Oracle® Solaris 11.1 のユーザーアカウントとユーザー環境の管理

Part No: E36539–02
2012 年 11 月

ORACLE®

121210@25097

目次

はじめに

『Oracle Solaris 11.1 のユーザーアカウントとユーザー環境の管理』は、Oracle Solaris システム管理に関する重要な情報を提供するドキュメントセットの一部です。このガイドには、SPARC および x86 の両方のシステムに関する情報が含まれています。

本書は、読者が次のタスクを終了済みであることを前提としています。

- Oracle Solaris ソフトウェアのインストールが完了していること
- 使用する予定のすべてのネットワークソフトウェアを設定済み

システム管理者にとって重要と思われる Oracle Solaris の新機能については、各章の初めにある新機能に関するセクションを参照してください。

注 – この Oracle Solaris のリリースでは、SPARC および x86 系列のプロセッサアーキテクチャーをサポートしています。サポートされるシステムは、Oracle Solaris OS: Hardware Compatibility Lists に記載されています。このドキュメントでは、プラットフォームにより実装が異なる場合は、それを特記します。

サポートされるシステムについては、Oracle Solaris OS: Hardware Compatibility Lists を参照してください。

対象読者

このマニュアルは、Oracle Solaris リリースを実行している 1 つまたは複数のシステムの管理を行うユーザーを対象にしています。本書を使用するには、UNIX のシステム管理について 1 - 2 年の経験が必要です。UNIX システム管理のトレーニングコースに参加することも役に立ちます。

Oracle サポートへのアクセス

Oracle のお客様は、My Oracle Support を通じて電子的なサポートを利用することができます。詳細は、http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info を参照してください。聴覚に障害をお持ちの場合は、http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs を参照してください。

表記上の規則

次の表では、このドキュメントで使用される表記上の規則について説明します。

表 P–1　表記上の規則

字体	説明	例
AaBbCc123	コマンド名、ファイル名、ディレクトリ名、画面上のコンピュータ出力、コード例を示します。	.login ファイルを編集します。 ls -a を使用してすべてのファイルを表示します。 machine_name% you have mail.
AaBbCc123	ユーザーが入力する文字を、画面上のコンピュータ出力と区別して示します。	machine_name% **su** Password:
aabbcc123	プレースホルダ: 実際に使用する特定の名前または値で置き換えます。	ファイルを削除するには、 rm *filename* と入力します。
AaBbCc123	書名、新しい単語、および強調する単語を示します。	『ユーザーズガイド』の第 6 章を参照してください。 キャッシュは、ローカルに格納されるコピーです。 ファイルを保存しないでください。 注: いくつかの強調された項目は、オンラインでは太字で表示されます。

コマンド例のシェルプロンプト

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 P–2　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#`

◆ ◆ ◆ 第 1 章

1 ユーザーアカウントとユーザー環境の管理 (概要)

この章の内容は次のとおりです。

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 (タスク)」 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 (タスク)」 を参照してください。

ユーザーアカウントとユーザー環境の管理の新機能と変更された機能

このリリースでは、次の機能が新しく導入または変更されています。

ユーザーアカウントの管理に影響するセキュリティーの変更

このリリースでは、次の機能が変更されました。

- password コマンドの状態遷移の微調整。この変更により、ロックできるユーザーアカウントとできないユーザーアカウントが明確になります。主な変更点は、LK および NL プロパティーの定義に影響するもので、次のとおりです。

  LK　アカウントがロックされています。passwd -l コマンドが実行されたか、認証の失敗回数が許容される構成済みの最大値に到達したためアカウントが自動的にロックされました。policy.conf(4) および user_attr(4) のマニュアルページを参照してください。

  NL　アカウントが UNIX 以外の認証用に構成されています。passwd -N コマンドが実行されました。このリリース以降、この状態のアカウントは passwd -l コマンドを実行してロックし、passwd -u コマンドを実行してロック解除することができます。

- 条件付きの承認。承認は、グループ、ゾーン、ファイル名などの特定のオブジェクトに適用するために制限することができます。13 ページの「管理エディタ (pfedit)」を参照してください。
- profiles コマンドは、ローカルおよび LDAP スコープの権利プロファイルを管理するように書き換えられました。役割に基づくアクセス制御 (RBAC) ファイルの直接編集はサポートされなくなりました。
- このリリースでは、権利プロファイルにユーザーごとのプラグイン可能認証モジュール (PAM) ポリシー (pam_policy) を設定する機能を使用できます。pam_policy は、pam_conf(4) 書式付きファイルの絶対パス名か、/etc/security/pam_policy ファイルにある pam.conf (4) 書式付きファイルの名前のいずれかである必要があります。pam_user_policy(5) を参照してください。

  権利プロファイルに PAM ポリシーを設定することに加えて、useradd または usermod コマンドを使用して、ユーザーの user_attr エントリに pam_policy を直接設定することもできます。例 2–1 を参照してください。
- ユーザーセキュリティー権利プロファイルが割り当てられたユーザーと役割は、新しいユーザーアカウントを作成できるほか、root 役割にならなくても、自分の権利の一部を他のアカウントに委任できます。

詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』のパート III「役割、権利プロファイル、特権」を参照してください。

ユーザーマネージャー GUI の概要

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) によって、ユーザー、役割、グループを設定し、管理できるようになりました。ユーザーマネージャー GUI は、デスクトップから使用でき、Visual Panels プロジェクトに含まれます。ユーザーマネージャー GUI はこのリリースで Solaris Management Console GUI に置き換わるものです。ユーザーマネージャー GUI を使用して実行できるタスクは、CLI を使用して実行できるタスクと基本的に同じで、たとえば、`useradd` 、`usermod`、`userdel`、`roleadd` 、`rolemod`、`roledel` コマンドなどがあります。

