Trusted Extensions ユーザーズガイド

Part No: E36545–02
2012 年 10 月

ORACLE

121210@25097

目次

図目次

表目次

はじめに

『Trusted Extensions ユーザーズガイド』は、Trusted Extensions 機能が有効になった Oracle Solaris オペレーティングシステム (Oracle Solaris OS) での作業方法を説明するガイドです。

対象読者

このガイドは、Trusted Extensions のすべてのユーザーを対象としています。前提条件として、Oracle Solaris OS およびオープンソースの GNOME デスクトップに精通している必要があります。

同時に、組織のセキュリティーポリシーにも精通している必要があります。

Trusted Extensions ガイドセットの構成

次の表に、Trusted Extensions ガイドで扱うトピックの一覧と、各ガイドの対象読者の一覧を示します。

ガイドのタイトル	トピック	対象読者
『Trusted Extensions ユーザーズガイド』	Trusted Extensions. の基本的な機能について説明しています。このガイドには用語集が含まれています。	エンドユーザー、管理者、開発者
『Trusted Extensions 構成と管理』	パート I では、Trusted Extensions の準備、有効化、および初期構成の方法が説明されています。 パート II では、Trusted Extensions システムの管理方法が説明されています。このガイドには用語集が含まれています。	管理者、開発者
『Trusted Extensions Developer's Guide 』	Trusted Extensions を使ってアプリケーションを開発する方法について説明しています。	開発者、管理者
『Trusted Extensions Label Administration 』	ラベルエンコーディングファイルでのラベルコンポーネントの指定方法について説明します。	管理者

ガイドのタイトル	トピック	対象読者
『Compartmented Mode Workstation Labeling: Encodings Format 』	ラベルエンコーディングファイルで使用される構文について説明します。構文を使用することにより、適格な形式のラベルに関するさまざまな規則がシステムに適用されます。	管理者

このガイドの構成

第 1 章「Trusted Extensions の紹介」では、Trusted Extensions 機能を備えた Oracle Solaris システムに実装されている基本的な概念について説明します。

第 2 章「Trusted Extensions へのログイン (タスク)」では、システムへのアクセス手順と Trusted Extensions システムの終了手順について説明します。

第 3 章「Trusted Extensions での作業 (タスク)」では、Trusted Extensions を使用して作業を行う方法について説明します。

第 4 章「Trusted Extensions の構成要素 (リファレンス)」では、Trusted Extensions 機能を備えたシステムの主な構成要素について説明します。

用語集では、Trusted Extensions で使われるセキュリティー用語について説明します。

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.`

表 P–1 表記上の規則 (続き)

字体	説明	例
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コマンドは、`rm` *filename* です。
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

次の表に、Oracle Solaris OS に含まれるシェルの UNIX システムプロンプトおよびスーパーユーザーのプロンプトを示します。コマンド例のシェルプロンプトは、そのコマンドを標準ユーザーで実行すべきか特権ユーザーで実行すべきかを示します。

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 Trusted Extensions の紹介

この章では、Trusted Extensions 機能によって Oracle Solaris オペレーティングシステム (Oracle Solaris OS) に追加される、ラベルやその他のセキュリティー機能について紹介します。

Trusted Extensions とは

Trusted Extensions は、Oracle Solaris システムに特別なセキュリティー機能を提供します。組織はこれらの機能を利用して、Oracle Solaris システムにラベル付きセキュリティーポリシーを定義し、実装できます。「セキュリティーポリシー」とは、サイト内の情報やコンピュータハードウェアなどのリソースの保護に役立つ、一連の規則と実践です。一般にはセキュリティー規則によって、だれがどの情報にアクセスできるか、またはだれがリムーバブルメディアへのデータ書き込みを許可されているかなどの内容が処理されます。「セキュリティー実践」とは、タスクを実行するために推奨される手順です。

以降の各セクションでは、Trusted Extensions によって提供される主なセキュリティー機能について説明します。どのセキュリティー機能を構成できるかについても説明しています。

Trusted Extensions による侵入者からの防御

Trusted Extensions は、侵入者から防御する機能を Oracle Solaris OS に追加します。Trusted Extensions は、パスワード保護などの Oracle Solaris のいくつかの機能も利用します。Trusted Extensions は、役割のパスワードを変更する GUI を追加します。デフォルトでは、ユーザーは、マイクロフォンやカメラなどの周辺デバイスを使用することを承認される必要があります。

トラステッドコンピューティングベースへのアクセス制限

「トラステッドコンピューティングベース (Trusted Computing Base、TCB)」という用語は、Trusted Extensions の中でセキュリティーに関するイベントを処理する部分を表します。TCB にはソフトウェア、ハードウェア、ファームウェア、ドキュメント、管理手順などが含まれます。セキュリティー関連のファイルにアクセス可能なユーティリティーやアプリケーションプログラムは、いずれも TCB の一部です。管理者は、各ユーザーが TCB と行う可能性のあるすべての対話に制限を設定します。このような対話には、業務の遂行に必要なプログラム、アクセスが許可されているファイル、セキュリティーに影響を与える可能性があるユーティリティーなどがあります。

必須アクセス制御による情報保護

侵入者がシステムへのログインに成功した場合でも、さらに妨害することで情報へのアクセスを防ぎます。ファイルなどのリソースはアクセス制御で保護されます。Oracle Solaris OS の場合と同様に、アクセス制御は情報の所有者が設定できます。Trusted Extensions ではシステムでもアクセスが制御されます。詳細は、17 ページの「Trusted Extensions による任意アクセス制御と必須アクセス制御」を参照してください。

周辺装置の保護

Trusted Extensions では、テープドライブ、CD-ROM ドライブ、USB デバイス、プリンタ、マイクロフォンなどローカルの周辺装置へのアクセスは管理者が制御します。アクセスはユーザーごとに付与できます。周辺装置へのアクセスは次のように制限されます。

- デフォルトでは、各デバイスを使用するには割り当てる必要がある。
- リムーバブルメディアを制御するデバイスへのアクセスには承認が必要。
- リモートユーザーは、マイクロフォンや CD-ROM ドライブなどのローカルデバイスを使用できない。ローカルユーザーのみがデバイスを割り当てることができる。

スプーフィングプログラム (騙しプログラム) の防止

「スプーフィング」とは、なりすましのことです。パスワードなどの機密データを盗むために、侵入者がログインプログラムやそのほかの正規のプログラムをスプーフィングすることがあります。Trusted Extensions では、次のような「トラステッドシンボル」と呼ばれる、ひと目でわかる不正操作防止アイコンを画面上部に表示することによって、悪意のあるスプーフィングプログラムからユーザーを守ります。

図 1–1 トラステッドシンボル

このシンボルは、トラステッドコンピューティングベース (TCB) との対話中は常に表示されます。このシンボルが表示されていれば、セキュリティー関連のトランザクションが確実に安全に実行されていることになります。シンボルが表示されていない場合は、セキュリティーが侵害される可能性があります。図 1–1 はトラステッドシンボルを示しています。

Trusted Extensions による任意アクセス制御と必須アクセス制御

Trusted Extensions では、任意と必須の両方のアクセス制御を提供することによって、どのユーザーがどの情報にアクセスできるかを制御します。

任意アクセス制御

「任意アクセス制御 (Discretionary Access Control、DAC)」は、ファイルとディレクトリに対するユーザーのアクセスを制御するためのソフトウェアメカニズムです。DAC では、ファイルおよびディレクトリに設定する保護の種類を所有者自身が決定できます。DAC には、UNIX アクセス権ビットを使用する方法と、アクセス制御リスト (ACL) を利用する方法があります。

アクセス権ビット方式では、「所有者」、「グループ」、「その他のユーザー」の単位で、読み取り保護、書き込み保護、実行保護を設定できます。従来の UNIX のシステムでは、スーパーユーザー (root ユーザー) が DAC 保護をオーバーライドできます。Trusted Extensions では、DAC をオーバーライドできるのは、管理者と承認さ

れたユーザーのみです。ACL では、アクセス制御をさらに細かく設定できます。所有者は ACL を使用することにより、特定のユーザーやグループに対して別個のアクセス権を指定できます。詳細は、『Oracle Solaris 11.1 の管理: ZFS ファイルシステム』の第 7 章「ACL および属性を使用した Oracle Solaris ZFS ファイルの保護」を参照してください。

必須アクセス制御

「必須アクセス制御 (Mandatory Access Control、MAC)」は、ラベル関係に基づいた、システムによって実施されるアクセス制御メカニズムです。システムにより、プログラムを実行するために作成されたすべてのプロセスに機密ラベルが対応付けられます。このラベルが、MAC ポリシーでのアクセス制御の決定に使用されます。通常、各プロセスでは、相手側のラベルが自身のラベルと同等でないかぎり、情報を格納することも、ほかのプロセスと通信することもできません。MAC ポリシーでは、ラベルが同等または自身よりも低いオブジェクトからのデータ読み取りが、プロセスに対して許可されます。ただし、管理者は、レベルの低いオブジェクトがほとんどまたはまったく存在しないような、ラベル付き環境を作成することもできます。

デフォルトでは、MAC ポリシーはユーザーには表示されません。通常のユーザーは、オブジェクトに対する MAC アクセスを持っていないかぎり、そのオブジェクトを表示できません。あらゆる場合において、ユーザーが MAC ポリシーに反する行為を行うことはできません。

機密ラベルと認可上限

ラベルには、次の 2 つのコンポーネントがあります。

- 格付け (「レベル」とも呼ばれる)

  セキュリティーの階層レベルを示すコンポーネントです。人に適用した場合、格付けは信用の程度を表します。データに適用した場合、格付けは必要な保護の度合いを表します。

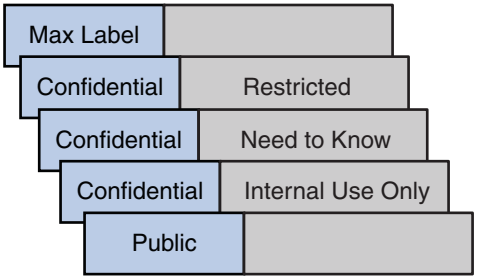
  米国政府で使用されている格付けは、`TOP SECRET`、 `SECRET`、`CONFIDENTIAL`、および `UNCLASSIFIED` です。産業界の格付けには、標準化されたものはありません。個々の企業が独自の格付けを設定できます。例については、図 1–2 を参照してください。左側の項目が格付けです。右側の項目がコンパートメントです。

- コンパートメント (「カテゴリ」とも呼ばれる)

  コンパートメントは、作業グループ、部門、プロジェクト、トピックなどのグループ化を表します。格付けに必ずしもコンパートメントがあるとはかぎりません。図 1–2 では、`Confidential` という格付けに 3 つの排他的なコンパートメントがあります。`Public` と `Max Label` にはコンパートメントがありません。図が示すように、この組織では 5 つのラベルが定義されています。

Trusted Extensions には 2 種類のラベルがあります。「機密ラベル」と「認可上限」です。作業の認可は 1 つ以上の機密ラベルで得ることができます。「ユーザー認可上限」と呼ばれる特殊なラベルは、そのユーザーが作業することを許されている最高ラベルを決定します。さらに、各ユーザーには最下位の機密ラベルが指定されています。 このラベルは、マルチレベルのデスクトップセッションにログインするときにデフォルトで使用されます。ログイン後は、この範囲内のほかのラベルで作業することを選択できます。最下位の機密ラベルとして `Public` を、認可上限として `Confidential: Need to Know` をユーザーに割り当てたとします。最初のログインでは、デスクトップのワークスペースのラベルは `Public` です。セッション中、ユーザーは `Confidential: Internal Use Only` および `Confidential: Need to Know` でワークスペースを作成できます。

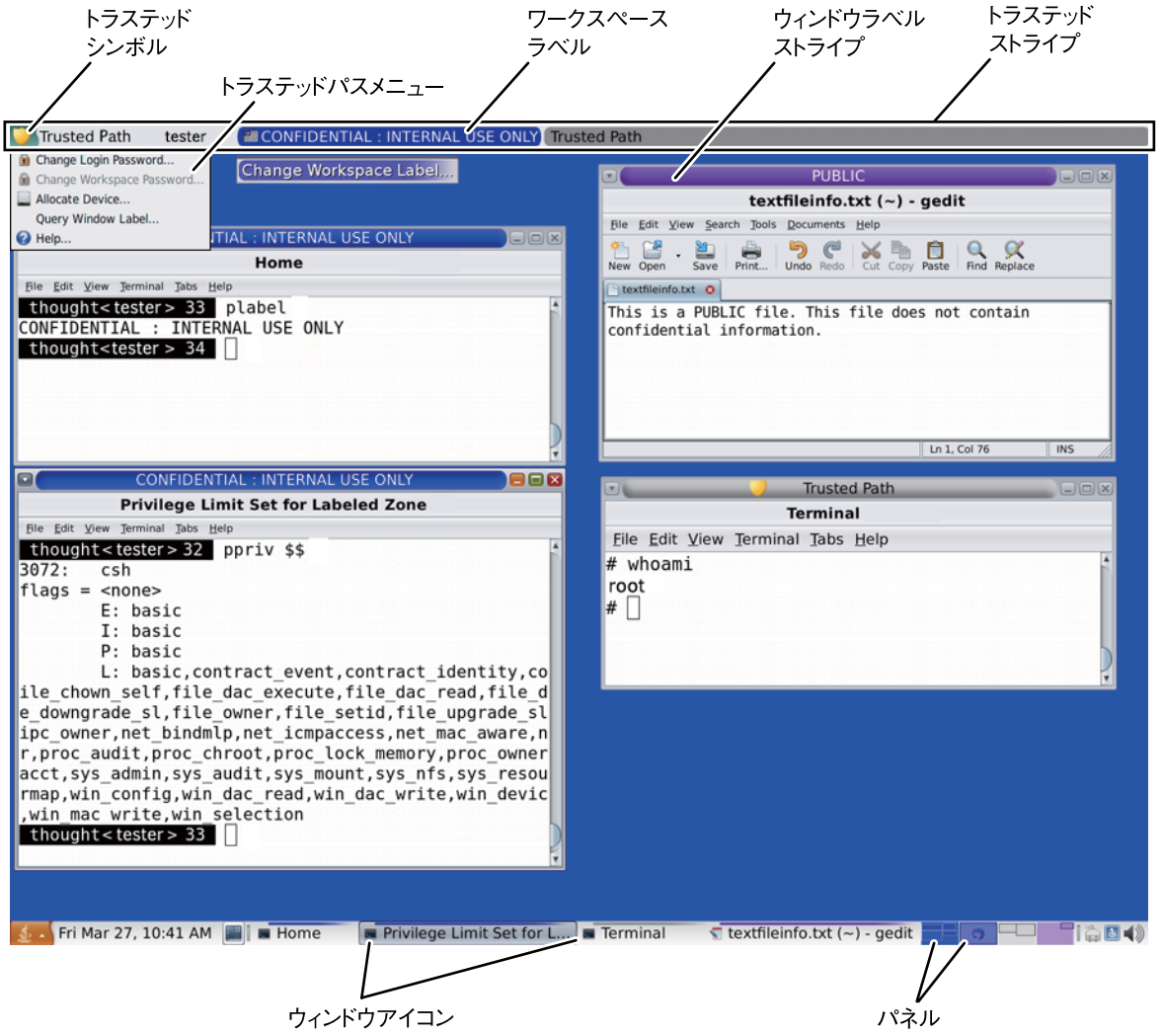
図 1–2　一般的な産業界向け機密ラベル



Trusted Extensions が構成されたシステムでは、すべてのサブジェクトとオブジェクトにラベルがあります。「サブジェクト」とは能動的な実体であり、通常はプロセスを指します。プロセスによって、情報がオブジェクト間を移動したり、システムの状態が変更されたりします。「オブジェクト」とは、データを保持したり、受け取ったりする受動的な実体であり、データファイルやディレクトリ、プリンタなどのデバイスを指します。プロセスに対して `kill` コマンドを使用するときのように、プロセスがオブジェクトになる場合もあります。

