Oracle® Solaris 11.3 のユーザーアカウントとユーザー環境の管理

Part No: E62601
2016 年 11 月

Part No: E62601

ドキュメントのアクセシビリティについて

オラクルのアクセシビリティについての詳細情報は、Oracle Accessibility ProgramのWeb サイト(http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc)を参照してください。

Oracle Supportへのアクセス

サポートをご契約のお客様には、My Oracle Supportを通して電子支援サービスを提供しています。詳細情報は(http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info) か、聴覚に障害のあるお客様は (http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs)を参照してください。

目次

このドキュメントの使用法

- **概要** – ユーザーアカウントとユーザー環境について説明します。
- **対象読者** – Oracle Solaris 11 リリースを使用しているシステム管理者
- **前提知識** – UNIX システムの管理経験

製品ドキュメントライブラリ

この製品および関連製品のドキュメントとリソースは http://www.oracle.com/pls/topic/lookup?ctx=E62101-01 で入手可能です。

フィードバック

このドキュメントに関するフィードバックを http://www.oracle.com/goto/docfeedback からお聞かせください。

♦ ♦ ♦ 第 1 章

1 ユーザーアカウントとユーザー環境について

この章では、次の内容を含む、ユーザーアカウントとユーザー環境の管理について説明します。

ユーザーアカウントとユーザー環境の管理に関するタスク関連の情報については、第2章「コマンド行インタフェースを使用したユーザーアカウントの管理」および第3章「ユーザーマネージャー GUI を使用したユーザーアカウントの管理」を参照してください。

Oracle Solaris 11.3 のユーザーアカウントの管理の新機能

このセクションでは、このリリースの新機能または変更された機能について説明します。

シャットダウン中に展開されるログインオプション

`shutdown` コマンドでシステムをシャットダウンしている場合、プロセスによって `/etc/nologin` ファイルが作成されます。このファイルには、システムがシャットダウン中でログインできないことを示すメッセージが表示されます。また、スーパーユーザーは、この `/etc/nologin` ファイルを個別に作成して管理できます。

このタイプのシャットダウンでは、スーパーユーザーのログインはブロックされません。このリリース以降、システムに nologin ファイルが存在する場合は、次の追加のユーザーはブロックされません。

- root 役割が割り当てられたユーザー
- solaris.system.maintenance 承認が割り当てられたユーザー

詳細は、nologin(4) および shutdown(1M) のマニュアルページを参照してください。

ユーザーアカウント管理に影響を与えるセキュリティーの変更

ユーザーアカウントを管理するシステム管理者は、このリリースで次のセキュリティー機能が変更されていることに注意してください。

- 拡張された特定の権利をファイルオブジェクト、ポート番号、およびユーザー ID に適用できます。これらの拡張された権利は、基本セットを除き、ほかに利用可能な権利のセットを置き換えます。

  ユーザーの権利の拡張については、『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「ユーザーまたは役割の特権の拡張」を参照してください。

  手順については、『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 第 4 章, 「アプリケーション、スクリプト、およびリソースへの権利の割り当て」を参照してください。また、ppriv(1) または privileges(5) のマニュアルページも参照してください。
- auth_profiles 権利を設定できるため、ユーザーは、権利プロファイルを通じて割り当てられているコマンドを実行する前に、パスワードを指定する必要があります。パスワードは、構成可能な期間有効です。

  policy.conf ファイルセットの AUTH_PROFS_GRANTED キーワードは、システムのすべてのユーザーで特権コマンドを実行するためのパスワード要件を設定します。

  詳細は、『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「ユーザーの権利の拡張」を参照してください。また、useradd(1M) および usermod(1M) のマニュアルページも参照してください。

ユーザーアカウントとグループとは

このセクションでは、次の情報について説明します。

- 13 ページの「ユーザーアカウントのコンポーネント」
- 19 ページの「ユーザー名、ユーザー ID、グループ ID の割り当てのガイドライン」

一般的なユーザーアカウントには、ユーザーがログインしてシステムを使用するために必要な情報が含まれます。ユーザーアカウントのコンポーネントについては、13 ページの「ユーザーアカウントのコンポーネント」で説明します。

ユーザーアカウントを設定するときに、ユーザーをあらかじめ定義されたユーザーグループに追加できます。グループは一般に、ファイルまたはディレクトリへのグループアクセス権を設定して、グループ内のユーザーだけがファイルとディレクトリにアクセスできるようにするために使用されます。

たとえば、ごく少数のユーザーだけにアクセスさせたい機密ファイルを入れるディレクトリを作成できます。非公開プロジェクトに携わるユーザーを含む `private` という名前のグループを設定できます。また、`private` グループのユーザーのみがファイルを読み取ることができるように、`private` グループの `read` アクセス権を `private` ファイルに設定できます。

role という名前の特殊なタイプのユーザーアカウントは、特定のユーザーに特殊な権利を付与します。詳細は、『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 第 1 章,「権利を使用したユーザーとプロセスの制御について」を参照してください。

ユーザーアカウントのコンポーネント

このセクションでは、ユーザーアカウントのさまざまなコンポーネントについて説明します。

ユーザー (ログイン) 名

ユーザーは、ログイン名とも呼ばれるユーザー名を使って、独自のシステムと、適切なアクセス権利を持つリモートシステムにアクセスできます。作成するアカウントごとに一意のユーザー名を選択する必要があります。

ユーザー名を探しやすいように、ユーザー名の標準的な割り当て方法を使用することを検討してください。また、ユーザー名はユーザーが覚えやすいものにしてください。単純なスキームの例としては、ユーザーのファーストネームの頭文字とラストネームの最初の 7 文字を使用します。たとえば、John Smith は `jsmith` になります。このスキームでほかのユーザー名と重複する場合は、ユーザーのファーストネームの頭文字、ミドルネームの頭文字、ラストネームの最初の 6 文字を使用します。たとえば、`John Jay Smith` は `jjsmith` になります。

このスキームでさらに重複する場合、ユーザー名の作成には次の方法を検討してください。

- ファーストネームの頭文字、ミドルネームの頭文字、ユーザーのラストネームの最初の 5 文字を使用する
- 一意の名前になるまで、1、2、3 などの番号を追加する

注記 - ユーザー名は、システムまたは NIS ドメインに登録されているどのメール別名とも異なるものでなければなりません。そうしないと、メールは実際のユーザーにではなく別名に送られることがあります。

ユーザー (ログイン) 名の設定方法の詳しいガイドラインについては、19 ページの「ユーザー名、ユーザー ID、グループ ID の割り当てのガイドライン」を参照してください。

ユーザー ID 番号

一意のユーザー識別 (UID) 番号は、各ユーザー名に関連付けられます。ユーザーがログインしようとするシステムは、UID 番号によってユーザー名を識別したり、ファイルとディレクトリの所有者をシステムが識別するのにも使用されます。多数の異なるシステムで個人のユーザーアカウントを作成する場合、常に同じユーザー名と ID 番号を使用してください。そうすれば、そのユーザーは、所有権の問題を起こすことなく、システム間で簡単にファイルを移動できます。

UID 番号は、2147483647 以下の整数でなければなりません。UID 番号は、通常のユーザーアカウントと特殊なシステムアカウントに必要です。次の表に、ユーザーアカウントとシステムアカウントに予約されている UID 番号を示します。

表 1 予約済みの UID 番号

UID 番号	ユーザー/ログインアカウント	説明
0 – 99	`root`、`daemon`、`bin`、`sys` など	オペレーティングシステムによる使用のために予約済み
100 – 2147483647	通常のユーザー	汎用アカウント
60001 と 65534	`nobody` および `nobody4`	NFS 匿名ユーザー
60002	`noaccess`	OS 用に予約済み

0 - 99 の UID 番号を割り当てないでください。これらの UID は、Oracle Solaris による割り当て用に予約されています。定義により、`root` には常に UID 0、`daemon` には UID 1、擬似ユーザー `bin` には UID 2 が設定されます。

UID の設定方法の詳しいガイドラインについては、19 ページの「ユーザー名、ユーザー ID、グループ ID の割り当てのガイドライン」を参照してください。

ユーザー (ログイン) 名と同様に、固有の UID 番号を割り当てるスキームを決めてください。企業によっては、従業員に固有の番号を割り当て、管理者がその従業員番号にある番号を加えて固有の UID 番号を作成している場合もあります。

セキュリティー上のリスクを最小限に抑えるため、削除したアカウントの UID を再利用することは避けてください。UID を再利用する必要がある場合は、前のユーザー

に設定されている属性の影響を新しいユーザーが受けないように、アカウント情報を完全に削除してください。たとえば、前のユーザーがプリンタの拒否リストに含まれている可能性があります。ただし、そのプリンタへのアクセスの拒否が、新しいユーザーに不適切な場合があります。

大きな数値のユーザー ID とグループ ID の使用

UID とグループ ID (GID) には、符号付き整数の最大値 (つまり 2147483647) までの数値を割り当てることができます。

次の表に、UID と GID の制限事項を示します。

表 2 大きな UID および GID の制限のサマリー

UID または GID	制限
262144 以上	ユーザーがデフォルトのアーカイブフォーマットで `cpio` コマンドを使用してファイルをコピーすると、ファイルごとにエラーメッセージが表示されます。UID と GID はアーカイブで `nobody` に設定されます。
2097152 以上	ユーザーが `cpio` コマンドに `-H odc` を付けた形式または `pax -x cpio` コマンドを使用してファイルをコピーすると、ファイルごとにエラーメッセージが返されます。UID と GID はアーカイブで `nobody` に設定されます。
1000000 以上	ユーザーが `ar` コマンドを使用すると、そのユーザーの UID と GID はアーカイブにおいて `nobody` に設定されます。
2097152 以上	ユーザーが `tar` コマンド、`cpio -H ustar` コマンド、または `pax -x tar` コマンドを使用すると、そのユーザーの UID と GID は `nobody` に設定されます。

UNIX グループ

グループとは、ファイルやその他のシステムリソースを共有できるユーザーの集合のことです。たとえば、同じプロジェクトで作業するユーザーはグループを構成することになります。グループは、従来の UNIX グループのことです。

各グループには、名前、グループ識別 (GID) 番号、およびそのグループに属しているユーザー名のリストが必要です。システムは GID 番号によって内部的にグループを識別します。

ユーザーは次の 2 つの種類のグループに所属できます。

- **プライマリグループ** – オペレーティングシステムが、ユーザーによって作成されたファイルに割り当てるグループを指定します。各ユーザーは、1 つのプライマリグループに所属していなければなりません。
- **セカンダリグループ** – ユーザーが所属できる 1 つまたは複数のグループを指定します。ユーザーは、最大 1024 個の補足グループに所属できます。

グループ名の設定方法の詳しいガイドラインについては、19 ページの「ユーザー名、ユーザー ID、グループ ID の割り当てのガイドライン」を参照してください。

ユーザーのセカンダリグループは、場合によっては重要でないことがあります。たとえば、ファイルの所有権は、プライマリグループだけが反映し、セカンダリグループは反映しません。ただし、アプリケーションによってはユーザーのセカンダリグループが関係することがあります。たとえば、ユーザーは以前の Oracle Solaris リリースで Admintool ソフトウェアを使用するとき `sysadmin` グループ (グループ 14) のメンバーでなければなりません。ただし、グループ 14 がユーザーの現在のプライマリグループであるかどうかは関係ありません。

`groups` コマンドは、ユーザーが所属しているグループのリストを表示します。ユーザーは一度に 1 つのプライマリグループにしか所属できません。ただし、ユーザーは、`newgrp` コマンドを使用して、ユーザーがメンバーであるほかのグループに自分のプライマリグループを一時的に変更できます。

ユーザーアカウントを追加するときは、ユーザーにプライマリグループを割り当てるか、デフォルトグループの `staff` (グループ 10) を適用する必要があります。プライマリグループは、すでに存在しているものでなければなりません。プライマリグループが存在しない場合は、GID 番号でグループを指定します。リストが長くなりすぎる場合があるため、ユーザー名はプライマリグループに追加されません。ユーザーを新しいセカンダリグループに割り当てる前に、そのグループを作成し、それに GID 番号を割り当てなければなりません。

グループは、システムにとってローカルにすることも、ネームサービスを介して管理することもできます。グループ管理を簡単に行うには、NIS などのネームサービスや LDAP などのディレクトリサービスを使用する必要があります。これらのサービスを使用すると、グループのメンバーを一元管理できます。

