、および監査情報は破棄されます。コピー先のファイルまたはディレクトリは、コピー先のディレクトリから新しいアクセス権を継承します。ファイルまたはディレクトリをコピーするユーザは、所有者になります。

4.2 ディレクトリの複製

ASU サーバが実行する便利な機能の 1 つに、共有資源を最新の状態に保つことがあります。この機能は Replicator サービスによって実現されます。多数のユーザに配布するディレクトリとファイルがある場合は、Replicator サービスを使用し、コントローラとワークステーション上に同一のディレクトリ・ツリーを設定して維持管理することにより、両者の間で負荷を分散できます。

Replicator サービスを使用するには、1 つのコンピュータをエクスポート・サーバとして構成し、ディレクトリとファイルのマスタ・コピーをこのサーバに置き、その他のコンピュータはインポート・コンピュータとして構

成します。必要なことは、エクスポート・サーバ上にディレクトリまたはファイルのコピーを1つだけ作成することだけです。すると、インポート・コンピュータは自動的にそのディレクトリまたはファイルの同一コピーを受け取ります。エクスポート・サーバ上でディレクトリ・ツリーにあるディレクトリまたはファイルを更新すると、更新されたディレクトリまたはファイルは自動的に、すべてのインポート・コンピュータにコピーされます。

すべてのエクスポート・サーバは、ディレクトリとファイルのエクスポート先コンピュータのリストを維持管理し、各インポート・コンピュータは、ディレクトリとファイルのインポート元コンピュータのリストを維持管理します。エクスポート・サーバはドメイン名に対してエクスポートでき、インポート・コンピュータはドメイン名からインポートできます。この方法は、多数のコンピュータに対してディレクトリの複製を設定する場合に便利です。各エクスポート・サーバとインポート・コンピュータでは、エクスポート先とインポート元としてドメイン名を指定するだけで、長いコンピュータ名を指定しなくて済みます。

ASU サーバは、エクスポート・サーバまたはインポート・コンピュータとして構成できます。

4.2.1 ディレクトリの複製の概要

Replicator サービスは、各エクスポート・サーバとインポート・コンピュータ上で実行する必要があります。Replicator サービスは、各エクスポート・サーバ上で更新されたディレクトリとファイルを、複製に参加しているインポート・コンピュータに送信します。各コンピュータ上の Replicator サービスは、同一のユーザ・アカウント (この機能の実行用に作成) を使用してログオンします。

1 つのドメインは、複数のエクスポート・サーバを持つことができます。ただし、複製された情報の一貫性を確保するために、重複したサブディレクトリをエクスポートしないようにする必要があります。エクスポート・サーバ上の省略時のエクスポート・パスは、`/usr/net/servers/lanman/shares/asu/repl/export` ディレクトリで、その中には複製されるディレクトリとファイルが含まれている必要があります。変更がディレクトリ内のサブディレクトリやファイルに保存されると、そのサブディレクトリやファイルは、自動的にすべてのインポート・コンピュータ上の、既存のサブディレクトリやファイルと置き換わります。

また指定によって、エクスポート・サーバに直ちにその変更内容を送信させることも、エクスポート・サーバが安定するまで2分間待たせることもできます。こうすることで、部分的に変更されたサブディレクトリ・ツリーがエクスポートされるのを防止できます。さらに、エクスポート・ディレクトリまたはインポート・ディレクトリをロックすることもできます。ロックされたディレクトリに対する変更は、そのディレクトリのロックを解除するまで、エクスポートまたはインポートされません。

エクスポート・サーバでは、エクスポートするディレクトリやファイルのコピーを受け取るインポート・コンピュータを指定します。エクスポート・サーバには、複製の送り先であるインポート・コンピュータのリストが1部しかありません。複製されるすべてのディレクトリは、エクスポート・パスのサブディレクトリとしてエクスポートされます。エクスポート・パスに作成されたサブディレクトリや、そのサブディレクトリ内のファイルは、自動的にエクスポートされます。エクスポート・サーバでは、複製できるサブディレクトリ数に制限はありません(利用できるメモリによって制限されます)。エクスポートされたサブディレクトリには、最大32レベルのサブディレクトリを作成することができます。

インポートされたサブディレクトリとファイルは、自動的に
`/usr/net/servers/lanman/shares/asu/repl/import` ディレクトリに格納されます。サブディレクトリはディレクトリを複製するとき自動的に作成されるので、インポート・サブディレクトリを作成する必要はありません。

4.2.2 ディレクトリの複製の構成

エクスポート・サーバとインポート・コンピュータ上でディレクトリの複製を構成するには、次の手順を実行します。

1. ログオンするときに使用する Replicator サービスのドメイン・ユーザ・アカウントを作成します。ユーザ・アカウントでは、[パスワードを無期限にする] オプションが選択されており、ログオン時間が制限されていないことを確認します。

ドメイン・ユーザ・アカウントの作成については、『*Advanced Server for UNIX* インストレーション/管理ガイド』を参照してください。

2. エクスポート・サーバとして構成される各コンピュータに対して、サーバー マネージャを使用し、[コンピュータ] メニューから [プロパティ]、続いて [複製] を選択し、次のように構成します。

- Replicator サービスを自動的にスタートさせる。
- Replicator サービス用に作成したドメイン・ユーザ・アカウントを使用してログオンする。
- インポート・コンピュータ名およびドメイン名を [エクスポート一覧] に追加する。

Replicator サービスの設定についての詳細は、サーバー マネージャのヘルプを参照してください。

3. エクスポート・サーバとして設定するコンピュータ上に、エクスポートされるディレクトリを作成します。そのディレクトリは複製エクスポート・パス `/usr/net/servers/lanman/shares/asu/repl/export` のサブディレクトリでなければなりません。
4. インポート・コンピュータとして構成される各コンピュータに対して、サーバー マネージャを使用して、[コンピュータ] メニューから [プロパティ]、続いて [複製] を選択し、次のように構成します。
 - Replicator サービスを自動的にスタートさせる。
 - Replicator サービス用に作成したドメイン・ユーザ・アカウントを使用してログオンする。
 - エクスポート・サーバ名およびドメイン名を [インポート元一覧] に追加する。

Replicator サービスの設定についての詳細は、サーバー マネージャのヘルプを参照してください。

エクスポート・サーバを設定して、ディレクトリ・ツリーをそれ自身に (そのエクスポート・ディレクトリを同じサーバのインポート・ディレクトリへ) 複製できます。こうすれば、ファイルのローカル・バックアップが作成できます。さらに、これらのファイルのインポート・バージョンをユーザ・アクセス用の別ソースとして使用し、ファイルのエクスポート・バージョンをソース・マスタとして保存することもできます。

4.2.3 エクスポート・サブディレクトリの管理

サーバー マネージャを使用して、[ディレクトリの複製] ダイアログ・ボックスで [ディレクトリのエクスポート] の [管理] をクリックすると、エクスポートされるサブディレクトリを管理できます。ディレクトリ複製に関して次のような管理ができます。

- サブディレクトリをロックすると、そのディレクトリはどのインポート・コンピュータにもエクスポートされなくなります。たとえば、あるディレクトリが一連の変更内容を受け取ることがわかっている場合に、エクスポート・パスのサブディレクトリを1つ以上ロックすると、変更内容が部分的に複製されるのを防ぐことができます。ロックを解除するまでサブディレクトリは複製されません。ロックした日時が表示されるので、ロックが有効になっている期間を知ることができます。
- サブディレクトリの安定化では、変更後2分間エクスポート・サーバを待たせてからサブディレクトリをエクスポートさせます。この待機期間を設けることで、後続の変更を行う時間的余裕が生じ、複製される前に、意図していたすべての変更が行われます。
- エクスポート対象を指定することにより、すべてのエクスポート・サブディレクトリ、またはエクスポート・ディレクトリ・パスの第1レベルのサブディレクトリだけをエクスポートできます。

4.2.4 インポート・サブディレクトリの管理

ロックを使用すると、インポート・コンピュータのサブディレクトリにインポートしないようにすることができます。インポート・コンピュータのサブディレクトリをロックすると、そのロックを解除しない限り、サブディレクトリはそのコンピュータに複製されなくなります。インポート・コンピュータのサブディレクトリをロックした場合、そのコンピュータへの複製だけに作用し、他のインポート・コンピュータへの複製には影響しません。

サーバー マネージャを使用して、[ディレクトリの複製] ダイアログ・ボックスの [ディレクトリのインポート] の [管理] をクリックすると、サブディレクトリへのロックを管理したり、各サブディレクトリの状態を表示したりできます。