図 1–3 は、一般的なマルチレベル Trusted Extensions セッションを示しています。トラステッドストライプが上部にあります。トラステッドパスメニューはトラステッドストライプから起動します。ある役割になるには、ユーザー名をクリックして役割メニューを起動します。下部パネルのワークスペーススイッチには、ワークスペースラベルの色が表示されます。下部パネルのウィンドウリストには、ウィンドウのラベルの色が表示されます。

図 1–3　一般的なマルチレベルセッション



コンテナとラベル

Trusted Extensions では、ラベル付けにコンテナが使用されます。コンテナは「ゾーン」とも呼ばれます。「大域ゾーン」は管理ゾーンであり、ユーザーは使用できません。非大域ゾーンは「ラベル付きゾーン」と呼ばれます。ラベル付きゾーンはユーザーが使用できます。大域ゾーンの一部のシステムファイルはユーザーと共有されます。これらのファイルがラベル付きゾーンに表示される場合、ファイルのラベルは ADMIN_LOW になります。ユーザーは ADMIN_LOW ファイルの内容を読み取ることはできますが、変更することはできません。

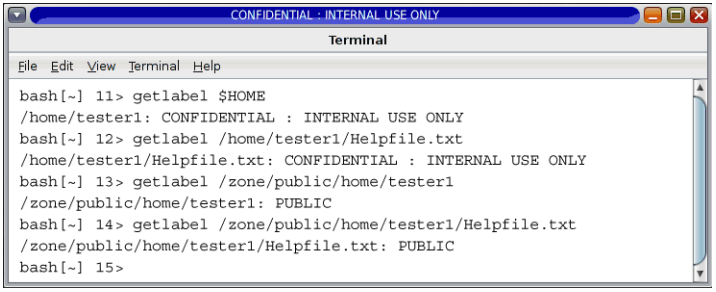
ネットワーク通信はラベルによって制限されます。デフォルトでは、それぞれのラベルが異なるため、ゾーン間の通信はできません。したがって、あるゾーンから別のゾーンへの書き込みはできません。

ただし、管理者が特定のゾーンを構成して、特定のディレクトリをほかのゾーンから読み取れるようにすることができます。ほかのゾーンは、同じホスト上にあるものでも、リモートシステム上のものでもかまいません。たとえば、レベルが低いゾーンにあるユーザーのホームディレクトリを、自動マウントサービスを使ってマウントできるようになります。このようなレベルの低いホームマウントのパス名表記では、ゾーン名を次のように含めます。

/zone/*name-of-lower-level-zone*/home/*username*

次の端末ウィンドウは、レベルの低いホームディレクトリの表示/非表示を示しています。ログインラベルが `Confidential: Internal Use Only` のユーザーは、レベルが低いゾーンを読み取れるように自動マウントサービスが構成されている場合に、`Public` ゾーンの内容を表示できます。`textfileInfo.txt` ファイルは 2 種類あります。`Public` ゾーンに置かれた方のファイルには、全員で共有できる情報が格納されます。`Confidential: Internal Use Only` ゾーンに置かれた方のファイルには、社内のみで共有できる情報が格納されます。

図 1–4　上位ラベルのゾーンからの Public 情報の表示



ラベルとトランザクション

Trusted Extensions ソフトウェアは、試みられたすべてのセキュリティー関連のトランザクションを管理します。サブジェクトのラベルがオブジェクトのラベルと比較され、どちらのラベルが「優位」であるかに応じてトランザクションが許可または拒否されます。ある実体のラベルは、次の 2 つの条件が満たされている場合に、もう一方の実体のラベルよりも「優位」だとみなされます。

- 1 つ目の実体のラベルの格付けコンポーネントが、もう一方の実体の格付けと同等またはそれよりも上である。
- もう一方の実体のラベルのすべてのコンパートメントが 1 つ目の実体のラベルに含まれている。

2 つのラベルは、同じ格付けと同じコンパートメントのセットを持つ場合に、「同等」だとみなされます。ラベルが同等であれば、これらは互いに優位です。よって、アクセスが許可されます。

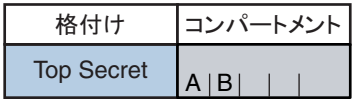
次の条件のいずれかを満たす場合、1 つ目のラベルは 2 つ目のラベルよりも「完全に優位」であると言えます。

- 1 つ目のラベルが 2 つ目のラベルよりも高い格付けを持っている
- 1 つ目のラベルの格付けが 2 つ目のラベルの格付けと同等であり、1 つ目のラベルに 2 つ目のラベルのコンパートメントがすべて含まれ、1 つ目のラベルに追加のコンパートメントがある

2 つ目のラベルよりも完全に優位なラベルには、2 つ目のラベルへのアクセスが許可されます。

どちらのラベルももう一方のラベルより優位ではない場合、これらのラベルは「無関係」とみなされます。無関係なラベル間ではアクセスは許可されません。

たとえば、次のような図を考えます。



これらのコンポーネントから、次の 4 つのラベルを作成できます。

- TOP SECRET
- TOP SECRET A
- TOP SECRET B
- TOP SECRET AB

TOP SECRET AB は自身に対して優位であり、ほかのラベルよりも完全に優位です。TOP SECRET A は自身に対して優位であり、TOP SECRET よりも完全に優位です。TOP SECRET B は自身に対して優位であり、TOP SECRET よりも完全に優位です。TOP SECRET A と TOP SECRET B は無関係です。

読み取りトランザクションでは、サブジェクトのラベルがオブジェクトのラベルよりも優位である必要があります。この規則により、サブジェクトの信頼レベルは、オブジェクトにアクセスするための条件を完全に満たすことになります。つまり、サブジェクトのラベルには、オブジェクトへのアクセスが許可されたすべてのコンパートメントが含まれます。TOP SECRET A は、TOP SECRET A と TOP SECRET のデータを読み取ることができます。同様に、TOP SECRET B は TOP SECRET B と TOP SECRET のデータを読み取ることができます。TOP SECRET A が TOP SECRET B のデータを読み取ることはできません。同様に、TOP SECRET B も TOP SECRET A のデータを読み取ることはできません。TOP SECRET AB は、すべてのラベルのデータを読み取ることができます。

書き込みトランザクション、つまり、サブジェクトによってオブジェクトが作成または変更される場合は、結果として得られるオブジェクトのラベル付きゾーンがサブジェクトのラベル付きゾーンと同等である必要があります。1 つのゾーンから別のゾーンへの書き込みトランザクションは許可されません。

実際には、読み取りや書き込みのトランザクションでのサブジェクトとオブジェクトは通常は同じラベルを持つので、完全に優位であるかどうかを気にする必要はありません。たとえば、TOP SECRET A のサブジェクトは、TOP SECRET A のオブジェクトを作成または変更できます。Trusted Extensions では、TOP SECRET A のオブジェクトは TOP SECRET A というラベルのゾーンにあります。

次の表は、米国政府のラベルおよび産業界のラベルでの優位性の関係を示しています。

表 1–1　Trusted Extensions のラベル関係の例

	ラベル 1	関係	ラベル 2
米国政府のラベル	TOP SECRET AB	ラベル 1 はラベル 2 より (完全に) 優位	SECRET A
	TOP SECRET AB	ラベル 1 はラベル 2 より (完全に) 優位	SECRET A B
	TOP SECRET AB	ラベル 1 はラベル 2 より (完全に) 優位	TOP SECRET A
	TOP SECRET AB	ラベル 1 はラベル 2 より優位 (または同等)	TOP SECRET AB
	TOP SECRET AB	無関係	TOP SECRET C
	TOP SECRET AB	無関係	SECRET C
	TOP SECRET AB	無関係	SECRET A B C
産業界のラベル	Confidential: Restricted	ラベル 1 はラベル 2 より優位	Confidential: Need to Know
	Confidential: Restricted	ラベル 1 はラベル 2 より優位	Confidential: Internal Use Only
	Confidential: Restricted	ラベル 1 はラベル 2 より優位	Public
	Confidential: Need to Know	ラベル 1 はラベル 2 より優位	Confidential: Internal Use Only
	Confidential: Need to Know	ラベル 1 はラベル 2 より優位	Public
	Confidential: Internal	ラベル 1 はラベル 2 より優位	Public
	Sandbox	無関係	その他すべてのラベル

異なるラベルを持つファイル間で情報を転送するとき、ファイルのラベル変更がそのユーザーに承認されている場合は、確認ダイアログボックスが Trusted Extensions によって表示されます。ユーザーが承認されていない場合、Trusted Extensions はトランザクションを許可しません。情報の昇格または降格をユーザーに承認できるのはセキュリティー管理者です。詳細は、46 ページの「トラステッドアクションの実行」を参照してください。

データ保護のためのユーザーの責任

ユーザーには、アクセス権を設定して自分のファイルとディレクトリを保護する責任があります。アクセス権を設定するためにユーザーが実行できるアクションでは、任意アクセス制御 (DAC) と呼ばれるメカニズムが使用されます。ファイルとディレクトリのアクセス権の確認は、`ls -l` コマンドを使用するか、ファイルブラウザ (第 3 章「Trusted Extensions での作業 (タスク)」を参照) を使用して行います。

必須アクセス制御 (MAC) はシステムによって自動的に実施されます。ラベルの付いた情報を昇格または降格することを承認されているユーザーには、情報のレベルを変更する必要性が正当なものであることを保証する重大な責任があります。

データ保護のもう 1 つの側面は電子メールに関するものです。管理者から電子メールで受け取った指示には決して従わないでください。たとえば、電子メールで送られてきた指示に従ってパスワードを特定の値に変更すると、その電子メールの送り手があなたのアカウントにログインするのを許すことになってしまいます。特別の場合として、指示に従う前にその指示を別の手段で確認することができます。

Trusted Extensions による情報のラベル別管理

Trusted Extensions では、次の方法で、情報がラベル別に分類されます。

- 電子メールをはじめとするすべてのトランザクションに MAC を実施する。
- ラベルに応じてファイルを個別ゾーンに格納する。
- デスクトップでラベル付きワークスペースを提供する。
- ユーザーがシングルレベルセッションまたはマルチレベルセッションを選択する。
- オブジェクトを再使用する前に、オブジェクトのデータを消去する。

シングルレベルセッションとマルチレベルセッション

Trusted Extensions のセッションに最初にログインするときは、シングルのラベルで作業するか、複数のラベルで作業するかを指定します。次に、自分の「セッション認可上限」または「セッションラベル」を設定します。この設定が、以降の作業のセキュリティーレベルになります。

シングルレベルセッションでは、自分のセッションラベルと同等のオブジェクトか、セッションラベルの方が優位であるオブジェクトにのみ、アクセスできます。

マルチレベルセッションでは、設定したセッション認可上限とラベルが同等、またはそれよりも下位の情報にアクセスできます。ワークスペースごとに異なるラベルを指定できます。また、同じラベルのワークスペースを複数持つこともできます。

セッションの選択例

表 1–2 は、シングルレベルセッションとマルチレベルセッションとの違いを示す例です。この例では、CONFIDENTIAL: NEED TO KNOW (CNF: NTK) のシングルレベルセッションで作業するよう選択したユーザーと、同じ CNF: NTK を指定してマルチレベルセッションを選択したユーザーとを対比しています。

左側の 3 つの列は、ログイン時に各ユーザーが選択したセッションを示します。シングルレベルセッションのユーザーは「セッションラベル」を設定し、マルチレベルセッションのユーザーは「セッション認可上限」を設定しています。システムにより、選択に応じて適切なラベルビルダーが表示されます。マルチレベルセッションのラベルビルダーの例については、図 3–4 を参照してください。

右側の 2 つの列は、セッションで使用可能なラベルの値を示しています。「初期ワークスペースラベル」列は、ユーザーがシステムに最初にアクセスしたときのラベルを表します。「使用可能なラベル」列には、セッション中にユーザーが切り替えることができるラベルが一覧表示されています。

表 1–2　使用可能なセッションラベルに対する初期ラベルの選択の影響

ユーザー選択項目			セッションラベルの値	
セッションの種類	セッションラベル	セッション認可上限	初期ワークスペースラベル	使用可能なラベル
シングルレベル	CNF: NTK	-	CNF: NTK	CNF: NTK
マルチレベル	-	CNF: NTK	Public	Public
				CNF: Internal Use Only
				CNF: NTK

表の 1 行目に示すように、ユーザーは CNF: NTK というセッションラベルのシングルレベルセッションを選択しています。ユーザーの初期ワークスペースラベルは CNF: NTKであり、これはユーザーが操作できる唯一のラベルでもあります。

表の 2 行目に示すように、ユーザーは CNF: NTK というセッション認可上限のマルチレベルセッションを選択しています。ユーザーの初期ワークスペースラベルは

Public に設定されます。これは、ユーザーのアカウントラベル範囲の中で Public がもっとも下位にある使用可能なラベルになるからです。ユーザーは Public と CNF: NTK の間の任意のラベルに切り替えることができます。Public が最下位ラベル、CNF: NTK がセッション認可上限です。

ラベル付きワークスペース

Trusted Extensions デスクトップでは、下部パネルの右側のワークスペースパネルを使ってワークスペースにアクセスします。

図 1–5　パネル上のラベル付きワークスペース

各ワークスペースにはラベルがあります。複数のワークスペースに同じラベルを割り当てたり、異なるラベルを異なるワークスペースに割り当てることができます。ワークスペース内で起動されたウィンドウには、そのワークスペースのラベルが付きます。ウィンドウが別のラベルのワークスペースに移動されても、ウィンドウは元のラベルを保持します。そのため、マルチレベルセッションでは、ラベルが異なる複数のウィンドウを 1 つのワークスペース内に配置できます。

電子メールトランザクションに MAC を適用する

Trusted Extensions では、電子メールに対して MAC が実施されます。電子メールを現在のラベルで送信したり読んだりできます。アカウント範囲内のラベルの電子メールを受信できます。マルチレベルセッションの場合は、別のラベルのワークスペースに切り替えて、そのラベルの電子メールを読むことができます。その際には、同じログインで、同じメーラーを使用します。システムは、現在のラベルでのみ電子メールを読むことを許可します。