ユーザーパスワード

ユーザーを追加するときにそのユーザーのパスワードを指定できます。または、ユーザーが最初にシステムにログインするときにパスワードを指定するよう強制できます。ユーザー名は公開されますが、パスワードは秘密にして、ユーザーのみが知っている必要があります。各ユーザーアカウントには、パスワードを割り当てる必要があります。

ユーザーのパスワードは、次の構文に準拠している必要があります。

- パスワードの長さは、`/etc/default/password` ファイルの `PASSLENGTH` の値によって定義されます。

  デフォルトのパスワードハッシュ生成アルゴリズムは `SHA256` です。その結果、ユーザーパスワードは、以前の Oracle Solaris リリースのように、8 文字に制限がなくなりました。8 文字の制限は、古い `crypt_unix`(5) アルゴリズムを使用するパスワードのみに適用され、既存の `passwd` ファイルのエントリと NIS マップとの下位互換性のために残されています。

新しいパスワードは、パスワードアルゴリズムに許可される最大文字数内で複雑さのルールに一致している必要があります。そのため、crypt_unix アルゴリズムを使用し、20 文字のパスワードを入力した場合、パスワードは先頭 8 文字内で複雑さのルールに一致している必要があります。パスワードアルゴリズムが他のアルゴリズムである場合、入力された完全なパスワード (この例では 20 文字) 内で、複雑さのルールに一致している必要があります。

- 各パスワードは /etc/default/passwd ファイルに指定されている構成済みの複雑さの制約を満たしている必要があります。
- 各パスワードは /etc/default/passwd ファイルに指定されている、構成済みの辞書のメンバーでない必要があります。
- 新しいパスワードは、名前サービスのパスワード履歴に含まれている必要があります。

パスワードルールについては、passwd(1) のマニュアルページで詳しく説明しています。

コンピュータシステムのセキュリティーを強化するには、ユーザーのパスワードを定期的に変更するようにしてください。高いレベルのセキュリティーを確保するには、ユーザーに 6 週間ごとにパスワードを変更するよう要求してください。低いレベルのセキュリティーなら、3 か月に 1 度で十分です。システム管理用のログイン (root や sys など) は、毎月変更するか、root のパスワードを知っている人が退職したり交替したりするたびに変更してください。

コンピュータのセキュリティーが破られる原因の多くは、正当なユーザーのパスワードが解読される場合です。ユーザーについて何か知っているだけで推測できるような固有名詞、名前、ログイン名、パスワードを使わないよう各ユーザーに対して指示してください。

良いパスワードの例としては次のようなものがあります。

- フレーズ (beammeup)。
- フレーズ内の各単語の頭文字だけを集めた、意味のない文字列 。たとえば、SomeWhere Over The RainBow から取った swotrb。
- 文字を数字や記号に代えた単語。たとえば、snoopy の場合 sn00py にします。

次のようなものは、パスワードに使用しないでください。

- 自分の名前そのもの、逆読み、飛ばし読みのもの
- 家族やペットの名前
- 免許証番号
- 電話番号
- 社会保険番号
- 従業員番号
- 趣味や興味に関連した単語
- 季節に関係のある名前 (たとえば 12 月に Santa を使うなど)

- 辞書にある単語

ホームディレクトリ

ホームディレクトリは、ユーザーが独自のファイルを格納するのに割り当てられるファイルシステムの一部分です。ホームディレクトリに割り当てる領域の量は、ディレクトリがホストされているシステムのサイズ、ユーザーが作成するファイルの種類、ファイルサイズ、および作成されるファイルの数によって異なります。

ホームディレクトリは、ユーザーのローカルシステムまたはリモートファイルサーバーのどちらにでも配置できます。どちらの場合も、慣例により、ホームディレクトリは `/export/home/`*username* として作成します。大規模なサイトでは、ホームディレクトリをサーバーに格納してください。`/export/home/alice` や `/export/home/bob` など、ユーザーごとに個別のファイルシステムを使用します。ユーザーごとに独立したファイルシステムを作成することにより、各ユーザーのニーズに基づいてプロパティーまたは属性を設定できます。

ホームディレクトリが配置される場所に関係なく、ユーザーは通常 `/home/`*username* という名前のマウントポイントを介してホームディレクトリにアクセスします。Autofs を使用してホームディレクトリがマウントされていると、どのシステムでも `/home` マウントポイントの下にディレクトリを作成することは許可されません。Autofs が使用されていると、システムはマウントされている `/home` を特別なステータスと認識します。ホームディレクトリの自動マウントの詳細は、『Oracle Solaris 11.3 でのネットワークファイルシステムの管理』 の 「autofs 管理」を参照してください。

ネットワーク上の任意の場所からホームディレクトリを使用するには、`/export/home/`*username* ではなく、常に `$HOME` に応じてホームディレクトリを参照するようにしてください。これは、`/export/home/`*username* ディレクトリがシステムに固有なためです 。さらに、ホームディレクトリがマウントされている場所に関係なくリンクが有効になるように、ユーザーのホームディレクトリに作成されるすべてのシンボリックリンクで相対パス (たとえば、`../../../x/y/x`) を使用するべきです。

コマンド行インタフェースを使用して、ユーザーアカウントを作成する場合に、ホームディレクトリを追加する方法の詳細は、41 ページの「ユーザーアカウントの設定のガイドライン」を参照してください。

ネームサービス

大規模サイトのユーザーアカウントを管理する場合は、LDAP や NIS などのネームサービスまたはディレクトリサービスの利用を検討することをお勧めします。ネームサービスまたはディレクトリサービスを使うと、ユーザーアカウント情報を各システムの `/etc` 内のファイルに格納するのではなく、一元管理できます。ユーザーアカウントにネームサービスまたはディレクトリサービスを使用すると、ユーザーの情報

をシステムごとに複製しなくても、同じユーザーアカウントのままシステム間を移動できます。ネームサービスまたはディレクトリサービスを利用することにより、ユーザーアカウント情報の一貫性も保証されます。

ユーザーの作業環境

ファイルを作成して格納するホームディレクトリのほかに、ユーザーには仕事をするために必要なツールとリソースにアクセスできる環境が必要です。ユーザーがシステムにログインすると、初期設定ファイルによってユーザーの作業環境が決定されます。これらのファイルは、ユーザーの起動シェルによって定義されますが、起動シェルはリリースによって異なる可能性があります。

ユーザーの作業環境を管理するのに便利な方法として、カスタマイズしたユーザー初期設定ファイル (`.bash_profile`、`.bash_login`、`.kshrc`、`.profile` など) をユーザーのホームディレクトリに置くという方法があります。

注記 - システム初期設定ファイル (`/etc/profile` や `/etc/.login` など) を使用してユーザーの作業環境を管理しないでください。これらのファイルはローカルシステムに存在するため、一元管理されません。たとえば、Autofs を使用してネットワーク上の任意のシステムからユーザーのホームディレクトリをマウントした場合、ユーザーがシステム間を移動しても環境が変わらないよう保証するには、各システムでシステム初期設定ファイルを修正しなければならなくなります。

ユーザー初期設定ファイルをユーザー用にカスタマイズする方法の詳細は、27 ページの「ユーザーの作業環境について」を参照してください。

ユーザー名、ユーザー ID、グループ ID の割り当てのガイドライン

ユーザー名、UID、および GID は、設定に複数のドメインが含まれる場合は特に組織内で一意になるようにしてください。

ユーザー名または役割名、UID、および GID を作成するときは、次のガイドラインに従ってください。

- **ユーザー名** – 2 - 8 文字の英数字を使用してください。最初の文字は英字にする必要があります。少なくとも 1 文字は小文字にする必要があります。

  注記 - ユーザー名にはピリオド (.)、下線 (_)、ハイフン (-) を使用できますが、これらの文字により障害が発生するソフトウェアもあるため、使用はお勧めできません。

- **システムアカウント** – デフォルトの `/etc/passwd` および `/etc/group` ファイルに含まれているユーザー名、UID、または GID を使用しないでください。0 - 99 の UID と GID は使用しないでください。これらの番号は、Oracle Solaris による割り当て用に予約されており、どのユーザーも使用しないでください。この制限は、現在使用されていない番号にも適用されます。

  たとえば、`gdm` は GNOME ディスプレイマネージャーデーモン用に予約されたユーザー名とグループ名であるため、ほかのユーザーは使用できません。デフォルトの `/etc/passwd` と `/etc/group` エントリの全リストについては、表3と表4を参照してください。

注意 - `nobody` と `nobody4` のアカウントは、プロセスの実行には使用しないでください。これらの 2 つのアカウントは NFS 用に予約されています。これらのアカウントをプロセスの実行に使用すると、予期しないセキュリティー上のリスクにさらされる可能性があります。root 以外として実行する必要があるプロセスでは、`daemon` または `noaccess` のアカウントを使用してください。

- **システムアカウント構成** – デフォルトのシステムアカウントの構成は変更しないでください (現在ロックされているシステムアカウントのログインシェルの変更を含む)。ただし、`root` アカウントのパスワードとパスワード有効期限のパラメータ設定だけはこの規則に当てはまりません。

注記 - ロックされたユーザーアカウントのパスワードを変更すると、パスワードは変更されますが、同時にアカウントのロックが解除されなくなります。`passwd -u` コマンドを使用してアカウントをロック解除する 2 番目の手順が必要になりました。

ユーザーアカウントとグループ情報の格納場所

このセクションでは、次の情報について説明します。

ユーザーアカウントとグループ情報は、サイトの方針に応じて、次のようにローカルシステムの /etc ファイル、ネームサービス、またはディレクトリサービスに格納されます。

- NIS ネームサービス情報はマップに格納されます。
- LDAP ディレクトリサービス情報はインデックス付きのデータベースファイルに格納されます。

注記 - 混乱を避けるために、ユーザーアカウントとグループ情報の格納場所は、データベース、テーブル、マップという呼び方ではなく、単にファイルと呼びます。

ほとんどのユーザーアカウント情報は、passwd ファイルに格納されます。パスワード情報は次のように格納されます。

- NIS を使用するときは passwd ファイルに
- /etc ファイルを使用するときは、/etc/shadow ファイルに
- LDAP を使用するときは、people コンテナに

パスワードの有効期限は、LDAP を使用するときは利用できますが、NIS を使用するときは利用できません。

グループ情報は、NIS の group ファイルに格納されます。LDAP の場合、グループ情報は group コンテナに格納されます。

passwd ファイルのフィールド

passwd ファイルの各フィールドはコロンで区切られ、次のような情報が入っています。

username:*password*:*UID*:*GID*:*comment*:*home-directory*:*login-shell*

例:

```
kryten:x:101:100:Kryten Series 4000 Mechanoid:/export/home/kryten:/bin/csh
```

passwd ファイルのフィールドの完全な説明については、passwd(1) のマニュアルページを参照してください。

デフォルトの passwd ファイル

デフォルトの passwd ファイルには、標準のデーモン用のエントリが入っています。デーモンとは、通常ブート時に起動され、システム全体で有効なタスク (印刷、ネットワーク管理、ポートのモニタリングなど) を実行するプロセスのことです。

次の表示は、サンプルの passwd ファイルの内容を示しています。

注記 - 追加のユーザーおよびグループは、パッケージがシステムに追加またはシステムから削除されると作成されたり削除されたりします。これらの進行中の変更は、passwd ファイルに反映されます。管理者は、このファイルをクリーンアップする必要はありません。

```
root:x:0:0:Super-User:/root:/usr/bin/bash
daemon:x:1:1::/:
bin:x:2:2::/usr/bin:
sys:x:3:3::/:
adm:x:4:4:Admin:/var/adm:
lp:x:71:8:Line Printer Admin:/:
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
dladm:x:15:65:Datalink Admin:/:
netadm:x:16:65:Network Admin:/:
netcfg:x:17:65:Network Configuration Admin:/:
smmsp:x:25:25:SendMail Message Submission Program:/:
gdm:x:50:50:GDM Reserved UID:/var/lib/gdm:
zfssnap:x:51:12:ZFS Automatic Snapshots Reserved UID:/:/usr/bin/pfsh
upnp:x:52:52:UPnP Server Reserved UID:/var/coherence:/bin/ksh
xvm:x:60:60:xVM User:/:
mysql:x:70:70:MySQL Reserved UID:/:
openldap:x:75:75:OpenLDAP User:/:
webservd:x:80:80:WebServer Reserved UID:/:
postgres:x:90:90:PostgreSQL Reserved UID:/:/usr/bin/pfksh
svctag:x:95:12:Service Tag UID:/:
unknown:x:96:96:Unknown Remote UID:/:
nobody:x:60001:60001:NFS Anonymous Access User:/:
noaccess:x:60002:60002:No Access User:/:
nobody4:x:65534:65534:SunOS 4.x NFS Anonymous Access User:/:
ikeuser:x:67:12:IKE Admin:/:
ftp:x:21:21:FTPD Reserved UID:/:
dhcpserv:x:18:65:DHCP Configuration Admin:/:
aiuser:x:60003:60001:AI User:/:
pkg5srv:x:97:97:pkg(5) server UID:/:
```

