Solaris Trusted Extensions
ユーザーズガイド

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 819–7605–14
2009 年 4 月

Copyright 2009 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. All rights reserved.

Sun Microsystems, Inc. (以下 米国 Sun Microsystems 社とします) は、本書に記述されている製品に含まれる技術に関連する知的財産権を所有します。特に、この知的財産権はひとつかそれ以上の米国における特許、あるいは米国およびその他の国において申請中の特許を含んでいることがありますが、それらに限定されるものではありません。

本製品の一部は、カリフォルニア大学からライセンスされている Berkeley BSD システムに基づいていることがあります。UNIX は、X/Open Company, Ltd. が独占的にライセンスしている米国ならびに他の国における登録商標です。フォント技術を含む第三者のソフトウェアは、著作権により保護されており、提供者からライセンスを受けているものです。

U.S. Government Rights Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

この配布には、第三者によって開発された素材を含んでいることがあります。

本製品に含まれる HG-MinchoL、HG-MinchoL-Sun、HG-PMinchoL-Sun、HG-GothicB、HG-GothicB-Sun、および HG-PGothicB-Sun は、株式会社リコーがリョービイマジクス株式会社からライセンス供与されたタイプフェースマスタをもとに作成されたものです。HeiseiMin-W3H は、株式会社リコーが財団法人日本規格協会からライセンス供与されたタイプフェースマスタをもとに作成されたものです。フォントとして無断複製することは禁止されています。

Sun、Sun Microsystems、Sun のロゴマーク、Solaris のロゴマーク、Java Coffee Cup のロゴマーク、docs.sun.com Sun Ray、 、Java および Solaris は、米国およびその他の国における米国 Sun Microsystems 社の商標、登録商標もしくは、サービスマークです。

すべての SPARC 商標は、米国 SPARC International, Inc. のライセンスを受けて使用している同社の米国およびその他の国における商標または登録商標です。SPARC 商標が付いた製品は、米国 Sun Microsystems 社が開発したアーキテクチャに基づくものです。

OPENLOOK、OpenBoot、JLE は、サン・マイクロシステムズ株式会社の登録商標です。

Wnn は、京都大学、株式会社アステック、オムロン株式会社で共同開発されたソフトウェアです。

Wnn8 は、オムロン株式会社、オムロンソフトウェア株式会社で共同開発されたソフトウェアです。Copyright(C) OMRON Co., Ltd. 1995-2000. All Rights Reserved. Copyright(C) OMRON SOFTWARE Co.,Ltd. 1995-2009 All Rights Reserved.

「ATOK for Solaris」は、株式会社ジャストシステムの著作物であり、「ATOK for Solaris」にかかる著作権、その他の権利は株式会社ジャストシステムおよび各権利者に帰属します。

「ATOK」および「推測変換」は、株式会社ジャストシステムの登録商標です。

「ATOK for Solaris」に添付するフェイスマーク辞書は、株式会社ビレッジセンターの許諾のもと、同社が発行する『インターネット・パソコン通信フェイスマークガイド』に添付のものを使用しています。

「ATOK for Solaris」に含まれる郵便番号辞書 (7 桁/5 桁) は日本郵政公社が公開したデータを元に制作された物です (一部データの加工を行なっています)。

Unicode は、Unicode, Inc. の商標です。

本書で参照されている製品やサービスに関しては、該当する会社または組織に直接お問い合わせください。

OPEN LOOK および Sun Graphical User Interface は、米国 Sun Microsystems 社が自社のユーザおよびライセンス実施権者向けに開発しました。米国 Sun Microsystems 社は、コンピュータ産業用のビジュアルまたはグラフィカル・ユーザインタフェースの概念の研究開発における米国 Xerox 社の先駆者としての成果を認めるものです。米国 Sun Microsystems 社は米国 Xerox 社から Xerox Graphical User Interface の非独占的ライセンスを取得しており、このライセンスは、OPEN LOOK のグラフィカル・ユーザインタフェースを実装するか、またはその他の方法で米国 Sun Microsystems 社との書面によるライセンス契約を遵守する、米国 Sun Microsystems 社のライセンス実施権者にも適用されます。

本書で言及されている製品や含まれている情報は、米国輸出規制法で規制されるものであり、その他の国の輸出入に関する法律の対象となることがあります。核、ミサイル、化学あるいは生物兵器、原子力の海洋輸送手段への使用は、直接および間接を問わず厳しく禁止されています。米国が禁輸の対象としている国や、限定はされませんが、取引禁止顧客や特別指定国民のリストを含む米国輸出排除リストで指定されているものへの輸出および再輸出は厳しく禁止されています。

本書は、「現状のまま」をベースとして提供され、商品性、特定目的への適合性または第三者の権利の非侵害の黙示の保証を含みそれに限定されない、明示的であるか黙示的であるかを問わない、なんらの保証も行われないものとします。

本製品が、外国為替および外国貿易管理法 (外為法) に定められる戦略物資等 (貨物または役務) に該当する場合、本製品を輸出または日本国外へ持ち出す際には、サン・マイクロシステムズ株式会社の事前の書面による承諾を得ることのほか、外為法および関連法規に基づく輸出手続き、また場合によっては、米国商務省または米国所轄官庁の許可を得ることが必要です。