ユーザーマネージャー GUI を使用する方法については、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 (タスク)」 およびオンラインヘルプを参照してください。

管理エディタ (`pfedit`)

このリリースでは、管理エディタ (`pfedit`) を使用して、システムファイルを編集できます。システム管理者によって定義された場合、このエディタの値は `$EDITOR` です。エディタが定義されていない場合、エディタのデフォルトは `vi` コマンドに設定されます。

次のようにエディタを起動します。

```
$ pfedit system-filename
```

`pfedit` コマンドを使用して、システムファイルを編集するには、ユーザーまたはユーザーの役割に、編集している特定のファイルの `solaris.admin.edit/`*system-filename* 承認が必要です。この `auth-sysfilename` を既存の権利プロファイルに割り当てることで、サービス管理機能 (SMF) コマンドと通常のファイル編集の組み合わせが含まれる手順が簡素化されます。たとえば、`solaris.admin.edit/etc/security/audit_warn` 承認が割り当てられている場合、`audit_warn` ファイルを編集できます。

`pfedit` コマンドを使用して、`/etc` ディレクトリにあるほとんどの構成ファイル、そのサブディレクトリ、および GNOME ファイルや Firefox ファイルなどのアプリケーション構成ファイルも編集できます。`pfedit` コマンドは、`/etc/security/policy.conf` ファイルなど、ユーザーにシステムの広範な権限を与えるシステムファイルの編集には使用できません。それらのファイルを編集するには、`root` アクセス権が必要です。`pfedit(1M)` のマニュアルページおよび『Oracle Solaris 11.1 の管理: セキュリティーサービス』の第 3 章「システムアクセスの制御 (タスク)」を参照してください。

/var/user/$USER サブディレクトリ

ユーザーがログインし、pam_unix_cred モジュールによって正常に認証すると、/var/user/$USER ディレクトリがまだ存在しない場合に、明示的に作成されます。このディレクトリを使用して、アプリケーションは、ホストシステム上の特定のユーザーに関連付けられている永続的データを保存できます。/var/user/$USER ディレクトリは、最初の資格情報の確立時と、su、ssh、rlogin、および telnet コマンドを使用したユーザーの変更時のセカンダリ認証時に作成されます。/var/user/$USER ディレクトリは管理を必要としません。ただし、ユーザーはディレクトリの作成方法、その機能、および /var ディレクトリで表示できることを知っておくべきです。

groupadd コマンドの変更

solaris.group.manage 承認を持つ管理者はグループを作成できます。グループの作成時に、solaris.group.assign /*groupname* が管理者に割り当てられ、これにより管理者は、そのグループを完全に制御できます。管理者は必要に応じてそのグループを変更または削除できます。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。

失敗したログイン回数の通知

システムは、ユーザーアカウントが失敗したログインを強制するように構成されていない場合でも、失敗した認証の試みをユーザーに通知するようになりました。正しい認証に失敗したユーザーには、認証の成功時に、次のようなメッセージが表示されます。

```
Warning: 2 failed authentication attempts since last successful
authentication. The latest at Thu May 24 12:02 2012.
```

それらの通知を抑止するには、/.hushlogin ファイルを作成します。

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。

- 15 ページの「ユーザーアカウントのコンポーネント」
- 22 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」

基本的なシステム管理タスクの 1 つに、サイトの各ユーザーにユーザーアカウントを設定することがあります。通常のユーザーアカウントには、ユーザーがシステムの root パスワードを知らなくても、システムにログインして、システムを使用するのに必要な情報が含まれています。ユーザーアカウントのコンポーネントについては、15 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。topsecret プロジェクトに携わるユーザーを含む topsecret という名前のグループを設定します。また、topsecret ファイルの読み取り権を topsecret グループに対して設定します。こうすれば、topsecret グループ内のユーザーだけが、ファイルを読み取ることができます。

役割という特別な種類のユーザーアカウントは、指定したユーザーに特別な特権を与えます。詳細は、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「役割に基づくアクセス制御 (概要)」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

次のセクションでは、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、ユーザー名 (ログイン名とも呼ばれる) を使って、適切なアクセス権を持つ自分のシステムとリモートシステムにアクセスできます。作成するユーザーアカウントそれぞれに、ユーザー名を選択しなければなりません。

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、Ziggy Ignatz は zignatz 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、Ziggy Top Ignatz は ztignatz 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、ラストネームの最初の 5 文字を使用します
- 固有の名前になるまで 1、2、3 などの数字を使用します

注 – それぞれの新しいユーザー名は、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 (エイリアス) 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、22 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

ユーザー名に関連するものとして、ユーザー識別 (UID) 番号があります。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識別したりします。多数の異なるシステム上で、ある個人用にユーザーアカウントを作成する場合は、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 1–1　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`	信頼できないユーザー

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。システム上の定義により、`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。また、UID が

passwd ファイルの先頭にくるように、uucp ログインや、who、tty、ttytype などの擬似ユーザーログインには低い UID を指定するようにしてください。

UID の設定方法の詳しいガイドラインについては、22 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。 どうしても UID を再利用する必要がある場合、はじめから作りなおして、新しいユーザーが前のユーザーの属性に影響されないようにしてください。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たためプリンタにアクセスできなかった場合、ただし、その属性を新しいユーザーに適用することが正しいとは限りません。

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 1–2　大きな UID および GID の制限のサマリー