前述の表示は、サンプルの passwd ファイルの内容 (説明なし) を示しています。次の表では、標準の passwd ファイルのデーモンごとの説明およびソースパッケージ情報について詳しく説明しています。

表 3 デフォルトの passwd ファイルのエントリ

ユーザー名	ユーザー ID	説明	パッケージ
root	0	スーパーユーザーアカウント用に予約済み	system/core-os
daemon	1	ルーチンシステムタスクに関連するシステム包括デーモン	system/core-os
bin	2	ルーチンシステムタスクを実行するシステムバイナリの実行に関連する管理デーモン	system/core-os
sys	3	システムのログの記録や一時ディレクトリのファイルの更新に関連する管理デーモン	system/core-os

ユーザー名	ユーザー ID	説明	パッケージ
adm	4	システムのログの記録に関連する管理デーモン	system/core-os
lp	71	ラインプリンタデーモン用に予約済み	system/core-os
uucp	5	uucp 関数に関連するデーモンに割り当てられる	system/core-os
nuucp	9	uucp 関数に関連する別のデーモンに割り当てられる	system/core-os
dladm	15	データリンク管理用に予約済み	system/core-os
netadm	16	ネットワーク管理用に予約済み	system/core-os
netcfg	17	ネットワーク構成管理用に予約済み	system/core-os
smmsp	25	Sendmail メッセージ送信プログラムデーモンに割り当てられる	system/core-os
gdm	50	GNOME ディスプレイマネージャーデーモンに割り当てられる	system/core-os
zfssnap	51	自動スナップショット用に予約済み	system/core-os
upnp	52	UPnP サーバー用に予約済み	system/core-os
xvm	60	xVM ユーザー用に予約済み	system/core-os
mysql	70	MySQL ユーザー用に予約済み	system/core-os
openldap	75	OpenLDAP ユーザー用に予約済み	library/ldap
webservd	80	WebServer アクセス用に予約済み	system/core-os
postgres	90	PostgresSQL アクセス用に予約済み	system/core-os
svctag	95	Service Tag Registry アクセス用に予約済み	system/core-os
unknown	96	NFSv4 ACL のマップ不能なリモートユーザー用に予約済み	system/core-os
nobody	60001	NFS 匿名アクセスユーザー用に予約済み	system/core-os
noaccess	60002	No Access ユーザー用に予約済み	system/core-os
nobody4	65534	SunOS 4.x NFS 匿名アクセスユーザー用に予約済み	system/core-os
ikeuser	67	Internet Key Exchange (IKE) アクセス用に予約済み	system/network/ike
ftp	21	FTP アクセス用に予約済み	service/network/ftp
dhcpserv	18	DHCP サーバーユーザー用に予約済み	service/network/dhcp/isc-dhcp
aiuser	60003	AI ユーザー用に予約済み	system/install/auto-install/auto-install-common
pkg5srv	97	pkg(5) 集積サーバー用に予約済み	package/pkg

shadow ファイルのフィールド

/etc/shadow ファイルには、暗号化されたユーザーのパスワードおよび関連する情報が格納されます。shadow ファイルの各フィールドはコロンで区切られ、次のような情報が入っています。

username:*password*:*lastchg*:*min*:*max*:*warn*:*inactive*:*expire*

デフォルトのパスワードハッシュ生成アルゴリズムは SHA256 です。ユーザーのパスワードハッシュは次のようになります。

```
$5$cgQk2iUy$AhHtVGx5Qd0.W3NCKjikb8.KhOiA4DpxsW55sP0UnYD
```

shadow ファイルのフィールドの完全な説明については、shadow(4) のマニュアルページを参照してください。

group ファイルのフィールド

group ファイルは、グループ情報のローカルソースです。group ファイルの各フィールドはコロンで区切られ、次のような情報が入っています。

group-name:*group-password*:*GID*:*user-list*

例:

```
bin::2:root,bin,daemon
```

group ファイルのフィールドの完全な説明については、group(4) のマニュアルページを参照してください。

デフォルトの group ファイル

デフォルトの group ファイルには、システム全体に有効なタスク (印刷、ネットワーク管理、電子メールなど) をサポートする次のようなシステムグループが記述されています。これらのグループのほとんどは、対応するエントリが passwd ファイルに存在します。

```
The following displays the contents of a sample group file.

root::0:
other::1:root
bin::2:root,daemon
sys::3:root,bin,adm
adm::4:root,daemon
```

前述の表示は、サンプルの group ファイルの内容 (説明なし) を示しています。次の表は、一般的な group ファイルに一覧表示されている各グループに関する詳細情報を示しています。

表 4 デフォルトの group ファイルのエントリ

グループ名	グループ ID	説明	pkg(5)
root	0	スーパーユーザーのグループ	system/core-os
other	1	オプションのグループ	system/core-os
bin	2	システムバイナリの実行に関連する管理グループ	system/core-os
sys	3	システムのログの記録や一時ディレクトリに関連する管理グループ	system/core-os
adm	4	システムのログの記録に関連する管理グループ	system/core-os

ユーザーアカウント情報を取得するためのコマンド

次の表に、システム管理者がユーザーアカウントに関する情報を取得するために使用できるコマンドを示します。この情報は /etc ディレクトリ内の各種ファイルに格納されています。これらのコマンドを使用してユーザーアカウント情報を取得する方法は、cat コマンドを使用して、同様の情報を表示するよりも推奨されます。

表 5 ユーザーに関する情報を取得するためのコマンド

コマンド	説明	マニュアルページの参照
auths	承認を一覧表示し、管理します。	auths(1)
getent	管理データベースからエントリのリストを表示します。情報は、通常 /etc/nsswitch.conf データベースに指定されている 1 つまたは複数のソースから取得されます。	getent(1M)
logins	ユーザー、役割、およびシステムログインに関する情報を表示します。出力は、指定されたコマンドオプションによって制御され、ユーザー、役割、システムログイン、UID、passwd アカウントフィールド値、プライマリグループ、プライマリグループ ID、複数のグループ名、複数のグループ ID、ホームディレクトリ、ログインシェル、パスワード有効期限パラメータなどを含めることができます。	logins(1M)
profiles	権利プロファイルを一覧表示し、管理します。	profiles(1)
roles	ユーザーに割り当てられた役割を表示します。	roles(1)

コマンド	説明	マニュアルページの参照
`userattr`	`attribute_name` で最初に検出された値を表示します。ユーザーが指定されていない場合、プロセスの実際のユーザー ID からユーザーが取得されます。属性名は、`user_attr`(4) および `prof_attr`(4) のマニュアルページに定義されています。 **注記 -** このコマンドは、Oracle Solaris 11 の新機能です。	`userattr`(1)

ユーザー、役割、およびグループの管理に使用されるコマンド

注記 - Solaris Management Console GUI、およびこの GUI に関連付けられるコマンド行インタフェース (CLI) はサポートされていません。

次の表に説明されているコマンドは、ユーザー、役割、およびグループの管理に使用できます。

表 6 ユーザー、役割、およびグループの管理に使用されるコマンド

コマンドのマニュアルページ	説明	追加情報
`useradd`(1M)	ユーザーをローカルまたは LDAP リポジトリに作成します。	45 ページの「ユーザーを追加する方法」
`usermod`(1M)	ローカルまたは LDAP リポジトリ内のユーザープロパティーを変更します。ユーザープロパティーが役割の割り当てなどのセキュリティー関連である場合、このタスクはセキュリティー管理者または `root` 役割に限定される場合があります。	46 ページの「ユーザーアカウントの変更方法」 『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「役割の作成」
`userdel`(1M)	システムまたは LDAP リポジトリからユーザーを削除します。`cron` ジョブの削除など、追加のクリーンアップが必要な可能性があります。	47 ページの「ユーザーを削除する方法」
`roleadd`(1M) `rolemod`(1M) `roledel`(1M)	ローカルまたは LDAP リポジトリ内の役割を管理します。役割はログインできません。割り当てられた役割をユーザーが引き受けて、管理タスクを実行します。	『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「ユーザーへの権利の割り当て」
`groupadd`(1M) `groupmod`(1M) `groupdel`(1M)	ローカルまたは LDAP リポジトリ内のグループを管理します。	48 ページの「グループを追加する方法」

ユーザーの作業環境について

このセクションでは、次の情報について説明します。

ユーザーのホームディレクトリの設定には、ユーザーのログインシェルにユーザー初期設定ファイルを提供することも含まれます。ユーザー初期設定ファイルは、ユーザーがシステムにログインしたあとにユーザーのために作業環境を設定するシェルスクリプトです。基本的にシェルスクリプトで行えるタスクはどれもユーザー初期設定ファイルで実行できます。ただし、ユーザー初期設定ファイルのプライマリジョブはユーザーの検索パス、環境変数、ウィンドウ表示環境などのユーザー作業環境の特性を定義することです。次の表に示すように、各ログインシェルには、1 つまたは複数の、固有のユーザー初期設定ファイルがあります。bash シェルと ksh93 シェルの両方で、デフォルトのユーザー初期設定ファイルは /etc/skel/local.profile であることに注意してください。

表 7 bash および ksh93 のユーザー初期設定ファイル

シェル	ユーザー初期設定ファイル	目的
bash	$HOME/.bash_profile	ログイン時のユーザー環境を定義します
	$HOME/.bash_login	
	$HOME/.profile	
ksh93	/etc/profile	ログイン時のユーザー環境を定義します
	$HOME/.profile	
	$ENV	ログイン時のユーザー環境をファイル内に定義し、Korn シェルの ENV 環境変数によって指定します

これらのファイルを開始点として使用して変更し、すべてのユーザーに共通の作業環境を提供する標準のファイルセットを作成できます。異なるタイプのユーザーごとに作業環境を提供する場合にも、これらのファイルを利用できます。

さまざまなタイプのユーザーにユーザー初期設定ファイルのセットを作成する方法の手順については、43 ページの「ユーザー初期設定ファイルをカスタマイズする方法」を参照してください。

サイト初期設定ファイルの使用方法

ユーザー初期設定ファイルは、管理者とユーザーの両者によってカスタマイズできます。この重要なタスクは、サイト初期設定ファイルと呼ばれる、一元管理され、大域的に配布されるユーザー初期設定ファイルによって実現します。サイト初期設定ファイルを使用して、ユーザーの作業環境に新しい機能を絶えず導入でき、しかもユーザーはユーザー初期設定ファイルをカスタマイズすることもできます。

ユーザー初期設定ファイルでサイト初期設定ファイルを参照するとき、サイト初期設定ファイルに対して行なったすべての更新は、ユーザーがシステムにログインするときかユーザーが新しいシェルを起動するとき自動的に反映されます。サイト初期設定ファイルでは、ユーザーを追加したときにはなかったサイト全体の変更をユーザーの作業環境に配布できます。

ユーザー初期設定ファイルでできるカスタマイズは、サイト初期設定ファイルでも行えます。これらのファイルは通常はサーバー、またはサーバーのグループにあり、ユーザー初期設定ファイルの最初の行に現れます。また、各サイト初期設定ファイルは、それを参照するユーザー初期設定ファイルと同じ型のシェルスクリプトでなければなりません。

bash または `ksh93` ユーザー初期設定ファイル内でサイト初期設定ファイルを参照するには、ユーザー初期設定ファイルの先頭に次のような行を記述します。

```
. /net/machine-name/export/site-files/site-init-file
```

ローカルシステムへの参照を避ける

ユーザー初期設定ファイルに、ローカルシステムへの個々の参照を追加しないでください。ユーザー初期設定ファイルの設定は、ユーザーがどのシステムにログインしても有効になるようにしてください。

例:

- ユーザーのホームディレクトリをネットワーク上の任意の位置で利用できるようにするには、常に環境変数の値 `$HOME` を使用してホームディレクトリを参照してください。たとえば、`/export/home/`*`username`*`/bin` ではなく `$HOME/bin` を使用してください。`$HOME` 変数は、ユーザーが別のシステムにログインする場合でも有効で、その場合ホームディレクトリは自動マウントされます。
- ローカルディスクのファイルにアクセスするには、`/net/`*`system-name/directory-name* などの大域パス名を使用してください。システムが AutoFS を実行していれ