原典: Solaris Trusted Extensions User's Guide

Part No: 819-0868–14

Revision A

090414@21990

目次

はじめに 11

1 Solaris Trusted Extensions ソフトウェアの紹介 15
Trusted Extensions ソフトウェアとは 15
Trusted Extensions による侵入者からの防御 16
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 16
必須アクセス制御による情報保護 16
周辺装置の保護 17
スプーフィングプログラム (騙しプログラム) の防止 17
Trusted Extensions による任意アクセス制御と必須アクセス制御 17
任意アクセス制御 18
必須アクセス制御 18
データ保護のためのユーザーの責任 24
Trusted Extensions による情報のラベル別管理 25
シングルレベルセッションとマルチレベルセッション 25
セッションの選択例 25
ラベル付きワークスペース 26
電子メールトランザクションに MAC を適用する 27
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 27
Trusted Extensions によるセキュリティー保護された管理 27
Trusted Extensions のアプリケーションへのアクセス 28
Trusted Extensions の役割による管理 29

2 Trusted Extensions へのログイン (手順) 31
Trusted Extensions のデスクトップとログイン 31
Trusted Extensions のログインプロセス 32
ログイン前のデスクトップの選択 33

ログイン時の識別と認証 33
ログイン時のセキュリティー属性の確認 33
Trusted Extensions へのログイン 34
▼ Trusted デスクトップを選択する 34
▼ システムにユーザーを識別および認証させる 34
▼ メッセージを確認し、セッションタイプを選択する 35
▼ ログインの問題のトラブルシューティング 37
Trusted Extensions に遠隔でログインする 38
▼ 遠隔 Trusted Extensions デスクトップにログインする方法 38

3 Trusted Extensions での作業 (手順) 41
Trusted Extensions のデスクトップセキュリティーの表示 41
Trusted Extensions のログアウトプロセス 42
ラベル付きシステムでの作業 42
▼ 画面をロックおよびロック解除する 42
▼ Trusted Extensions からログアウトする 43
▼ Trusted CDE でシステムをシャットダウンする 44
▼ ラベル付きワークスペースにファイルを表示する 45
▼ Trusted Extensions のマニュアルページにアクセスする 46
▼ Trusted Extensions のオンラインヘルプにアクセスする 47
▼ CDE のワークスペースメニューをカスタマイズする 48
▼ あらゆるラベルの初期設定ファイルにアクセスする 49
▼ ウィンドウラベルを対話的に表示する 50
▼ Trusted Extensions の共通デスクトップタスクを実行する 51
トラステッドアクションの実行 53
▼ Trusted Extensions でパスワードを変更する 53
▼ 別のラベルにログインする 54
▼ Trusted Extensions でデバイスを割り当てる 55
▼ Trusted Extensions でデバイスの割り当てを解除する 59
▼ Trusted Extensions で役割になる 59
▼ ワークスペースのラベルを変更する 60
▼ 特定のラベルのワークスペースを追加する 60
▼ 別のラベルのワークスペースに切り替える 62
▼ ウィンドウを別のワークスペースに移動する 62
▼ ファイルのラベルを判断する 63

▼ ラベル間でデータを移動する 64
▼ Trusted CDE でラベル間でファイルを移動する 67

4 Trusted Extensions の構成要素 (リファレンス) 71
Trusted Extensions の代表的な機能 71
Trusted Extensions デスクトップ上のラベル 73
トラステッドストライプ 73
Trusted Extensions のファイルとアプリケーション 75
`.copy_files` ファイル 76
`.link_files` ファイル 76
Solaris OS のパスワードのセキュリティー 76
フロントパネルのセキュリティー (Trusted CDE) 77
ワークスペーススイッチ領域 78
トラステッドパスメニュー 78
クロックのセキュリティー 79
カレンダのセキュリティー 79
ファイルマネージャーのセキュリティー 79
テキストエディタのセキュリティー 80
個人アプリケーションサブパネル 80
メールプログラムのセキュリティー 80
プリンタのセキュリティー 80
スタイルマネージャーのセキュリティー 81
アプリケーションマネージャーのセキュリティー 82
ごみ箱のセキュリティー 82
ワークスペースのセキュリティー (Trusted JDS) 82