[状態] 欄には、次の4つの項目のいずれかが表示されます。

- [OK] は、サブディレクトリがエクスポート・サーバから通常の更新を受け取ったことと、インポートされたデータがエクスポートされたデータと同一であることを示します。
- [マスタなし] は、サブディレクトリが過去には更新を受け取っていたが、現在は更新を受け取っていないことを示します。エクスポート・サーバが起動していないか、またはエクスポート・サーバでロックが有効になっている可能性があります。

- [同期なし] は、サブディレクトリが更新を受け取っているにもかかわらず、そのデータが最新のものでないことを示します。原因としては、通信障害、インポート・コンピュータまたはエクスポート・サーバ上でファイルが開かれていること、インポート・コンピュータがエクスポート・サーバでのアクセス権を持っていないこと、エクスポート・サーバの誤動作、大規模なサブディレクトリの複製が進行中であることなどが考えられます。
- 空白 (項目が表示されない場合) は、そのサブディレクトリでは複製が行われていないことを示します。インポート・コンピュータまたはエクスポート・サーバ、あるいはその両方で、複製が正しく構成されていない可能性があります。

[最終更新日時] 欄には、インポート・サブディレクトリまたはそのサブディレクトリのいずれかに最後の更新が行われた日時が表示されます。

ロックの管理についての詳細は、サーバー マネージャのヘルプの「インポートするサブディレクトリの一覧を表示する、またはロックを管理する」を参照してください。

4.2.5 ログオン・スクリプトの複製

ログオン・スクリプトとは、ドメイン・ユーザ・アカウントに割り当てることができるファイルのことです。割り当てられたログオン・スクリプトは、ユーザがログオンするたびに実行されます。ログオン・スクリプトを使用すると、管理者は、ユーザ環境のすべての側面を管理しなくても、ドメイン・ユーザの環境を管理することができます。コントローラがログオン要求を処理すると、システムは指定されているログオン・スクリプトを探します。ログオン・スクリプトの割り当てについての詳細は、3.1.2 項を参照してください。

PDC と 1 つ以上の BDC を持つドメイン内でログオン・スクリプトを使用する場合には、ドメイン・コントローラ間でログオン・スクリプトを複製する必要があります。ドメインのすべてのログオン・スクリプトのマスタ・コピーを、1 つのサーバ (PDC でもかまわないが、PDC 以外でも可能) 上の複製エクスポート・ディレクトリに格納する必要があります。ログオン・スクリプトの複製は、ドメインへのログオン認証を行うすべてのコントローラに対して行います。これにより、各ログオン・スクリプトのコピーを 1 つだけ維持管理するだけで、ドメインのログオン認証を行う

すべてのコントローラで、すべてのユーザのログオン・スクリプトの同一コピーを利用できるようになります。

省略時の設定では、ASU サーバは、`/usr/net/servers/lanman/shares/asu/repl/export/scripts` ディレクトリからインポート・コンピュータの `/usr/net/servers/lanman/shares/asu/repl/import/scripts` ディレクトリにログオン・スクリプトをエクスポートします。

4.2.6 ディレクトリの複製の使用

ドメイン内に、複製したいディレクトリ・ツリーが 2 つ (ログオン・スクリプト用と他のデータ用) あるとします。この 2 つのディレクトリ・ツリーのインポートが必要なコンピュータは異なっています。4 つのドメイン・コントローラにはログオン・スクリプトが必要で、他のデータのインポートが必要なのは、2 つのドメイン・コントローラと 2 つの Windows NT サーバだけだとします。

最良の解決策は、2 つのエクスポート・サーバを設定し、一方はスクリプトのディレクトリ・ツリー用に、もう一方はデータのディレクトリ・ツリー用に使用することです。1 つのエクスポート・サーバには、複製するインポート・コンピュータのリストが 1 つしかないことに注意してください。2 つのディレクトリに対して 1 つのエクスポート・サーバを設定すると、すべてのインポート・コンピュータが両方のディレクトリ・ツリーを必要としない場合でも、両方のディレクトリ・ツリーが、すべてのインポート・コンピュータにエクスポートされます。

4.2.7 複製に関する問題解決のヒント

ディレクトリの複製に関する問題は、さまざまな原因で発生します。Replicator サービスでエラーが発生した場合は、イベント ビューアに表示されます。イベント ビューアには、[インポート ディレクトリの管理] ダイアログ・ボックスの [状態] 欄についての情報と、ディレクトリの複製を構成中に表示されるメッセージに関する情報が表示されます。

イベント ビューアについての詳細は、第 6 章を参照してください。

4.2.7.1 アクセスの拒否

イベント ビューアに、Replicator サービスに対してアクセス拒否を示す `access denied` エラーが表示された場合は、次のことを確認してください。

- エクスポート・サーバとインポート・コンピュータ上の Replicator サービスが、同じドメイン・ユーザ・アカウントを使用してログインするように設定されている。
- インポート・コンピュータの Replicator サービスが使用したドメイン・ユーザ・アカウントに、エクスポート・コンピュータ上のファイルを読み取るアクセス権が与えられている。

エクスポート・ディレクトリに対する省略時のアクセス権は、Replicator ローカル・グループに「フル コントロール」アクセス権が与えられます。「フル コントロール」アクセス権がディレクトリから削除されると、エクスポートされたファイルはインポート・コンピュータにコピーされますが、アクセス権が正しい設定ではないので、アクセス拒否エラーがイベント・ログに記録されます。必要に応じて、サーバー マネージャを使用して、エクスポート・ディレクトリに関連付けられた共有のプロパティを選択し、[アクセス権] を選択し、Replicator ローカル・グループに「フル コントロール」アクセス権を与えます。

4.2.7.2 特定のコンピュータへのエクスポート

[ディレクトリの複製] ダイアログ・ボックスの [エクスポート先一覧] と [インポート元一覧] にエクスポート・サーバとインポート・コンピュータが指定されていることを確認します。指定されていない場合は、ローカル・ドメインのすべてのインポート・コンピュータにエクスポートが行われ、ローカル・ドメインのすべてのエクスポート・サーバからインポートが行われることになります。

エクスポート・サーバには、複製するインポート・コンピュータのリストが 1 つしかありません。そのリストにあるすべてのインポート・コンピュータは、エクスポートされたディレクトリとファイルをすべて受け取ります。どのインポート・コンピュータがどのエクスポート・ファイルやディレクトリを受け取るかは選択できません。この制御レベルでは、複数のエクスポート・サーバを使用し、それに応じてそれらのサーバを構成する必要があります。

4.2.7.3 インポート・ディレクトリのアクセス権の喪失

エクスプローラやファイル・マネージャを使用して、
/usr/net/servers/lanman/shares/asu/repl/import ディ
レクトリにあるアクセス権を調べないでください。これを行うと、あらかじめ設定されている特殊なアクセス権を喪失する可能性があります。この初期設定のアクセス権は、ディレクトリの複製ができるようにするためのもので、変更する必要はありません。

4.2.7.4 WAN 接続を経由したドメイン名への複製

一部またはすべてのインポート・コンピュータがエクスポート・サーバから WAN (ワイド・エリア・ネットワーク) ブリッジを経由して接続されている場合には、ドメイン名への複製が正しく行われないことがあります。エクスポート・サーバ上の [エクスポート先一覧] に名前を追加する場合や、インポート・コンピュータ上の [インポート元一覧] に名前を追加する場合には、WAN ブリッジで隔てられているコンピュータに対しては、(ドメイン名の代わりに、またはドメイン名の指定に加えて) コンピュータ名を指定してください。

4.3 ディスク共有の使用管理

表 4-4 は、サーバー マネージャの [プロパティ] オプションまたは net コマンドを使用して表示できる、ディスク共有の使用についての情報を示しています。

表 4-4: ディスク共有の使用

オプション	説明	net コマンド
セッション	コンピュータにリモートで接続しているユーザ数、ユーザが接続されている共有	# net session
開いているファイル	コンピュータ上で開いている共有資源の数	# net file
ファイルのロック	コンピュータ上で開いている資源に対するファイル・ロックの数	# net file
開いている名前付きパイプ	コンピュータ上で開いている名前付きパイプの数。プリント・ジョブは開いている名前付きパイプとして監視される場合がある。	# net file

net コマンドについての詳細は、『*Advanced Server for UNIX* インストレーション/管理ガイド』および net help コマンドを参照してください。