オブジェクトを再使用する前にオブジェクトのデータを消去する

Trusted Extensions では、ユーザーアクセス可能なオブジェクトの再使用前に古い情報を自動的に消去することによって、機密情報の不用意な漏洩を防ぎます。たとえば、メモリーやディスク領域などが、再使用される前にクリアされます。オブジェクトが再使用される前に機密データを消去しないと、不適当なユーザーにデータが漏洩する恐れがあります。Trusted Extensions ではデバイスの割り当てを解除することにより、ユーザーアクセス可能なオブジェクトをすべてクリアしてか

ら、各ドライブをプロセスに割り当てます。ただし、DVD や USB デバイスなどのリムーバブルストレージメディアについては、ほかのユーザーによるドライブへのアクセスを許可する前に、ユーザー自身がすべてをクリアしておく必要があります。

Trusted Extensions によるセキュリティー保護された管理

従来の UNIX システムと異なり、Trusted Extensions の管理にはスーパーユーザー (root) を使用しません。その代わりに、可能な作業がそれぞれ異なる管理上の役割によってシステムが管理されます。これにより、1 人のユーザーがシステムのセキュリティーを危険にさらすことはできなくなります。「役割」とは、特定のタスクを実行するのに必要な権限を使って特定のアプリケーションへのアクセスを提供する特殊なユーザーアカウントです。この場合の権限とは、承認、特権、実効 UID、実効 GID などを指します。

Trusted Extensions が構成されたシステムでは、次のようなセキュリティー処理が実施されます。

- ユーザーには必要に応じてアプリケーションへのアクセスと承認が与えられる。
- 管理者から特別な承認または特権が与えられたユーザーだけが、セキュリティーポリシーをオーバーライドする機能を実行できる。
- システム管理者の任務は、複数の役割に分割される。

Trusted Extensions のアプリケーションへのアクセス

Trusted Extensions では、業務の遂行に必要なプログラムだけにアクセスできます。Oracle Solaris OSの場合と同様に、管理者はユーザーのアカウントに 1 つ以上の権利プロファイルを割り当てることによって、アクセスを可能にします。「権利プロファイル」とは、プログラムとセキュリティー属性をまとめた特殊なコレクションです。これらのセキュリティー属性は、権利プロファイル内のプログラムを正常に使えるようにするものです。

Oracle Solaris OS では、「特権」や「承認」などのセキュリティー属性が提供されます。Trusted Extensions ではラベルが提供されます。これらの属性のいずれかが欠けている場合は、プログラムまたはその一部を利用されないようにできます。たとえば、データベースを読み取れるようにする承認が権利プロファイルに含まれているとします。このデータベースを変更したり、Confidential と格付けされた情報を読み取るには、別のセキュリティー属性を持つ権利プロファイルが必要な場合があります。

セキュリティー属性が関連付けられたプログラムが含まれる権利プロファイルを使用することにより、ユーザーがプログラムを悪用したり、システム上のデータを損傷したりするのを防ぐことができます。セキュリティーポリシーをオーバーライド

するようなタスクを実行する必要があるユーザーには、必要なセキュリティー属性が含まれる権利プロファイルを管理者が割り当てることができます。実行できないタスクがある場合は、管理者に確認してください。必要なセキュリティー属性が足りない可能性があります。

さらに、管理者がユーザーのログインシェルとしてプロファイルシェルを割り当てる場合があります。「プロファイルシェル」とは特殊なバージョンの共通シェルで、特定のアプリケーションや機能に対するアクセスを可能にします。プロファイルシェルは Oracle Solaris OS の機能です。詳細については、`pfexec(1)` のマニュアルページを参照してください。

注 – プログラムを実行しようとして `Not Found` エラーメッセージが表示されたり、コマンドを実行しようとして `Not in Profile` エラーメッセージが表示されたりする場合は、プログラムの使用が許可されていない可能性があります。セキュリティー管理者に確認してください。

Trusted Extensions の役割による管理

Trusted Extensions では、管理用の役割を使用することをお勧めします。自分のサイトでだれがどの任務を実行しているのかを確認しておいてください。一般的な役割を次に示します。

- root 役割 – 主にスーパーユーザーによる直接ログインを防止するために使用します。
- セキュリティー管理者役割 – デバイスの割り当ての承認、権利プロファイルの割り当て、ソフトウェアプログラムの評価など、セキュリティーに関連するタスクを行います。
- システム管理者役割 – ユーザーの作成、ホームディレクトリの設定、ソフトウェアプログラムのインストールなど、標準的なシステム管理タスクを行います。
- オペレータ役割 – システムのバックアップ、プリンタの管理、リムーバブルメディアのマウントなどを行います。

◆ ◆ ◆ 第 2 章

Trusted Extensions へのログイン (タスク)

この章では、Trusted Extensions システムのトラステッドデスクトップとログインプロセスについて説明します。この章で扱う内容は、次のとおりです。

Trusted Extensions のデスクトップログイン

Trusted Extensions で使用するデスクトップは保護されています。ラベルは、保護されていることを視覚的に示します。アプリケーション、データ、および通信にラベルが付きます。デスクトップは、Oracle Solaris デスクトップのトラステッドバージョンです。

ログイン画面にはラベルが付きません。ログインプロセスでは、実行するセッションのラベルを設定する必要があります。ラベルを選択すると、デスクトップ、そのウィンドウ、およびすべてのアプリケーションにラベルが付きます。さらに、セキュリティーに影響を与えるアプリケーションは、保護されていることがトラステッドパスインジケータによって示されます。

Trusted Extensions のログインプロセス

Trusted Extensions が構成されたシステムでのログインプロセスは、Oracle Solaris でのログインプロセスとほぼ同じです。ただし、Trusted Extensions では、デスクトップセッションを開始する前に、いくつかの画面でセキュリティー関連の情報を確認する手順があります。プロセスの詳細は後続のセクションで説明します。ここでは簡単な概要を示します。

1. 識別 – 「ユーザー名」フィールドにユーザー名を入力します。

2. 認証 – 「パスワード」フィールドにパスワードを入力します。

   識別と認証が完了すると、システムの使用権利が確認されます。

3. メッセージの確認とセッションタイプの選択 – 「本日のメッセージ」ダイアログボックスで情報を確認します。このダイアログボックスには、最後にログインした日時、管理者からのメッセージ、セッションのセキュリティー属性が表示されます。複数のラベルで操作することが許可されている場合は、セッションのタイプ (シングルレベルまたはマルチレベル) を指定できます。

   注 – 1 つのラベルで操作するように制限されたアカウントの場合は、セッションのタイプを指定できません。この制限は、「シングルラベル」または「シングルレベル構成」と呼ばれます。例については、25 ページの「セッションの選択例」を参照してください。

   ---

4. ラベルの選択 – ラベルビルダーで、セッション中の操作に適用する最上位のセキュリティーレベルを選択します。

注 – デフォルトでは、Trusted Extensions での通常のユーザーのリモートログインはサポートされません。管理者が Oracle Solaris Xvnc ソフトウェアを構成してある場合は、VNC クライアントを使用してマルチレベルデスクトップをリモートで表示できます。手順については、34 ページの「Trusted Extensions にリモートでログインする」を参照してください。

ログイン時の識別と認証

ログイン中の識別と認証は Oracle Solaris OS によって処理されます。ログイン画面には、最初に「Username」プロンプトが表示されます。ログインプロセスのこの段階が、「識別」と呼ばれます。

ユーザー名を入力すると、パスワードのプロンプトが表示されます。プロセスのこの段階が、「認証」と呼ばれます。パスワードは、ユーザー名を入力したユーザーが本当にそのユーザー名の使用を承認されているユーザーであることを認証します。

「パスワード」とは、キー入力の非公開の組み合わせで、ユーザー ID の妥当性をシステムに対して証明するものです。パスワードは暗号化形式で格納されるため、システム上のほかのユーザーからはアクセスできません。自分のパスワードがほかのユーザーに使用されて不正なアクセスが行われないよう、パスワードはユーザー自身の責任で保護する必要があります。パスワードを書き留めたり、他人に見せたりしないでください。ユーザーが使用しているパスワードを持った人間は、そのユーザーがアクセスできるすべてのデータに本人であることの識別も確認もされずにアクセスできるからです。最初のパスワードはセキュリティー管理者が設定します。

ログイン時のセキュリティー属性の確認

セキュリティー属性の確認は、Oracle Solaris OS ではなく Trusted Extensions によって処理されます。ログインが完了する前に、Trusted Extensions によって「本日のメッセージ」(MOTD) ダイアログボックスが表示されます。このダイアログボックスには、確認するステータス情報が表示されます。そのステータスには、自分が最後にシステムを使った日時など過去の情報が含まれます。これから行うセッションで有効となるセキュリティー属性も確認できます。複数のラベルで操作するように構成されたアカウントの場合は、シングルレベルセッションかマルチレベルセッションかを選択できます。

その後、ラベルビルダーでシングルラベルを表示したり、ラベルと認可上限を選択したりできます。

Trusted Extensions へのログイン

Trusted Extensions にログインするためのタスクを次に示します。デスクトップを表示する前に、セキュリティー情報を確認して指定してください。

▼ システムにユーザーを識別および認証させる

1 ログイン画面の「**Username**」フィールドにユーザー名を入力します。

管理者から割り当てられたユーザー名を正確に入力してください。スペリング、大文字、小文字を確認してください。

間違えた場合は偽のパスワードを入力してください。「ユーザー名」フィールドが表示されます。

2 入力を確認します。

Return キーを押してユーザー名を確定します。

注意 – ログイン画面の表示中は、トラステッドストライプが表示されることはありません。ログインしようとしたとき、または画面のロックを解除しようとしたときにトラステッドストライプが表示された場合は、パスワードを入力しないでください。スプーフィングが行われている可能性があります。「スプーフィング」とは、侵入者のプログラムがログインプログラムであるかのように偽って、パスワードを手に入れようとすることです。ただちにセキュリティー管理者に連絡してください。

3 パスワードの入力フィールドにパスワードを入力して、**Return** キーを押します。

セキュリティー保護のため、入力した文字はフィールドには表示されません。ログイン名とパスワードが、承認されたユーザーのリストと照合されます。

注意事項　入力したパスワードが正しくない場合は、画面に次のようなメッセージが表示されます。

認証に失敗しました (Authentication failed)

「了解」をクリックしてエラーダイアログボックスを閉じます。ユーザー名と正しいパスワードを再度入力してください。

▼ メッセージを確認し、セッションタイプを選択する

シングルラベルに制限していないユーザーは、異なるラベルのデータを表示できます。操作可能な範囲は、上限がセッション認可上限、下限が管理者によって割り当てられた最下位ラベルに制限されます。

1 **MOTD ダイアログボックスを確認します。**

a. 前回のセッションの日時が正しいことを確認します。

通常の時間外であるなど、最後のログインに疑わしいところがないかを常に確認してください。ログイン時間が正しくないと考える理由がある場合は、セキュリティー管理者に連絡してください。

b. 管理者からのメッセージがないかどうかを確認します。

「本日のメッセージ」フィールドには、予定されているメンテナンスやセキュリティー上の問題に関する警告が表示されていることがあります。このフィールドの情報は必ず確認してください。

c. セッションのセキュリティー属性を確認します。
MOTD ダイアログボックスには、ユーザーがなれる役割や最下位ラベルなどのセキュリティー特性が表示されます。

d. (省略可能) マルチレベルセッションへのログインが許可されている場合は、シングルレベルセッションにするかどうかを決定します。
「シングルラベルにセッションを制限」ボタンをクリックして、シングルレベルのセッションにログインします。

e. 「了解」をクリックします。

2 ラベルの選択を確定します。
ラベルビルダーが表示されます。シングルラベルでログインしている場合は、ラベルビルダーによりそのセッションラベルが示されます。マルチレベルのシステムの場合は、ラベルビルダーによりセッション認可上限を選択できます。マルチレベルセッションのラベルビルダーの例については、図 3–4 を参照してください。

- デフォルトを拒否する理由がないかぎり、デフォルトを受け入れます。
- マルチレベルセッションの場合は、認可上限を選択します。
認可上限を変更するには、トラステッドパス認可上限をクリックし、必要な認可上限をクリックします。
- シングルレベルセッションの場合は、ラベルを選択します。
ラベルを変更するには、トラステッドパスラベルをクリックし、必要なラベルをクリックします。

3 「了解」をクリックします。
トラステッドデスクトップが表示されます。

▼ ログインの問題のトラブルシューティング

1 ユーザー名やパスワードが認識されない場合は、管理者に確認してください。

2 設定したラベル範囲がワークステーションに許可されていない場合は、管理者に確認してください。
セッション認可上限およびラベルの範囲は、ワークステーションごとに制限することができます。たとえば、ロビーに置かれたワークステーションは PUBLIC ラベル専用に制限されている可能性があります。指定したラベルまたはセッション認可上限が拒否される場合は、そのワークステーションが制限されていないかどうかを管理者に確認してください。

3 シェルの初期設定ファイルをカスタマイズしている場合にログインできないときは、次の 2 つの対処方法があります。

- システム管理者に連絡して状況を改善してもらう。
- **root** になれる場合は、復旧セッションにログインする。
  標準的なログインでは、起動時にシェルの初期設定ファイルが参照され、カスタマイズされた環境が構築されます。復旧ログインの場合は、デフォルトの設定値がそのままシステムに適用され、シェルの初期設定ファイルは参照されません。

  Trusted Extensions では、復旧ログインは保護されています。root アカウントだけが復旧ログインにアクセスできます。

  a. ログイン画面でユーザー名を入力します。

  b. 画面下部で、デスクトップメニューから **Solaris Trusted Extensions** の「復旧セッション」を選択します。

  c. 要求された場合は、パスワードを入力します。

  d. 追加のパスワードを要求されたら、**root** のパスワードを入力します。

Trusted Extensions にリモートでログインする

仮想ネットワークコンピューティング (Virtual Network Computing、VNC) を利用すると、ラップトップコンピュータまたはホームコンピュータから中央 Trusted Extensions システムにアクセスできます。サイトの管理者は、Oracle Solaris Xvnc ソフトウェアが Trusted Extensions サーバーで動作し、VNC ビューアがクライアントシステムで動作するように構成する必要があります。サーバーにインストールされたラベル範囲のいずれかのラベルで作業できます。

▼ リモート Trusted Extensions デスクトップにログインする方法

始める前に 管理者が Xvnc サーバーを設定しておきます。ポインタについては、『Trusted Extensions 構成と管理』の「リモートアクセス用に Xvnc で Trusted Extensions システムを構成する」を参照してください。

1 端末ウィンドウでは、**Xvnc** サーバーに接続します。
管理者が Xvnc で構成したサーバーの名前を入力します。

```
% /usr/bin/vncviewer Xvnc-server
```

2 ログインします。

31 ページの「Trusted Extensions へのログイン」の手順に従います。

VNC ビューア内の Trusted Extensions デスクトップで作業できるようになります。

◆ ◆ ◆ 第 3 章

Trusted Extensions での作業 (タスク)

この章では、Trusted Extensions のワークスペースで作業する方法について説明します。この章で扱う内容は、次のとおりです。

Trusted Extensions のデスクトップセキュリティーの表示

Trusted Extensions では、マルチレベルデスクトップが提供されます。

Trusted Extensions が構成されたシステムでは、ログイン時および画面ロック時を除き、トラステッドストライプが表示されます。上記の場合以外は常にトラステッドストライプが表示されています。