用語集 85

索引 95

図目次

図 1–1 CDE での Trusted Extensions のロゴ 15
図 1–2 トラステッドシンボル 17
図 1–3 一般的な産業界向け機密ラベル 19
図 1–4 一般的な Trusted CDE のセッション 20
図 1–5 上位ラベルのゾーンからの Public 情報の表示 21
図 1–6 ワークスペーススイッチ領域 27
図 2–1 「最後のログイン (Last Login)」ダイアログボックス 36
図 2–2 ラベルビルダー 37
図 3–1 フロントパネルのスイッチ領域 43
図 3–2 ラベルの付いたファイルマネージャー 45
図 3–3 Trusted Extensions のオンラインヘルプ 47
図 3–4 「ウィンドウのラベルを照会 (Query Window Label)」の操作画面 51
図 3–5 Trusted CDE の「デバイス割り当て (Device Allocation)」アイコン 55
図 3–6 「デバイス割り当てマネージャー (Device Allocation Manager)」 56
図 3–7 異なるラベルのスイッチがあるフロントパネル 62
図 3–8 「配置するワークスペース (Occupy Workspace)」の選択 63
図 3–9 1 つのワークスペース内のラベルの異なるウィンドウ 63
図 3–10 1 つのワークスペース内のラベルの異なるアプリケーション 65
図 3–11 選択マネージャーの確認ダイアログボックス 66
図 3–12 1 つのワークスペース内のラベルの異なるファイルマネージャー 68
図 3–13 異なるラベルのファイルマネージャー間でのファイルのドラッグ 69
図 3–14 ファイルマネージャーの確認ダイアログボックス 70
図 4–1 マルチレベルの Trusted CDE デスクトップ 72
図 4–2 トラステッドストライプに表示された PUBLIC ウィンドウラベル 74
図 4–3 トラステッドストライプ内の Trusted Path 表示 75
図 4–4 トラステッドパスメニュー – 基本バージョン 78
図 4–5 トラステッドパスメニュー – ワークスペース名 (Workspace Name)バージョン 79
図 4–6 ラベル付き印刷ジョブの一般的なバナーページ 81

表目次

表 1–1 Trusted Extensions のラベル関係の例 23
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 26

はじめに

『Solaris Trusted Extensions ユーザーズガイド』は、Solaris Trusted Extensions がインストールされた Solaris™ オペレーティングシステム (Solaris OS) での操作方法を説明するマニュアルです。

対象読者

このマニュアルは、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、 Solaris OS と次のデスクトップ環境のいずれかに精通している必要があります。

- 共通デスクトップ環境 (CDE)
- オープンソースの GNOME デスクトップ
- Sun Java™ Desktop System

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。

Solaris Trusted Extensions の関連マニュアル

Solaris Trusted Extensions のマニュアルセットは、次のマニュアルで構成されています。

マニュアルのタイトル	内容	対象読者
『Solaris Trusted Extensions 移行ガイド』	旧版。Trusted Solaris 8 ソフトウェア、&Solaris 10; ソフトウェア、および Solaris Trusted Extensions ソフトウェア間の違いについて、概要を説明しています。 このリリースでは、Trusted Extensions の変更点を『Solaris OS の概要』のマニュアルで概説しています。	すべて

マニュアルのタイトル	内容	対象読者
『Solaris Trusted Extensions リファレンスマニュアル』	旧版。Solaris 10 11/06 と Solaris 10 8/07 リリースの Trusted Extensions における Solaris Trusted Extensions マニュアルページが記載されています。 このリリースでは、Trusted Extensions のマニュアルページは Solaris のマニュアルページに含まれています。	すべて
『Solaris Trusted Extensions ユーザーズガイド』	Solaris Trusted Extensions の基本的な機能について説明しています。用語集も付属しています。	エンドユーザー、管理者、開発者
『Solaris Trusted Extensions インストールと構成 (Solaris 10 11/06 および Solaris 10 8/07 リリース用)』	旧版。Solaris 10 11/06 と Solaris 10 8/07 リリースの Trusted Extensions における Solaris Trusted Extensions を計画、インストール、および構成する方法について説明しています。	管理者、開発者
『Solaris Trusted Extensions 構成ガイド』	Solaris 10 5/08 リリース以降において、Solaris Trusted Extensions を有効化、および最初に構成する方法を説明しています。旧版の『Solaris Trusted Extensions インストールと構成』に替わるものです。	管理者、開発者
『Solaris Trusted Extensions 管理の手順』	具体的な管理業務の実行方法を示します。	管理者、開発者
『Solaris Trusted Extensions 開発ガイド』	Solaris 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
『Solaris Trusted Extensions ラベルの管理』	ラベルエンコーディングファイルでのラベル構成要素の指定方法について説明します。	管理者
『コンパートメントモードワークステーションのラベル作成: エンコード形式』	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

このマニュアルの構成

第 1 章「Solaris Trusted Extensions ソフトウェアの紹介」では、Trusted Extensions が設定された Solaris システム上で実現される基本概念について説明します。

第 2 章「Trusted Extensions へのログイン (手順)」では、Trusted Extensions が設定されたシステムにアクセスする手順、およびシステムへのアクセスを終了する手順を示します。

第 3 章「Trusted Extensions での作業 (手順)」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 が設定され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。

マニュアル、サポート、およびトレーニング

Sun の Web サイトでは、次のサービスに関する情報も提供しています。

- マニュアル (http://jp.sun.com/documentation/)
- サポート (http://jp.sun.com/support/)
- トレーニング (http://jp.sun.com/training/)

表記上の規則

このマニュアルでは、次のような字体や記号を特別な意味を持つものとして使用します。

表 P–1 表記上の規則

字体または記号	意味	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。 system%
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。	system% **su** password:
AaBbCc123	変数を示します。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。
『』	参照する書名を示します。	『コードマネージャ・ユーザーズガイド』を参照してください。
「」	参照する章、節、ボタンやメニュー名、強調する単語を示します。	第 5 章「衝突の回避」を参照してください。 この操作ができるのは、「スーパーユーザー」だけです。
\	枠で囲まれたコード例で、テキストがページ行幅を超える場合に、継続を示します。	sun% **grep '^#define ** **XV_VERSION_STRING'**