4.3.1 共有からのユーザの切断

サーバー マネージャまたは net コマンドを使用して、共有から 1 ユーザまたはすべてのユーザの接続を切断できます。データの喪失を防ぐには、接続を切断する前に必ずユーザに通知します。メッセージ送信についての詳細は、4.3.2 項を参照してください。

net コマンドを使用して、すべてのユーザの接続を切断するには、次のコマンドを入力します。

```
# net session /delete
```

サーバー マネージャを使用して、共有から 1 ユーザまたはすべてのユーザの接続を切断するときは、次の手順に従います。

1. リモート・コントローラ上の共有に接続しているユーザの接続を切断する場合は、[ドメインの選択] を選択し、コントローラのドメインを入力します。別のコンピュータをリモートで管理している場合、ユーザ・アカウントは IPC\$ 資源に接続されたユーザとして表示されます。そのユーザの接続は切断できません。
2. [コンピュータ] メニューから [プロパティ] を選択します。
[プロパティ] ダイアログ・ボックスが表示されます。
3. 次の選択をします。
 - [ユーザー] を選択し、接続されているすべての共有から 1 ユーザまたはすべてのユーザの接続を切断します。
[ユーザー セッション] ダイアログ・ボックスが表示されます。
ユーザの接続を切断するには、リスト中のユーザを選択し、[切断] を選択します。すべてのユーザの接続を切断するには、[すべて切断] を選択します。
 - [共有] を選択し、接続されている特定の共有から 1 ユーザまたはすべてのユーザの接続を切断します。
[共有資源] ダイアログ・ボックスが表示されます。[共有名] ウィンドウにある共有資源の名前を選択します。1 ユーザの接続を切断するには、[接続中のユーザー] ウィンドウにある 1 ユーザを選

択し、[切断] を選択します。すべてのユーザを選択するには、
[すべて切断] を選択します。

4.3.2 ユーザへのメッセージ送信

サーバー マネージャ の [コンピュータ] メニューで [メッセージの送信] コマンドを実行することにより、共有に接続されているすべてのユーザにメッセージを送信できます。たとえば、1 人以上のユーザの接続を切断する前に、またはコントローラ上で Server サービスを停止する前に、このコマンドを実行できます。

メッセージを送受信するには、メッセージを送信するコンピュータ上とメッセージを受信するコンピュータ上で Messenger サービスが実行されていなければなりません。

メッセージの送信についての詳細は、サーバー マネージャのヘルプの「接続しているユーザーにメッセージを送信する」を参照してください。

ASU プリンタ共有

ASU ソフトウェアをインストールした Tru64 UNIX サーバでプリンタを動作させ、そのプリンタをプリンタ共有として Windows ユーザが使用できるようにすることができます。

Windows ユーザは、ネットワークをブラウズしてプリンタ共有を調べたり、[プリンタの追加ウィザード] を使ってプリンタ共有を使用するように Windows システムを構成したりすることができます。一度構成されると、プリンタ共有に関連付けられたプリンタは、ユーザのローカル・コンピューティング環境の透過的な拡張のように見えます。たとえば、Microsoft Word などのアプリケーションを使用して、ユーザがプリンタ共有に直接プリントすれば、ジョブはプリンタに転送されます。

この章では、次のトピックについて説明します。

- 印刷の操作についての計画
- プリンタ共有のプロパティ

ASU プリンタ共有の作成については、『*Advanced Server for UNIX* インストレーション/管理ガイド』を参照してください。

5.1 印刷の操作についての計画

ネットワークで印刷を効率的にしかも高い費用対効果で行うには、次の事項について決めておく必要があります。

- どのプリンタを使用するか。
- どのコンピュータが ASU プリンタ共有を提供するか。
- 最大限利用できるようにするには、どのようにプリンタ共有を構成するか。

5.1.1 プリンタの選択

印刷装置は、ネットワークで使用するために特別に設計された印刷装置の中から選択することもできます。このような印刷装置には、ポートとエミュレーションの自動切り替え、複数の用紙トレイ、両面印刷などのオプションが付いています。ネットワーク・プリンタを決定するときには、次の項目を考慮してください。

- 処理能力の優れた印刷装置が 2, 3 台必要なのか、または低価格の個人用印刷装置が多数必要なのか。

一般に、処理能力の優れたプリンタの方が多くの機能を備えています。が、故障した場合には多数のユーザに影響が及びます。

- どのくらいの量を印刷するのか。

印刷量がプリンタの負荷サイクル (1 ヶ月に印刷できるページ数) に見合っていれば、保守上の問題は少なくなります。

- 精密なグラフィックス機能のサポートを必要とするか。

Windows NT と TrueType 技術を組み合わせることで、通常はビットマップとテキストしかサポートしないプリンタでも、精密なグラフィックスとフォントを印刷できます。TrueType フォントは動作環境に統合されているため、すべての Windows NT アプリケーションは、変更またはアップグレードをしなくても TrueType フォントを使用できます。グラフ、チャート、ハーフトーンの写真などを多く印刷する場合は、600 dpi 以上の解像度をサポートするプリンタの使用を検討します。

- 印刷速度はどれくらい重要か。

印刷装置は、コンピュータ上のシリアル・ポートまたはパラレル・ポートを経由してネットワークに接続したり、内蔵されたローカル・エリア・ネットワーク (LAN) カードを使用して直接ネットワークに接続したりできます。ネットワークに直接接続されているプリンタは通常、パラレル・バスやシリアル・バスよりも処理速度は高速になります。ただし、印刷の処理速度はネットワーク・トラフィック、ネットワーク・インタフェース・カード (NIC)、プロトコル、および印刷装置の種類によっても異なります。

5.1.2 プリント・サーバにするコンピュータの選択

通常は、ネットワークの規模とは関係なく、いくつかのサーバにプリンタを集中して設置することになります。プリント・サーバのコンピュータは、同時にファイル・サーバまたはデータベース・サーバとして動作させることができます。ファイル操作が、サーバに直接接続されたプリンタに与える影響は、あまり大きくありません。

サーバが、頻繁に利用されるプリンタを多数管理する必要がある場合は、専用のプリント・サーバを設置した方が望ましい場合もあります。プリント・サーバとファイル・サーバをいっしょにするかどうかは、セキュリティに対する考え方によっても異なります。プリンタは使用するユーザが常に利用できるようにしておく必要がある一方で、ファイル・サーバではセキュリティが確保された部屋に設置することによって、アクセスを物理的に制限することが必要になる場合もあります。

パラレルまたはシリアル・インタフェースの印刷装置を使用する場合は、適切なプリンタ出力ポートを持っていること以外、プリント・サーバに特別なハードウェア要件はありません。多数のプリンタまたは大容量のドキュメントを管理するには、多くのメモリが必要になります。ASU サーバは、サーバの処理能力、実装されているメモリ、および一般的にプリント・サーバに送信するドキュメントのサイズと量に応じて、多数のネットワーク・インタフェース・プリンタを管理できます。サーバの処理能力を高いレベルで維持するには、印刷装置にメモリを増設します。サイズの大きいドキュメントや多数のドキュメントが蓄積するような場合を除けば、ディスク・スペースは最小限ですみます。

5.1.3 プリンタ共有へユーザがアクセスする方法の計画

プリンタ共有を構成する前に、ネットワーク・プリンティングの柔軟性と効率を向上させるさまざまな ASU 構成オプションについて考慮する必要があります。ASU では、プリンタ共有と印刷装置との間に 1 対 1 の対応関係を持たせる必要はありません。プリンタ共有と印刷装置をさまざまな方法で関連付けることにより、ユーザの印刷操作に軟性を持たせることができます。たとえば、次のように構成できます。

- 1 つのプリンタ共有と 1 台の印刷装置
- 複数のプリンタ共有と 1 台の印刷装置

複数のプリンタ共有を 1 台の印刷装置に割り当てることができるため、ドキュメントの印刷を柔軟に行うことができます。たとえば、1 台の印刷装置に 2 つのプリンタ共有が関連付けられている場合には、異なる印刷プロパティを設定できます。つまり、一方のプリンタ共有では区切りページを印刷して、もう一方のプリンタ共有では印刷しないというように設定することができます。または、一方のプリンタ共有ではドキュメントをためておいて夜間に印刷し、もう一方のプリンタ共有では 1 日 24 時間ドキュメントを印刷するというような設定もできます。

- 1 つのプリンタ共有と複数の同じ印刷装置 (プリンタ・プール)

プールでは、プリンタの数に制限はありません。アイドル状態の印刷装置があれば、それが次のドキュメントを受け入れます。この構成では、印刷装置の利用率が最大になり、ユーザがドキュメントを待つ時間が最小になります。

プールにある印刷装置はすべて同じハードウェア・モデルで、1 つの単位として動作します。プリンタ共有のプロパティ設定は、プール全体に適用されます。プリンタ・ポートは、同じタイプにすることも違うタイプを混在させることもできます (パラレル、シリアル、およびネットワーク)。

5.1.4 プリンタ・ドライバ

ハードウェア・プラットフォームとオペレーティング・システムが異なる場合は、別々のプリンタ・ドライバが必要になります。たとえば、Alpha コンピュータ上で Windows NT が動作するクライアントが、ASU サーバ上に作成されたプリンタ共有を使用するには、そのプリンタ用の適切な Alpha プリンタ・ドライバが必要です。