ストライプは画面上部にあります。トラステッドシンボルは、トラステッドコンピューティングベース (TCB) との対話が行われるときに、トラステッドストライプに表示されます。たとえば、パスワードを変更するときは TCB と対話します。

マルチヘッドの Trusted Extensions システムのモニターが水平に構成されている場合、1 つのトラステッドストライプが複数のモニターにまたがって表示されます。ただし、マルチヘッドのシステムが垂直に表示するよう構成されているか、または別個のデスクトップがモニターごとに 1 つずつ存在する場合、トラステッドストライプは 1 つのモニターにだけ表示されます。

注意 – マルチヘッドのシステム上で 2 つめのトラステッドストライプが表示される場合、それはオペレーティングシステムによって生成されたものではありません。システムに承認されていないプログラムが存在する可能性があります。

ただちにセキュリティー管理者に連絡してください。正しいトラステッドストライプを確認するには、44 ページの「マウスポインタを見つける方法」を参照してください。

アプリケーション、メニュー、ラベル、およびデスクトップの機能の詳細は、第 4 章「Trusted Extensions の構成要素 (リファレンス)」を参照してください。

Trusted Extensions のログアウトプロセス

ログインしたまま放置されたワークステーションは、セキュリティー上のリスクを招きます。ワークステーションから離れるときは、ワークステーションのセキュリティー保護を行う習慣をつけてください。すぐに端末に戻るつもりであれば、画面をロックしてください。ほとんどのサイトでは、一定時間アイドル状態のままにしておくと、画面が自動的にロックされます。長時間席をはずしたり、ほかのユーザーがワークステーションを使用すると思われる場合は、ログアウトしてください。

ラベル付きシステムでの作業

注意 – ワークスペースにトラステッドストライプが表示されない場合は、セキュリティー管理者に連絡してください。システムに重大な問題が起きている可能性があります。

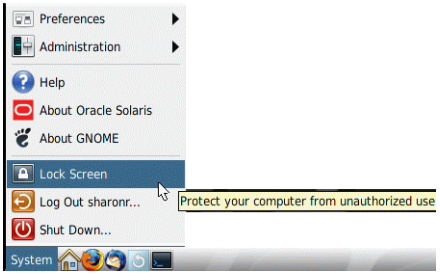
ログイン時および画面ロック時は、トラステッドストライプは表示されないはずです。トラステッドストライプが表示されている場合は、ただちに管理者に連絡してください。

▼ 画面をロックおよびロック解除する

ワークステーションから短時間離れるときは、画面をロックしてください。

1 メインメニューから「画面ロック」を選択します。

図 3–1　ロック画面の選択

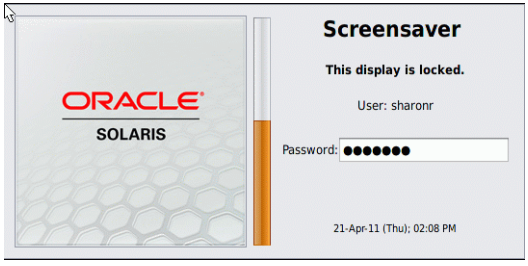


画面が消えます。この時点でふたたびログインできるのは、画面をロックしたユーザーのみです。

注 – 画面がロックされているときはトラステッドストライプは表示されないはずです。トラステッドストライプが表示されている場合は、ただちにセキュリティー管理者に報告してください。

2　画面のロックを解除するには、次の操作を行います。

a.　「スクリーンセーバー」ダイアログボックスが表示されるまでマウスを動かします。



「スクリーンセーバー」ダイアログボックスが表示されない場合は、Return キーを押します。

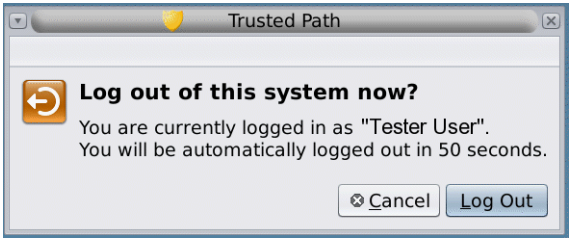
b.　パスワードを入力します。

これにより、画面をロックする前の状態のセッションに戻ります。

▼ Trusted Extensions からログアウトする

ほとんどのサイトでは、一定時間アイドル状態のままにしておくと、画面が自動的にロックされます。ワークステーションから長時間離れたり、ほかのユーザーがワークステーションを使用すると思われる場合は、ログアウトしてください。

1 **Trusted Extensions** からログアウトするには、メインメニューから「*your-name* をログアウト」を選択します。



2 ログアウトを確認するか、または「取消し」をクリックします。

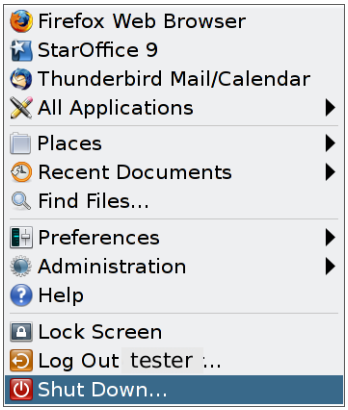
▼ システムをシャットダウンする方法

Trusted Extensions のセッションを終了する正規の方法はログアウトです。次の手順は、ワークステーションの電源を切る必要がある場合に使用してください

注 – コンソール上で操作していない場合、システムをシャットダウンできません。たとえば、VNC クライアントはシステムをシャットダウンできません。

始める前に 「Maintenance and Repair」権利プロファイルが割り当てられている必要があります。

- メインメニューから「停止」を選択します。



シャットダウンを確認します。

注 – デフォルトでは、Stop-A (L1-A) キーの組み合わせは Trusted Extensions では使用できません。このデフォルト設定はセキュリティー管理者が変更できます。

▼ ラベル付きワークスペースにファイルを表示する

ファイルを表示するには、Oracle Solaris システムのデスクトップで使用するものと同じアプリケーションを使用します。複数のラベルで作業している場合は、ワークスペースのラベルのファイルのみが表示されます。

- 端末ウィンドウまたはファイルブラウザを開きます。
  - 端末ウィンドウを開き、ホームディレクトリの内容を一覧表示します。
    背景でマウスボタン 3 をクリックします。メニューから、「端末エミュレータを開く」を選択します。
  - デスクトップまたはデスクトップパネルのホームフォルダをクリックします。
    このフォルダがファイルブラウザに表示されます。ファイルブラウザアプリケーションは、現在のワークスペースと同じラベルで開きます。このアプリケーションでは、同じラベルのファイルのみにアクセスできます。別のラベルのファイルの表示に関する詳細は、20 ページの「コンテナとラベル」を参照してください。異なるラベルのファイルを 1 つのワークスペースで表示するには、54 ページの「ウィンドウを別のワークスペースに移動する」を参照してください。

▼ Trusted Extensions のマニュアルページにアクセスする

- **Oracle Solaris** リリースでは、端末ウィンドウで **trusted_extensions(5)** のマニュアルページを確認します。

  ```
  % man trusted_extensions
  ```

  Trusted Extensions に固有のユーザーコマンドのリストについては、『Trusted Extensions 構成と管理』の付録 D「Trusted Extensions マニュアルページのリスト」を参照してください。マニュアルページは、Oracle のドキュメント Web サイト (http://www.oracle.com/technetwork/indexes/documentation/index.html)からも入手できます。

▼ あらゆるラベルの初期設定ファイルにアクセスする

別のラベルにファイルをリンクまたはコピーする操作は、ラベルの低いファイルを高いラベルで表示できるようにするのに便利です。リンクされたファイルへの書き込みは、低い方のラベルでのみ実行できます。コピーされたファイルはラベルごとに一意であり、各ラベルで変更できます。詳細は、『Trusted Extensions 構成と管理』の「.copy_files ファイルと .link_files ファイル」を参照してください。

始める前に　マルチレベルセッションにログインしている必要があります。 サイトのセキュリティーポリシーでリンクが許可されている必要があります。

これらのファイルの変更は管理者とともに行なってください。

1. ほかのラベルにリンクする初期設定ファイルを決定します。
2. **~/.link_files** ファイルを作成または変更します。

   1 行につき 1 つのファイルのエントリを入力します。ホームディレクトリ内のサブディレクトリへのパスを指定できますが、先頭のスラッシュは使用できません。すべてのパスがホームディレクトリ内にある必要があります。
3. ほかのラベルにコピーする初期設定ファイルを決定します。

   初期設定ファイルのコピーは、常に特定の名前でファイルへの書き込みを行うアプリケーションで、そのデータを複数のラベルに分ける必要があるときに便利です。
4. **~/.copy_files** ファイルを作成または変更します。

   1 行につき 1 つのファイルのエントリを入力します。ホームディレクトリ内のサブディレクトリへのパスを指定できますが、先頭のスラッシュは使用できません。すべてのパスがホームディレクトリ内にある必要があります。

例 3–1 .copy_files ファイルの作成

この例のユーザーは、複数の初期設定ファイルをラベルごとにカスタマイズしたいと望んでいます。ユーザーの組織では、会社の Web サーバーを Restricted レベルで使用できます。そのため、このユーザーは、.mozilla ファイル内のさまざまな初期設定を、Restricted レベルで行なっています。同様に、このユーザーは Restricted レベルの特殊なテンプレートと別名を持っています。そのため、.aliases 初期設定ファイルと .soffice 初期設定ファイルの変更を、Restricted レベルで行なっています。.copy_files ファイルをユーザー自身の最下位ラベルで作成したあとは、前述のファイルを簡単に変更できるようになります。

```
% vi .copy_files
# Copy these files to my home directory in every zone
.aliases
.mozilla
.soffice
```

例 3–2 .link_files ファイルの作成

この例では、ユーザーが自分のメールのデフォルトと C シェルのデフォルトをすべてのラベルで同一にすることを望んでいます。

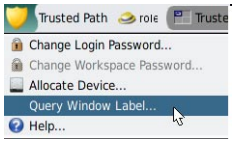
```
% vi .link_files
# Link these files to my home directory in every zone
.cshrc
.mailrc
```

注意事項 これらのファイルには、異常に対処する予防策がありません。両方のファイルでエントリが重複したり、ファイルエントリがほかのラベルですでに存在したりすると、エラーが起きる可能性があります。

▼ ウィンドウラベルを対話的に表示する

この操作は、一部が隠れたウィンドウのラベルを識別するために役立つことがあります。

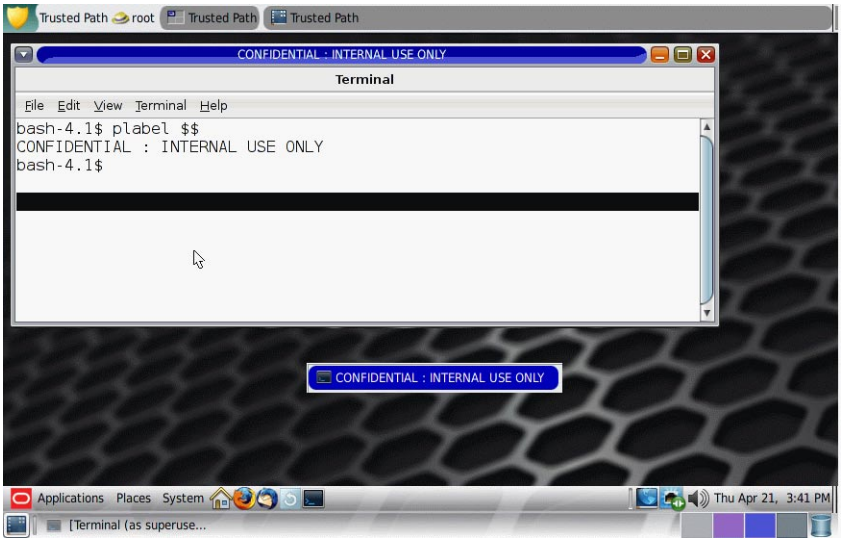
1 トラステッドパスメニューから「ウィンドウのラベルを照会」を選択します。



2 ポインタを画面上で動かします。

ポインタの位置のラベルが、画面中央の小さな四角形のボックスに表示されます。

図 3–2 「ウィンドウのラベルを照会」の操作画面



3 マウスボタンをクリックして操作を終了します。

▼ マウスポインタを見つける方法

信頼できないアプリケーションがキーボードやマウスポインタの制御を取得することがあります。ポインタを見つけることにより、デスクトップのフォーカスの制御を取り戻すことができます。

1 **Sun 製キーボードの制御を取り戻すには、Meta-Stop を押します。**

キーを同時に押して、現在のデスクトップのフォーカスの制御を取り戻します。Sun 製キーボードでは、スペースバーのどちら側かにあるダイヤモンドマークの付いたキーが Meta キーです。

キーボードまたはマウスポインタの占有が信頼できない場合、ポインタはトラステッドストライプに移動します。信頼できるポインタはトラステッドストライプには移動しません。

2 **Sun 製以外のキーボードを使用している場合は、Alt-Break を押します。**

例 3–3 マウスポインタを強制的にトラステッドストライプに移動させる

この例では、ユーザーはトラステッドプロセスを実行していませんが、マウスポインタを確認できません。ポインタをトラステッドストライプの中央に移動させるためには、ユーザーは Meta-Stop キーを同時に押します。

例 3–4 本物のトラステッドストライプを見つける

マルチヘッドの Trusted Extensions システムで、モニターがそれぞれ個別のデスクトップを表示するように構成されている場合に、モニターごとに 1 つのトラステッドストライプが表示されています。つまり、Trusted Extensions 以外のプログラムがトラステッドストライプを生成しています。マルチヘッドのシステムで、モニターごとに個別のデスクトップを表示するように構成されている場合は、1 つのトラステッドストライプだけが表示されます。

ユーザーは作業を中止し、ただちにセキュリティー責任者に連絡します。次に、ユーザーはワークスペースの背景などの信頼できない場所にマウスポインタを置いて、本物のトラステッドストライプを見つけます。ユーザーが Alt-Break キーを同時に押すと、Trusted Extensions で生成されたトラステッドストライプにポインタが移動します。

▼ Trusted Extensions の共通デスクトップタスクを実行する

一部の共通タスクは、ラベルおよびセキュリティーによって影響を受けます。特に次のタスクは Trusted Extensions の影響を受けます。

- ごみ箱を空にする
- カレンダイベントの検索する

1 ごみ箱を空にする。

デスクトップの「ごみ箱」アイコンの上でマウスボタン 3 をクリックします。「ごみ箱を空にする」を選択してから確定します。

注 – ごみ箱には、ワークスペースのラベルのみのファイルを格納できます。機密情報は、ごみ箱に入れた直後に削除してください。

---

2 あらゆるラベルのカレンダイベントを検索する。

カレンダには、そのカレンダを開いたワークスペースのラベルのイベントのみが表示されます。

- マルチレベルセッションでは、それぞれ異なるラベルを持つワークスペースからカレンダを開きます。

- シングルレベルセッションでは、ログアウトします。次に別のラベルでログインし、そのラベルのカレンダイベントを表示します。

3 あらゆるラベルのカスタマイズ済みデスクトップを保存する。

ログインするあらゆるラベルについて、ワークスペース構成をカスタマイズできます。

a. デスクトップを構成します。

注 – ユーザーはデスクトップの構成を保存できます。役割はデスクトップの構成を保存できません。

---

i. メインメニューから、「システム」、「設定」、「表示」の順にクリックします。

ii. ウィンドウの整列、フォントサイズの設定、およびその他のカスタマイズを実行します。

b. 現在のデスクトップを保存するには、メインメニューをクリックします。

i. 「システム」、「設定」、「自動起動するアプリ」の順にクリックします。

ii. 「オプション」タブをクリックします。

iii. 「現在実行中のアプリケーションを記憶する」をクリックし、ダイアログボックスを閉じます。

このラベルで次回ログインするときは、デスクトップがこの構成で復元されます。

トラステッドアクションの実行

次に説明するセキュリティー関連のタスクは、トラステッドパスを必要とします。

注意 – セキュリティー関連のアクションを実行しようとしたときにトラステッドシンボルが表示されない場合は、ただちにセキュリティー管理者に連絡してください。システムに重大な問題が起きている可能性があります。