UID または GID の値	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。そして、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 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。そして、UID と GID はアーカイブにおいて 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です。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。
- 補足グループ – ユーザーがさらに所属する 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、22 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 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が、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` コマンドを使用すると、ユーザーが所属しているグループのリストを表示できます。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、`newgrp` コマンドを使用して、ユーザーがメンバーとなっているほかのグループに一時的にプライマリグループを変更することはできます。

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、デフォルトの `staff` グループ (グループ 10) を使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。ユーザー名は、プライマリグループに追加されません。ユーザー名がプライマリグループに追加されると、リストが長くなりすぎるからです。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。

- パスワード長は少なくとも /etc/passwd ファイル内の PASSLENGTH 変数に指定された値に一致している必要があります。デフォルトで、この値は 6 に設定されます。

  このリリースでは、デフォルトのパスワードハッシュアルゴリズムが、SHA256 に変更されています。その結果、以前の Oracle Solaris リリースにあった、ユーザーパスワードの 8 文字制限は存在しなくなりました。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。

  パスワードの最大文字数は、古いパスワード用の crypt_unix アルゴリズムと他のすべてのパスワード用の SHA256 のいずれかのアルゴリズムによって異なります。パスワードの変更が既存のパスワードからで、crypt_unix パスワードである場合、policy.conf ファイルでパスワードアルゴリズムの変更を必要としない限り、最大長は 8 に設定されます。

  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。
- パスワード履歴チェックをサポートするネームサービスのユーザーアカウントでは、前のパスワード履歴が定義されている場合、新しいパスワードが前のパスワード履歴に含まれていない必要があります。

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必要があります。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大きさは、ユーザーが作成するファイルの種類、サイズ、および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。ユーザーごとに独立したファイルシステムを使用します。たとえば、/export/home/alice や /export/home/bob などです。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オートマウントの詳細については、『Oracle Solaris 11.1 でのネットワークファイルシステムの管理』の「autofs 管理タスクの概要」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 という環境変数の値によって参照するようにしてください。前者はマシンに固有の指定です。さらに、ユーザーのホームディレクトリで作成されるシンボリックリンクはすべて相対パス (たとえば ../../../x/y/x) を使用する必要があります。こうすることによって、そのリンクはどのシステムにホームディレクトリがマウントされても有効になります。

CLI 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については、47 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コピーしなくても、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。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 – システム初期設定ファイル (/etc/profile または /etc/.login) 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については、31 ページの「ユーザーの作業環境のカスタマイズ」を参照してください。

RBAC を利用してユーザーアカウントをカスタマイズする方法については、『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「役割に基づくアクセス制御 (概要)」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、複数のドメインにまたがることもあるユーザーの組織内で一意でなければなりません。

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する必要があります。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 – 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てはいけません。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 のエントリの全リストについては、表 1–3 と表 1–4 を参照してください。

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の構成 – デフォルトのシステムアカウントの構成は絶対に変更しないでください。この設定には、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が含まれています。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 – 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した。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 – 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 3 種類の呼び方ではなく、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。

NIS および files の場合、グループ情報は 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、ポートの監視など) を実行するプロセスのことです。

```
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:/:
listen:x:37:4:Network Admin:/usr/net/nls:
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:/:
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:/:
```

表 1–3 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
root	0	スーパーユーザーアカウント用に予約済み
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
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
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
adm	4	システムのログの記録に関連する管理デーモン
lp	71	ラインプリンタデーモン用に予約済み
uucp	5	uucp 関数に関連するデーモンに割り当てられる
nuucp	9	uucp 関数に関連する別のデーモンに割り当てられる
dladm	15	データリンク管理用に予約済み
netadm	16	ネットワーク管理用に予約済み
netcfg	17	ネットワーク構成管理用に予約済み
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
listen	37	ネットワークリスナーデーモンに割り当てられる
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
zfssnap	51	自動スナップショット用に予約済み
upnp	52	UPnP サーバー用に予約済み

表 1–3 デフォルトの passwd ファイルのエントリ (続き)

ユーザー名	ユーザー ID	説明
xvm	60	xVM ユーザー用に予約済み
mysql	70	MySQL ユーザー用に予約済み
openldap	75	OpenLDAP ユーザー用に予約済み
webservd	80	WebServer アクセス用に予約済み
postgres	90	PostgresSQL アクセス用に予約済み
svctag	95	Service Tag Registry アクセス用に予約済み
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
nobody	60001	NFS 匿名アクセスユーザー用に予約済み
noaccess	60002	No Access ユーザー用に予約済み
nobody4	65534	SunOS 4.x NFS 匿名アクセスユーザー用に予約済み
ftp	21	FTP アクセス用に予約済み
dhcpserv	18	DHCP サーバーユーザー用に予約済み
aiuser	60003	AI ユーザー用に予約済み
pkg5srv	97	pkg(5) 集積サーバー用に予約済み

shadow ファイルのフィールド

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。

```
root::0:
other::1:root
bin::2:root,daemon
sys::3:root,bin,adm
adm::4:root,daemon
uucp::5:root
mail::6:root
tty::7:root,adm
lp::8:root,adm
nuucp::9:root
staff::10:
daemon::12:root
sysadmin::14:
games::20:
smmsp::25:
gdm::50:
upnp::52:
xvm::60:
netadm::65:
mysql::70:
openldap::75:
webservd::80:
postgres::90:
slocate::95:
unknown::96:
nobody::60001:
noaccess::60002:
nogroup::65534:
ftp::21
pkg5srv::97:
```