プリンタ・ドライバはローカルでインストールすることも、ASU サーバにインストールすることもできます。ASU サーバは、Windows 95、Alpha、Power PC、MIPS、および x86 ベースのクライアント向けのプリンタ・ドライバを、PRINT\$ というディスク共有に格納できます。こうしておけばクライアントは、プリンタ・ドライバを自動的にダウンロードすることができます。

ASU サーバは、受け取った印刷要求が Alpha、Power PC、MIPS、または x86 ベースのいずれに該当するかを判断して、適切なドライバを自動的にクライアントに送ります。

Windows NT Version 3.1 , 3.5 , 3.51 , または 4.0 をサポートするには , クライアントごとに適切なプリンタ・ドライバをインストールする必要があります。

プリンタ・ドライバのインストールについては , 『 *Advanced Server for UNIX* インストレーション/管理ガイド 』を参照してください。

表 5-1 は , サポートされていないプリンタに対する設定について説明しています。使用している印刷装置がこの表にない場合は , 利用可能なドライバがあるかどうかを製造元に問い合わせてください。

表 5-1: サポートしていない印刷装置

プリンタの種類	次のプリンタと同じ設定にする
HPPCL (LaserJet) 互換	Hewlett-Packard LaserJet Plus
Color PostScript	QMS-ColorScript
35-font Plus フォント・セット またはスーパセット	Apple LaserWriter® Plus
9 ピン・ドット・マトリックス IBM 互換	IBM Proprinter
9 ピン・ドット・マトリックス Epson® 互換	キャリッジの幅が狭い場合は Epson FX-80 , 広い場合は FX-100
24 ピン・ドット・マトリックス IBM 24 ピン互換	IBM Proprinter X24
24 ピン・ドット・マトリックス Epson LQ 互換	Epson LQ-1500

5.2 プリンタ共有のプロパティ

この節では , プリンタ共有のプロパティについて説明します。

5.2.1 区切りページ

ASU サーバは , 各プリント・ジョブの前に , 区切りページつまりバナーを自動的に印刷します。省略時のバナー・ページを変更したり , 必要に応じてもう 1 つ作成したりすることができます。

区切りページを設定または変更するには `net print` コマンドを使用します。

`net` コマンドについての詳細は , 『 *Advanced Server for UNIX* インストレーション/管理ガイド 』 および `net help` コマンドを参照してください。

5.2.2 プリント・プロセッサ・スクリプトの使用

プリント・プロセッサ・スクリプトを使用すると、プリント・ジョブをプリンタではなくファイルまたは端末に直接送るか、`uucp` コマンドを使用してリモートの Tru64 UNIX システムのコンピュータに送るか、または `troff` や `nroff` などの別の Tru64 UNIX システムのプロセスに送ることができます。

プリント・プロセッサ・スクリプトを作成する場合は、ユーザがアクセスできるように、そのスクリプトを使用するキューを共有しなければなりません。ユーザは、他のプリント・キューと同様にこのキューにアクセスします。他のユーザへのサービスに影響を及ぼさないように、このスクリプトはバックグラウンドで実行してください。表 5-2 は、プリント・プロセッサ・スクリプトに使用できる環境変数を示しています。

表 5-2: プリント・プロセッサ・スクリプトの環境変数

変数	説明
<code>\$CLIENT</code>	ジョブの送信元のコンピュータ名
<code>\$COPIES</code>	印刷部数 (1 部以上)
<code>\$PRIO</code>	プリント・ジョブの Tru64 UNIX システムの <code>lpr</code> 優先順位 (1 ~ 39)
<code>\$DEST</code>	ジョブの送信先である Tru64 UNIX システムの <code>lpr</code> プリンタ・クラス (サーバ・キュー)
<code>\$FILENAME</code>	処理するファイルの絶対パス名

プリント・プロセッサ・スクリプトを作成するには、次の手順に従います。

1. テキスト・エディタを使用して、シェル・スクリプトを作成し、それを `lanman/customs` ディレクトリに保存します。
2. そのスクリプトを `chmod +x` コマンドを実行して実行可能ファイルにします。
3. `net print /PROCESSOR:pathname` コマンドを使用して、プリンタ共有を構成し、プリント・プロセッサ・スクリプトを使用します。

`net` コマンドについての詳細は、『*Advanced Server for UNIX* インストレーション/管理ガイド』および `net help` コマンドを参照してください。

5.2.3 スケジュールとスプールの設定

印刷装置の使用率を最大にする 1 つの方法は、印刷時間をずらすことです。たとえば、プリンタ・トラフィックが一日中多い場合には、時間外に印刷するプリンタ共有に優先度の低いドキュメントを送ることによって印刷を遅らせることができます。印刷時間を指定すると、プリント・スプーラは任意の時間にドキュメントを受け付けますが、指定した時間が来るまで、指定の印刷装置にプリントしません。印刷停止時間になると、スプーラは印刷装置へのドキュメント送付を停止し、印刷が再び開始するようにスケジュールされている時間まで、残っているドキュメントを保存します。

表 5-3 は、スケジュールとスプールのオプションについての説明です。これらのオプションは、プリンタの [プロパティ] シートの [スケジュール] タブを使用するか、`net` コマンドを使用して設定できます。

表 5-3: スケジュールのオプション

オプション	説明	net コマンド
利用可能時間	プリンタが利用できる時間を定義する。	# net print /AFTER:time # net print /UNTIL:time:time
優先順位	ドキュメントの優先度に基づいて、優先度の異なるプリント・キューを設定する。	# net print /PRIORITY:# (1 が最高で 9 が最低)
全ページ分のデータをスプールしてから印刷データをプリンタに送る	クライアントが印刷するページを送信するよりも、プリント・サーバの印刷速度の方が速い場合に、遅延が生じるのを防止する (省略時の設定は変更できない)。	同等な net コマンドはない。

`net` コマンドについての詳細は、『*Advanced Server for UNIX* インストール/管理ガイド』および `net help` コマンドを参照してください

5.2.4 プリンタ共有へのアクセスの制御

プリンタの使用を制御するには、各プリンタ共有にアクセス権を設定します。省略時の設定では、作成したすべてのプリンタ共有は、すべてのネットワーク・ユーザが利用できます。プリンタ共有へのアクセスを制限するには、ドメイン・ユーザ・アカウントまたはグループに対するアクセス権を

変更しなければなりません。表 5-4 は、プリンタ共有に設定できるアクセス権について説明しています。プリンタ共有のアクセス権を変更できるのは、プリンタの所有者または「フル コントロール」アクセス権が与えられたユーザだけです。

表 5-4: プリンタ共有のアクセス権

アクセス権	可能な操作
アクセス権なし	プリンタ共有へのプリント不可
印刷	プリンタ共有へのプリント
ドキュメント管理	ドキュメントの設定の制御、ドキュメントの一時停止、再開、再印刷、および削除
フル コントロール	「印刷」および「ドキュメント管理」のアクセス権に加えて、次の操作が可能： <ul style="list-style-type: none">ドキュメントの印刷順序の変更プリンタの一時停止、再開、および削除プリンタのプロパティの変更プリンタ共有の削除アクセス権の変更所有権の取得 省略時の設定では、Administrators、Print Operators、および Server Operators は、「フル コントロール」アクセス権を持っている。

アクセス権は累積されます。ただし、「アクセス権なし」アクセス権は、他のすべてのアクセス権より優先されます。

5.2.5 プリンタ共有の監査

プリンタ共有を監査すると、その使用状況を追跡できます。特定のプリンタについて、監査の対象となるドメイン・ユーザ・アカウントおよびグループの操作を指定できます。成功した操作も失敗した操作も監査できます。ASU サーバは、監査で生成された情報をログ・ファイルに格納します。この情報はイベント ビューアを使用して表示できます。イベント ビューアについての詳細は、第 6 章を参照してください。

プリンタ共有を監査するには、スプーラ・イベントのログ収集を有効にし、ドメイン ユーザー マネージャを使用して監査の原則を設定してください。

表 5-5 は、監査できるプリンタ共有のイベントについて説明しています。

表 5-5: プリンタ共有の監査オプション

オプション	監査項目
印刷	ドキュメントの印刷
フル コントロール	<ul style="list-style-type: none">ドキュメントに対するジョブ設定の変更ドキュメントの一時停止，再印刷，移動，および削除プリンタの共有プリンタ共有のプロパティ変更
削除	プリンタ共有の削除
アクセス権の変更	プリンタ共有のアクセス権変更
所有権の取得	所有権の取得