コード例は次のように表示されます。

- C シェル

  ```
  machine_name% command y|n [filename]
  ```

- C シェルのスーパーユーザー

  ```
  machine_name# command y|n [filename]
  ```

- Bourne シェルおよび Korn シェル

  ```
  $ command y|n [filename]
  ```

- Bourne シェルおよび Korn シェルのスーパーユーザー

  ```
  # command y|n [filename]
  ```

[ ] は省略可能な項目を示します。上記の例は、*filename* は省略してもよいことを示しています。

| は区切り文字 (セパレータ) です。この文字で分割されている引数のうち 1 つだけを指定します。

キーボードのキー名は英文で、頭文字を大文字で示します (例: Shift キーを押します)。ただし、キーボードによっては Enter キーが Return キーの動作をします。

ダッシュ (-) は 2 つのキーを同時に押すことを示します。たとえば、Ctrl-D は Control キーを押したまま D キーを押すことを意味します。

一般規則

- このマニュアルでは、英語環境での画面イメージを使っています。このため、実際に日本語環境で表示される画面イメージとこのマニュアルで使っている画面イメージが異なる場合があります。本文中で画面イメージを説明する場合には、日本語のメニュー、ボタン名などの項目名と英語の項目名が、適宜併記されています。

◆ ◆ ◆ 第 1 章

1 Solaris Trusted Extensions ソフトウェアの紹介

この章では、Solaris™ Trusted Extensions ソフトウェアによって Solaris オペレーティングシステム (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。

- 15 ページの「Trusted Extensions ソフトウェアとは」
- 16 ページの「Trusted Extensions による侵入者からの防御」
- 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」
- 25 ページの「Trusted Extensions による情報のラベル別管理」
- 27 ページの「Trusted Extensions によるセキュリティー保護された管理」

Trusted Extensions ソフトウェアとは

次のロゴに示すように、Trusted Extensions ソフトウェアパッケージは Solaris OS に対して追加されます。

図 1–1 CDE での Trusted Extensions のロゴ

Trusted Extensions により、システムに特別なセキュリティー機能が提供されます。組織はこれらの機能を利用して、Solaris システムに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。

以降の各節では、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設定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 ソフトウェアにより、Solaris OS を侵入者から防御する機能が追加されます。Trusted Extensions は、パスワード保護などの Solaris の機能も利用します。Trusted Extensions によって、役割のパスワードを変更する GUI が追加されます。監査機能はデフォルトで有効になります。

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 ソフトウェア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、文書、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。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、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。パスワードや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模倣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、一目でわかる不正操作防止アイコンを画面の下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 1–2 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。次の図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機構です。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 保護を上書きできます。Trusted Extensions ソフトウェアでは、DAC を上書きできるのは、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、『System Administration Guide: Security Services』の第 6 章「Controlling Access to Files (Tasks)」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機構です。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 つの構成要素があります。

- 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構成要素です。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 1–3 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 1–3 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。

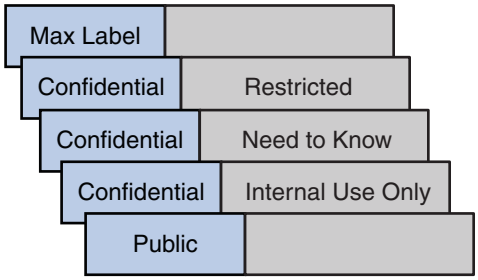


図 1–3　一般的な産業界向け機密ラベル

Trusted Extensions が設定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。

ラベルは、ウィンドウのタイトルバーと、画面の特殊なストライプである「トラステッドストライプ」に表示することができます。ラベルを表示しないことも可能です。ラベルが表示されるかどうかは、管理者によるシステムの設定に応じて決まります。図 1–4 は、ラベルを表示するように設定されたシステムでの一般的なマルチレベルの Trusted Extensions セッションを示しています。ラベルとトラステッドストライプが表示されています。