表 1–4 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
root	0	スーパーユーザーのグループ
other	1	オプションのグループ
bin	2	システムバイナリの実行に関連する管理グループ
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
adm	4	システムのログの記録に関連する管理グループ
uucp	5	uucp 関数に関連するグループ
mail	6	電子メールのグループ
tty	7	tty デバイスに関連するグループ
lp	8	ラインプリンタのグループ
nuucp	9	uucp 関数に関連するグループ
staff	10	一般的な管理グループ
daemon	12	ルーチンシステムタスクに関連するグループ
sysadmin	14	システム管理者にとって有用な管理グループ
smmsp	25	Sendmail メッセージ送信プログラム用のデーモン
gdm	50	GNOME ディスプレイマネージャーデーモン用に予約されたグループ
upnp	52	UPnP サーバー用に予約されたグループ
xvm	60	xVM ユーザー用に予約されたグループ
netadm	65	ネットワーク管理用に予約されたグループ
mysql	70	MySQL ユーザー用に予約されたグループ
openldap	75	OpenLDAP ユーザー用に予約済み
webservd	80	WebServer アクセス用に予約されたグループ
postgres	90	PostgresSQL アクセス用に予約されたグループ
slocate	95	Secure Locate アクセス用に予約されたグループ
unknown	96	NFSv4 ACL のマップ不能なリモートグループ用に予約されたグループ
nobody	60001	匿名の NFS アクセス用に割り当てられたグループ

表 1–4 デフォルトの group ファイルのエントリ (続き)

グループ名	グループ ID	説明
noaccess	60002	あるアプリケーションを経由するが実際にログインをせずに、システムにアクセスする必要があるユーザーまたはプロセスに割り当てられるグループ
nogroup	65534	既知のグループのメンバーでないユーザーに割り当てられるグループ
ftp	21	FTP アクセス用に割り当てられるグループ
pkg5srv	97	pkg(5) 集積サーバーに割り当てられるグループ

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 1–5 ユーザーに関する情報を取得するために使用するコマンド

コマンド	説明	マニュアルページ
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取得します。 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)

表 1–5 ユーザーに関する情報を取得するために使用するコマンド (続き)

コマンド	説明	マニュアルページ
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)
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) に定義されています。 注 – このコマンドは Oracle Solaris 11 の新しいコマンドです。	Example 2–1

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 – Solaris Management Console GUI およびこの GUI に関連付けられた CLI はサポートされなくなりました。

ユーザー、役割、およびグループの管理には、次のコマンドを使用できます。

表 1–6 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	補足情報
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。	48 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。	50 ページの「ユーザーを変更する方法」 『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「ユーザーのセキュリティー属性を変更する方法」
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。	51 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 11.1 の管理: セキュリティーサービス』の「役割を作成する方法」 『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「RBAC の初期構成 (タスクマップ)」
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。	52 ページの「グループを追加する方法」

ユーザーの作業環境のカスタマイズ

このセクションでは次の情報について説明します。

- 32 ページの「サイト初期設定ファイルの使用方法」
- 33 ページの「ローカルシステムへの参照を避ける」
- 33 ページの「シェル機能」
- 35 ページの「bash および ksh93 シェルの履歴」
- 35 ページの「bash および ksh93 のシェル環境変数」
- 38 ページの「Bash シェルのカスタマイズ」
- 38 ページの「MANPATH 環境変数」
- 39 ページの「PATH 環境変数」
- 39 ページの「ロケール変数」
- 40 ページの「デフォルトのファイルアクセス権 (umask)」
- 41 ページの「ユーザー初期設定ファイルのカスタマイズ」

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 1–7　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変更して、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。

異なるタイプのユーザーにユーザー初期設定ファイルを作成する手順については、45 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、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するよう設計されています。

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必要があるからです。

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、次のシェル機能と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表示するにはいくつかの方法があります。
  - 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 1–8 Oracle Solaris リリースでの基本的なシェル機能

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。 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 Oracle Solaris リリースのデフォルトシェルです。
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 – 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。