5.2.6 独自の印刷フォーム

「フル コントロール」アクセス権を持つユーザは、サーバの [用紙] プロパティ・シートを使用して新しいフォーム (用紙) を定義できます。たとえば、レター・サイズ of 用紙で余白が標準とは異なる「Customer Receipt Form (受領証)」という名前のフォームを作成することができます。また、特定のユーザの要求に対応するために、同じ用紙サイズまたは余白 (またはその両方) を持つ複数のフォームを作成することもできます。たとえば、用紙サイズとイメージ領域 (余白) を同じにして、各事業部ごとにレターヘッドだけを変えたフォームを作成し、フォームごとに一意の名前を付けます。

新しいフォームの定義は、プリント・サーバのデータベースに追加され、プリンタごとではなくコントローラごとに格納されます。フォームは、プリンタの [プロパティの設定] プロパティ・シートを使用して、特定の印刷装置とトレイに割り当てます。

5.2.7 デバイス固有のプロパティの設定

デバイス固有のプロパティは、どの用紙トレイがセットされ、デバイスにどれだけのメモリがあるかなど、印刷装置の物理構成を示します。これらのプ

ロパティは装置ごとに異なります。プリンタ共有を作成するときは、省略時の設定になっています。省略時の設定でも、多くの印刷要求を満たしますが、PostScript プリンタのドライバで利用できるオプションなど、特殊な印刷オプションには特別な設定が必要になります。

次の各項で、デバイス固有のプロパティについて説明します。デバイス固有のプロパティを表示または変更するには、[プリンタ] フォルダのプリンタ・アイコンを選択し、[プリンタ] メニューの [プロパティ]、プリンタの [デバイスの設定] タブの順に選択します。

5.2.7.1 プリンタ・メモリの設定

ページ・プリンタは、1 ページ全体をメモリに格納しなければならないため、比較的大容量のメモリが必要になります。レーザ・プリンタなどのページ・プリンタを使用する場合は、装置の利用可能なメモリ容量が、[デバイスの設定] タブに表示されている値と一致していることを確認してください。印刷装置の実際のメモリ容量が、[デバイスの設定] タブに表示される値より多かったり少なかったりすると、印刷の処理速度が低下することがあります。

5.2.7.2 印刷フォームの使用

ASU サーバでは、トレイ・ベースの印刷モデルではなくフォーム (用紙)・ベースの印刷モデルを使用します。フォーム・ベースの印刷モデルでは、プリント・サーバの管理者が、各給紙方法 (トレイ) で供給されるフォーム (用紙) を定義することによって ASU サーバを構成します。フォームは次の基準で定義されます。

- サイズ
- 印刷範囲を定める余白
- フォーム名

各ユーザは、Windows NT ベースのコンピュータで実行される Windows ベースのアプリケーションを使用して、希望する印刷フォームを選択できます。このため、ユーザは、どのトレイにどのフォーム (用紙) が入っているかを知らなくても構いません。ASU サーバは、トレイとフォームの割り当てに関するデータを解釈して、印刷装置に適切なトレイを選択するよう指示を送ります。

Windows ベースのアプリケーションでは、1 つのドキュメント内で異なるフォームを使用できます。たとえば、1 ページ目には封筒 (Envelope) を使

い、2 ページ目にはレターヘッド (Letterhead) を使い、3 ページ目以降ではレター (Letter) を使用することができます。

5.2.7.3 フォントの種類を選択

フォントとは、特定のデザインと解像度を持つ文字と記号の集合のことです。印刷装置では、次の 3 種類のフォントが使われます。

- デバイス・フォントは、印刷装置のハードウェア内にあるフォントです。印刷装置自体に組み込まれている場合と、フォント・カートリッジやフォント・カードによって供給される場合があります。
- スクリーン・フォントは、印刷装置への出力用に変換できる Windows NT フォント (TrueType フォントも含む) です。スクリーン・フォントを Windows NT コンピュータにインストールするには、[コントロール パネル] フォルダの [フォント] オプションを使用します。
- ダウンロード可能なソフト・フォントは、プリンタの [プロパティ] シートの [デバイスの設定] タブを使用してインストールされるフォントです。ソフト・フォントを使用して ASU プリンタ共有に印刷するクライアントは、ソフト・フォントをローカルにインストールする必要があります。

ASU サーバは、プリンタで再現できる次の 3 種類のスクリーン・フォントをサポートします。

- TrueType フォントは、装置の仕様に依存せず、すべての印刷装置で再現できるフォントです。TrueType フォントはアウトラインとして保存されているので、サイズを変更したり回転させたりすることができます。ドキュメントを作成するコンピュータ上にフォントがあれば、印刷装置で再現できます。ネットワーク環境で TrueType フォントを使用する最大の利点は、その可搬性にあります。つまり、TrueType フォントを使用するドキュメントは、印刷装置、アプリケーション、およびシステムに依存しません。
- ラスタ・フォントは、ビットマップとして保存されており、印刷装置に依存するフォントです。印刷装置がラスタ・フォントをサポートしていない場合、ラスタ・フォントは印刷されません。ラスタ・フォントでは、サイズの変更や回転はできません。
- ベクタ・フォントは、ビットマップを再現できないペン・プロッタなどの装置で使用する则便利です。ラスタ・フォントは、サイズとアスペクト比を任意に変更できます。

クライアント・コンピュータは、ドキュメントごとに、必要なスクリーン・フォントやソフト・フォントを ASU サーバにダウンロードします。次に、ASU サーバはそれらのフォントを印刷装置に送ります。印刷時間を短縮するには、印刷装置が持っているデバイス・フォントを使用してください。

すべての印刷装置で 3 種類のプリンタ・フォントをすべて使用できるわけではありません。たとえば、一般的なペン・プロッタでは通常、ダウンロードされたソフト・フォントを使用したり、ラスタ・スクリーン・フォントを印刷したりすることはできません。

5.2.8 ドキュメントの省略時の設定

印刷装置固有の設定とドキュメントのプロパティとは、しばしば混同されがちです。ドキュメントのプロパティは、印刷装置の物理的な設定には依存しません。アプリケーションが新しいドキュメントを作成するときは、ほとんどの場合、省略時のドキュメント設定をプリンタに要求します。

表 5-6 は、一般的な印刷装置固有のプロパティとドキュメントのプロパティを一覧表示しています。

表 5-6: 一般的な設定

印刷装置固有のプロパティ	ドキュメントのプロパティ
色	部数
解像度	印刷の向き
メモリ	両面印刷
フォント・カートリッジの名前	部単位の印刷
用紙の位置	用紙
プロッタ・ペン	

プリンタ共有のドキュメントのプロパティを表示するには、[プリンタ] フォルダを開き、そのプリンタを選択し、次に [ファイル] メニューから [ドキュメントの既定値] を選択します。

注意

アプリケーションで設定されるドキュメントのプロパティは、プリンタの [プロパティ] シートで設定されているドキュメントの既定値 (省略時の設定) より常に優先されます。ただし、アプリケー

ションでドキュメントのプロパティ (印刷の向きや用紙サイズなど) が設定されていない場合、印刷装置は、プリンタのドキュメントの [プロパティ] シートで設定されているドキュメントのプロパティを省略時の設定として使用します。



イベントの監視

イベントとは、システム (またはアプリケーション) で発生し、ユーザに通知される必要がある重要なできごとのことです。重大なイベントは、画面にメッセージを表示することによってユーザに通知されます。一方、すぐにユーザに知らせなくてもよいイベントは、イベント・ログ・ファイルの監査エントリに記録されます。監査エントリには、発生したアクティビティ、処理を行ったユーザ、およびアクティビティの発生日時が入っています。成功した操作も失敗した操作も監査できます。監査証跡では、ネットワークで誰が実際に操作を行い、誰が許可されていない操作を実行しようとしたかが示されます。

イベント・ログの中の情報を使用すると、ハードウェアおよびソフトウェアのさまざまな問題に対処したり、ASU サーバのセキュリティ・イベントを監視したりすることができます。次の方法でイベント・ログを表示できます。

- Windows ベースのイベント ビューアのグラフィカル・ユーザ・インタフェース
- Tru64 UNIX の `elfread` コマンド

この章では、イベント ビューアを使用してイベントを監視および表示する方法について説明します。`elfread` コマンドについての詳細は、`elfread(8)` を参照してください。

この章では、次のトピックについて解説します。

- イベント ビューアの概要
- 監査の有効化
- イベント・ログ・オプション
- イベントの解釈
- イベント ビューアの使用方法
- イベント・ログによる問題解決