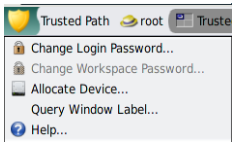
▼ Trusted Extensions でパスワードを変更する

Oracle Solaris OS とは異なり、Trusted Extensions では自分のパスワードを変更するための GUI が提供されています。この GUI により、パスワードの操作が完了するまでポインタが占有されます。ポインタを占有したプロセスを停止するには、例 3–5 を参照してください。

1 トラステッドメニューから「ログインパスワードを変更」または「ワークスペースパスワードを変更」を選択します。

パスワードメニュー項目を選択するには、トラステッドストライプ内のトラステッドパスをクリックします。

図 3–3 トラステッドパスメニュー



注 – トラステッドパスメニュー項目「ワークスペースパスワードを変更」は、サイトでゾーンごとに個別のネームサービスが実行されている場合にアクティブになります。

---

2 現在のパスワードを入力します。

これにより、このユーザー名の正当なユーザーであることが確認されます。セキュリティー保護のため、入力するパスワードは表示されません。

注意 – パスワードを入力するときは、カーソルが「パスワード変更」ダイアログボックス上にあること、およびトラステッドシンボルが表示されていることを必ず確認してください。カーソルがダイアログボックス上にない場合に、誤ってパスワードを別のウィンドウに入力すると、ほかのユーザーにパスワードを見られる恐れがあります。トラステッドシンボルが表示されていない場合は、だれかがパスワードを盗もうとしている可能性があります。ただちにセキュリティー管理者に連絡してください。

---

3 新しいパスワードを入力します。

4 パスワードをもう一度入力して確定します。

注 – サイトでローカルアカウントが使用されている場合に「パスワード変更 (Change Password)」を選択したときは、ゾーンまたはシステムがリブートされるまで新しいパスワードは有効になりません。ゾーンをリブートするには、「Zone Security」権利プロファイルが割り当てられている必要があります。ゾーンをリブートするには、「Maintenance and Repair」権利プロファイルが割り当てられている必要があります。これらのプロファイルのいずれも割り当てられていない場合は、システム管理者に連絡してリブートをスケジュールしてください。

例 3–5 パスワードのプロンプトが信頼できるかどうかテストする

Sun 製キーボードを使用している x86 システム上で、ユーザーがパスワードの入力を求められました。マウスポインタは占有された状態になり、パスワードダイアログボックスの中にあります。プロンプトが信頼できることを確認するために、ユーザーは Meta-Stop キーを同時に押します。ポインタがダイアログボックスの中に残る場合は、信頼できるパスワードプロンプトであるとわかります。

ポインタがダイアログボックスの中に残らない場合は、信頼できないパスワードプロンプトであるとわかります。その場合、ユーザーは管理者に連絡する必要があります。

▼ 別のラベルにログインする

最初のログインのあとに続くログインセッションで表示される最初のワークスペースのラベルは、許可されているラベル範囲内の任意のラベルに設定できます。

ユーザーは、ログインしているすべてのラベルに対して、起動セッション特性を構成できます。

始める前に　マルチレベルセッションにログインしている必要があります。

1. すべてのラベルでワークスペースを作成します。
   詳細については、53 ページの「自分の最下位ラベルでワークスペースを追加する方法」を参照してください。
2. それぞれのワークスペースを、希望する表示になるように構成します。
3. ラベルにログインしたときに表示するラベル付きワークスペースに移動します。
4. この現在のワークスペースを保存します。
   詳細は、45 ページの「Trusted Extensions の共通デスクトップタスクを実行する」を参照してください。

▼ Trusted Extensions でデバイスを割り当てる

「デバイスを割り当てる」メニュー項目を使用して、デバイスを自分専用にマウントして割り当てることができます。デバイスを割り当てないまま使おうとすると、「アクセス権がありません」というエラーメッセージが表示されます。

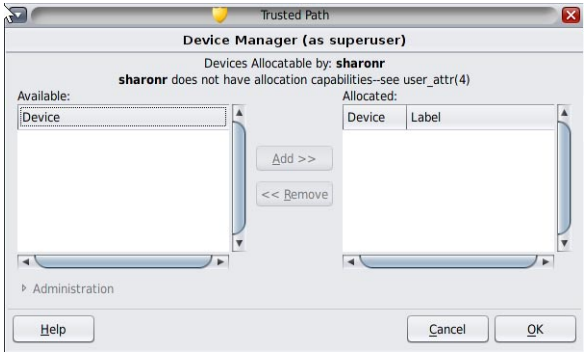
始める前に　デバイスを割り当てるには承認が必要です。

1. トラステッドパスメニューから「デバイスを割り当てる」を選択します。
2. 使用するデバイスをダブルクリックします。

   現在のラベルで割り当てが許可されているデバイスが「使用可能デバイス」に表示されます。

   - `audio`*n* – マイクロフォンとスピーカーを表します
   - `cdrom`*n* – CD-ROM ドライブを表します
   - `floppy`*n* – フロッピーディスクドライブを表します
   - `mag_tape`*n* – テープドライブ (ストリーマテープドライブ) を表します
   - `rmdisk`*n* – JAZ ドライブや ZIP ドライブなどのリムーバブルディスク、または USB ホットプラグ対応媒体を表します

   次のダイアログボックスは、ユーザーがデバイスの割り当てを承認されていないことを示しています。



3. デバイスを選択します。

   「使用可能デバイス」リストから「割り当てられたデバイス」リストにデバイスを移動します。

   - 「使用可能デバイス」リストのデバイス名をダブルクリックします。

- または、デバイスを選択してから割り当てボタン (右向き矢印) をクリックします。

この操作で clean スクリプトが起動されます。clean スクリプトは、ほかのトランザクションからのデータが媒体に残るのを防ぎます。

デバイスには、現在のワークスペースのラベルが適用されます。このラベルは、デバイスの媒体に転送される、またはデバイスの媒体から転送されるすべてのデータのラベルよりも優位である必要があります。

4 画面の指示に従います。

指示により、媒体のラベルが正しいことが確認されます。たとえば、マイクロフォンの使用に関して次の指示が表示されます。

次にデバイスがマウントされます。この段階で、デバイス名が「割り当てられたデバイス」リストに表示されます。これで、このデバイスがユーザー専用のデバイスとして割り当てられました。

注意事項 使用するデバイスがリストに表示されない場合は、管理者に確認してください。デバイスがエラー状態にあるか、だれかが使用中である可能性があります。あるいは、そのデバイスの使用を承認されていない可能性があります。

別の役割のワークスペースや、異なるラベルのワークスペースに切り替えた場合、割り当てられているデバイスはそのラベルでは機能しません。デバイスを新しいラベルで使用するには、まず最初のラベルでデバイスの割り当てを解除してから、新しいラベルでデバイスを割り当てる必要があります。デバイスマネージャーを別のラベルのワークスペースに移動すると、「使用可能デバイス」リストと「割り当てられたデバイス」リストの内容も、状況に合わせて変化します。

ファイルブラウザウィンドウが表示されない場合は、ウィンドウを手動で開き、ルートディレクトリ (/) に移動します。このディレクトリで、割り当てたデバイスに移動して内容を表示します。

▼ Trusted Extensions でデバイスの割り当てを解除する

1 デバイスの割り当てを解除します。

   a. デバイスマネージャーが表示されたワークスペースに移動します。

   b. 割り当てられたデバイスのリストから、割り当てを解除するデバイスを移動します。

2 メディアを取り出します。

3 「割り当て解除」ダイアログボックスで、「了解」をクリックします。
別の承認されたユーザーがデバイスを利用できるようになります。

▼ Trusted Extensions で役割になる

Oracle Solaris OS とは異なり、Trusted Extensions では役割を選択するための GUI が提供されています。

1 トラステッドシンボルの右側にあるユーザー名をクリックします。

2 メニューから役割名を選択します。

3 役割のパスワードを入力し、**Return** キーを押します。
これにより、この役割になるのが正当なユーザーであることが確認されます。セキュリティー保護のため、入力するパスワードは表示されません。

注意 – パスワードを入力するときは、カーソルが「パスワード変更」ダイアログボックス上にあること、およびトラステッドシンボルが表示されていることを必ず確認してください。カーソルがダイアログボックス上にない場合に、誤ってパスワードを別のウィンドウに入力すると、ほかのユーザーにパスワードを見られる恐れがあります。トラステッドシンボルが表示されていない場合は、だれかがパスワードを盗もうとしている可能性があります。ただちにセキュリティー管理者に連絡してください。

役割のパスワードが受け入れられると、現在のワークスペースが役割のワークスペースになります。ここは大域ゾーンです。自分の役割の権利プロファイルで許可されているタスクを実行できます。

▼ ワークスペースのラベルを変更する

Trusted Extensions では複数のワークスペースラベルを設定できるので、同じマルチレベルセッション内で異なるラベルで作業するのに便利です。

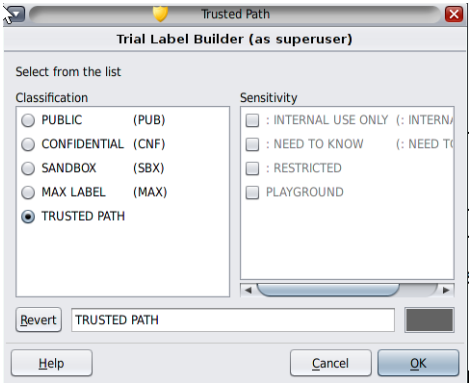
ラベルが異なる同じワークスペースで作業する場合は、この手順を使用します。別のラベルのワークスペースを作成するには、53 ページの「自分の最下位ラベルでワークスペースを追加する方法」を参照してください。

始める前に　マルチレベルセッションにログインしている必要があります。

1. トラステッドストライプ内のウィンドウラベルをクリックします。
   ワークスペースパネルをクリックすることもできます。
2. 「ワークスペースラベルを変更」をクリックします。

3. ラベルビルダーからラベルを選択します。
   次の図は、ユーザーがトラステッドパスボタンをクリックする様子を示しています。

図 3–4　ラベルビルダー



このボタンをクリックしたあと、ユーザーラベルから選択できます。ワークスペースラベルが新しいラベルに変更されます。ラベルが色分けされているシステムでは、新しいウィンドウが新しい色で区別されます。

4 パスワードを要求された場合は、パスワードを入力します。

サイトでゾーンごとに個別のネームサービスが実行されている場合、ユーザーは新しいラベルのワークスペースに入るときにパスワードを要求されます。

▼ 自分の最下位ラベルでワークスペースを追加する方法

Trusted Extensions では複数のワークスペースラベルを設定できるので、同じマルチレベルセッション内で異なるラベルで作業するのに便利です。ユーザーは自分の最下位ラベルでワークスペースを追加できます。

現在のワークスペースのラベルを変更するには、52 ページの「ワークスペースのラベルを変更する」を参照してください。

始める前に マルチレベルセッションにログインしている必要があります。

1 自分の最下位ラベルでワークスペースを追加するには、次の手順に従います。

a. ワークスペースパネルの上でマウスボタン 3 をクリックします。

b. メニューから「設定」を選択します。

c. 「ワークスペースの数」フィールドの数を増やします。

ワークスペースが最下位ラベルで作成されます。このダイアログボックスを使用して、ワークスペースに名前を付けることもできます。名前がツールチップに表示されます。

d. (省略可能) ワークスペースに名前を付けます。

ワークスペースパネルの上にマウスを移動すると、この名前がツールチップに表示されます。

2 ワークスペースラベルを変更するには、ワークスペースパネルを選択し、そのラベルを変更します。

詳細は、52 ページの「ワークスペースのラベルを変更する」を参照してください。

▼ 別のラベルのワークスペースに切り替える

始める前に　マルチレベルセッションにログインしている必要があります。

1. 別の色のワークスペースパネルをクリックします。

2. パスワードを要求された場合は、パスワードを入力します。

   サイトでゾーンごとに個別のネームサービスが実行されている場合、ユーザーは新しいラベルのワークスペースに入るときにパスワードを要求されます。

注意事項　シングルレベルセッションにログインしている場合、別のラベルで作業するにはログアウトする必要があります。その後、希望するラベルにログインしてください。許可されている場合は、マルチレベルセッションにログインする方法もあります。

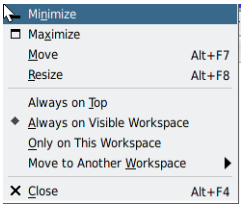
▼ ウィンドウを別のワークスペースに移動する

ウィンドウを別のラベルのワークスペースにドラッグした場合、ウィンドウは元のラベルを保持します。そのウィンドウで行われるすべてのアクションは、ウィンドウが置かれているワークスペースのラベルではなく、ウィンドウのラベルで行われます。ウィンドウの移動は、情報を比較するときに便利です。アプリケーションをワークスペース間で移動せずに、異なるラベルで使うこともできます。

1. パネル画面で、ウィンドウを元のパネルから別のパネルにドラッグします。

   ドラッグしたウィンドウが、2 つ目のワークスペースに表示されます。

2. このウィンドウをすべてのワークスペースに表示するには、タイトルバーの右ボタンメニューから「常に表示」を選択します。



これで、選択したウィンドウがすべてのワークスペースに表示されるようになります。

▼ ファイルのラベルを判断する

通常は、ファイルのラベルは明らかです。しかし、現在のワークスペースよりも低いラベルのファイルの表示を許可されている場合は、ファイルのラベルが明らかではないことがあります。具体的には、ファイルのラベルがファイルブラウザのラベルと異なる場合があります。

- ファイルブラウザを使用する。

ヒント – トラステッドパスメニューの「ラベル問い合わせ」メニュー項目を使用することもできます。

▼ ラベルの異なるウィンドウ間でデータを移動する方法

Oracle Solaris システムの場合と同様に、Trusted Extensions でもウィンドウ間でデータを移動できます。ただし、データは同じラベルである必要があります。ラベルの異なるウィンドウ間で情報を転送するときは、その情報の機密度を昇格または降格することになります。

始める前に　サイトのセキュリティーポリシーでこのような転送が許可され、含まれるゾーンでラベルの付け直しが許可されている必要があります。また、ユーザーはラベル間のデータ移動を承認されている必要があります。