ば、/net/*system-name* で参照されるディレクトリはすべてユーザーがログインする任意のシステムに自動的にマウントできます。

シェル機能

この Oracle Solaris リリースでは、次のシェル機能および動作をサポートしています。

- Oracle Solaris リリースのインストール時に作成されるユーザーアカウントには、デフォルトで GNU Bourne-Again Shell (bash) が割り当てられます。
- 標準のシステムシェルである bin/sh は現在、Korn Shell 93 (ksh93) です。
- デフォルトの対話型シェルは Bourne-again (bash) シェル (/usr/bin/bash) です。
- bash シェルと ksh93 シェルはどちらもコマンド行編集機能を備えており、コマンドを実行する前にコマンドを編集できます。
- デフォルトのシェルおよびパス情報を複数の方法で表示できます。
  - echo $SHELL コマンドおよび which コマンドを使用します。

```
$ grep root /etc/passwd
root:x:0:0:Super-User:/root:/usr/bin/bash

$ echo $SHELL
/usr/bin/bash

$ which ksh93
/usr/bin/ksh93
```

  - pargs コマンドを使用します。

```
~$ pargs -l $$
/usr/bin/i86/ksh93
```

- ksh93 シェルには、.sh.version という組み込みの変数もあり、次のようにして表示できます。

```
~$ echo ${.sh.version}
Version jM 93u 2011-02-08
```

- 別のシェルに変更するには、使用するシェルのパスを入力します。
- シェルを終了するには、exit と入力します。

次の表は、Oracle Solaris でサポートされているシェルオプションの説明です。

表 8 Oracle Solaris リリースの基本シェル機能

シェル	パス	Comments
Bourne-Again Shell (bash)	/usr/bin/bash	インストーラによって作成されるユーザーおよび root 役割のデフォルトシェル。

シェル	パス	Comments
		useradd コマンドによって作成されるユーザーと、root 役割のデフォルトの (対話型) シェルは /usr/bin/bash です。デフォルトのパスは /usr/bin:/usr/sbin です。
Korn シェル	/usr/bin/ksh	ksh93 は、この Oracle Solaris リリースのデフォルトのシェルです。
C シェルと拡張 C シェル	/usr/bin/csh および /usr/bin/tcsh	C シェルと拡張 C シェル
POSIX 準拠シェル	/usr/xpg4/bin/sh	POSIX 準拠シェル
Z シェル	/usr/bin/zsh	Z シェル

注記 - Z シェル (zsh) および拡張 C シェル (tsch) は、デフォルトではシステムにインストールされません。これらのシェルを使用するには、まず、必要なソフトウェアパッケージをインストールする必要があります。

Oracle Solaris OS に含まれるシェルで使用する、UNIX® のデフォルトのシステムプロンプトとスーパーユーザープロンプトを次に示します。コマンド例に示されるデフォルトのシステムプロンプトは、Oracle Solaris のリリースによって異なります。

表 9 シェルプロンプト

シェル	プロンプト
Bash シェル、Korn シェル、および Bourne シェル	$
Bash シェル、Korn シェル、および Bourne シェルのスーパーユーザー	#
C シェル	machine_name%
C シェルのスーパーユーザー	machine_name#

bash および ksh93 シェルの履歴

bash シェルと ksh93 シェルはどちらも、ユーザーが実行するすべてのコマンドの履歴を記録します。この履歴はユーザー単位で保持されます。つまり、履歴は複数のログインセッションにまたがって永続し、ユーザーのすべてのログインセッションを表現します。

たとえば、bash シェルを使用している場合、実行したコマンドの完全な履歴を次のように表示できます。

```
$ history
1 ls
```

```
2 ls -a
3 pwd
4 whoami
.
.
.
```

以前のコマンドの数を表示するには、コマンドに整数を含めます。

```
$ history 2
12 date
13 history
```

詳細は、history(1) のマニュアルページを参照してください。

bash および Korn シェル環境変数

bash シェルと ksh93 シェルは、シェルが認識している特殊な変数情報を環境変数として格納します。bash シェルで、現在の環境変数の完全なリストを表示するには、次のように declare コマンドを使用します。

```
$ declare
BASH=/usr/bin/bash
BASH_ARGC=()
BASH_ARGV=()
BASH_LINEND=()
BASH_SOuRCE=()
BASH_VERSINFO=([0]=''3'' [1]=''2'' [2]=''25'' [3]=''1''
[4]=''release'' [5]''
.
.
.
```

ksh93 シェルでは、bash シェルの declare コマンドに相当する set コマンドを使用します。

```
$ set
  COLUMNS=80
  ENV='$HOME/.kshrc'
  FCEDIT=/bin/ed
  HISTCMD=3
  HZ=''
  IFS=$' \t\n'
  KSH_VERSION=.sh.version
  LANG=C
  LINENO=1
  .
  .
  .
```

どちらのシェルでも、環境変数を出力するには echo または printf コマンドを使用します。例:

```
$ echo $SHELL
/usr/bin/bash
$ printf "$PATH\n"
/usr/bin:/usr/sbin
```

注記 - 環境変数はセッション間で持続しません。持続的な環境変数値を設定するには、.bashrc ファイルに値を設定します。

シェルには次の 2 種類の変数があります。

環境変数
: シェルによって生成されるすべてのプロセスにエクスポートされる変数を指定します。変数のエクスポートには export コマンドが使用されます。例:

```
export VARIABLE=value
```

これらの設定は env コマンドを使用して表示できます。PATH などを含む環境変数の一部が、シェルそのものの動作に影響を与えます。

シェル (ローカル) 変数
: 現在のシェルのみに影響を及ぼす変数を指定します。

ユーザー初期設定ファイルで、定義済み変数の値を変更するか、または追加の変数を指定することによって、ユーザーのシェル環境をカスタマイズすることができます。

次の表は、Oracle Solaris リリースで使用可能なシェルおよび環境変数の詳細について説明しています。

表 10 シェル変数と環境変数の説明

変数	説明
CDPATH	cd コマンドで使用する変数を設定します。cd コマンドの対象ディレクトリを相対パス名で指定すると、cd コマンドは対象ディレクトリをまず現在のディレクトリ (.) 内で検索します。対象ディレクトリが見つからない場合、CDPATH 変数内のパス名のリストが順に検索され、見つかると、ディレクトリの変更が行われます。CDPATH で対象ディレクトリが見つからなかった場合は、現在の作業ディレクトリは変更されません。たとえば、CDPATH 変数が /home/jean に設定されており、/home/jean の下に bin と rje の 2 つのディレクトリがあるとします。/home/jean/bin ディレクトリ内で cd doc と入力した場合、フルパスを指定していなくても、ディレクトリが /home/jean/doc に変更されます。
HOME	ユーザーのホームディレクトリへのパスを設定します。
LANG	ロケールを設定します。
LOGNAME	現在ログインしているユーザーの名前を定義します。LOGNAME のデフォルト値は、passwd ファイルに指定されているユーザー名にログインプログラムによって自動的に設定されます。この変数は参照用にのみ使用し、設定を変更してはいけません。
MAIL	ユーザーのメールボックスへのパスを設定します。
MANPATH	アクセスできるマニュアルページの階層を設定します。 **注記 -** Oracle Solaris 11 以降は、MANPATH 環境変数は不要になりました。man コマンドは、PATH 環境変数の設定に基づいて適切な MANPATH を決定します。
PATH	ユーザーがコマンドを入力したときに実行するプログラムについて、シェルが検索するディレクトリを順番に指定します。ディレクトリが検索パス上にない場合は、ユーザーはコマンドの絶対パス名を入力しなければなりません。

変数	説明
	デフォルトの PATH は、ログインプロセスで .profile の指定どおりに自動的に定義され、設定されます。 検索パスの順序が重要です。同じコマンドが異なる場所にそれぞれ存在するときは、その名前で最初に見つかったコマンドが使用されます。たとえば、PATH がシェル構文で PATH=/usr/bin:/usr/sbin:$HOME/bin のように定義されており、sample というファイルが /usr/bin と /home/jean/bin の両方にあるものとします。ユーザーが sample コマンドを、その絶対パスを指定しないで入力した場合は、/usr/bin で見つかったバージョンが使用されます。
PS1	bash または ksh93 シェルのシェルプロンプトを定義します。
SHELL	make、vi、その他のツールが使うデフォルトシェルを設定します。
TERMINFO	代替の terminfo データベースが保存されているディレクトリに名前を付けます。/etc/profile または /etc/.login ファイルで TERMINFO 変数を使用します。詳細は、terminfo(4) のマニュアルページを参照してください。 TERMINFO 環境変数を設定すると、システムはまずユーザーが定義した TERMINFO パスを調べます。ユーザーが定義した TERMINFO ディレクトリ内に端末の定義が見つからなかった場合は、デフォルトディレクトリ /usr/share/lib/terminfo で定義を探します。どちらの場所でも定義が見つからなかった場合、端末は dumb として定義されます。
TERM	端末を定義します。この変数は、/etc/profile または /etc/.login ファイルで再設定するようにしてください。ユーザーがエディタを起動すると、システムはこの環境変数で定義される名前と同じ名前のファイルを探します。システムは、TERMINFO が参照するディレクトリ内を探して端末の特性を知ります。
TZ	タイムゾーンを設定します。タイムゾーンは、たとえば ls -l コマンドで日付を表示する場合に使われます。TZ をユーザーの環境に設定しない場合、システムの設定が使用されます。それ以外の場合は、グリニッジ標準時が使用されます。

Bash シェルのカスタマイズ

bash シェルをカスタマイズするには、ホームディレクトリにある .bashrc ファイルの情報を追加または変更します。Oracle Solaris のインストール時に作成される初期ユーザーは、PATH、MANPATH、およびコマンドプロンプトを設定するための .bashrc ファイルを持っています。詳細は、bash(1) のマニュアルページを参照してください。

MANPATH 環境変数

MANPATH 環境変数は、man コマンドがリファレンスマニュアル (man) ページを探す場所を指定します。MANPATH はユーザーの PATH の値に基づいて自動的に設定されますが、通常、/usr/share/man と usr/gnu/share/man が含まれます。

ユーザーの MANPATH 環境変数は、PATH 環境変数とは無関係に変更できることに注意してください。関連付けられたマニュアルページの場所と、ユーザーの $PATH 内のディレクトリが 1 対 1 で対応している必要ありません。

PATH 環境変数

ユーザーがフルパスを使用してコマンドを実行すると、シェルはそのパス名を使ってコマンドを探します。ただし、ユーザーがコマンド名しか指定しないと、シェルは PATH 変数で指定されているディレクトリの順でコマンドを探します。コマンドがいずれかのディレクトリで見つかれば、シェルはコマンドを実行します。

デフォルトのパスがシステムで設定されます。しかし、大部分のユーザーはそれを変更してほかのコマンドディレクトリを追加します。環境の設定や、正しいバージョンのコマンドまたはツールへのアクセスに関連して発生するユーザーの問題の多くは、パス定義の誤りが原因です。

PATH 変数を設定するためのガイドライン

PATH 変数を設定する場合は、次のガイドラインに注意してください。

- カレントディレクトリ (.) をパスに含める必要がある場合は、最後に配置してください。悪意のある人物が、改ざんされたスクリプトまたは実行可能ファイルをカレントディレクトリに隠す可能性があるため、パスにカレントディレクトリを含めることはセキュリティー上のリスクとなります。代わりに絶対パス名を使用することを検討してください。
- 検索パスはできるだけ短くしておきます。シェルはパスで各ディレクトリを探します。コマンドが見つからないと、検索に時間がかかり、システムのパフォーマンスが低下します。
- 検索パスは左から右に読まれるため、通常使用するコマンドをパスの初めの方に指定するようにしてください。
- パスでディレクトリが重複していないか確認してください。
- 可能であれば、大きなディレクトリの検索は避けてください。大きなディレクトリはパスの終わりに指定します。
- NFS サーバーが応答しない場合に、システムが応答しなくならないようにするには、NFS マウントされたディレクトリの前にローカルディレクトリを配置します。この方法によって、不要なネットワークトラフィックも減少します。