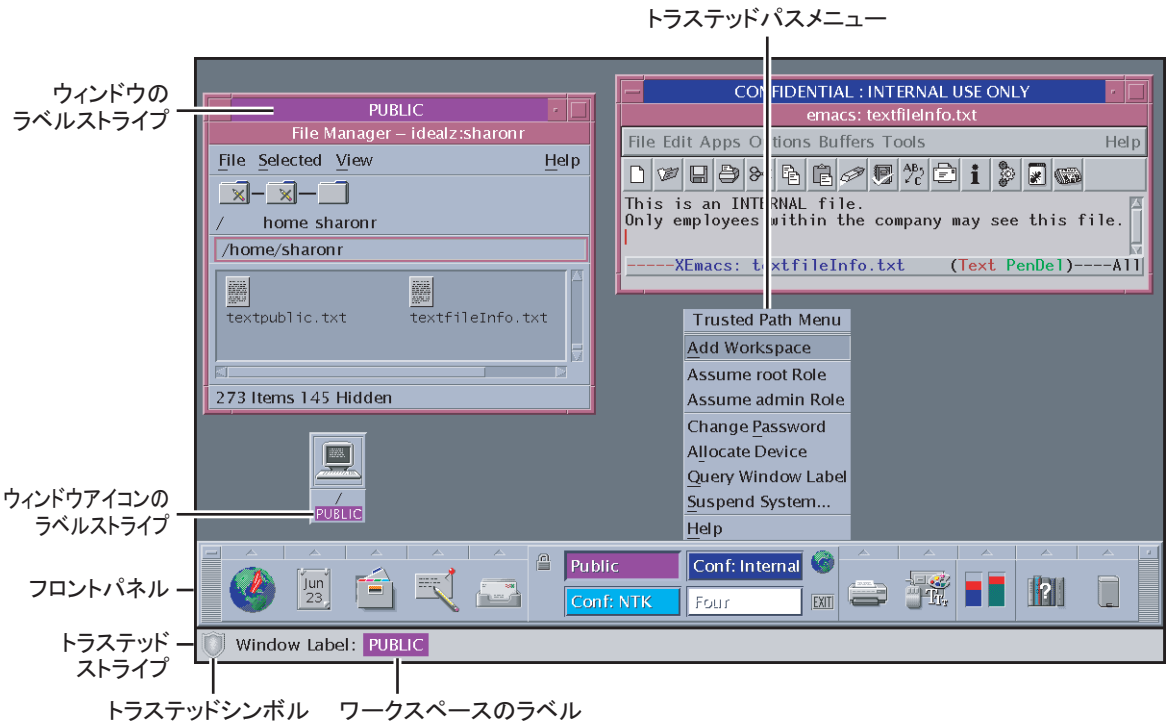


図 1–4 一般的な Trusted CDE のセッション

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します。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。

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設定して、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設定されている場合に、`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。

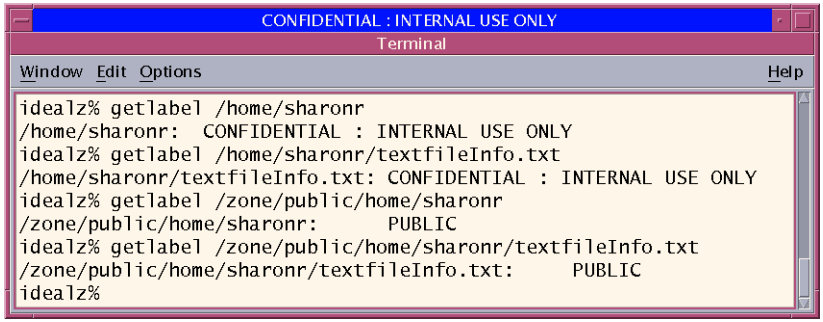


図 1–5　上位ラベルのゾーンからの Public 情報の表示

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要素が、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。

格付け	コンパートメント
Top Secret	A | B | | |

これらの構成要素から、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

表 1–1 Trusted Extensions のラベル関係の例 (続き)

	ラベル 1	関係	ラベル 2
	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、53 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、ファイルマネージャー (第 3 章「Trusted Extensions での作業 (手順)」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。

- 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。
- デスクトップでラベル付きワークスペースを提供する。
- ラベルに応じてファイルを個別ゾーンに格納する。
- 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。
- 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。

シングルラベルセッションでは、設定した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を表示する場合は、図 2–2 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

Solaris Trusted Extensions (CDE) または Trusted CDE では、Trusted Extensions のワークスペースに、Solaris OS の場合と同様に、フロントパネルの中央にあるボタンを使ってアクセスします。ただし、Trusted Extensions では、ワークスペース全体をシングルのラベルにまとめることができます。この設定は、マルチレベルセッションでの作業中にさまざまなラベルで情報が混乱しないようにする場合に非常に便利です。次の図は、4 つのスイッチがあるワークスペーススイッチ領域を示しています。それぞれのスイッチにより、異なるラベルのワークスペースが開きます。複数のワークスペースを同じラベルに割り当てることもできます。

図 1–6　ワークスペーススイッチ領域

Solaris Trusted Extensions (JDS) または Trusted JDS では、下部パネルの右側にあるボタンを使ってワークスペースにアクセスします。Trusted CDE の場合と同様に、ワークスペースをシングルのラベルに割り当てることができます。複数のワークスペースに同じラベルを割り当てることもできます。

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 JAZ ドライブ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 が設定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上書き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。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パッケージです。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。

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、特定のセキュリティー属性を持つ権利プロファイルが必要です。

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無効に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」とは特殊な型の Bourne 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 Solaris OS の機能です。詳しくは、`pfsh(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 ソフトウェアでは、複数の役割を使用して管理が行われます。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。
- 主管理者役割 – ほかの役割で可能な機能を超える特権を必要とするタスクを行います。
- セキュリティー管理者役割 – パスワードの設定、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 – ホームディレクトリの設定、バックアップの復元、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 (手順)