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参照するには、次のように入力します。

```
$ 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 ksh93 のシェル環境変数

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一覧を表示するには、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 – 環境変数は複数のセッション間で持続しません。複数のログインにまたがって一貫性を保つ環境変数を設定するには、.bashrc ファイルで変更を行う必要があります。

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。

次の表に、Oracle Solaris リリースで使用可能なシェルと環境変数の詳細を示します。

表 1–9 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 rje 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/rje 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 – Oracle Solaris 11 から、MANPATH 環境変数は必要なくなりました。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。 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いて、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。

表 1–9 シェル変数と環境変数の説明 (続き)

変数	説明
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、システム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	端末を設定します。この変数は /etc/profile または /etc/.login ファイルで再設定する必要があります。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場合は、ホームディレクトリにある .bashrc ファイルに必要な情報を追加します。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。詳細については、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

ユーザーが絶対パス名でコマンドを入力すると、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。

パスの設定のガイドライン

次に、効率的な PATH 変数を設定するためのガイドラインをいくつか示します。

- 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ときに「ハング」の可能性が小さくなるように、NFS がマウントするディレクトリより前にローカルディレクトリを指定します。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 変数を使用します。
LC_COLLATE、LC_CTYPE、LC_MESSAGES、LC_NUMERIC、LC_MONETARY、および LC_TIME です。

注 – 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 1–10 LANG と LC 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 1–1 LANG 変数によるロケールの設定

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

LANG-de_DE.UTF-8; 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したときに設定され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。

また、次の表から umask 値を決めることもできます。この表は、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 1–11　umask 値のアクセス権

umask 8 進値	ファイルのアクセス権	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

次に示すのは、.profile ユーザー初期設定ファイルの例です。このファイルを使用して、自分自身のユーザー初期設定ファイルをカスタマイズすることができます。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 1–2 .profile ファイル

(Line 1) `PATH=$PATH:$HOME/bin:/usr/local/bin:/usr/gnu/bin:.`
(Line 2) `MAIL=/var/mail/$LOGNAME`
(Line 3) `NNTPSERVER=server1`
(Line 4) `MANPATH=/usr/share/man:/usr/local/man`
(Line 5) `PRINTER=printer1`
(Line 6) `umask 022`
(Line 7) `export PATH MAIL NNTPSERVER MANPATH PRINTER`

1. ユーザーのシェル検索パスを設定する
2. ユーザーのメールファイルへの検索パスを設定する
3. ユーザーの時間/クロックサーバーを設定する
4. マニュアルページへのユーザーの検索パスを設定する
5. ユーザーのデフォルトプリンタを設定する
6. ユーザーのデフォルトのファイル作成アクセス権を設定する
7. 指定された環境変数をエクスポートする

◆ ◆ ◆ 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 (タスク)

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の管理 (概要)」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 (タスク)」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

次のタスクでは、CLI を使用して、ユーザーアカウントを設定し、管理する方法について説明します。

CLI を使用したユーザーアカウントの設定と管理 (タスクマップ)

タスク	説明	参照先
ユーザー情報を収集します。	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。	45 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できます。	45 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」

タスク	説明	参照先
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。	46 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。	48 ページの「ユーザーを追加する方法」
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。	50 ページの「ユーザーを変更する方法」
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。	51 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 11.1 の管理: セキュリティーサービス』の「役割を作成する方法」 『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「役割を割り当てる方法」
グループを作成します。	groupadd コマンドを使用して、新しいグループを作成します。	52 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 11.1 の管理: セキュリティーサービス』の「ユーザーのセキュリティー属性を変更する方法」
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。	53 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。	54 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」

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することができます。

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:	

▼ ユーザー初期設定ファイルをカスタマイズする方法

1 **root** 役割またはユーザーマネージャー権利プロファイルを持つ役割になります。

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

『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」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 各ユーザータイプ用にユーザー初期設定ファイルを編集し、必要に応じてカスタマイズします。

ユーザー初期設定ファイルをカスタマイズする方法については、31 ページの「ユーザーの作業環境のカスタマイズ」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 **root** 役割またはユーザーマネージャー権利プロファイルを持つ役割になります。

『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」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。

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 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」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、コマンド構文に、-m オプションを指定する必要があります。そうしないと、ユーザーのホームディレクトリが作成されません。

  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 – このルールの唯一の例外は、pam_zfs_key モジュールでユーザーの暗号化ホームディレクトリを作成する場合です。この場合、useradd コマンドで -m オプションを指定しません。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、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
  ```

  ただし、-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。

▼ ユーザーを追加する方法

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。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。

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、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。

1 **root** 役割またはユーザーマネージャー権利プロファイルを持つ役割になります。

『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」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。

次のように `-d` *dir* オプションを指定した場合、`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
```

次のように、`-d` *dir* オプションを指定した場合、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
```

注 – `pam_zfs_key` モジュールでユーザーの暗号化ホームディレクトリを作成する場合。この場合、`useradd` コマンドで `-m` オプションを指定しません。47 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。

`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 – 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:       Type user password
Re-enter new password:       Retype password
```

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、ユーザーへの役割の追加と割り当て、ユーザーの権利プロファイルの表示と変更、ユーザーの RBAC プロパティーの変更などの追加のタスクを実行する必要がある場合があります。詳細は、次のマニュアルページを参照してください。

- 『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「役割を作成する方法」および『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「役割を割り当てる方法」
- 『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「定義済みのすべてのセキュリティー属性を表示する方法」
- 『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「権利プロファイルを作成する方法」
- 『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「ユーザーのセキュリティー属性を変更する方法」

▼ ユーザーを変更する方法

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 **root** 役割またはユーザーマネージャー権利プロファイルを持つ役割になります。

『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」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については、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 2–1 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。詳細については、pam_user_policy(5) を参照してください。

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

参照　ユーザーの変更の追加の例については、次のリファレンスを参照してください。

- 『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「役割を割り当てる方法」
- 『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「ユーザーのセキュリティー属性を変更する方法」

▼ ユーザーを削除する方法

1. **root** 役割になります。

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

注 – 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. 次のいずれかのコマンドを実行します。
   - ユーザーのローカルホームディレクトリがある場合、ユーザーとホームディレクトリを削除します。

     # userdel -r *username*

     usesrdel　指定されたユーザーのアカウントを削除します。

     -r　システムからアカウントを削除します。

     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。

   - 指定しない場合、ユーザーのみを削除します。

     # userdel *username*

     リモートサーバー上にあるユーザーのホームディレクトリは手動で削除する必要があります。

   すべてのコマンドオプションの一覧は、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. **root** 役割または **solaris.group.manage** 承認を持つ管理者になります。

   『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」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 18 exadata
   ```

   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 2–2　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 ファイルシステムとして作成されたホームディレクトリを共有する方法

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して、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。次の手順で、これらの手順について説明します。

ファイルシステムの共有および共有解除の詳細については、『Oracle Solaris 11.1 の管理: ZFS ファイルシステム』の「ZFS ファイルシステムを共有および共有解除する」を参照してください。