ロケール変数

LANG と LC の各環境変数は、ロケール固有の変換と表記をシェルに指定します。指定できる変換と表記には、タイムゾーンや照合順序、および日付、時間、通貨、番号

の書式などがあります。さらに、ユーザー初期設定ファイルで stty コマンドを使って、端末のセッションが複数バイト文字をサポートするかどうかを指定できます。

LANG 変数は、ロケールのすべての変換と表記を設定します。
ロケールの各種の設定を個別に行うには、次の LC 変数の
LC_COLLATE、LC_CTYPE、LC_MESSAGES、LC_NUMERIC、LC_MONETARY、および
LC_TIME を使用します。

注記 - Oracle Solaris 11 はデフォルトで、UTF-8 ベースのロケールのみをインストールします。

次の表では、コア Oracle Solaris 11 ロケールの環境変数の値について説明します。

表 11 ロケール変数の値

値	ロケール
en_US.UTF-8	英語、米国 (UTF-8)
fr_FR.UTF-8	フランス語、フランス (UTF-8)
de_DE.UTF-8	ドイツ語、ドイツ (UTF-8)
it_IT.UTF-8	イタリア語、イタリア (UTF-8)
ja_JP.UTF-8	日本語、日本 (UTF-8)
ko_KR.UTF-8	韓国語、韓国 (UTF-8)
pt_BT.UTF-8	ポルトガル語、ブラジル (UTF-8)
zh_CN.UTF-8	簡体字中国語、中華人民共和国 (UTF–8)
es_ES.UTF-8	スペイン語、スペイン (UTF-8)
zh_TW.UTF-8	繁体字中国語、台湾 (UTF-8)

例 1 ロケールの設定

Bourne または Korn シェルのユーザー初期化ファイルでは、次の行を追加してください。

```
LANG=de_DE.ISO8859-1; export LANG
```

デフォルトのファイルアクセス権 (umask)

ファイルまたはディレクトリを作成する場合、ファイルまたはディレクトリに割り当てられているデフォルトのファイルアクセス権は、ユーザーマスクによって制御されます。ユーザーマスクは、初期設定ファイルで umask コマンドによって設定されます。現在のユーザーマスクの値は、umask と入力して Return キーを押すと表示できます。

ユーザーマスクは、次の 8 進値で構成されます。

- 最初の桁でそのユーザーのアクセス権を設定する
- 2 桁目でグループのアクセス権を設定する
- 3 桁目でその他 (「ワールド」とも呼ばれる) のアクセス権を設定する

最初の桁がゼロの場合、その桁は表示されません。たとえば、ユーザーマスクを 022 に設定すると、22 が表示されます。

設定する umask の値は、与えたいアクセス権の値を 666 (ファイルの場合) または 777 (ディレクトリの場合) から差し引きます。引いた残りが umask に使用する値です。たとえば、ファイルのデフォルトモードを 644 (rw-r--r--) に変更するとします。666 と 644 の差である 022 が、umask コマンドの引数として使用する値です。

次の表に、umask の値を示します。これは、umask の各 8 進値から作成される、ファイルとディレクトリのアクセス権を示しています。

表 12 umask 値のアクセス権

umask 8 進値	ファイルアクセス権	ディレクトリアクセス権
0	rw-	rwx
1	rw-	rw-
2	r--	r-x
3	r--	r--
4	-w-	-wx
5	-w-	-w-
6	--x	--x
7	--- (なし)	--- (なし)

次の例は、デフォルトのファイルアクセス権を rw-rw-rw- に設定します。

```
umask 000
```

ユーザー初期設定ファイルのカスタマイズ

次の例は、.profile ユーザー初期設定ファイルのサンプルを示しています。このサンプルファイルをテンプレートとして使用し、独自のユーザー初期設定ファイルをカスタマイズできます。この例では、特定のサイト用に変更する必要があるシステム名とパスを使用します。

例 2 .profile ファイル

```
PATH=$PATH:$HOME/bin:/usr/local/bin:/usr/gnu/bin:      ユーザーのシェル検索パス
```

```
MAIL=/var/mail/$LOGNAME       ユーザーのメールファイルへのパス
NNTPSERVER=server1      ユーザーの時間/クロックサーバー
MANPATH=/usr/share/man:/usr/local/man       マニュアルページへのユーザーの検索パス
PRINTER=printer1      ユーザーのデフォルトプリンタ
umask 022      ユーザーのデフォルトファイル作成アクセス権
export PATH MAIL NNTPSERVER MANPATH PRINTER       指定された環境変数をエクスポートする
```

Oracle Enterprise Manager Ops Center を使用したユーザーの管理

個々のシステムではなく、大規模な配備内の物理および仮想オペレーティングシステム、サーバー、およびストレージデバイスを管理している場合は、Oracle Enterprise Manager Ops Center の管理ソリューションを使用できます。

Enterprise Manager Ops Center を使用すると、データセンター全体のユーザーおよび役割を管理できます。各システムから既存のローカルユーザーを Ops Center のユーザーとしてに追加し、これらのユーザーに使用を承認するセットと機能を制御できます。

詳細は、http://www.oracle.com/pls/topic/lookup?ctx=oc122 を参照してください。

♦ ♦ ♦ 第 2 章

2 コマンド行インタフェースを使用したユーザーアカウントの管理

この章では、コマンド行インタフェース (CLI) を使用して、ユーザーアカウントを設定し、管理するための基本情報を示します。

ユーザーアカウントおよびユーザー環境の管理に関する概要については、第1章「ユーザーアカウントとユーザー環境について」を参照してください。

ユーザーマネージャーのグラフィカルユーザーインタフェース (GUI) を使用したユーザーおよび役割の管理については、第3章「ユーザーマネージャー GUI を使用したユーザーアカウントの管理」を参照してください。

CLI を使用したユーザーアカウントの設定と管理のタスクマップ

次のタスクでは、コマンド行インタフェース (CLI) を使用したユーザーアカウントの設定および管理方法について説明します。

タスク	説明	手順の参照先
ユーザー情報の収集。	標準の書式を使ってユーザー情報を収集すると、情報を整理しやすくなります。	42 ページの「ユーザー情報の収集」
ユーザー初期設定ファイルをカスタマイズします。	新規ユーザーに一貫した環境を提供するようにユーザー初期設定ファイルを設定します。	43 ページの「ユーザー初期設定ファイルをカスタマイズする方法」
すべての役割についてアカウントのデフォルトを変更します。	すべての役割について、デフォルトのホームディレクトリとスケルトンディレクトリを変更します。	44 ページの「すべての役割についてアカウントのデフォルトを変更する方法」
ユーザーアカウントを作成します。	設定したアカウントのデフォルト値と `useradd` コマンドを使用して、ローカルユーザーを作成します。	45 ページの「ユーザーを追加する方法」

タスク	説明	手順の参照先
ユーザーアカウントを変更します。	システムにあるユーザーのログイン情報を変更します。	46 ページの「ユーザーアカウントの変更方法」
ユーザーアカウントをロック解除します。	`passwd -u` コマンドを使用してユーザーアカウントをロック解除します。	46 ページの「ユーザーアカウントをロック解除する方法」
ユーザーアカウントを削除します。	`userdel` コマンドを使用してユーザーアカウントを削除します。	47 ページの「ユーザーを削除する方法」
管理タスクを実行するための役割を作成し、割り当てます。	ユーザーが特定の管理コマンドまたはタスクを実行できるように、設定したアカウントのデフォルト値を使用して、ローカルの役割を作成します。	『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の「役割の作成」
グループの作成。	`groupadd` コマンドを使用して、新しいグループを作成します。	48 ページの「グループを追加する方法」
セキュリティー属性をユーザーアカウントに追加します。	ローカルユーザーアカウントを設定したあとに、必要なセキュリティー属性を追加できます。	『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の「役割の作成」
ユーザーのホームディレクトリを共有します。	ユーザーのホームディレクトリを共有して、ユーザーのシステムからそのディレクトリをリモートでマウントできるようにする必要があります。	49 ページの「ZFS ファイルシステムとして作成されたホームディレクトリを共有する方法」
ユーザーのホームディレクトリを手動でマウントします。	通常は、ZFS ファイルシステムとして作成されたユーザーのホームディレクトリを手動でマウントする必要はありません。ホームディレクトリは作成時に、また SMF ローカルファイルシステムサービスからのブート時に自動的にマウントされます。	50 ページの「ユーザーのホームディレクトリの手動マウント」

CLI を使用したユーザーアカウントの設定

このセクションの内容は次のとおりです。

ユーザーアカウントの設定のガイドライン

CLI を使用してユーザーアカウントを設定する場合に、次のガイドラインに注意してください。

- このリリースでは、ユーザーアカウントは Oracle Solaris ZFS ファイルシステムとして作成されます。管理者として、ユーザーアカウントを作成すると、ユーザーに固有のファイルシステムと固有の ZFS データセットを付与することになります。`useradd` および `roleadd` コマンドを使用して作成されるすべてのホームディレクトリは、ユーザーのホームディレクトリを個別の ZFS ファイルシステムとして `/export/home` ファイルシステム上に配置します。その結果、ユーザーは自分のホームディレクトリをバックアップしたり、自分のホームディレクトリの ZFS スナップショットを作成したり、自分の現在のホームディレクトリ内のファイルを、自分が作成した ZFS スナップショットから置き換えたりできるようになります。
- ユーザーアカウントを設定するには、`root` 役割または適切な権利プロファイル (ユーザー管理権利プロファイルなど) を持つ役割になる必要があります。『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「割り当てられている管理権利の使用」を参照してください。
- `useradd` コマンドでユーザーアカウントを作成する場合は、`-m` オプションを指定して、ユーザーのホームディレクトリを作成します。

  たとえば、次のコマンドはユーザー `jdoe` のホームディレクトリを作成します。

  ```
  # useradd -m jdoe
  ```

  ただし、次の構文はユーザーのホームディレクトリを作成しません:

  ```
  # useradd jdoe
  ```

  注記 - `pam_zfs_key` モジュールで、暗号化されたユーザーのホームディレクトリを作成する場合は、`-m` オプションを `useradd` コマンドに指定しないでください。`pam_zfs_key(5)` および `zfs_encrypt(1M)` のマニュアルページを参照してください。

- `useradd` コマンドは、`-d` オプションが *hostname*`:`*/pathname* とともに指定された場合にのみ、`auto_home` マップにエントリを作成します。それ以外の場合は、指定されたパス名が `passwd` データベース内のユーザーのホームディレクトリとして更新され、`auto_home` マップエントリが作成されません。`auto_home` オートマウンタマップに指定されたホームディレクトリは、`autofs` サービスが有効な場合にのみマウントされます。

  たとえば、`-d` オプションを指定して、次のようにユーザーを作成すると、`auto_home` エントリなしでユーザーが作成され、`passwd` エントリでユーザーのホームディレクトリとして `/export/home/user1` が指定されます。

  ```
  # useradd -d /export/home/user1 user1
  ```

-d オプションを使用して、次のようにユーザーを作成すると、ユーザーは auto_home エントリを持ち、passwd データベースに /home/user1 が含まれ、autofs サービスへの依存関係が示されます。

```
# useradd -d localhost:/export/home/user1 user1
```

- ホームディレクトリのパス名に foobar:/export/home/jdoe などのリモートホスト指定が含まれている場合は、jdoe のホームディレクトリをシステム foobar 上に作成する必要があります。デフォルトのパス名は localhost:/export/home/*username* です。
- Oracle Solaris 11 のすべての状況にあてはまる、ファイルシステムが ZFS データセットである場合、ユーザーのホームディレクトリは子の ZFS データセットとして作成され、スナップショットを作成するための ZFS アクセス許可がユーザーに委任されます。ZFS データセットに対応しないパス名が指定された場合、通常のディレクトリが作成されます。-S ldap オプションを指定した場合は、ローカルの auto_home マップではなく、LDAP サーバーで auto_home マップエントリが更新されます。

ユーザー情報の収集

ユーザーアカウントを設定するときは、アカウントを設定する前にユーザーについての情報を収集するために、次のようなフォームを作成できます。

項目	説明
ユーザー名	
役割名	
プロファイルまたは承認	
UID	
プライマリグループ	
セカンダリグループ	
コメント	
デフォルトシェル	
パスワードのステータスと有効期限	
ホームディレクトリのパス名	
マウント方法	
ホームディレクトリのアクセス権	
メールサーバー	
メール別名への追加	
デスクトップシステム名	

パッケージによるユーザーの識別

このシステムでパッケージによって配信された (人間を表していない) すべてのユーザーを検索するには、--l オプションを指定する必要があります。この検索では、useradd コマンドによって手動で作成されたユーザーパッケージは除外されます。

```
:$ pkg search -lo username, pkg.name user::
```