この章では、Solaris Trusted Extensions が設定されたシステムの 2 つの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。

- 31 ページの「Trusted Extensions のデスクトップとログイン」
- 32 ページの「Trusted Extensions のログインプロセス」
- 34 ページの「Trusted Extensions へのログイン」
- 38 ページの「Trusted Extensions に遠隔でログインする」

Trusted Extensions のデスクトップとログイン

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。

デスクトップには、共通デスクトップ環境 (CDE)および Sun Java™ Desktop System のトランステッドバージョンがあります。

- Solaris Trusted Extensions (CDE) – CDE のトラステッドバージョンです。このデスクトップは、シングルレベルセッションおよびマルチレベルセッションで有効です。CDE を使い慣れている場合、またはサイトポリシーでこのデスクトップを使用する必要がある場合は、Trusted CDE デスクトップを使用してください。
- Solaris Trusted Extensions (JDS) – Java Desktop System, Release *number* のトラステッドバージョンです。このデスクトップは、シングルレベルセッションおよびマルチレベルセッションで有効です。Trusted JDS には、画面拡大機能などのアクセシビリティー機能があります。GNOME や Java Desktop System を使い慣れている場合、またはサイトポリシーでこのデスクトップを使用する必要がある場合は、このデスクトップを使用してください。ファイルのラベルを変更する権限があり、ファイルをドラッグ & ドロップしてラベルを変更する予定の場合、このデスクトップを使用しないでください。ファイルをドラッグ & ドロップしてラベルを変更するには、Trusted CDE デスクトップを使用してください。

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 が設定されたシステムでのログインプロセスは、Solaris OS 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節で説明します。ここでは簡単な概要を示します。

1. デスクトップの選択 – Solaris OS の場合と同様に、使用するデスクトップを選択します。Trusted Extensions では、2 つのトラステッドデスクトップのいずれかを選択する必要があります。
2. 識別 – Solaris OS の場合と同様に、「ユーザー名 (Username)」フィールドにユーザー名を入力します。
3. 認証 – Solaris OS の場合と同様に、「パスワード (Password)」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。
4. メッセージの確認とセッションタイプの選択 –「最後のログイン (Last Login)」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、「シングルレベル設定」または「シングルラベル設定」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。

   ---
5. 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。サイトでリモートログインがサポートされている場合は、管理者に手順を確認してください。Solaris 10 5/09 リリースから、仮想ネットワークコンピューティング (Virtual Network Computing、VNC) が遠隔でマルチレベルデスクトップの表示に使用できます。手順については、38 ページの「Trusted Extensions に遠隔でログインする」を参照してください。

ログイン前のデスクトップの選択

Solaris ワークステーションが作業セッション中でないときは、ログイン画面が表示されています。Trusted Extensions のログイン画面は Solaris のログイン画面によく似ています。Solaris のログイン画面と同様に、「オプション (Options)」メニューからデスクトップを選択できます。

ログイン時の識別と認証

ログイン中の識別と認証は 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、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「最後のログイン (Last Login)」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、確認する状態情報が表示されます。自分が最後にシステムを使った日時など過去の情報を確認できます。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設定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手順を次に示します。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。

▼ Trusted デスクトップを選択する

1. ログイン画面で、「オプション (Options)」メニューから「Sessions」を選択します。
   - Trusted CDE を使用する場合は、「Solaris Trusted Extensions (CDE)」を選択します。
   - Trusted JDS を使用する場合は、「Solaris Trusted Extensions (JDS)」を選択します。
2. 34 ページの「システムにユーザーを識別および認証させる」に進みます。

▼ 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。
2. 間違えた場合はやり直します。
   - ユーザー名の入力をやり直すには、「やり直し (Start Over)」をクリックします。
   - ウィンドウシステムを完全に再起動するには、「オプション (Options)」メニューから「ログイン画面のリセット (Reset Login)」をクリックします。
     再起動のあと、34 ページの「Trusted デスクトップを選択する」に進みます。
3. 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。

4 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、次のようなメッセージを示すダイアログボックスが表示されます。

ログインが正しくありません。再度行って下さい。(Login incorrect; please try again.)

「了解 (OK)」をクリックしてエラーダイアログボックスを閉じます。その後、正しいパスワードを入力します。

▼ 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 「最後のログイン **(Last Login)**」ダイアログボックスで、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。

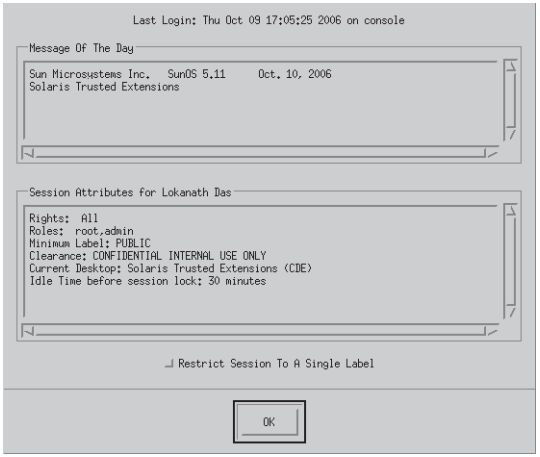


図 2–1 「最後のログイン (Last Login)」ダイアログボックス

2 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 (Message of the Day)」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。