6.1 イベント ビューアの概要

ASU サーバは、次の 3 種類のログにイベントと監査エントリを記録します。

- システム・ログには、ASU サーバ・システムの構成要素が記録したイベントが入っています。たとえば、ASU が起動時に ASU サービスの開始に失敗すると、そのイベントはシステム・ログに記録されます。システムの構成要素が記録するイベントの種類は、ASU サーバによって決められています。
- セキュリティ・ログには、有効なログオンと無効なログオンの試行、および資源の使用に関連するイベント (ファイルや他のオブジェクトの作成、使用、削除など) が入っています。たとえば、ドメイン ユーザー マネージャを使用して、ログオンとログオフを監視するように設定した場合、システムにログオンしようとする、そのイベントはセキュリティ・ログに記録されます。
- アプリケーション・ログには、アプリケーションが記録したイベントが入っています。たとえば、データベース・プログラムでファイル・エラーが発生すると、そのイベントはアプリケーション・ログに記録されます。どのイベントをログするかは、アプリケーション開発者が決めます。

システム・ログとアプリケーション・ログは、すべてのユーザが見ることができますが、セキュリティ・ログは、システム管理者しか見ることができません。

6.2 監査の有効化

イベントのロギングは、ASU サーバが起動すると自動的に開始します。ただし、省略時の設定では、イベントは監査されません。管理者はドメイン ユーザー マネージャを使用して、監査の原則を指定できます。監査の原則では、ログに記録するイベントの量と種類を決定します。イベント・ログにはサイズに制限があるため、ログに使用するディスク・スペースについて検討し、監査するイベントを注意深く選択してください。セキュリティ・ログの最大サイズは、イベント ビューアで指定します。

ファイルまたはフォルダを監査しているときは、それらのファイルまたはフォルダが一定の方法でアクセスされるたびにセキュリティ・ログにエン

トリが記録されます。管理者は、どのファイルとフォルダを監査するか、およびどんな操作を監査するかを決定します。

ファイルまたはフォルダを監査するには、ドメイン ユーザー マネージャを使用して、[ファイルとオブジェクトへのアクセス] の監査を有効にします。次に、エクスプローラを使用して、監査するファイルと、監査するファイル・アクセス・イベントの種類を指定します。表 6-1 では、監査できるディレクトリとファイルに対する操作について説明します。

表 6-1: ディレクトリとファイルの監査

ディレクトリの監査	ファイルの監査
ディレクトリ内のファイル名の表示	ファイル・データの表示
ディレクトリの属性の表示	ファイルの属性の表示
ディレクトリの属性の変更	ファイルの所有者とアクセス権の表示
サブディレクトリとファイルの作成	ファイルの変更
ディレクトリ内のサブディレクトリへの移動	ファイルの属性の変更
ディレクトリの所有者とアクセス権の表示	ファイルの実行
ディレクトリの削除	ファイルの削除
ディレクトリのアクセス権の変更	ファイルのアクセス権の変更
ディレクトリの所有権の変更	ファイルの所有権の変更

6.3 イベントのログ・オプション

イベント・ログがいっぱいになり、既存のイベントに上書きできなくなると、ロギングは中止されます。これは、手動でログを消去するように設定してあるか、またはログの中の最初のイベントがあまり古くないためです。ログがいっぱいになったときは、それを消去すれば再び使用することができます。

[ログ] メニューの [ログの設定] コマンドを使用して、各種のログに対するロギング・パラメータを定義してください。ログの最大サイズの設定、イベントの上書きまたは一定期間保存の指定ができます。最大ログ・サイズを (ディスクとメモリの容量の範囲内で) 増やしたり減らしたりできますが、各ログ・ファイルには 512 KB という省略時の最大サイズが指定されています。ログのサイズを減らす前に、ログを消去する必要があります。

[イベント ログの設定] オプションを使用すると、[設定の変更] ダイアログ・ボックスで選択したログにイベントを保存する方法を定義できます。省略時のロギングの原則では、7 日間よりも古いログを上書きするように設定されています。このオプションはそれぞれのログについてカスタマイズできます。表 6-2 では、イベントのログ・オプションについて説明しています。

表 6-2: イベントのログ・オプション

オプション	保存方法
必要に応じてイベントを上書きする	ログがいっぱいになっても、引き続き新しいイベントを記録する。新しいイベントが記録されるたびに、ログの最も古いイベントが消去される。このオプションは、保守が少ないシステムに適している。
指定日数経過後にイベントを上書きする	指定した日数が経過するまでログを保存し、その後はイベントを上書きする。このオプションは、週ごとにログ・ファイルを保存する場合に最も適している。この方法を使用すると、重要なログ・エントリを失う可能性を最小限に抑えられるだけでなく、ログを妥当なサイズで維持することもできる。
イベントを上書きしない	ログを手動で消去し、自動的に消去しない。このオプションは、イベントを失うことが許されない場合にだけ選択する。たとえば、セキュリティが非常に重要なサイトのセキュリティ・ログなどに適している。

監査の原則を設定する方法については、ドメイン ユーザー マネージャのヘルプの「監査の原則を管理するには」を参照してください。

6.4 イベントの解釈

イベント・ログは、ヘッダ、イベントの説明 (イベントの種類に基づく)、およびオプションとして付加される追加のデータからなります。ほとんどのセキュリティ・ログのエントリは、ヘッダと説明で構成されます。

イベント ビューアでは、イベントはログの種類別に表示されます。1 つのイベントの情報は 1 行に表示され、日付、時刻、ソース、イベントの分類、イベント ID、ユーザ・アカウント、およびコンピュータ名が含まれます。

6.4.1 イベントのヘッダ

表 6-3 は、イベントのヘッダの内容について説明しています。

表 6-3: イベントのヘッダ

フィールド	表示
日付	イベントが発生した日付。
時刻	イベントが発生した時刻。
ユーザー	イベントを発生させたユーザの名前。イベントがユーザによってログされていない場合は、ロギング・エンティティのセキュリティ ID が表示される。
コンピュータ	イベントが発生したコンピュータの名前。
イベント ID	特定のイベントの種類を示す番号。通常、イベントの種類の名前は、説明の 1 行目に表示される。たとえば、6005 という番号は、イベント・ログ・サービスの開始時に発生するイベントの ID であり、このイベントの説明の 1 行目には、「イベント ログ サービスが開始されました。」と表示される。イベント ID とソースは、システムの問題解決のために、製品サポート担当者が使用する場合があります。
ソース	イベントのログを取ったソフトウェア・モジュール。アプリケーション名、またはサービス名など、システムや大きなアプリケーションの構成要素。
種類	イベントの重大度による分類。システム・ログとアプリケーション・ログでは、[エラー]、[情報]、[警告]のいずれかが表示される。セキュリティ・ログでは、[成功の監査]または[失敗の監査]のいずれかが表示される。イベントビューアの通常のリスト表示では、これらはアイコンで表される。
分類	イベントのソース別分類。この情報は、主にセキュリティ・ログで使用される。たとえば、セキュリティ監査では、この分類は、ドメインユーザー マネージャの [監査の原則] ダイアログ・ボックスで設定されるイベントの種類の 1 つに対応する。このダイアログ・ボックスでは、イベントの種類ごとに、成功と失敗を監査するように設定できる。

6.4.2 イベントの説明

イベントの説明の形式や内容は、イベントの種類ごとに異なります。ほとんどの場合、この説明は何が起きたのかを調べたり、そのイベントの重大度を判断したりするために最も役立つ情報となります。

表 6-4 は、イベントの種類を示しています。

表 6-4: イベントの種類

イベントの種類	意味
エラー	データの損失や機能の停止などの重大な問題。たとえば、ASU サーバの起動時に ASU サービスが開始しなかった場合に、エラー・イベントが記録される。
警告	必ずしも重大ではないが、後になって問題が生じる可能性があることを示すイベント。たとえば、ASU サーバの重要な資源が少なくなった場合に、警告イベントが記録される。
情報	主要な ASU サーバ・サービスが正常に行われていることを示すもので、通常はあまり重要ではないイベントである。たとえば、ASU サービスが正常に起動した場合に情報イベントが記録される。
成功の監査	監査されていたセキュリティ・アクセスの成功した試行。たとえば、ユーザが正常にシステムへのログオンができた場合に、成功の監査のイベントが記録される。
失敗の監査	監査されていたセキュリティ・アクセスの失敗した試行。たとえば、ユーザがネットワーク・ドライブにアクセスしようとして失敗した場合に、失敗の監査のイベントが記録される。

オプションのデータ・フィールド (使用されている場合) には、バイナリ・データがバイト単位またはワード単位で表示されます。この情報は、イベント・レコードのソースであるアプリケーションによって生成されます。このデータは 16 進形式で表示されるため、その意味はソース・アプリケーションに精通している技術者にしか解釈できません。