1 **root** 役割になります。

『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」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。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。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 11.1 でのネットワークファイルシステムの管理』の「autofs 管理タスクの概要」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/alice
```

注 – 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、53 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

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 (タスク)

この章では、Oracle Solaris ユーザーマネージャー GUI を使用して、ユーザーを設定し、管理するため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 CLI (`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。ユーザーマネージャー GUI の詳細については、オンラインヘルプを参照してください。

この章の内容は次のとおりです。

- 55 ページの「ユーザーマネージャー GUI の概要」
- 59 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」
- 62 ページの「ユーザーマネージャー GUI による詳細設定の管理」

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の管理 (概要)」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 (タスク)」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情報について説明します。

- 56 ページの「ユーザーマネージャー GUI の起動」
- 57 ページの「ユーザーマネージャーパネルの構成」
- 58 ページの「デフォルトのネームサービスのスコープとタイプの選択」
- 59 ページの「役割の引き受けまたはユーザー資格情報の変更」

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。ユーザーと役割のリモート管理は、リモート管理デーモン (RAD) によって可能になります。GUI はそのすべての操作を実

行するために、User/Role Manager RAD モジュールに依存しています。RAD モジュールは、GUI のすべての管理機能を実行する役割ベースのアクセス制御 (RBAC) CLI を呼び出して機能します。

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パネル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。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。GUI で実行できるタスクは、CLI を使用して実行できるタスクと同じで、たとえば、`useradd`、`usermod`、`userdel`、 `roleadd`、`groupadd` などです。CLI を使用したユーザーと役割の管理については、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 (タスク)」を参照してください。

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 の起動

▼ ユーザーマネージャー GUI を起動する方法

1. **root** 役割になるか、ユーザー管理権利プロファイルが割り当てられているユーザーとしてログインします。

   『Oracle Solaris 11.1 の管理: セキュリティーサービス』の「割り当てられている管理権限を使用する方法」を参照してください。

2. 次のいずれかの方法を選択してユーザーマネージャー GUI を起動します。

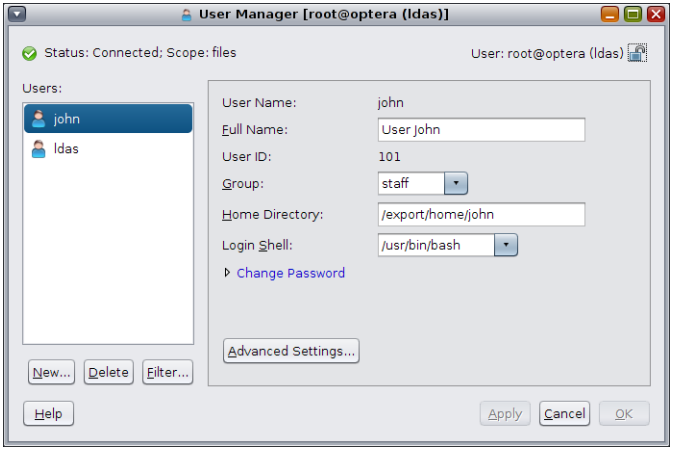
   - 「システム」→「管理」→「ユーザーマネージャー」を選択して、デスクトップからユーザーマネージャー GUI を起動します。
   - 次のようにして、コマンド行からユーザーマネージャー GUI を起動します。

     ```
     # vp usermgr &
     ```

ユーザーマネージャーパネルの構成

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のメインパネルが表示されます。ユーザーマネージャーパネルは、ユーザーと役割を管理するために使用します。パネルの左側は「ステータス」フィールドで、ローカルホストで現在実行しているサービスのステータスが表示されます。パネルの右側には、「ユーザー」フィールドがあります。「ユーザー」フィールドには、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。資格情報を変更するには、パネルの右端にある「ロック」ボタンをクリックします。59 ページの「役割の引き受けまたはユーザー資格情報の変更」を参照してください。

次の図では、ユーザーマネージャーのメインパネルが表示されています。



ユーザーマネージャーパネル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が含まれます
- 基本設定 – ユーザー名や氏名などのユーザーの基本設定を表示します

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パネルの右側に表示されます。

ユーザーマネージャーパネル内から、次のアクションが可能です。

- 新しいユーザーまたは役割を作成する。60 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を削除する。62 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の削除」を参照してください