3 セッションのセキュリティー属性を確認します。

図 2–1 に示すように、「最後のログイン (Last Login)」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。

4 (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、シングルラ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 (Restrict Session to a Single Label)」ボタンをクリックして、シングルラベルのセッションにログインします。

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。マルチラ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。

5 ラベルの選択を確定します。

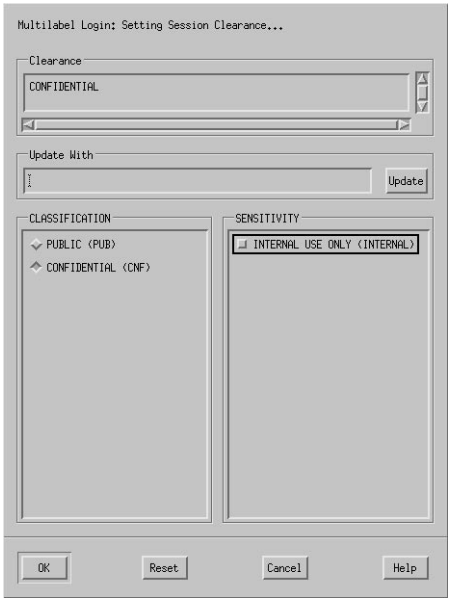


図 2–2 ラベルビルダー

- 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。
  - 現在の認可上限の選択を解除し、格付けと機密ラベルをクリックします。
  - または、「認可上限 (Clearance)」フィールドに認可上限を入力します。
  - または、「更新後のラベル (Update With)」フィールドにラベルを入力します。
- 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。
  - 現在のラベルの選択を解除し、別の格付けをクリックします。
  - または、「更新後のラベル (Update With)」フィールドにラベルを入力します。

6 「了解 (OK)」をクリックします。

選択したトラステッドデスクトップ (Trusted CDE または Trusted JDS) 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。スーパーユーザーだけが復旧ログインにアクセスできます。

     a. Solaris OS の場合と同様に、ログイン画面で「オプション (Options)」メニューから「復旧セッション (Failsafe Session)」を選択します。

     b. 要求に応じてユーザー名とパスワードを入力します。

     c. 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 に遠隔でログインする

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。自分のサイトの管理者は、サーバーとクライアントシステムで実行する Solaris Xvnc ソフトウェアを設定します。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。

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

始める前に　管理者は『Solaris Trusted Extensions 管理の手順』の「Xvnc を使用して Trusted Extensions システムに遠隔アクセスする」を完了しています。

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

Xvnc ウィンドウ内の 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 (手順)

この章では、Solaris 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。

- 41 ページの「Trusted Extensions のデスクトップセキュリティーの表示」
- 42 ページの「Trusted Extensions のログアウトプロセス」
- 42 ページの「ラベル付きシステムでの作業」
- 53 ページの「トラステッドアクションの実行」

Trusted Extensions のデスクトップセキュリティーの表示

Trusted Extensions では、Solaris Trusted Extensions (CDE) デスクトップおよび Solaris Trusted Extensions (JDS) デスクトップの 2 種類のデスクトップが提供されます。どちらのデスクトップにもラベルが付きますが、シングルラベルで作業している場合にはラベルが表示されないことがあります。ラベルを表示するように設定されたシステムの例については、図 1–4 を参照してください。

Trusted Extensions が設定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。Trusted CDE では、トラステッドストライプは画面の最下部に表示されます。Trusted JDS では、画面の最上部に表示されます。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設定されている場合、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設定されているか、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、『Solaris Trusted Extensions 管理の手順』の「デスクトップの現在のフォーカスへの制御を取り戻す」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ません。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 画面をロックするには、次の操作のいずれかを行います。

- **Trusted CDE** では、フロントパネルのワークスペーススイッチ領域にある画面ロック用のアイコンをクリックします。

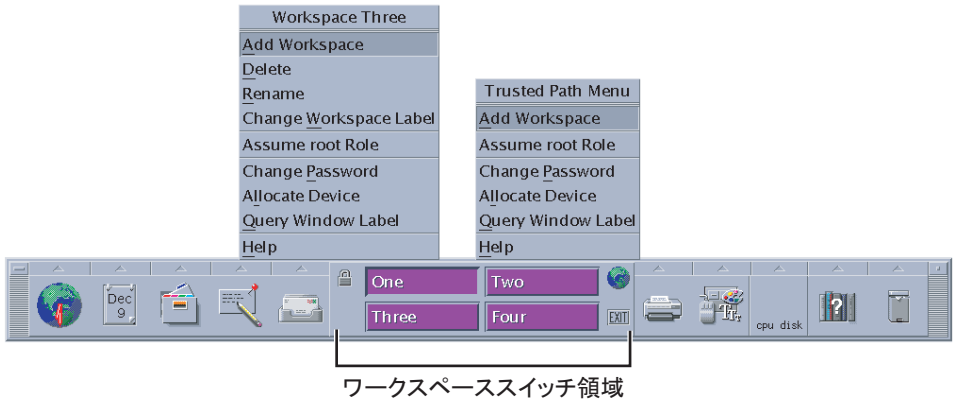


図 3–1 フロントパネルのスイッチ領域

- **Trusted JDS** では、「メイン (Main)」メニューから「画面ロック (Lock Screen)」を選択します。

  画面が消えます。この時点で再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に、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。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. マウスを動かして、「画面ロック (Lock Screen)」ダイアログボックスを表示します。