注意 - pkg search コマンドを使用してユーザーの出力を変更しないでください。

▼ ユーザー初期設定ファイルをカスタマイズする方法

次のタスクでは、システム上のユーザーに対して、カスタマイズされた初期設定ファイルの設定方法について説明します。

1. **root の役割を持つ管理者になります。**

```
$ su -
Password:
#
```

『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「割り当てられている管理権利の使用」を参照してください。

2. **各タイプのユーザー用にスケルトンディレクトリを作成します。**

```
# mkdir /shared-dir/skel/user-type
```

shared-dir ネットワーク上の別のシステムで利用できるディレクトリの名前。

user-type ユーザーのタイプに応じて初期設定ファイルを格納するディレクトリの名前。

3. **デフォルトのユーザー初期設定ファイルを、異なるタイプのユーザー用に作成したディレクトリにコピーします。**

4. **ユーザータイプごとにユーザー初期設定ファイルをカスタマイズします。**

ユーザー初期設定ファイルのカスタマイズ方法の詳細は、27 ページの「ユーザーの作業環境について」を参照してください。

5. **ユーザー初期設定ファイルのアクセス権を設定します。**

```
# chmod 744 /shared-dir/skel/user-type/.*
```

6. **ユーザー初期設定ファイルのアクセス権が正しいことを確認します。**

```
# ls -la /shared-dir/skel/*
```

▼ すべての役割についてアカウントのデフォルトを変更する方法

次の手順では、管理者が roles ディレクトリをカスタマイズ済みです。管理者はすべての役割についてデフォルトのホームディレクトリとスケルトンディレクトリを変更します。

1. **管理者になるか、User Management 権利プロファイルを持つユーザーとしてログインします。**

   『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「割り当てられている管理権利の使用」を参照してください。

2. **カスタムの roles ディレクトリを作成します。**

   例:

```
# roleadd -D
group=other,1  project=default,3  basedir=/home
skel=/etc/skel  shell=/bin/pfsh  inactive=0
expire=  auths=  profiles=All  limitpriv=
defaultpriv=  lock_after_retries=
```

3. **すべての役割について、デフォルトのホームディレクトリとスケルトンディレクトリを変更します。**

   例:

```
# roleadd -D -b /export/home -k /etc/skel/roles
# roleadd -D
group=staff,10  project=default,3  basedir=/export/home
skel=/etc/skel/roles  shell=/bin/sh  inactive=0
expire=  auths=  profiles=  roles=  limitpriv=
defaultpriv=  lock_after_retries=
```

   以後、roleadd コマンドを使用すると、ホームディレクトリが /export/home に作成され、役割の環境が /etc/skel/roles ディレクトリから取り込まれます。

CLI を使用したユーザーアカウントの管理

このセクションの内容は次のとおりです。

▼ ユーザーを追加する方法

1. **管理者になるか、User Management 権利プロファイルを持つユーザーとしてログインします。**

   『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「割り当てられている管理権利の使用」を参照してください。

2. **ローカルユーザーを作成します。**

   デフォルトでは、ユーザーはローカルに作成されます。-S ldap オプションを含めると、ユーザーは既存の LDAP リポジトリに作成されます。

   ```
   # useradd -d dir -m username
   ```

useradd	指定されたユーザーのアカウントを作成します。
-d	ユーザーのホームディレクトリの場所を指定します。 エントリが auto_home に強制的に書き込まれるようにするには、-d /export/home/*username* の代わりに -d localhost:/export/home/*username* を使用します。
-m	ユーザーのローカルホームディレクトリをシステム上に作成します。

   useradd コマンドで指定できるすべてのオプションと引数の詳細な説明については、useradd(1M) のマニュアルページを参照してください。

   注記 - ユーザーにパスワードを割り当てるまで、アカウントはロックされます。

3. **ユーザーにパスワードを割り当てます。**

   ```
   # passwd username
   New password:       ユーザーパスワードを入力します
   Re-enter new password:       パスワードを再入力します
   ```

その他のコマンドオプションについては、useradd(1M) および passwd(1) のマニュアルページを参照してください。

参照 ユーザーの作成後に、ユーザーへの役割の追加および割り当て、ユーザーの権利プロファイルの表示または変更などの追加のタスクの実行が必要になる場合があります。詳細は、『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「役割の作成」を参照してください。

▼ ユーザーアカウントの変更方法

usermod コマンドは、ユーザーのログインの定義を変更し、ユーザーの適切なログイン関連ファイルシステムの変更を行うために使用します。

1. **管理者になるか、User Management 権利プロファイルを持つユーザーとしてログインします。**
   『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「割り当てられている管理権利の使用」を参照してください。

2. **必要に応じて、ユーザーアカウントを変更します。**
   usermod コマンドで指定できる引数とオプションの詳細は、usermod(1M) のマニュアルページを参照してください。
   たとえば、ユーザーに役割を追加するには、次のように入力します。

   ```
   # usermod -R role username
   ```

例 3 ユーザーのアカウントの変更によるユーザーごとの PAM ポリシーの設定

次の例に、PAM ポリシーを設定するためにユーザーを変更する方法を示します。この特定の変更では、ユーザー jdoe が、すべての PAM サービスについて、Kerberos V5 プロトコルによってのみ認証されることを指定します。詳細は、pam_user_policy(5) のマニュアルページを参照してください。

```
# usermod -K pam_policy=krb5_only jdoe
```

参照 詳細は、『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「役割の作成」を参照してください。

▼ ユーザーアカウントをロック解除する方法

1. **管理者になるか、User Security 権利プロファイルを持つユーザーとしてログインします。**

『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』の『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「割り当てられている管理権利の使用」を参照してください。

2. **ロック解除する必要のあるユーザーアカウントのステータスを確認します。**

```
$ passwd -s username
username      LK
```

3. **ユーザーアカウントをロック解除します。**

```
$ passwd -u username
passwd: password information changed for username
```

4. **目的のユーザーアカウントがロック解除されたかどうかを確認します。**

```
$ passwd -s
username      PS
```

注記 - ユーザーアカウントのロック解除の詳細は、19 ページの「ユーザー名、ユーザー ID、グループ ID の割り当てのガイドライン」および passwd(1) のマニュアルページを参照してください。

▼ ユーザーを削除する方法

1. **管理者になります。**

```
$ su -
Password:
#
```

注記 - この方法は、root がユーザーアカウントと役割のどちらであっても有効です。

2. **ユーザーのホームディレクトリをアーカイブします。**

3. **ユーザーを削除します。**

```
# userdel -r username

The -r option removes the account from the system.
```

ユーザーのホームディレクトリは現在は ZFS データセットであるため、削除するユーザーのローカルホームディレクトリを削除する場合は、userdel コマンドの -r オプションを指定する方法を推奨します。

4. **ユーザーのホームディレクトリがリモートサーバーにある場合は、手動で削除します。**

```
# userdel username
```

すべてのコマンドオプションの完全なリストは、userdel(1M) のマニュアルページを参照してください。

次の手順 削除したユーザーが cron ジョブの作成などの管理権限を持っていた場合や、そのユーザーが非大域ゾーンに追加のアカウントを持っていた場合、追加のクリーンアップが必要な場合があります。

▼ グループを追加する方法

管理者がグループを作成すると、システムによって solaris.group.assign/*groupname* がその管理者に割り当てられ、管理者はそのグループを完全に制御できます。同じ承認を持つ別の管理者がグループを作成すると、その管理者はそのグループを制御できます。グループを制御する管理者は、他の管理者のグループを管理できません。詳細については、groupadd(1M) および groupmod(1M) のマニュアルページを参照してください。

1. **管理者または solaris.group.manage 承認を持つユーザーになります。**

   『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「割り当てられている管理権利の使用」を参照してください。

2. **既存のグループを一覧表示します。**

   ```
   # cat /etc/group
   ```

3. **新しいグループを作成します。**

   ```
   $ groupadd -g group-id group-name
   ```

groupadd	/etc/group ファイルに適切なエントリを追加して、新しいグループ定義をシステム上に作成します。
-g	新しいグループのグループ ID を割り当てます。

   詳細は、groupadd(1M) のマニュアルページを参照してください。

例 4 groupadd および useradd コマンドを使用したグループとユーザーの設定

次の例では、groupadd および useradd の各コマンドを使って、グループ scutters やユーザー scutter1 をローカルシステムのファイルに追加します。

```
# groupadd -g 102 scutters
# useradd -u 1003 -g 102 -d /export/home/scutter1 -s /bin/csh \
-c "Scutter 1" -m -k /etc/skel scutter1
```

```
64 blocks
```

詳細は、groupadd(1M) および useradd(1M) のマニュアルページを参照してください。

ZFS ファイルシステムを共有する

この Oracle Solaris リリースでは、share.nfs プロパティーまたは share.smb プロパティーを設定することで、ZFS ファイルシステムを共有できます。または zfs share コマンドを使用して、ファイルシステム共有を作成できます。デフォルトでは、すべてのファイルシステムが共有されません。

デフォルトで、pool/export/home データセットが /export/home にすでにマウントされています。useradd コマンドは、このデータセットの子として、ユーザーごとのデータセットを自動的に作成します。管理者として、ユーザーのホームディレクトリの新しいプールを作成するように選択できます。

ファイルシステムの共有または共有解除の詳細は、『Oracle Solaris 11.3 でのネットワークファイルシステムの管理』 の 「autofs 管理」を参照してください。

▼ ZFS ファイルシステムとして作成されたホームディレクトリを共有する方法

1. **管理者になるか、User Management 権利プロファイルが割り当てられたユーザーとしてログインします。**

   『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「割り当てられている管理権利の使用」を参照してください。

2. **ユーザーのホームディレクトリ用に独立したプールを作成します。**

   ```
   # zpool create pool mirror disk 1 disk 2 mirror disk 3 disk 4
   ```

   例:

   ```
   # zpool create users mirror c1t1d0 c1t2d0 mirror c2t1d0 c2t2d0
   ```

3. **ホームディレクトリのコンテナを作成します。**

   ```
   # zfs create filesystem
   ```

   例:

   ```
   # zfs create users/home
   ```

4. **ホームディレクトリの共有プロパティーを設定します。**

たとえば、NFS 共有を作成し、users/home に share.nfs プロパティーを設定するには、次のように入力します。

```
# zfs set share.nfs=on users/home
```

この新しい構文を使用すると、各ファイルシステムの share.nfs プロパティー (または share.smb プロパティー) が on に設定されるとただちに作成される「自動共有」が、そのファイルシステムに含まれます。前のコマンドは、users/home というファイルシステムとそのすべての子を共有します。

5. **下位ファイルシステム共有も公開されることを確認します。**

   例:

   ```
   # zfs get -r share.nfs users/home
   ```

   -r オプションは、すべての下位ファイルシステムを表示します。

ユーザーのホームディレクトリの手動マウント

ZFS ファイルシステムとして作成されるユーザーアカウントは通常、手動でマウントする必要がありません。ZFS では、ファイルシステムは作成時に自動マウントされ、それ以降は、SMF ローカルファイルシステムサービスからのブート時にマウントされます。

ユーザーアカウントを作成するときは必ず、ネームサービスと同じように、ホームディレクトリを /home/*username* に設定してください。次に、auto_home マップがユーザーのホームディレクトリの NFS パスを指していることを確認してください。タスク関連情報については、『Oracle Solaris 11.3 でのネットワークファイルシステムの管理』 の 「autofs 管理」を参照してください。

ユーザーのホームディレクトリを手動でマウントする必要がある場合は、zfs mount コマンドを使用します。例:

```
# zfs mount users/home/jdoe
```

注記 - ユーザーのホームディレクトリが共有されていることを確認します。詳細は、49 ページの「ZFS ファイルシステムとして作成されたホームディレクトリを共有する方法」を参照してください。

♦ ♦ ♦ 第 3 章

3 ユーザーマネージャー GUI を使用したユーザーアカウントの管理

この章では、Oracle Solaris ユーザーマネージャーグラフィカルユーザーインタフェース (GUI) を使用して、ユーザーの設定および管理の概要とタスク関連情報について説明します。ユーザーマネージャー GUI を使用して、同等のコマンド (`useradd`、`usermod`、`userdel` など) を使用して実行できるほとんどのタスクを実行できます。ただし、これらのコマンドを使用して、作成しなかったアカウントは変更できません。ユーザーマネージャー GUI の詳細は、GUI のオンラインヘルプを参照してください。