したがって、管理者は次のタスクを完了している必要があります。

- 『Trusted Extensions 構成と管理』の「ラベル付きゾーンからファイルに再ラベル付けできるようにする」
- 『Trusted Extensions 構成と管理』の「ユーザーによるデータのセキュリティーレベルの変更を有効にする」

マルチレベルセッションにログインしている必要があります。

1. 両方のラベルでワークスペースを作成します。

   詳細については、53 ページの「自分の最下位ラベルでワークスペースを追加する方法」を参照してください。

2. 移動元ファイルのラベルを確認します。

   詳細は、55 ページの「ファイルのラベルを判断する」を参照してください。

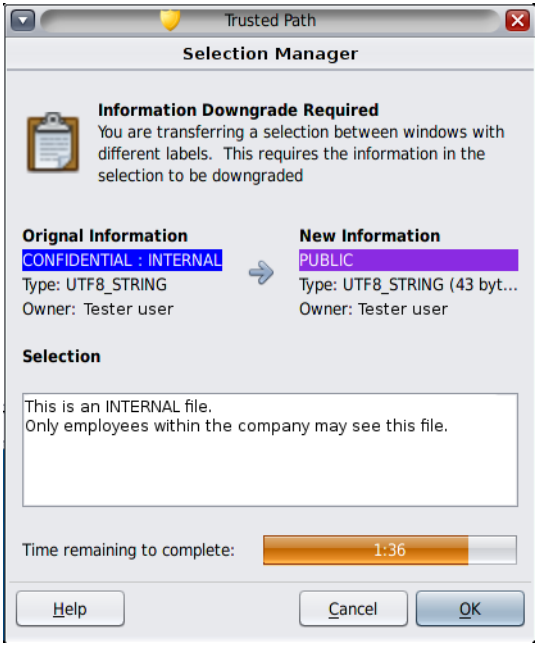
3 ソース情報が表示されたウィンドウを、ターゲットラベルのワークスペースに移動します。

詳細は、54 ページの「ウィンドウを別のワークスペースに移動する」を参照してください。

4 移動する情報を強調表示し、選択したものをターゲットウィンドウに貼り付けます。

選択マネージャーの確認ダイアログボックスが表示されます。

図 3–5 選択マネージャーの確認ダイアログボックス



5 選択マネージャーの確認ダイアログボックスを確認し、トランザクションを確定するか取り消します。

このダイアログボックスには、次の情報が表示されます。

- トランザクションの確認が必要な理由。
- ソースファイルのラベルと所有者。
- ターゲットファイルのラベルと所有者。
- 転送用に選択されたデータの種類、ターゲットファイルの種類、およびデータのサイズ (バイト単位)。デフォルトでは、選択されたデータはテキスト形式で表示されます。

- トランザクションを完了するための残り時間。時間の長さおよびタイマーの使用は、サイトの構成により異なります。

▼ マルチレベルデータセットのデータをアップグレードする方法

Trusted Extensions のマルチレベルデータセットを使用すると、ファイルの再ラベル付けタスクが簡単になります。マルチレベルデータセットの詳細については、『Trusted Extensions 構成と管理』の「ファイルのラベル変更に使用されるマルチレベルのデータセット」を参照してください。

始める前に ファイルに再ラベル付けする権限が必要です。1 つのラベルがその他のラベルより優位にある、2 つ以上のラベルで操作することができます。

マルチレベルデータセットはラベル付きゾーンの少なくとも 1 つにマウントされ、そのデータセットがマウントされるすべてのゾーンでマウント名は同じ (`/multi` など) になります。

再ラベル付けを許可するには、管理者が次のタスクを完了している必要があります。

- 『Trusted Extensions 構成と管理』の「マルチレベルのデータセットを作成および共有する方法」
- 『Trusted Extensions 構成と管理』の「ラベル付きゾーンからファイルに再ラベル付けできるようにする」
- 『Trusted Extensions 構成と管理』の「ユーザーによるデータのセキュリティーレベルの変更を有効にする」

マルチレベルセッションにログインしている必要があります。

1. より高位のラベルでワークスペースを作成します。

   たとえば、ファイルを `PUBLIC` から `INTERNAL` にアップグレードするには、`INTERNAL` ラベルでワークスペースを作成します。

   詳細については、53 ページの「自分の最下位ラベルでワークスペースを追加する方法」を参照してください。

2. 端末ウィンドウを開き、アップグレードするファイルが入っているディレクトリの内容を一覧表示します。

   この例では、ファイル名は `temppub1` です。

```
$ ls /multi/public
temppub1
```

3 ファイルに再ラベル付けします。

```
$ setlabel "cnf : internal" /multi/public/temppub1
```

4 ラベルの変更を確認します。

```
$ getlabel  /multi/public/temppub1
/multi/public/temppub1: "CONFIDENTIAL : INTERNAL USE ONLY"
```

5 (省略可能) ターゲットラベルのディレクトリにファイルを移動します。

```
$ mv /multi/public/temppub1 /multi/internal/temppub1
```

▼ マルチレベルデータセットのデータをダウングレードする方法

データをダウングレードするには、まずファイルをそのターゲットディレクトリに移動してから、再ラベル付けします。詳細は、『Trusted Extensions 構成と管理』の「ファイルのラベル変更に使用されるマルチレベルのデータセット」を参照してください。

始める前に ファイルをダウングレードする権限が必要です。管理者は、ラベル付きゾーンの少なくとも 1 つにマルチレベルデータセットをマウントし、ユーザーがアクセスできるすべてのマウントで標準の名前 (`/multi` など) を使用し、そのゾーンでの再ラベル付けを許可してあります。

したがって、管理者は次のタスクを完了している必要があります。

- 『Trusted Extensions 構成と管理』の「マルチレベルのデータセットを作成および共有する方法」
- 『Trusted Extensions 構成と管理』の「ラベル付きゾーンからファイルに再ラベル付けできるようにする」
- 『Trusted Extensions 構成と管理』の「ユーザーによるデータのセキュリティーレベルの変更を有効にする」

マルチレベルセッションにログインしている必要があります。

1 元のファイルのラベルでワークスペースを作成します。

たとえば、`internal` ワークスペースを作成します。

詳細については、53 ページの「自分の最下位ラベルでワークスペースを追加する方法」を参照してください。

2 端末ウィンドウを開き、プロファイルシェルを開きます。

```
% pfbash
$
```

3 (省略可能) 元のファイルおよびそれが入っているディレクトリのラベルを確認します。

詳細は、55 ページの「ファイルのラベルを判断する」を参照してください。

注 – 元のファイルがその親ディレクトリと同じラベルの場合は、同じ場所でダウングレードすることはできません。ファイルを移動する必要があります。ファイルの移動は特権操作です。

---

4 ターゲットラベルのディレクトリに元のファイルを移動します。

```
$ mv /multi/internal-directory/file /multi/public-directory
```

5 ラベルをターゲットディレクトリのラベルに変更します。

```
$ cd /multi/public-directory
$ setlabel public file
```

6 (省略可能) ファイルに再ラベル付けされたことを確認します。

```
$ getlabel /multi/public-directory/file
/multi/public-directory/file: PUBLIC
```

PUBLIC ラベルでファイルを編集できます。

例 3–6 ディレクトリのラベルを変更する

この例では、承認されたユーザーがディレクトリに再ラベル付けします。

まず、ユーザーはディレクトリからすべてのファイルを移動または削除します。

```
$ getlabel /multi/conf
/multi/conf: CONFIDENTIAL : NEED TO KNOW
$ mv /multi/conf/* /multi/confNTK/temp
```

次に、ユーザーはディレクトリのラベルを設定し、新しいラベルを確認します。

```
$ setlabel "Confidential : Internal Use Only" /multi/conf
getlabel /multi/conf
/multi/conf: "CONFIDENTIAL : INTERNAL USE ONLY"
```

◆ ◆ ◆ 第 4 章

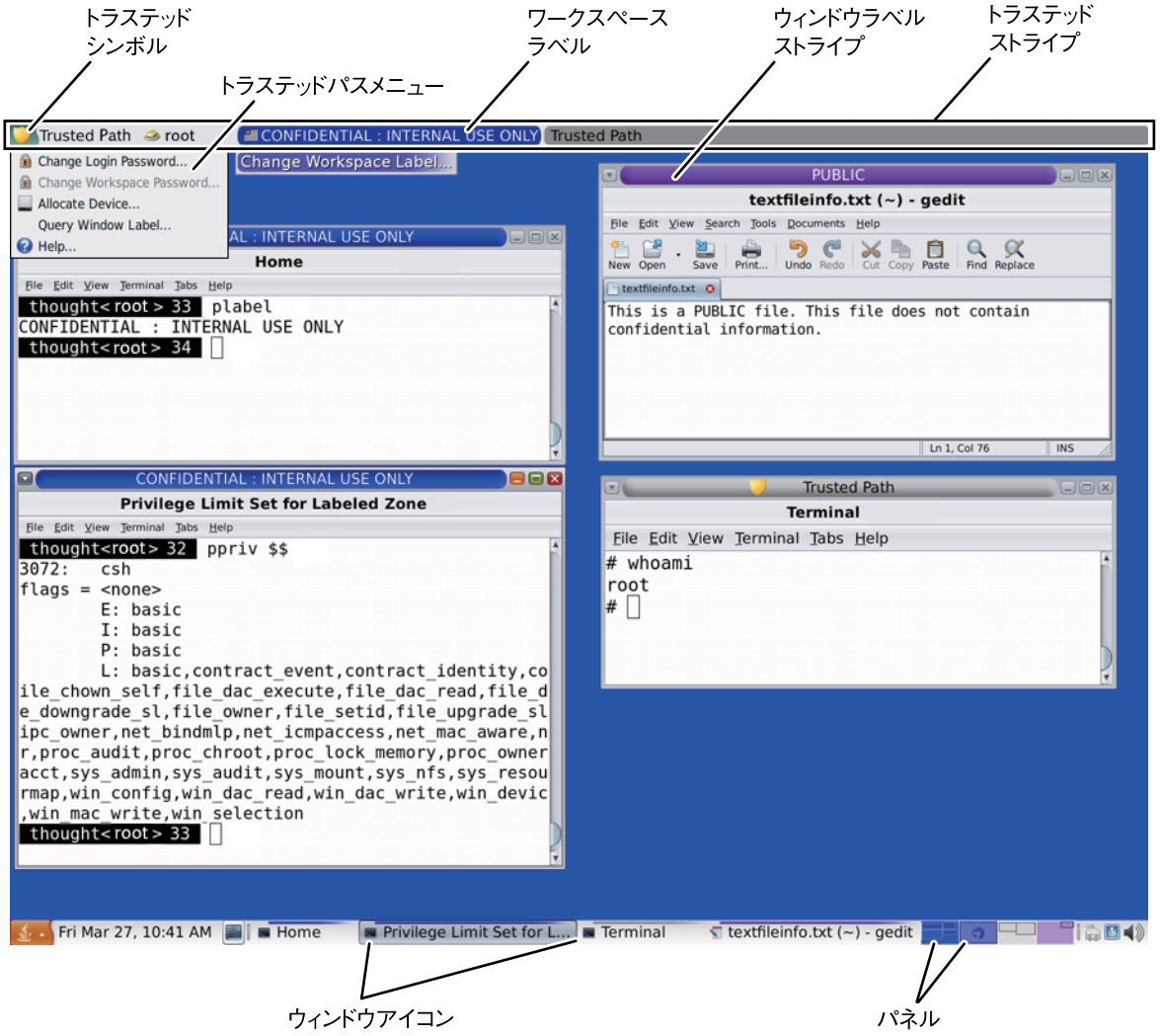
Trusted Extensions の構成要素 (リファレンス)

この章では、Trusted Extensions の主な構成要素について説明します。この章で扱う内容は、次のとおりです。

Trusted Extensions の代表的な機能

ログインプロセスが正常に完了すると、第 2 章「Trusted Extensions へのログイン (タスク)」で説明したように、Trusted Extensions 内で作業できるようになります。作業にはセキュリティー制限が適用されます。Trusted Extensions に固有の制限には、システムのラベル範囲、ユーザー認可上限、シングルレベルセッションかマルチレベルセッションかの選択などがあります。次の図が示すように、Trusted Extensions が構成されたシステムは、いくつかの特徴によって Oracle Solaris システムから区別されます。

図 4–1 Trusted Extensions マルチレベルデスクトップ



- ラベル表示 – ウィンドウ、ワークスペース、ファイル、アプリケーションのすべてにラベルがあります。実体のラベルは、ラベルストライプやその他のインジケータでデスクトップに表示されます。
- トラステッドストライプ – このストライプは特殊なグラフィカルセキュリティーメカニズムです。このストライプは各ワークスペースの画面上部に表示されます。
- ワークスペースからアプリケーションへのアクセス制限 – アカウントで許可されているアプリケーションに対してのみ、ワークスペースからアクセスできます。

- トラステッドパスメニュー – トラステッドシンボルからメニューにアクセスできます。

Trusted Extensions デスクトップ上のラベル

18 ページの「必須アクセス制御」で説明したように、Trusted Extensions ではすべてのアプリケーションとファイルにラベルがあります。Trusted Extensions では、次の場所にラベルが表示されます。

- ウィンドウのラベルストライプ: ウィンドウのタイトルバーの上
- ラベルカラーストライプ: ウィンドウリスト内のウィンドウアイコンの上
- ウィンドウラベルインジケータ: トラステッドストライプ内
- ウィンドウラベル照会インジケータ: ポインタの場所によって指定される、ウィンドウまたはウィンドウアイコンのラベルを表示するトラステッドパスメニューから

さらに、パネルの色はワークスペースのラベルを示します。

図 4–2 各種ラベルのワークスペースを示すパネル

図 4–1 は、Trusted Extensions デスクトップでラベルがどのように表示されるかを示しています。また、「ウィンドウのラベルを照会」メニュー項目を使用してウィンドウのラベルを表示することもできます。図については、図 3–2 を参照してください。

トラステッドストライプ

トラステッドストライプは画面上部に表示されます。

図 4–3 デスクトップ上のトラステッドストライプ

トラステッドストライプの目的は、正規の Trusted Extensions セッションにいることを視覚的に確認できるようにすることです。ユーザーとトラステッドコンピューティングベース (TCB) の対話中は、そのことがストライプに表示されます。また、現在のワークスペースおよび現在のウィンドウのラベルも表示します。

トラステッドストライプは、ほかのウィンドウやダイアログボックスが原因で位置が変わったり背面に隠れたりすることはありません。

トラステッドストライプには次の構成要素があります。

- トラステッドシンボル – 画面のフォーカスがセキュリティーに関連しているときに表示されます
- ウィンドウラベル – 画面のフォーカスがセキュリティーに関連していないときは、アクティブウィンドウのラベルが表示されます
- 役割マーカー – アカウントが役割アカウントの場合は、トラステッドシンボルの右側、アカウント名の前に、帽子アイコンが表示されます
- 現在のアカウント名 – トラステッドシンボルの右側に、ワークスペースの新しいプロセスの所有者の名前が表示されます
- ラベル付きウィンドウ – ワークスペースのすべてのウィンドウのラベルが表示されます