6.5 イベント ビューアの使用

イベント・ログを表示するときは、システム、セキュリティおよびアプリケーションの各ログを切り替えて選択します。イベントビューアを使用すると、他のコンピュータ上のログを表示させることもできます。

6.5.1 ログの選択

イベント ビューアを初めて起動したときは、ローカル・コンピュータのシステム・ログが表示されますが、セキュリティ・ログまたはアプリケーション

ン・ログに切り替えることができます。[ログ] メニューを使用して、表示するログを選択します。

6.5.2 コンピュータの選択

イベント ビューアを起動すると、最初はローカル・コンピュータのイベントが表示されます。

他のコンピュータのイベントを表示するには、[ログ] メニューの [コンピュータの選択] をクリックします。選択できるのは、Windows NT ワークステーション、ASU サーバ、Windows NT サーバ、または LAN Manager 2.x サーバのいずれかです。

選択したコンピュータが伝送速度の遅いリンクを経由している場合は、[低速回線接続] を選択します。このオプションを選択すると、ASU サーバは省略時のドメイン内にあるすべてのコンピュータをリスト表示しなくなるので、リンクを経由するネットワーク・トラフィックを最小限に抑えることができます。伝送速度の遅いリンクを利用することが多い場合は、[オプション] メニューの [低速回線接続] をクリックします。

LAN Manager 2.x サーバを選択した場合、イベント ビューアはそのサーバのエラー・ログ (システム・ログ) と監査ログ (セキュリティ・ログ) を表示できます。

イベントを表示するコンピュータを選択する方法については、イベント ビューアのヘルプの「別のコンピュータのイベント ログを選択するには」を参照してください。

6.5.3 表示の更新

ログ・ファイルを開くと、イベント ビューアによりそのログの現在の情報が表示されます。この情報は、自動的に更新されません。最新のイベントを表示し、上書きされたエントリを削除するには、[最新の情報に更新] コマンドを選択します。

詳細は、イベント ビューアのヘルプの「ログを最新の表示にする」を参照してください。

6.5.4 フォントの変更

イベントビューアで使用しているフォントを変更することができます。フォントが変更されるのは、メインの[イベントビューア]ウィンドウにあるイベントのリスト表示だけです。

詳細については、イベントビューアのヘルプの「イベント一覧で使うフォントを更新するには」を参照してください。

6.5.5 ログ・ファイルの保存

ログ・ファイル形式でイベント・ログを保存すると、後でイベントビューアで再表示することができます。ログはテキスト形式またはコンマ区切りテキスト形式で保存すると、その情報を他のアプリケーションで使用することができます。

たとえば、セキュリティ・ログを保存しておくと、一定期間にわたってセキュリティ・イベントを監視できます。また、アプリケーション・ログを保存しておくと、特定のアプリケーションで発生した警告イベントとエラー・イベントを追跡できます。

ログ・ファイルを保存すると、イベントビューアで指定したイベントだけを表示していた場合でも、ログ全体が保存されます。イベントビューアでソート順序を変更していた場合、テキスト・ファイルまたはコンマ区切りテキスト形式で保存すると、イベント・レコードは表示されている順序と同じ順序で保存されます。

ログ・ファイルは次の形式で保存できます。

- ログ・ファイル形式。この形式で保存したログは、イベントビューアで再表示できます。
- テキスト・ファイル形式。この形式で保存した情報は、ワード・プロセッサや電子メールなどのアプリケーションで使用できます。
- コンマ区切りテキスト・ファイル形式。この形式で保存した情報は、スプレッドシートやフラット・ファイルのデータベースなどのアプリケーションで使用できます。

バイナリ・イベント・データは、ログ・ファイル形式で保存した場合には保存されますが、テキスト・ファイル形式またはコンマ区切りテキスト・

ファイル形式で保存した場合には破棄されます。イベントの説明は、どの形式でログを保存した場合にでも保存されます。

ソート済みログを保存する場合、イベント・レコードの順序は、テキスト・ファイル形式またはコンマ区切りテキスト・ファイル形式では、ソートした順序になります。ただし、ログ・ファイル形式で保存されたログのイベント・レコードの順序はソートした順序の影響を受けません。どの形式で保存した場合でも、各イベント・レコード内のデータ・シーケンスは次の順序で保存されます。

- 日付 ([表示] メニューで指定したソート順序によって異なる)
- 時刻
- ソース
- 種類
- 分類
- イベント
- ユーザー
- コンピュータ
- 説明

ログ・ファイルを保存しても、現在使用中のログの内容には影響を与えません。もとのログを消去するには、[ログ] メニューの [すべてのイベントを消去] を選択する必要があります。保存されたログ・ファイルの削除方法は、他の種類のファイルを削除する場合と同じです。

イベント・ログ・ファイル形式で保存した場合に限り、保存されたファイルをイベント ビューアで表示することができます。[最新の情報に更新] コマンドまたは [すべてのイベントを消去] コマンドをクリックしても、表示の更新、保存されているログの消去はできません。

注意

ログの種類 (アプリケーション、セキュリティ、またはシステム) を正しく指定しなければ、[イベントの詳細] ダイアログ・ボックスの [説明] に保存されたログに対する正しい説明が表示されません。

6.5.6 特定のイベントの表示

イベントビューアで表示するイベントを選択した後、次の操作を行うことができます。

- イベントのソースによって記録された説明と追加情報を表示する。
- イベントを古いものから順番に、または新しいものから順番にソートする。
- 指定した特性を持つイベントだけを選別して表示する。
- 指定した特性やイベントの説明を基にしてイベントを検索する。

6.5.6.1 イベントの詳しい情報の表示

ほとんどのイベントについて、そのイベントをダブルクリックすると、イベントビューアに表示されているよりも詳しい情報を表示させることができます。

[イベントの詳細] ダイアログ・ボックスには、選択したイベントを説明するテキストと、そのイベントのバイナリ・データ (含まれている場合) が表示されます。バイナリ・データは、イベント・レコードのソースであるアプリケーションによって生成されます。このデータは 16 進形式で表示されるため、具体的な意味は、ソースのアプリケーションに精通している技術者でなければ解釈できません。また、バイナリ・データは、すべてのイベントで生成されるわけではありません。

6.5.6.2 イベントのソート

イベントビューアで表示されるイベントは、省略時の設定では、発生の日時に基づいて、新しいイベントから順番に表示されます。古いイベントから順番に表示するには、[表示] メニューの [古いイベント順] をクリックします。イベントビューアの終了時に [オプション] メニューの [終了時の状態を保存] コマンドにチェック・マークを付けると、現在のソート順序が次回イベントビューアを起動するときにも適用されます。

ログを保存するとき、イベント・レコードをテキスト形式またはコンマ区切りテキスト形式で保存すると、ソート順序はイベント・レコードの順序に影響します。一方、ログ・ファイル形式で保存すると、イベント・レコードの順序には影響しません。

6.5.6.3 イベントの選別

イベント ビューアは、省略時の設定では、選択したログに記録されているすべてのイベントを一覧表示します。特定の特性を持つイベントだけを表示するには、[表示] メニューの [イベントのフィルタ] をクリックします。フィルタ処理がオンになっている場合は、[表示] メニューの [フィルタ] コマンドにチェック・マークが付き、タイトル・バーには (フィルタ) と表示されます。イベント ビューアの終了時に、[オプション] メニューの [終了時の状態を保存] にチェック・マークを付けると、イベント ビューアを次回起動する際にもフィルタ処理が適用されます。

フィルタは、表示のしかたを変更するだけで、ログの実際の内容には影響しません。フィルタ処理の有無にかかわらず、ログにはすべてのイベントが引き続き記録されます。フィルタ表示した状態でログを保存する場合、ファイル形式がテキスト形式またはコンマ区切りテキスト形式にかかわらず、すべてのレコードが保存されます。

表 6-5 は、[フィルタ] ダイアログ・ボックスで利用できるオプションについて説明しています。

表 6-5: イベント・フィルタ

オプション	説明
表示の先頭	特定の日付と時刻以降に発生したイベント。省略時の設定では、ログ・ファイルの最初のイベントの日付が設定されている。
表示の末尾	特定の日付と時刻以前に発生したイベント。省略時の設定では、ログ・ファイルの最後のイベントの日付が設定されている。
情報	主要なサーバ・サービスの操作が正常に行われたことを示す、あまり重要ではないイベント。たとえば、サービスが正常に開始した場合に、情報イベントが記録される。
警告	必ずしも重大ではないが、後になって問題が発生する可能性があることを示すイベント。たとえば、サーバの重要な資源が少なくなった場合に、警告イベントが記録される。
エラー	データの損失や機能の停止などの重大な問題。たとえば、ASU サーバの起動時に ASU サービスが開始しなかった場合に、エラー・イベントが記録される。
成功の監査	監査されていたセキュリティ・アクセスの成功した試行。たとえば、ユーザがシステムに正常にログオンできた場合に、成功の監査のイベントが記録される。