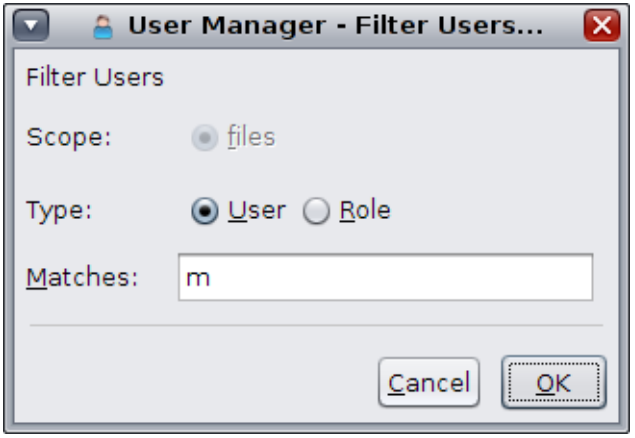
- ユーザーの情報をフィルタする。58 ページの「デフォルトのネームサービスのスコープとタイプの選択」を参照してください。
- 既存のユーザーの詳細設定を管理する。61 ページの「ユーザーマネージャー GUI によるユーザーまたは役割を変更する方法」を参照してください。

デフォルトのネームサービスのスコープとタイプの選択

ユーザーマネージャー GUI のデフォルトのネームサービスのスコープとタイプは `files` と `User` です。`ldap` や `roles` などの別のスコープ内でユーザーマネージャー GUI を管理するには、「フィルタ」ボタンをクリックします。「フィルタ」ボタンをクリックすると、デフォルトのスコープ、タイプ、またはその両方を変更できるダイアログボックスが起動します。

- 「スコープ」オプションの選択肢は `files` と `ldap` です。
- 「タイプ」オプションの選択肢は `User` と `Role` です。「了解」をクリックして変更を保存します。

操作を取り消すには「キャンセル」をクリックします。



注 – システムが `ldap` クライアントとして構成されていない場合、`files` スコープのみが使用できます。

役割の引き受けまたはユーザー資格情報の変更

ユーザー管理権利プロファイルのあるユーザーは、作成するユーザーまたは役割の高度な属性が、管理を実行するユーザーの高度な属性のサブセットである場合に限り、新しいユーザーを作成できます。管理を実行するユーザーに十分な承認がないが、十分な承認を持つ管理役割がある場合は、その役割を引き受けて、ユーザーマネージャーメインパネルの「ロック」ボタンをクリックして、必要な管理を実行することができます。

▼ ユーザーの資格情報を変更する方法

1. ユーザーマネージャー **GUI** を起動します。
   56 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パネルで、「ロック」アイコンをクリックすると、次のオプションを含むサブメニューが開きます。
   - 役割の変更
   - ユーザーの変更
   - 新しいホストの管理
   - 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、指定されたユーザーに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て、「ログイン」をクリックして役割を変更します。
   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、削除は、それぞれ `useradd`、`usermod`、`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詳細については、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 (タスク)」を参照してください。

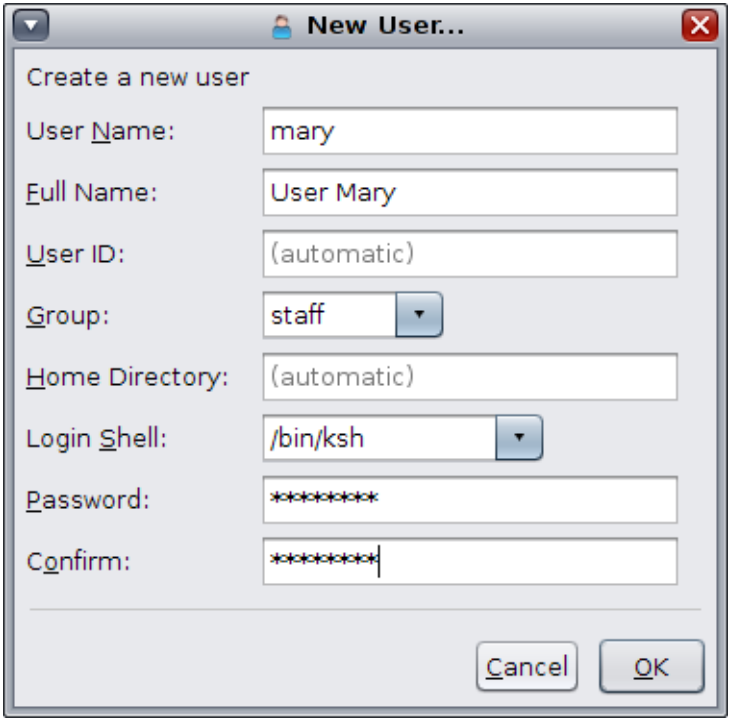
このセクションでは次の情報について説明します。

- 60 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」
- 61 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」
- 62 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の削除」

▼ 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

1 ユーザーマネージャー GUI を起動します。
56 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 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するには、ユーザーマネージャーメインパネルの「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 「新規ユーザー」ダイアログ・ボックスで、次のフィールドに入力します。

- ユーザー名
- 氏名
- ユーザー ID

  このフィールドはオプションです。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」フィールドの使用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

  このフィールドはオプションです。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` などです。
- ログインシェル

  「ログインシェル」フィールドのオプションは、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。

注 – オプションのフィールドを除くすべてのフィールドに入力する必要があります。

---

4 新しいユーザーまたは役割を作成し、ユーザーマネージャーメインパネルに表示されるユーザーのリストにユーザーまたは役割を追加するには、「**OK**」をクリックします。

操作を取り消すには、「キャンセル」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。

56 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 既存のユーザーまたは役割を変更するには、ユーザーマネージャーメインパネルで、表示された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、パネルの右側に、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 – フィールドを変更すると、変更されたフィールドの横に、インジケーターが表示されます。

---

4 「適用」をクリックして変更を保存します。

5 (省略可能) 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。62 ページの「ユーザーマネージャー GUI による詳細設定の管理」を参照してください。

6 「OK」をクリックして変更を保存し、ユーザーマネージャーパネルを閉じます。
保存していない変更を破棄するには「キャンセル」をクリックしてパネルを閉じます。

ユーザーマネージャー GUI によるユーザーまたは役割の削除