トラステッドシンボル

TCB のいずれかの部分にアクセスすると、トラステッドストライプ領域の左側にトラステッドシンボルが必ず表示されます。

ポインタが置かれているウィンドウや画面領域が、セキュリティーに影響を与えるものでないときは、トラステッドシンボルは表示されません。トラステッドシンボルは偽造できません。トラステッドシンボルが表示されている場合は、TCB と安全に対話していることを確認できます。

注意 – ワークスペースにトラステッドストライプが表示されていない場合は、セキュリティー管理者に連絡してください。システムに重大な問題が起きている可能性があります。

ログイン時および画面ロック時は、トラステッドストライプは表示されないはずです。トラステッドストライプが表示されている場合は、ただちに管理者に連絡してください。

ウィンドウラベルインジケータ

「ウィンドウラベル」インジケータには、アクティブなウィンドウのラベルが表示されます。この表示は、マルチレベルセッションにおいて、同じワークスペース内

にある異なるラベルのウィンドウを識別するのに役立ちます。また、インジケータは TCB と対話中であることも示します。たとえば、パスワードを変更するときは、「トラステッドパス」という表示がトラステッドストライプに表示されます。

Trusted Extensions でのデバイスのセキュリティー

Trusted Extensions のデフォルトでは、デバイスはデバイス割り当て要求によって保護されます。ユーザーは、デバイスを割り当てるための明示的認可を与えられないかぎりデバイスを使用できず、割り当てられたデバイスをほかのユーザーが使用することもできません。あるラベルで使用中のデバイスは、最初のラベルから割り当て解除されて次のラベルに割り当てられるまでは別のラベルで使用できません。

デバイスを使用するには、49 ページの「Trusted Extensions でデバイスを割り当てる」を参照してください。

Trusted Extensions のファイルとアプリケーション

Trusted Extensions のすべてのアプリケーションには、ラベルで示された機密レベルがあります。アプリケーションは、任意のデータトランザクションにおける動作の「サブジェクト」です。サブジェクトは、アクセス対象となる「オブジェクト」よりも優位である必要があります。オブジェクトはファイルの場合もあれば、ほかのプロセスの場合もあります。アプリケーションのラベル情報は、ウィンドウのラベルストライプに表示されます。ラベルが表示されるのは、ウィンドウが開いているときと、アイコン化されているときです。また、ポインタがアプリケーションのウィンドウ内にあるときは、トラステッドストライプにもアプリケーションのラベルが表示されます。

Trusted Extensions では、ファイルはデータトランザクションにおけるオブジェクトです。ファイルには、そのファイルのラベルよりも優位にあるラベルを持つアプリケーションによってのみアクセスできます。ファイルは、そのファイルと同じラベルを持つウィンドウに表示することができます。

一部のアプリケーションでは、初期設定ファイルを使用してユーザーの環境を構成します。ホームディレクトリにある 2 つの特殊ファイルを使用すると、初期設定ファイルにあらゆるラベルでアクセスできます。これらのファイルは、あるラベルのアプリケーションで、別のラベルのディレクトリで生成された初期設定ファイルを使用できるようにします。2 つの特殊ファイルとは、`.copy_files` と `.link_files` です。

`.copy_files` ファイル

`.copy_files` ファイルにファイル名が格納されていると、より高いラベルを持つワークスペースにはじめて移動するときに、そのファイルがコピーされます。この

ファイルは、ユーザーの最下位ラベルで、ホームディレクトリに格納されます。このファイルは、常に特定の名前でホームディレクトリ内のファイルに書き込みを行うアプリケーションがある場合に便利です。`.copy_files` ファイルを使用すると、アプリケーションで該当のファイルをあらゆるラベルで更新できるように指定できます。

`.link_files` ファイル

`.link_files` ファイルには、より高いラベルを持つワークスペースに最初に移動するときにリンクされるファイルの名前が格納されます。このファイルは、ユーザーの最下位ラベルで、ホームディレクトリに格納されます。`.link_files` ファイルは、特定のファイルを複数のラベルで使用できるようにする必要があるものの、その内容がすべてのラベルで同一でなければならないときに便利です。

Oracle Solaris OS のパスワードのセキュリティー

パスワードを頻繁に変更すると、侵入者が違法に入手したパスワードを利用する機会を減らすことができます。そのため、サイトのセキュリティーポリシーで、パスワードの定期的な変更を必須とする場合があります。Oracle Solaris OS では、パスワードの内容に関する要件を設定したり、パスワードの再設定の要件を強制したりできます。再設定の要件にできるものは次のとおりです。

- パスワード変更までの最小日数 – 設定した日数内は、そのユーザーを含め、だれもパスワードを変更できないようにします。
- パスワード変更までの最大日数 – 設定した日数が過ぎたらパスワードの変更を要求します。
- 非使用期間の最大日数 – 設定した非使用日数を過ぎてもパスワードが変更されなかった場合に、そのユーザーのアカウントをロックします。
- 有効期限 – 指定日までにパスワードを変更するよう要求します。

前述のオプションのいずれかを管理者が設定している場合は、パスワードを変更するように警告する電子メールメッセージが、期日前に送信されます。

パスワードに内容の基準を設定できます。Oracle Solaris OS のパスワードは、少なくとも次の条件を満たす必要があります。

- パスワードの長さは 8 文字以上にする。
- パスワードには、最低 2 個のアルファベットと、最低 1 個の数字または特殊文字を使用する。
- 新しいパスワードは以前と違うものにする。以前のパスワードの文字を逆順に並べたり、語順の何文字かを語尾に移動したりして使用することはできません。この比較では、大文字と小文字は同じものとみなされます。

- 新しいパスワードには、以前のパスワードで使用されていなかった文字を 3 個以上含める。この比較では、大文字と小文字は同じものとみなされます。
- パスワードは推測されにくいものにする。一般的な語句や固有名詞を使わないでください。アカウントに侵入しようとするプログラムや個人は、複数のリストを使ってユーザーのパスワードを推測しようとします。

パスワードは、トラステッドメニューの「パスワード変更」メニュー項目を使用して変更できます。手順については、47 ページの「Trusted Extensions でパスワードを変更する」を参照してください。

Trusted Extensions のワークスペースのセキュリティー

Trusted Extensions では、ワークスペースとデスクトップアプリケーションはラベルを認識します。アプリケーションは現在のワークスペースのラベルで動作し、アプリケーションを開いたプロセスのラベルの情報だけを表示します。

トラステッドデスクトップのセキュリティー機能の動作と場所は次のとおりです。

- トラステッドパスメニューはトラステッドストライプから使用できます。
- ウィンドウの上にマウスを移動すると、パネル上のタスクリストにあるウィンドウのラベル名がツールチップに表示されます。同様に、スイッチ領域にあるワークスペースのラベル名もツールチップに表示されます。
- 役割を変更するには、トラステッドストライプ内のアカウント名をクリックし、役割を選択します。
- 特定のラベルにワークスペースを追加するには、既存のワークスペースを選択してそのラベルを変更します。
- デスクトップは、それぞれのワークスペースが作業中のワークスペースのラベルの色を反映するように構成されます。下部ストライプのパネルにもラベルの色が表示されます。

用語集

Trusted GNOME セッションマネージャー、ウィンドウマネージャーなどさまざまなデスクトップツールが含まれるラベル付きのグラフィカルなデスクトップ。デスクトップは完全にアクセス可能です。

アカウントラベル範囲 Trusted Extensions が構成されたシステムで作業するために、セキュリティー管理者によってユーザーまたは役割に割り当てられたラベルのセット。ユーザー認可上限によって上限が定義され、ユーザーの最下位ラベルによって下限が定義されます。このセットには、適格な形式のラベルだけが含まれます。

アクセス権 ほとんどのコンピュータシステムで利用されているセキュリティー保護機能。ファイルやディレクトリの読み取り、書き込み、実行、または名前の表示を行う権利をユーザーに与えます。任意アクセス制御 (DAC)および必須アクセス制御 (MAC)も参照してください。

アクセス権 (アクセス権ビット) ファイルやディレクトリ (フォルダ) に対する読み取り、書き込み、実行を許可されているユーザーを示す一連のコード。ユーザーは、所有者、グループ (所有者のグループ)、その他 (残るすべてのユーザー) に分類されます。読み取り権 (*r* で示される) は、ユーザーに対してファイルの内容の読み取り、またはディレクトリ (フォルダ) 内のファイルの一覧表示を許可します。書き込み権 (*w*) は、ファイルの変更、またはフォルダ内のファイルの追加や削除を許可します。実行権 (*e*) は、実行可能ファイルの実行を許可します。または、ディレクトリ内のファイルの読み取りや検索を許可します。UNIX アクセス権またはアクセス権ビットとも呼ばれます。

アクセス制御リスト **(ACL)** Oracle Solaris OS のセキュリティー機能。 特定のユーザーやグループに適用するアクセス権指定リスト (ACL エントリ) を使用できるように、任意アクセス制御 (DAC)を拡張します。標準的な UNIX のアクセス権 (アクセス権ビット)よりもきめの細かい制御が可能です。

一般ユーザー システムの標準的なセキュリティーポリシーに反する処理を実行できる特別な承認を 1 つも持たないユーザー。通常は一般ユーザーが管理的な役割になることはできません。

オブジェクト データを格納したり、受け取ったりする受動的な実体であり、データファイルやディレクトリ、プリンタなどのデバイスを指します。オブジェクトはサブジェクトの作用を受けます。プロセスにシグナルを送る場合など、プロセスがオブジェクトになる場合もあります。

オペレータ システムのバックアップの責任を負う 1 人以上のユーザーに割り当てられる役割。

下位読み取り
: サブジェクトが、オブジェクトよりも優位なラベルを持つときに、そのオブジェクトを表示できる能力。一般に、セキュリティーポリシーでは下位読み取りが許可されます。たとえば、Secret で実行されるテキストエディタプログラムで Unclassified データを読み取ることができます。必須アクセス制御 (MAC)も参照してください。

拡張構成
: セキュリティーポリシーに違反する変更を行なったために、もはや評価可能な構成ではなくなったコンピュータシステム。

格付け
: 認可上限またはラベルのコンポーネント。格付けは、TOP SECRET や UNCLASSIFIED など、セキュリティーの階層レベルを示します。

監査
: Oracle Solaris OS のセキュリティー機能。 ユーザーの活動などシステム上のイベントを取り込み、その情報を「監査証跡」と呼ばれるファイルのセットに格納するプロセス。監査によって、サイトのセキュリティーポリシーを満たすためのシステムアクティビティーレポートが作成されます。

監査 ID (AUID)
: Oracle Solaris OS のセキュリティー機能。 ログインユーザーを表す ID。ユーザーが役割になっても変わらないことから、監査の目的でユーザーを識別するために使用されます。監査 ID は、ユーザーが実効 UID、実効 GID を取得した場合でも、常に監査の目的でそのユーザーを表します。ユーザー ID (UID)も参照してください。

完全な優位
: 優位なラベルを参照してください。

管理ラベル
: 管理ファイル専用の特別なラベルで、ADMIN_LOW と ADMIN_HIGH の 2 種類があります。ADMIN_LOW はシステム内の最下位のラベルであり、コンパートメントを持ちません。システム内のほかのすべてのラベルは、このラベルよりも完全に優位です。ADMIN_LOW の情報は、すべてのユーザーが読み取れますが、書き込みは ADMIN_LOW ラベルで作業中の役割のユーザーしか行えません。ADMIN_HIGH はシステム内の最高位のラベルであり、すべてのコンパートメントを持ちます。このラベルは、システム内のほかのすべてのラベルよりも完全に優位です。ADMIN_HIGH の情報は、ADMIN_HIGH で作業する役割のユーザーだけが読み取れます。管理ラベルは、役割およびシステムのラベルまたは認可上限として使用されます。優位なラベルも参照してください。

機密ラベル
: ラベルを参照してください。

グループ ID (GID)
: Oracle Solaris OS のセキュリティー機能。 GID は、共通のアクセス権を持つユーザーのグループを識別する整数です。任意アクセス制御 (DAC)も参照してください。

ゲートウェイ
: 複数のネットワークインタフェースを持つホスト。複数のネットワークの接続に使用されます。ゲートウェイが Trusted Extensions ホストである場合は、特定のラベルに対するトラフィックを制限できます。

権利プロファイル
: Oracle Solaris OS のセキュリティー機能。 権利プロファイルによって、サイトのセキュリティー管理者は、コマンドをセキュリティー属性でまとめることができます。ユーザーの承認や特権などの属性によって、コマンドが成功できるようになります。通常、1 つの権利プロファイルには、相互に関連するタスクが含まれます。プロファイルはユーザーと役割に割り当てることができます。

降格されたラベル
: 以前の値よりも優位でない値に変更された、オブジェクトのラベル。

コンパートメント
: ラベルの非階層コンポーネントで、格付けとともに使用して認可上限やラベルを形成します。コンパートメントは、エンジニアリング部門や学際的プロジェクトチームなど、その情報にアクセスする必要があると考えられるユーザーの集団を表すために使われます。

コンパートメントモードワークステーション (CMW)
: (米国国防総省の) 国防情報局 (DIA) のドキュメント DDS-2600-5502-87、『Security Requirements for System High and Compartmented Mode Workstations』に記述された、信頼できるワークステーションに関する政府の要件を満たすコンピューティングシステム。具体的には、UNIX ワークステーション用の、X ウィンドウシステムをベースにした信頼性の高いオペレーティング環境を定義します。

最下位ラベル
: ユーザーが作業できる一連のラベルの下限としてユーザーに割り当てられるラベル。ユーザーが Trusted Extensions のセッションをはじめて開始したときは、最下位ラベルがユーザーのデフォルトラベルになります。ユーザーはログイン時に、別のラベルを初期ラベルとして選択できます。

  最下位ラベルは、管理者以外のユーザーに許可されるもっとも下位のラベルでもあります。セキュリティー管理者によって割り当てられ、ユーザー認可範囲の下限を定義します。

最少特権
: 最少特権の原則を参照してください。

最少特権の原則
: ジョブの遂行に必要な機能だけにユーザーを制限するセキュリティーの原則。Oracle Solaris OS では、必要に応じてプログラムに対して特権を有効にすることによってこの原則が適用されます。特権は、特定の目的のためだけに必要に応じて有効になります。

サブジェクト
: 能動的な実体であり、通常はユーザーまたは役割の代わりに実行されるプロセスを指します。サブジェクトによって情報がオブジェクト間を移動したり、システムの状態が変更されたりします。

システム管理者
: Oracle Solaris OS のセキュリティー機能。 システム管理者の役割は、ユーザーアカウントのセキュリティーに関係しない部分の設定など、標準のシステム管理タスクを実行する 1 人以上のユーザーに割り当てられます。セキュリティー管理者も参照してください。

システム認可範囲
: サイトで有効なすべてのラベルのセット。この中には、サイトのセキュリティー管理者とシステム管理者が使用できる管理ラベルが含まれます。システム認可範囲は、ラベルエンコーディングファイルに定義されます。