この章で扱う内容は、次のとおりです。

- 51 ページの「ユーザーマネージャー GUI の概要」
- 56 ページの「ユーザーマネージャー GUI を使用したユーザーと役割の追加、変更、削除」
- 59 ページの「ユーザーマネージャー GUI を使用した詳細属性の割り当て」

ユーザーアカウントの管理に関する概要については、第1章「ユーザーアカウントとユーザー環境について」を参照してください。

CLI を使用したユーザーアカウントの管理については、第2章「コマンド行インタフェースを使用したユーザーアカウントの管理」を参照してください。

ユーザーマネージャー GUI の概要

このセクションでは、次の内容について説明します。

- 52 ページの「ユーザーマネージャー GUI を起動する方法」
- 52 ページの「「ユーザーマネージャー」ダイアログボックスの構成」
- 53 ページの「GUI に表示される情報のフィルタリング」
- 55 ページの「役割の引き受け」

ユーザーマネージャー GUI は Visual Panels フレームワークに基づき、Visual Panels インタフェースとして提供されています。ユーザー認証と役割の引き受けは、Visual

Panels フレームワーク自体で提供され、ユーザーマネージャー GUI を含むすべてのパネルで使用可能です。ユーザーマネージャー GUI は、Oracle Solaris 10 でサポートされている Solaris Management Console のユーザーと役割ツールに置き換わるものです。Solaris Management Console とまったく同じではありませんが、GUI にはいくつかの同じ機能があります。

注記 - Solaris Management Console は、このリリースではサポートされていません。

ユーザーマネージャー GUI は使いやすく簡単で明確なインタフェースを提供します。エラーの可能性を最小にするため、GUI は認証されたユーザーまたは役割の承認と権利プロファイルに基づいて、有効なオプションのみを表示します。

ユーザーマネージャー GUI は `pkg:/system/management/visual-panels/panel-usermgr` IPS パッケージによって提供されます。

▼ ユーザーマネージャー GUI を起動する方法

1. **管理者になるか、User Management 権利プロファイルが割り当てられたユーザーとしてログインします。**

   『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 「割り当てられている管理権利の使用」を参照してください。

2. **ユーザーマネージャー GUI を起動します。**

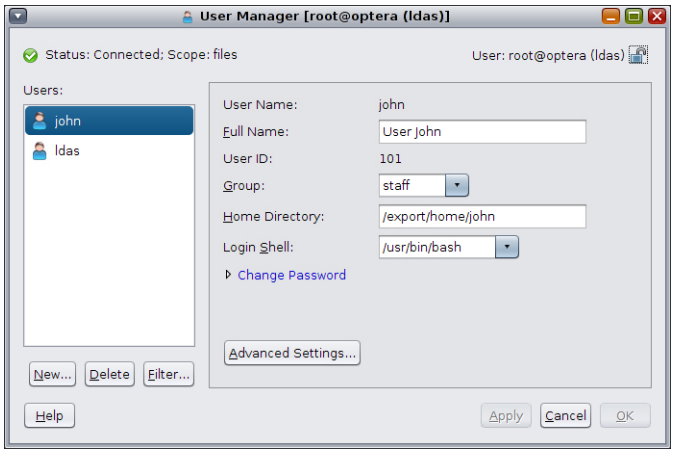
   - **デスクトップ:「システム」->「管理」->「ユーザーマネージャー」の順に選択します。**
   - **コマンド行:**

     ```
     # vp usermgr &
     ```

「ユーザーマネージャー」ダイアログボックスの構成

ユーザーマネージャー GUI を起動すると、「ユーザーマネージャー」メインダイアログボックスが表示されます。「ユーザーマネージャー」ダイアログボックスは、ユーザーと役割を管理するために使用します。ダイアログボックスの左上にある「Status」フィールドには、ローカルシステムで現在実行中のサービスのステータスが表示されます。 ダイアログボックスの右上には「ユーザー」フィールドがあり、ユーザーマネージャー GUI で現在使用されている資格情報が表示されます。資格情報の変更方法を見つけるには、55 ページの「役割の引き受け」を参照してください。

次の図は、ユーザー john が選択された「ユーザーマネージャー」メインダイアログボックスを示しています。



「ユーザーマネージャー」ダイアログボックスには次のコンポーネントがあります。

- ユーザーと役割のリスト – 管理するために選択できるユーザーのリスト
- 基本設定 – ユーザー名や氏名などのユーザーの基本設定

既存のユーザーの情報を表示または変更するには、表示されるユーザーのリストからユーザーを選択します。ユーザーを選択すると、そのユーザーの情報がダイアログボックスの右側に表示されます。

「ユーザーマネージャー」ダイアログボックス内から、次のアクションが可能です。

- 新規ユーザーまたは役割の作成 – 56 ページの「ユーザーマネージャー GUI によるユーザーまたは役割を追加する方法」を参照してください。
- 既存のユーザーまたは役割の削除 – 58 ページの「ユーザーマネージャー GUI を使用したユーザーまたは役割の削除方法」を参照してください。
- ユーザーの情報のフィルタ – 53 ページの「GUI に表示される情報のフィルタリング」を参照してください。
- 既存のユーザーの詳細設定の管理 – 58 ページの「ユーザーマネージャー GUI によるユーザーまたは役割を変更する方法」を参照してください。

GUI に表示される情報のフィルタリング

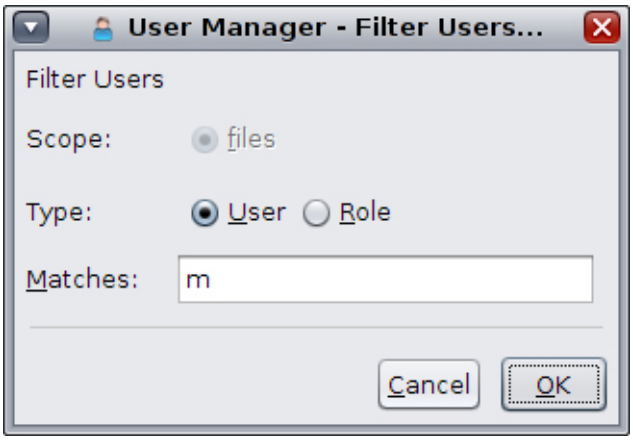
ユーザーマネージャー GUI に表示される情報をフィルタできます。ユーザーのみを表示したり、役割のみを表示したりするように選択できます。また、システムが LDAP

クライアントとして構成されている場合の表示のスコープ (ファイル情報または LDAP 情報のいずれか) を制限することもできます。

デフォルトの設定はユーザーおよびファイルです。これらの設定では、役割ではなくユーザーが表示され、ユーザーの LDAP 仕様ではなく、ユーザーのファイル情報が表示されます。

フィルタダイアログボックスでは、入力した検索基準に一致するユーザー名または役割名を検索することもできます。

次のダイアログボックスでは、システムは LDAP 用に構成されていないため、スコープオプションは使用できません。タイプは、役割ではなくユーザーを表示するようにフィルタされています。また、「m」で始まるユーザー名を検索するように検索が指定されています。



▼ デフォルトのネームサービスのタイプおよびスコープのフィルタの設定方法

1. **ユーザーマネージャー GUI を起動します。**
   52 ページの「ユーザーマネージャー GUI を起動する方法」を参照してください。
2. **「フィルタ」ボタンをクリックします。**
3. **「スコープ」オプションをファイルまたは LDAP (使用可能な場合) のいずれかに設定します。**
4. **「タイプ」オプションを「ユーザー」または「役割」のいずれかに設定します。**

5. **オプションで、特定の役割名またはユーザー名をフィルタするには、検索基準となるテキストを入力します。**

6. **「OK」をクリックします。**

役割の引き受け

ユーザーマネージャー権利プロファイルがある場合は、作成するユーザーまたは役割の詳細属性が、権限の詳細属性のサブセットであるかぎり、新規ユーザーまたは役割を作成できます。十分な承認はないが、十分な承認のある管理役割がある場合は、この手順で説明されているように、「ユーザーマネージャー」メインダイアログボックスの「ロック」ボタンをクリックすることで、必要な管理を実行する役割になることができます。

▼ 役割になる方法

1. **ユーザーマネージャー GUI を起動します。**
   52 ページの「ユーザーマネージャー GUI を起動する方法」を参照してください。

2. **「ユーザーマネージャー」メインダイアログボックスの右上のセクションで、ユーザー名の横の「ロック」アイコンをクリックします。**
   次のオプションを含むサブメニューが表示されます。

   - 役割の変更
   - ユーザーの変更
   - 新規ホストの管理
   - 履歴のクリア

3. **「役割の変更」オプションを選択します。**
   認証ダイアログボックスが表示されます。認証ダイアログボックスには、使用可能な役割を一覧表示するドロップダウンメニューが含まれます。

4. **適切な役割を選択します。**

5. **「ログイン」をクリックして、その役割になります。**
   役割を引き受けたあとに、必要な管理タスクを実行できます。

ユーザーマネージャー GUI を使用したユーザーと役割の追加、変更、削除

ユーザーマネージャー GUI を使用したユーザーの追加、変更、および削除は、それぞれ `useradd`、`usermod`、および `userdel` コマンドを使用した場合と同じです。コマンド行からユーザーを追加する方法の詳細は、第2章「コマンド行インタフェースを使用したユーザーアカウントの管理」を参照してください。

このセクションでは、次の情報について説明します。

▼ ユーザーマネージャー GUI によるユーザーまたは役割を追加する方法

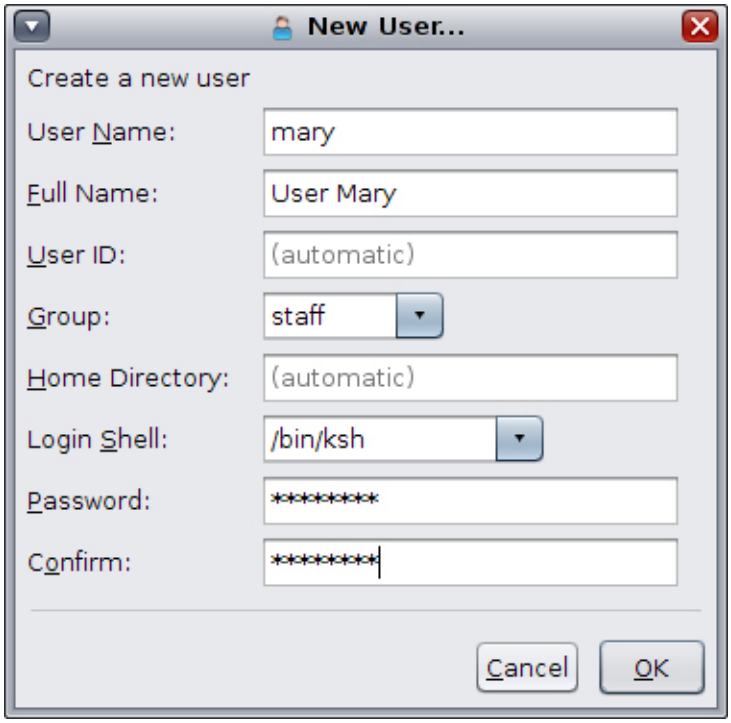
この手順では、現在 GUI で使用されているフィルタのスコープ内に新しいユーザーまたは役割を追加します。

1. **ユーザーマネージャー GUI を起動します。**

   52 ページの「ユーザーマネージャー GUI を起動する方法」を参照してください。

2. **「ユーザーマネージャー」メインダイアログボックスの「新規」ボタンをクリックします。**

「新規ユーザー」ダイアログボックスが表示されます。



3. **ユーザーアカウント情報を指定します。**

   - ユーザー名
   - フルネーム
   - ユーザーID - この情報はオプションです。情報を指定しない場合、自動的にデフォルト値が割り当てられます。
   - グループ -「グループ」フィールドで選択可能なオプションは、システムの構成によって異なります。
   - ホームディレクトリ - この情報はオプションです。情報を指定しない場合、自動的にデフォルト値が割り当てられます。

     オートマウントされるユーザーのホームディレクトリが必要な場合、パス名の前にホスト名またはローカルホストを付けます。たとえば、`localhost:/export/home/test1` です。
   - ログインシェル -「ログインシェル」フィールドの選択項目は、システムの構成によって異なります。
   - パスワード - ユーザーに一時パスワードを割り当てます。

- 確認 - ユーザーに割り当てられる一時パスワードを確認します。

4. **「OK」をクリックします。**
   「ユーザーマネージャー」メインダイアログボックスに表示されるユーザーのリストにユーザーまたは役割が追加されたら、「OK」をクリックします。