現在ユーザーマネージャー GUI によって使用されているフィルタのスコープ内のユーザーや役割を削除するには、ユーザーマネージャーメインパネルでユーザーまたは役割を選択し、「削除」ボタンをクリックします。変更を保存するには、確認ダイアログボックスが表示されたら、「OK」をクリックします。操作を取り消すには、「キャンセル」をクリックします。

ユーザーマネージャー GUI による詳細設定の管理

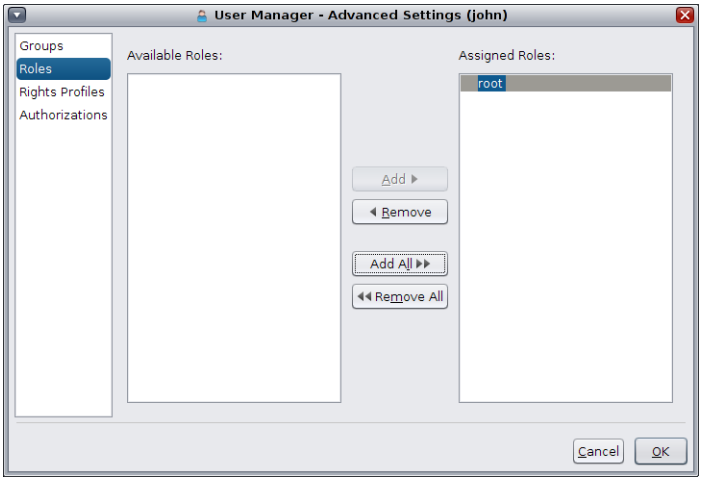
このセクションでは次の情報について説明します。

ユーザーマネージャー GUI 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。

Oracle Solaris でサポートされているセキュリティー機能の概要については、『Oracle Solaris 11.1 の管理: セキュリティーサービス』のパート I「セキュリティーの概要」を参照してください。このリリースでの役割ベースのアクセス制御 (RBAC) のしくみの詳細な説明については、『Oracle Solaris 11.1 の管理: セキュリティーサービス』のパート III「役割、権利プロファイル、特権」を参照してください。

ユーザーまたは役割の詳細属性を管理するには、ユーザーマネージャーメインパネルでユーザーまたは役割を選択し、「詳細設定」ボタンをクリックします。現在のユーザーまたは役割の「詳細設定」パネルが表示されます。現在のユーザーの名前は、パネルのいちばん上にかっこ内に表示されます。

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」パネルを示しています。



「詳細設定」パネルで次のセキュリティー属性を管理できます。

- 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 によるグループの管理

グループは、「詳細設定」ボタンをクリックして、ユーザーマネージャー GUI のユーザーマネージャーメインダイアログボックスで管理します。

▼ グループを管理する方法

1. ユーザーマネージャー **GUI** を起動します。
   56 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パネル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」パネルが表示されます。

3. パネルの左側の「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。

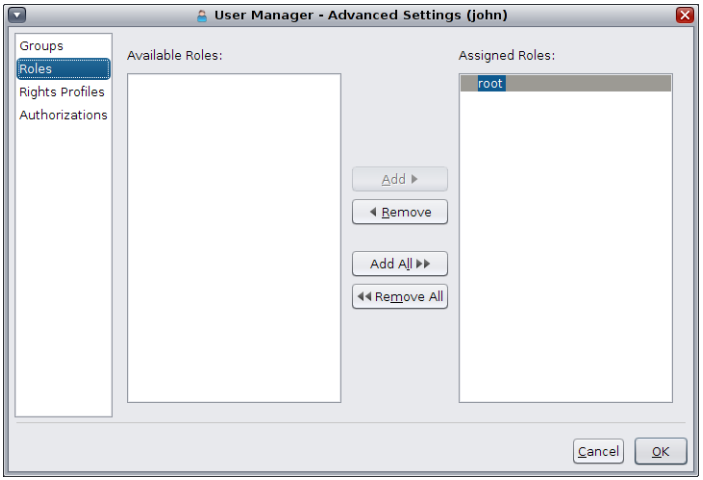
4. 「**OK**」をクリックして設定を保存します。
   ユーザーマネージャーメインパネルで「適用」または「OK」をクリックするまで、変更は適用されません。

ユーザーマネージャー **GUI** による役割の管理

役割は、ユーザーマネージャー GUI のユーザーマネージャーメインダイアログボックスで「詳細設定」ボタンをクリックして、管理します。

注 – 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」パネルを示しています。



▼ ユーザーマネージャー GUI による役割の管理方法

1 ユーザーマネージャー GUI を起動します。
56 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パネル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」パネルが表示されます。

3 パネルの左側の「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。

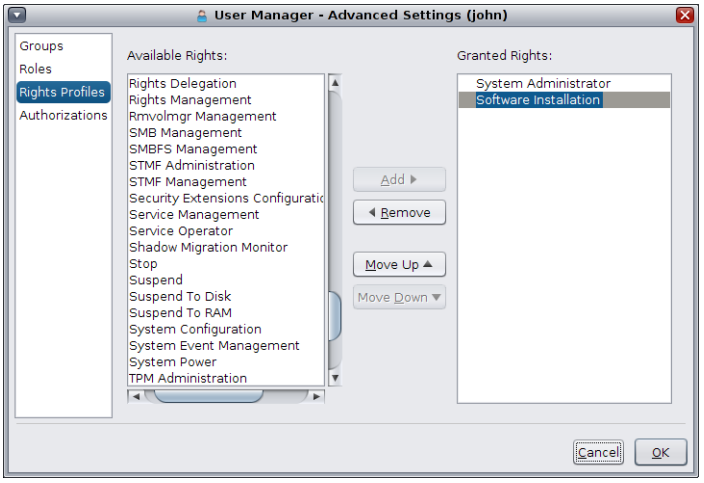
- 役割 (または複数の役割) をユーザーに割り当てるには、「使用可能な役割」リストから役割 (または複数の役割) を選択し、「追加」をクリックします。
  追加した役割が「割り当てられた役割」リストに表示されます。
- 「割り当てられた役割」リストから役割を削除するには、リストから役割 (または複数の役割) を選択し、「削除」をクリックします。
- 現在のユーザーのすべての役割を追加または削除するには、「すべてを追加」または「すべてを削除」ボタンをクリックします。

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パネルで「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 による権利プロファイルの管理

権利プロファイルは、ユーザーマネージャー GUI のユーザーマネージャーメインダイアログボックスで「詳細設定」ボタンをクリックして、管理します。

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」パネルを示しています。



注 – 権利プロファイルの割り当てには、優先順位があります。必要に応じて、「上へ移動」および「下へ移動」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。
56 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パネル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」パネルが表示されます。

3 パネルの左側の「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パネルで「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** による承認の管理

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** による承認の管理方法

1 ユーザーマネージャー **GUI** を起動します。
56 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パネル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」パネルが表示されます。

3 パネルの左側の「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パネルで「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