実効 UID、実効 GID
: Oracle Solaris OS のセキュリティー機能。 特定のプログラム、またはプログラムのオプションを実行するために、必要に応じて実際の ID にオーバーライドして有効になる ID。特定のユーザーがコマンドやアクションを実行しなければならない場合 (その多くはコマンドを root として実行しなければならない場合) に、セキュリティー管理者が権利プロファイルのコマンドまたはアクションに実効 UID を割り当てます。実効グループ ID の使用も、これと同様です。ただし、`setuid` コマンドは特権を必要とするため、従来の UNIX システムのようには機能しないことがあります。

昇格されたラベル
: 以前のラベルの値よりも優位な値に変更された、オブジェクトのラベル 。

承認
: Oracle Solaris OS のセキュリティー機能。セキュリティーポリシーによって禁止されているアクションを実行するために、ユーザーにアクセス権を与えること。承認は、セキュリティー管理者が権利プロファイルに割り当てます。権利プロファイルはその後、ユーザーアカウントまたは役割アカウントに割り当てられます。コマンドやアクションの中には、ユーザーが必要な承認を持っていないかぎり十分に機能しないものもあります。特権も参照してください。

シングルレベル構成
: 1 つのラベルだけで操作するように構成されたユーザーアカウント。シングルレベル構成とも呼ばれます。

スプーフィング
: システム上の情報に不正にアクセスするために、ソフトウェアプログラムを模倣すること。

セキュリティー管理者
: Trusted Extensions が構成されたシステム上で、セキュリティーポリシーを定義して実行する責任を負う 1 人以上のユーザーに割り当てられる役割。セキュリティー管理者は、システム認可範囲内のどのラベルでも作業することができ、場合によってはサイトのすべての情報に対してアクセスできます。すべてのユーザーおよび装置のセキュリティー属性は、セキュリティー管理者によって構成されます。ラベルエンコーディングファイルも参照してください。

セキュリティー属性
: Oracle Solaris OS のセキュリティー機能。プロセス、ゾーン、ユーザー、デバイスなどの実体の、セキュリティーに関連するプロパティーを指します。セキュリティー属性には、ユーザー ID (UID)やグループ ID (GID)などの識別値が含まれます。Trusted Extensions 固有の属性には、ラベルやラベル範囲などがあります。ただし、実体の種類により、それぞれのセキュリティー属性は異なります。

セキュリティーポリシー
: 情報がだれによってどのようにアクセスされるのかを定義する DAC、MAC、およびラベルの規則のセット。顧客のサイトでは、そのサイトで処理される情報の機密度を定義する一連の規則を指します。ポリシーには、承認されていないアクセスから情報を保護するために使われる手段が含まれます。

セッション
: Trusted Extensions ホストにログインしてからログアウトするまでの時間。Trusted Extensions のすべてのセッションにはトラステッドストライプが表示され、模倣されたシステムによってユーザーがスプーフィングされていないことを確認します。

セッション認可上限
: ログイン時に設定され、Trusted Extensions セッションのラベルの上限を定義する認可上限。セッション認可上限の設定を許可されているユーザーは、自分のアカウントラベル範囲内であれば任意の値を指定できます。ユーザーのアカウントが強制シングルレベルのセッションに構成されている場合には、セッション認可上限はセキュリティー管理者が指定したデフォルトの値に設定されます。認可上限も参照してください。

セッション範囲
: Trusted Extensions セッション中にユーザーが使用できるラベルのセット。セッション範囲は、ユーザーのセッション認可上限によって定義される上限から、最下位ラベルによって定義される下限までとなります。

選択マネージャー
: Trusted Extensions のトラステッドアプリケーションの 1 つ。この GUI は、承認されているユーザーが情報を昇格または降格しようとしたときに表示されます。

代替メカニズム
: `tnrhtp` データベースの IP アドレスを指定するためのショートカット手段。IPv4 のアドレスでは、`0` がサブネットのワイルドカードとして認識されます。

適格な形式のラベル　ラベルエンコーディングファイルに定義された適用可能なすべての規則によって許可されているため、範囲に追加できるラベル。

デバイス　割り当て可能なデバイスを参照してください。

デバイスの割り当て　Oracle Solaris OS のセキュリティー機能。割り当て可能なデバイス上の情報を、そのデバイスを割り当てたユーザー以外がアクセスできないように保護するメカニズム。デバイスの割り当てが解除されると、そのデバイスに別のユーザーがふたたびアクセスできるようになる前に、デバイス上の情報を消去するための clean スクリプトが実行されます。Trusted Extensions では、デバイスの割り当てはデバイスマネージャーによって処理されます。

デバイスマネージャー　Trusted Extensions のトラステッドアプリケーションの 1 つ。デバイスの構成、デバイスの割り当てまたは割り当て解除にはこの GUI が使用されます。デバイスの構成には、デバイスへの承認条件の追加などがあります。

特権　Oracle Solaris OS のセキュリティー機能。セキュリティー管理者によってプログラムに与えられるアクセス権。特権は、セキュリティーポリシーのいくつかの側面をオーバーライドするために必要となることがあります。承認も参照してください。

特権プロセス　Oracle Solaris OS のセキュリティー機能。 特権プロセスは割り当てられた特権で実行されます。

トラステッドアプリケーション　1 つまたは複数の特権が割り当てられたアプリケーション。

トラステッド機能管理　従来の UNIX システムのシステム管理に関連するすべての作業に、分散型システムおよびシステムに格納されたデータのセキュリティー維持に必要なすべての管理作業を追加したもの。

トラステッドコンピューティングベース **(TCB)**　Trusted Extensions が構成されたシステムの、セキュリティーに影響を与える部分。TCB にはソフトウェア、ハードウェア、ファームウェア、ドキュメント、管理手順などが含まれます。セキュリティー関連のファイルにアクセス可能なユーティリティープログラムやアプリケーションプログラムは、いずれもトラステッドコンピューティングベースの一部です。

トラステッドシンボル　トラステッドストライプ領域の左側に表示されるシンボル。ユーザーがトラステッドコンピューティングベース (TCB)のどこかの部分にアクセスしているときに常に表示されます。

トラステッドストライプ　画面の予約領域に表示される、画面幅いっぱいの長方形のグラフィック。トラステッドストライプは Trusted Extensions のすべてのセッションで表示され、有効な Trusted Extensions セッションであることを確認します。トラステッドストライプには 2 つのコンポーネントがあります。1 つ目は必須のトラステッドシンボルで、トラステッドコンピューティングベース (TCB) と対話中であることを示します。2 つ目はラベルで、現在のウィンドウやワークスペースのラベルを示します。

トラステッドパス　トラステッドコンピューティングベース (TCB)との対話が許可されているアクションやコマンドにアクセスするためのメカニズム。トラステッドパスメニュー、トラステッドシンボル、トラステッドストライプも参照してください。

トラステッドパスメニュー	フロントパネルのスイッチ領域でマウスボタン 3 を押すと表示される Trusted Extensions 操作のメニュー。メニューの選択肢は、3 種類に分類されます。ワークスペース用、役割変更用、およびセキュリティー関連タスク用です。
任意アクセス制御 (DAC)	ファイルやディレクトリの所有者が、ほかのユーザーに対してアクセスを許可または拒否できるようにするアクセス制御メカニズム。所有者は、「所有者」、所有者が属する「ユーザーグループ」、それ以外のすべての特定されないユーザーを指す「その他」と呼ばれる分類に対し、読み取り、書き込み、および実行のアクセス権 (アクセス権ビット)を割り当てます。 所有者は、アクセス制御リスト (ACL)も指定できます。ACL を使用すると、所有者は、特定のユーザーやグループにアクセス権を追加で割り当てることができます。必須アクセス制御 (MAC)と対照的に使用する用語です。
認可上限	ラベルの上限を定義するラベル範囲。認可上限には、1 つの格付けと任意の数のコンパートメントという 2 つのコンポーネントがあります。認可上限は適格な形式のラベルである必要はありません。理論上の範囲を定義するものであり、必ずしも実際のラベルでなくてもかまいません。ユーザー認可上限、セッション認可上限、およびラベルエンコーディングファイルも参照してください。
認可範囲	ユーザーまたはリソースのクラスに対して認可されたラベルのセット。システム認可範囲、ユーザー認可範囲、ラベルエンコーディングファイル、およびネットワーク認可範囲も参照してください。
ネットワーク認可範囲	Trusted Extensions ホストがネットワーク上で通信を許可されているラベルのセット。4 つの異なるラベルのリストを使用できます。
必須アクセス制御 (MAC)	システムが実施するアクセス制御メカニズムで、認可上限とラベルを使用してセキュリティーポリシーが実施されます。認可上限とラベルはセキュリティーレベルです。MAC は、ユーザーが実行するプログラムを、そのユーザーがセッションで作業するために選択したセキュリティーレベルに対応付けます。その後、それと同等または下位レベルの情報、プログラム、およびデバイスに対してのみアクセスを許可します。さらに、対応付けたレベルよりも下位のファイルにユーザーが書き込むことを禁止します。特別な承認または特権がないかぎり、MAC を無効にすることはできません。任意アクセス制御 (DAC) と対照的に使用する用語です。
秘密チャネル	通信チャネル (経路) の 1 つで、通常はデータ通信には使用されません。このチャネルを介することで、プロセスが間接的に情報を転送することになり、結果としてセキュリティーポリシーが守られません。
評価可能な構成	政府のセキュリティー要件が規定された標準を満たすコンピュータシステム。拡張構成も参照してください。
プロセス	実行中のプログラム。Trusted Extensions のプロセスには、ユーザー ID (UID)、グループ ID (GID)、ユーザーの監査 ID (AUID)、特権など、Oracle Solaris のセキュリティー属性があります。Trusted Extensions では、すべてのプロセスにラベルが追加されます。
プロファイル	権利プロファイルを参照してください。
プロファイルシェル	Oracle Solaris OS のセキュリティー機能。 Bourne シェルの一種で、ユーザーはセキュリティー属性を持つプログラムを実行できるようになります。
ホスト	ネットワークに接続されたコンピュータ。

ホストタイプ
: ホストの格付け。格付けはネットワーク通信に使用されます。ホストタイプの定義は tnrhtp データベースに格納されます。ホストタイプによって、ネットワーク上のほかのホストとの通信に CIPSO ネットワークプロトコルを使用するかどうかが決まります。「ネットワークプロトコル」とは、通信情報をパッケージ化するための規則です。

ホストテンプレート
: Trusted Extensions ネットワークにアクセスできるホストのクラスのセキュリティー属性を定義する tnrhtp データベースのレコードの 1 つ。

無関係なラベル
: 優位なラベルを参照してください。

役割
: Oracle Solaris OS のセキュリティー機能。 役割は特別なアカウントであり、役割になったユーザーは、特定のタスクを実行するために必要なセキュリティー属性を持つ特定のアプリケーションにアクセスできるようになります。

優位なラベル
: 2 つのラベルを比較したときに、他方のラベルよりも上位または同等の格付けコンポーネントを持ち、他方のラベルのコンパートメントコンポーネントをすべて持ち合わせているラベル。これらのコンポ?ネントが同じである場合、2 つのラベルは互いに優位であり「同等」であると言います。片方のラベルが他方のラベルよりも優位であり、かつ、両方のラベルが同等でない場合は、最初のラベルが他方のラベルよりも「完全に優位」であると言います。2 つのラベルが同等でなく、どちらのラベルも優位ではない場合、これらのラベルは「無関係」です。

ユーザー **ID (UID)**
: Oracle Solaris OS のセキュリティー機能。 任意アクセス制御 (DAC)、必須アクセス制御 (MAC)、監査などを行う目的でユーザーを識別するために使用されます。アクセス権も参照してください。

ユーザー認可上限
: セキュリティー管理者が割り当てる認可上限。ユーザーのアカウントラベル範囲の上限を定義します。ユーザーの認可上限により、そのユーザーが作業できる最上位のラベルが決まります。認可上限およびセッション認可上限も参照してください。

ユーザー認可範囲
: セキュリティー管理者が特定サイトのユーザーに割り当てる可能性のあるラベルのもっとも広範なセット。ユーザー認可範囲には、管理ラベルおよび管理者だけが使用できるラベルの組み合わせは含まれません。ユーザー認可範囲は、ラベルエンコーディングファイルに定義されます。

ラベル
: 機密ラベルとも呼ばれます。ラベルは実体のセキュリティーレベルを示します。実体とはファイルやディレクトリ、プロセス、デバイス、ネットワークインタフェースなどを指します。実体のラベルは、特定のトランザクションでアクセスを許可するかどうかの決定に使用されます。ラベルには 2 つのコンポーネントがあります。セキュリティーの階層レベルを示す 1 つの格付けと、特定の格付けの実体にアクセスできるユーザーを定義する任意の数のコンパートメントです。ラベルエンコーディングファイルも参照してください。

ラベルエンコーディングファイル
: セキュリティー管理者によって管理されるファイル。エンコーディングファイルには、すべての有効な認可上限およびラベルの定義が格納されています。さらに、システム認可範囲、ユーザー認可範囲、およびサイトでの印刷のセキュリティー情報の定義にも使用されます。

ラベル付きワークスペース	ラベルに関連付けられたワークスペース。ラベル付きワークスペースでは、ワークスペースから起動したすべてのアクティビティーに、そのワークスペースのラベルが付きます。ユーザーがウィンドウを別のラベルのワークスペースに移動しても、そのウィンドウは元のラベルを保持します。トラステッドデスクトップではすべてのワークスペースにラベルが付けられます。2 つのワークスペースを同じラベルに関連付けることができます。
ラベル範囲	認可上限、つまり最上位ラベルによって上限が、最下位ラベルによって下限が定義され、適格な形式のラベルで構成されたラベルの任意のセット。ラベル範囲は必須アクセス制御 (MAC)の実施に使用されます。ラベルエンコーディングファイル、アカウントラベル範囲、認可範囲、ネットワーク認可範囲、セッション範囲、システム認可範囲、およびユーザー認可範囲も参照してください。
ラベル表示	管理ラベルを表示したり、管理ラベルを機密外の内容に置き換えるセキュリティー機能。たとえば、`ADMIN_HIGH` と `ADMIN_LOW` というラベルを公開することがセキュリティーポリシーに違反する場合に、`RESTRICTED` と `PUBLIC` というラベルを代わりに表示できます。
ラベルビルダー	Trusted Extensions のトラステッドアプリケーションの 1 つ。ユーザーはこの GUI を使用して、セッション認可上限やセッションラベルを選択できます。認可上限やラベルは、セキュリティー管理者がユーザーに割り当てたアカウントラベル範囲内にある必要があります。
ワークスペース	ラベル付きワークスペースを参照してください。
割り当て解除されたデバイス	Oracle Solaris OS のセキュリティー機能。 排他的に使用するためのユーザーへの割り当てが解除されたデバイス。デバイスの割り当ても参照してください。
割り当て可能なデバイス	Oracle Solaris OS のセキュリティー機能。 一度に 1 人のユーザーが使用でき、システムとのデータのインポートやエクスポートが可能なデバイス。どのユーザーにどの割り当て可能なデバイスへのアクセスを承認するかは、セキュリティー管理者が決定します。 割り当て可能なデバイスには、テープドライブ、フロッピーディスクドライブ、オーディオデバイス、CD-ROM デバイスなどがあります。デバイスの割り当ても参照してください。

索引

と

に

は

ひ

よ

ら

り

ろ

わ