▼ ユーザーマネージャー GUI によるユーザーまたは役割を変更する方法

1. **ユーザーマネージャー GUI を起動します。**
   52 ページの「ユーザーマネージャー GUI を起動する方法」を参照してください。

2. **表示されるリストから、変更するユーザーまたは役割を選択します。**
   ユーザーを選択すると、ダイアログボックスの右側に、現在のユーザーに関する情報が入力されます。

3. **現在のユーザーまたは役割の情報の一部またはすべてを変更します。**

   注記 - フィールドを変更すると、フィールドの横にインジケータが表示されます。

4. **「適用」をクリックして変更を保存します。**

5. **(オプション) ユーザーまたは役割の追加のセキュリティー属性を変更するには、「詳細設定」ボタンをクリックします。**
   59 ページの「ユーザーマネージャー GUI を使用した詳細属性の割り当て」を参照してください。

6. **「OK」をクリックして変更内容を保存し、ダイアログボックスを閉じます。**

▼ ユーザーマネージャー GUI を使用したユーザーまたは役割の削除方法

この手順では、現在ユーザーマネージャー GUI で使用されているフィルタのスコープ内のユーザーまたは役割を削除します。

1. **「ユーザーマネージャー」メインダイアログボックスで、ユーザーまたは役割を選択します。**

2. 「削除」ボタンをクリックします。
3. 確認のダイアログボックスで「OK」をクリックします。

ユーザーマネージャー GUI を使用した詳細属性の割り当て

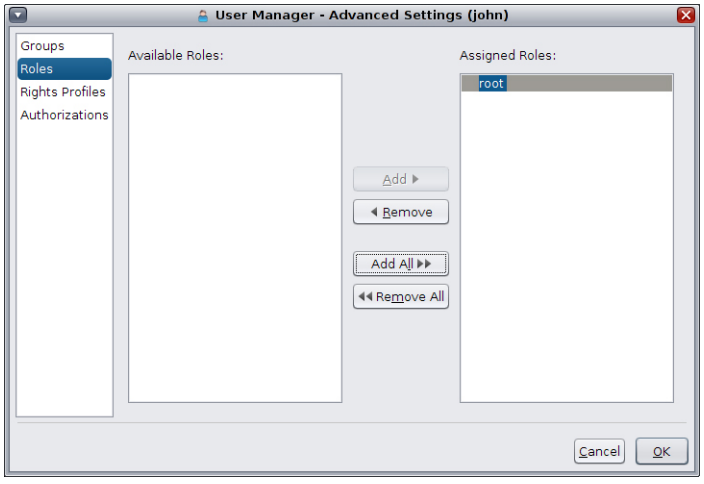
このセクションでは、次の情報について説明します。

- 60 ページの「ユーザーマネージャー GUI を使用したグループの割り当て」
- 61 ページの「ユーザーマネージャー GUI を使用した役割の割り当て」
- 62 ページの「ユーザーマネージャー GUI を使用した権利プロファイルの割り当て」
- 63 ページの「ユーザーマネージャー GUI を使用した承認の割り当て」

ユーザーマネージャー GUI の「詳細設定」ダイアログボックスを使用して、権利プロファイル、役割、承認などの追加のセキュリティー属性をユーザーに割り当てます。

概要については、『Oracle Solaris 11.3 でのユーザーとプロセスのセキュリティー保護』 の 第 1 章,「権利を使用したユーザーとプロセスの制御について」を参照してください。

次の図は、ユーザー john の「役割」セキュリティー属性が選択された「詳細設定」ダイアログボックスを示しています。選択したユーザーの名前は、ダイアログボックスのタイトルバーの括弧内に表示されます。



「詳細設定」ダイアログボックスでは、次のセキュリティー属性を割り当てることができます。

- グループ
- 役割
- 権利プロファイル
- 承認

ユーザーマネージャー GUI を使用したグループの割り当て

グループは、ユーザーマネージャー GUI の「詳細設定」から割り当てられます。

▼ グループの割り当て方法

1. **ユーザーマネージャー GUI を起動します。**
   52 ページの「ユーザーマネージャー GUI を起動する方法」を参照してください。

2. **「ユーザーマネージャー」メインダイアログボックスでユーザーを選択し、「詳細設定」ボタンをクリックします。**
   「詳細設定」ダイアログボックスが表示されます。

3. **ダイアログボックスの左側の「グループ」属性をクリックします。**
   使用可能なグループのリストおよび現在のユーザーが属しているグループのリストが表示されます。

   - **ユーザーにグループ (または複数のグループ) を割り当てるには、「使用可能なグループ」リストからグループを選択し、「追加」をクリックします。**
     追加したグループが「割り当てられたグループ」リストに表示されます。

   - **「割り当てられたグループ」リストからグループを削除するには、リストからグループを選択し、「削除」をクリックします。**

   - **現在のユーザーのすべてのグループを追加または削除するには、「すべてを追加」または「すべてを削除」ボタンをクリックします。**

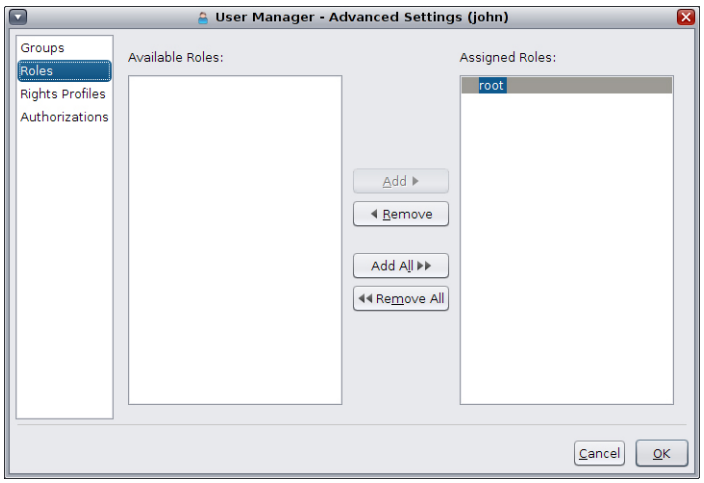
4. **「OK」をクリックして設定を保存します。**
   「ユーザーマネージャー」メインダイアログボックスで「適用」または「OK」をクリックするまで、変更は適用されません。

ユーザーマネージャー GUI を使用した役割の割り当て

役割は、ユーザーマネージャー GUI の「詳細設定」から割り当てられます。

注記 - 役割はユーザーにのみ割り当てることができるため、「役割」属性は、役割ではなくユーザーに対してのみ使用できます。

次の図は、ユーザー john の「役割」セキュリティー属性が選択された「詳細設定」ダイアログボックスを示しています。



▼ ユーザーマネージャー GUI を使用した役割の割り当て方法

1. **ユーザーマネージャー GUI を起動します。**
   52 ページの「ユーザーマネージャー GUI を起動する方法」を参照してください。

2. **「ユーザーマネージャー」メインダイアログボックスでユーザーを選択し、「詳細設定」ボタンをクリックします。**
   「詳細設定」ダイアログボックスが表示されます。

3. **ダイアログボックスの左側の「役割」属性をクリックします。**
   使用可能な役割のリストおよび現在のユーザーに割り当てられている役割のリストが表示されます。

- **役割 (または複数の役割) をユーザーに割り当てるには、「使用可能な役割」リストから役割 (または複数の役割) を選択し、「追加」をクリックします。**
  追加した役割が「割り当てられた役割」リストに表示されます。

- **「割り当てられた役割」リストから役割を削除するには、リストから役割 (または複数の役割) を選択し、「削除」をクリックします。**

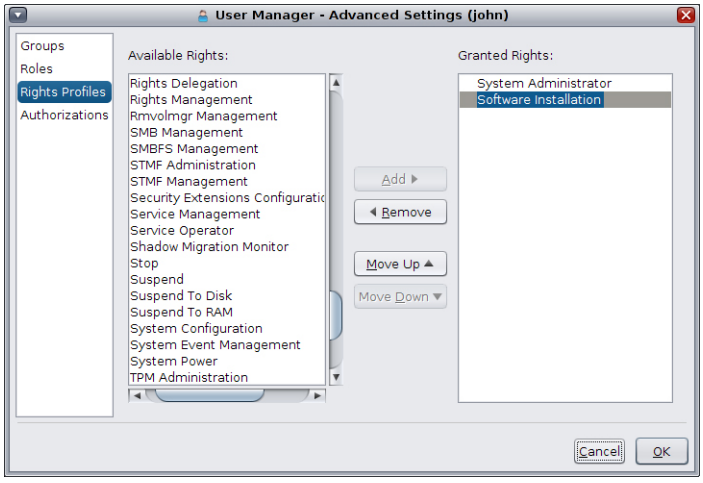
- **現在のユーザーのすべての役割を追加または削除するには、「すべてを追加」または「すべてを削除」ボタンをクリックします。**

4. **「OK」をクリックして設定を保存します。**
   「ユーザーマネージャー」メインダイアログボックスで「適用」または「OK」をクリックするまで、変更は適用されません。

ユーザーマネージャー GUI を使用した権利プロファイルの割り当て

権利プロファイルは、ユーザーマネージャー GUI の「詳細設定」から割り当てられます。

次の図は、ユーザー john の「権利プロファイル」セキュリティー属性が選択された「詳細設定」ダイアログボックスを示しています。



注記 - 権利プロファイルの割り当てには、優先順位があります。「上に移動」および「下に移動」ボタンを使用して、現在のユーザーに付与されている権利プロファイルの順番を変更します。

▼ ユーザーマネージャー GUI による権利プロファイルの管理方法

1. **ユーザーマネージャー GUI を起動します。**
52 ページの「ユーザーマネージャー GUI を起動する方法」を参照してください。

2. **「ユーザーマネージャー」メインダイアログボックスでユーザーを選択し、「詳細設定」ボタンをクリックします。**
「詳細設定」ダイアログボックスが表示されます。

3. **ダイアログボックスの左側の「権利プロファイル」属性をクリックします。**
使用可能な権利プロファイルのリストおよび現在のユーザーに付与されている権利プロファイルのリストが表示されます。

   - **権利プロファイル (または複数の権利プロファイル) をユーザーに割り当てるには、「使用可能な権利」プロファイルリストから権利プロファイル (または複数の権利プロファイル) を選択し、「追加」をクリックします。**
   「付与された権利」プロファイルリストに追加されたプロファイルが表示されます。

   - **「付与された権利プロファイル」リストから権利プロファイルを削除するには、リストから権利プロファイル (または複数の権利プロファイル) を選択し、「削除」をクリックします。**

   - **現在のユーザーのすべての権利プロファイルを追加または削除するには、「すべてを追加」または「すべてを削除」ボタンをクリックします。**

4. **「OK」をクリックして設定を保存します。**
「ユーザーマネージャー」メインダイアログボックスで「適用」または「OK」をクリックするまで、変更は適用されません。

ユーザーマネージャー GUI を使用した承認の割り当て

ユーザーは一般に権利プロファイルを通じて、間接的に承認が付与されます。承認設定を使用すると、ユーザーまたは役割に特定の承認を付与できます。 承認によって

は、オブジェクト名などの追加の属性があるものがあります。たとえば、管理者がグループ games を作成すると、管理者には暗黙的な承認 solaris.group.manage/games が付与されます。オブジェクト名が「付与された承認」リストに表示されます。

▼ ユーザーマネージャー GUI を使用した承認の割り当て方法

1. **ユーザーマネージャー GUI を起動します。**
   52 ページの「ユーザーマネージャー GUI を起動する方法」を参照してください。

2. **「ユーザーマネージャー」メインダイアログボックスでユーザーを選択し、「詳細設定」ボタンをクリックします。**
   「詳細設定」ダイアログボックスが表示されます。

3. **ダイアログボックスの左側の「承認」属性をクリックします。**
   使用可能な承認のリストおよび現在のユーザーに付与されている承認のリストが表示されます。

   - **承認 (または複数の承認) をユーザーに割り当てるには、「使用可能な承認」リストから承認 (または複数の承認) を選択し、「追加」をクリックします。**
     追加された承認が「付与された承認」リストに表示されます。

   - **「付与された承認」リストから承認を削除するには、リストから承認 (または複数の承認) を選択し、「削除」をクリックします。**

   - **現在のユーザーのすべての承認を追加または削除するには、「すべてを追加」または「すべてを削除」ボタンをクリックします。**

4. **「OK」をクリックして設定を保存します。**
   「ユーザーマネージャー」メインダイアログボックスで「適用」または「OK」をクリックするまで、変更は適用されません。

索引

た

な

は