表 6-5: イベント・フィルタ (続き)

オプション	説明
失敗の監査	監査されていたセキュリティ・アクセスの失敗した試行。たとえば、ユーザがネットワーク・ドライブにアクセスしようとして失敗した場合に、失敗の監査のイベントが記録される。
ソース	アプリケーション、システム構成要素、サービスなど、イベントを記録するソース。
分類	ソースによって定義されるイベントの分類。たとえば、セキュリティ・イベントの分類には、[ログオン/ログオフ]、[原則の変更]、[特権の使用]、[システム イベント]、[オブジェクト アクセス]、[詳細追跡]、および [アカウント管理] がある。
ユーザー	実際のユーザ名と一致する特定のユーザ名。このオプションでは、大文字と小文字は区別されない。
コンピュータ	実際のコンピュータ名と一致する特定のコンピュータ。このオプションでは、大文字と小文字は区別されない。
イベント ID	実際のイベントに対応する特定の番号。

6.5.6.4 イベントの検索

イベントの種類、ソース、分類を指定して、条件に一致するイベントを検索するには、[表示] メニューで [検索] をクリックします。検索は、多数のログを表示している場合に便利です。たとえば、特定のアプリケーションに関連するすべての警告イベントを検索したり、すべてのソースのすべてのエラー・イベントを検索したりできます。

[検索] ダイアログ・ボックスで指定した設定内容は、現在のセッションを終了するまで保持されます。イベント ビューアの終了時に、[オプション] メニューの [終了時の状態を保存] にチェック・マークを付けると、現在の検索の設定は、次回イベント ビューアを起動する際にも適用されます。

6.6 イベント・ログによる問題解決

イベント・ログを注意深く監視すると、問題の発生を予測したり、問題の原因の特定に役立てることができます。また、ログを調べることによって、アプリケーション・ソフトウェアの問題も確認できます。たとえば、アプリケーションがクラッシュした場合は、アプリケーション・イベント・ログを調べると、クラッシュが起きるまでの動作の記録を確認できます。

イベント・ログを使用して問題を診断する場合は、次のガイドラインを参考にしてください。

- ログはログ形式で保存する。テキスト形式やコンマ区切りテキスト形式で保存すると、イベントに関連付けられているバイナリ・データが廃棄される。
- 特定のイベントがシステムの問題に関連していると考えられる場合は、イベント・ログを検索して、同じ性質のイベントが他にないかや、エラーの頻度を調べる。
- イベント ID をメモしておく。この番号は、ソース・メッセージ・ファイル内の説明のテキストと対応しているので、システムで何が起きたのかを製品サポート担当者が判断する際の手がかりとなる。



索引

A

ASU サーバ

アーキテクチャ	1-4
概要	1-1
管理	1-5
プロセス・モデル	1-3

G

Guest アカウント

有効化	3-14
-----------	------

T

Tru64 UNIX ユーザ・アカウント

ト	3-14
---------	------

あ

アクセス権

ディスク共有	4-1
--------------	-----

い

イベント ビューア

イベント説明	6-5
イベントのヘッダ	6-4
オプション	6-3
解釈	6-4

概要	6-2
検索	6-12
更新	6-7
コンピュータの選択	6-7
使用	6-6
選別	6-11
ソート	6-10
表示	6-10
フォントの変更	6-8
問題解決	6-12
有効化	6-2
ログの選択	6-6
ログ・ファイルの保存	6-8

印刷

アクセス	5-7
監査	5-8
区切り文字	5-5
計画	5-3
スケジュールの設定	5-7
スプールの設定	5-7
デバイスのプロパティの設定	5-9
ドキュメントの省略時の設定	5-12
独自の印刷フォーム	5-9
ドライバ	5-4
プリンタ	5-2
プリント・サーバ	5-3
プリント・プロセッサ・スクリプト	5-6

か

監査	
印刷	5-8
原則	2-17
管理	
ASU コマンド.....	1-6
ASU サーバ.....	1-5
net コマンド	1-6
Tru64 UNIX コマンド.....	1-6
Tru64 UNIX の GUI	1-6
Windows の GUI	1-7
グループ	3-23
信頼	2-18
ディスク共有	4-16
ドメイン.....	2-11
ドメインのセキュリティの原則	2-14
複製	4-8

く

グループ	3-15
管理	3-23
グローバル.....	3-18
戦略	3-21
特殊	3-20
ローカル	3-16

こ

降格	
ドメイン・コントローラ	2-13
構成	
ディレクトリの複製.....	4-10

バックアップ・ドメイン・コントローラ	2-2
プライマリ・ドメイン・コントローラ	2-1
メンバ・サーバ	2-2
コントローラの同期	
ディレクトリ・データベース	2-12
コンピュータ・アカウント	2-8

さ

作成	
ログオン・スクリプト	3-5

し

昇格	
ドメイン・コントローラ	2-13
信頼	
確立	2-18
管理	2-18

て

ディスク共有	
管理	4-16
考慮事項.....	4-7
ユーザ接続の切断.....	4-17
ディスク共有のアクセス権	
NTFS.....	4-4
Tru64 UNIX.....	4-7
Windows NT	4-3
概要	4-1
ディレクトリ・データベース	
完全同期化.....	2-12
コントローラの同期.....	2-12

同期	2-11
部分同期化.....	2-12
変更	2-12
ディレクトリの複製	
構成	4-10

と

同期	
ディレクトリ・データベース	2-11
ドメイン	2-1
ASU サーバ・ロール.....	2-1
管理	2-11
対話形式のログオン.....	2-9
リモート・ログオン.....	2-10
ログオン	2-8
ログオン情報のキャッシュ...	2-11
ログオン・プロセス.....	2-8
ドメイン・コントローラ	
降格	2-13
昇格	2-13
ドメインのセキュリティの原則	
管理	2-14
ドメイン・モデル	
共通	2-2
シングル	2-7
シングル・マスタ.....	2-3
信頼される.....	2-3
マルチ・マスタ	2-5
ドメイン・ユーザ・アカウント..	3-1
Administratortor	3-12
Guest	3-13
Tru64 UNIX との関連付け ...	3-15
原則	2-15

システム・ポリシー.....	3-9
パスワード・オプション	3-3t
ビルトイン.....	3-12
プロファイル	3-10
ホーム・ディレクトリ	3-6
ユーザ権利.....	3-10, 3-12
ユーザ・プロファイル	3-8
要素	3-2t
ログオン時間	3-4
ログオン・スクリプト	3-5

は

バックアップ・ドメイン・コントローラ	
構成	2-2

ふ

複製	
WAN 接続	4-16
アクセス権.....	4-16
インポート・サブディレクトリ	4-12
エクスポート・サブディレクトリ	4-11
概要	4-9
管理	4-8
使用	4-14
問題解決.....	4-14
ログオン・スクリプト	4-13
プライマリ・ドメイン・コントローラ	
構成	2-1

ほ

ホーム・ディレクトリ
割り当て 3-7

め

メッセージ送信 4-18
メンバ・サーバ
構成 2-2

も

問題解決
イベント ビューア 6-12
複製 4-14

ゆ

ユーザ・プロフィール
移動 3-8

固定 3-8
ローカル 3-8

ろ

ログオン・スクリプト
作成 3-5
ドメイン・ユーザ・アカウント 3-5
パラメータ 3-5
複製 4-13
割り当て 3-6
ログ・ファイルの保存
イベント ビューア 6-8

わ

割り当て
ホーム・ディレクトリ 3-7
ログオン・スクリプト 3-6

マニュアルに対するご意見

Advanced Server for UNIX
コンセプトとプランニング・ガイド
AA-R9P9B-TE

弊社のマニュアルに関して、ご意見、ご要望、または内容の不明確な部分など、お気づきの点がございましたら、下記にご記入の上、弊社社員にお渡しくださるようお願い申し上げます。

マニュアルの採点：

	大変良い	良い	普通	良くない
正確さ(説明どおりに動作するか)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
情報量(十分か)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
分かり易さ	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
マニュアルの構成	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
図(役立つか)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
例(役立つか)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
索引(項目の検索性)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ページ・レイアウト(情報の検索性)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

内容の不明確な部分がありましたら、以下にご記入ください：

ペー ジ

その他お気づきの点がございましたら、以下にご記入ください：

ご使用のソフトウェアのバージョン： _____

貴社名/部課名 _____

御名前 _____

記入日 _____

(注) 当用紙を受け取った弊社社員は、すみやかに下記にお送りください。

ビジネスクリティカルシステム統括本部 **BCS** 技術本部 **Alpha** ソフトウェア技術部