      「画面ロック (Lock Screen)」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。

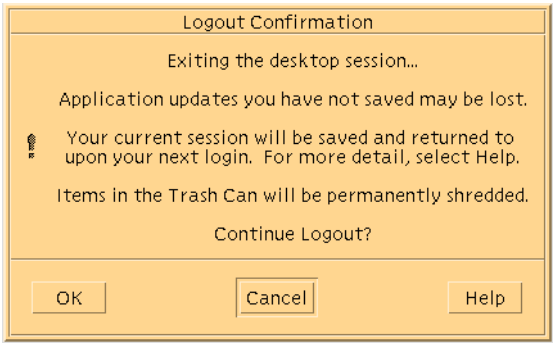
      これにより、画面をロックする前の状態のセッションに戻ります。

▼ 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 ログアウトするには、次のいずれかの操作を行います。

- **Trusted CDE** では、フロントパネルのワークスペーススイッチ領域にある「**EXIT**」アイコンをクリックします。
  フロントパネルの画面は、図 3–1 を参照してください。
  「ログアウト確認 (Logout Confirmation)」ダイアログボックスが表示されます。



- **Trusted JDS** では、「メイン **(Main)**」メニューから「*your-name* をログアウト **(Log Out your-name)**」を選択します。

2 ログアウトを続行することを確定します。

- ログアウトするには「了解 **(OK)**」をクリックします。
- それ以外の場合は「取り消し **(Cancel)**」をクリックします。

▼ Trusted CDE でシステムをシャットダウンする

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

始める前に Trusted CDE をデスクトップとして使用している必要があります。

1 ワークスペースメニューから、「システム保存停止 **(Suspend System)**」を選択します。
メニューを表示するには、背景でマウスボタン 3 をクリックしてください。

2 続行する操作を確定します。

- システムをシャットダウンするには、「停止 **(Shutdown)**」をクリックします。

- システムを省電力モードにするには、「保存停止 (Suspend)」をクリックします。
- それ以外の場合は「取り消し (Cancel)」をクリックします。

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、Solaris システムでの Trusted CDE または Trusted JDS 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。

1 **Trusted CDE** のワークスペースで、端末ウィンドウまたはファイルマネージャーを開きます。

- 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。ワークスペースメニューから、「ツール (Programs)」->「端末エミュレータ (Terminal)」の順に選択します。
- フロントパネルで、ファイルマネージャーをクリックします。

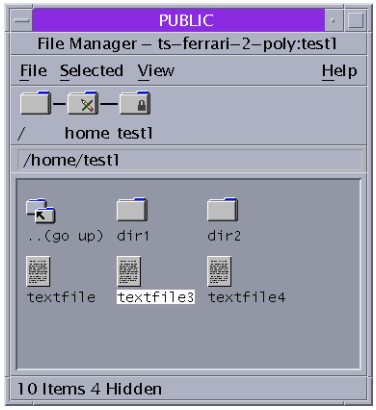


図 3–2 ラベルの付いたファイルマネージャー

ファイルマネージャーは、そのラベルのホームディレクトリの内容を示した状態で表示されます。

ファイルマネージャーは、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、21 ページの「コンテナとラベル」を参照してください。

2 **Trusted JDS** のワークスペースで、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 (Open Terminal)」を選択します。
- デスクトップのドキュメントフォルダ、またはこのコンピュータフォルダをダブルクリックします。
  これら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、21 ページの「コンテナとラベル」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

1 **Solaris Trusted Extensions** の **Solaris 10 11/06** および **Solaris 10 8/07** リリースでは、`Intro(3TSOL)` のマニュアルページを参照してください。

a. 端末ウィンドウを開きます。

- **Trusted CDE** では、背景でマウスボタン **3** をクリックします。次に「ツール **(Programs)**」->「端末エミュレータ **(Terminal)**」の順に選択します。
- **Trusted JDS** では、背景でマウスボタン **3** をクリックします。次に、「端末エミュレータを開く **(Open Terminal)**」を選択します。

b. **Trusted Extensions** の紹介マニュアルページを開きます。

```
% man -s 3tsol intro
```

Trusted Extensions に固有のユーザーコマンドのリストは、『Solaris Trusted Extensions 管理の手順』の付録 B「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、 Sun の マニュアル Web サイト (`http://jp.sun.com/documentation/`) からも入手できます。

2 **Solaris 10 5/08** リリース以降では、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は、『Solaris Trusted Extensions 管理の手順』の付録 B「Trusted Extensions マニュアルページのリスト」を参照してください。

▼ Trusted Extensions のオンラインヘルプにアクセスする

1 **Trusted CDE** では、フロントパネルの「**Help**」アイコンをクリックします。

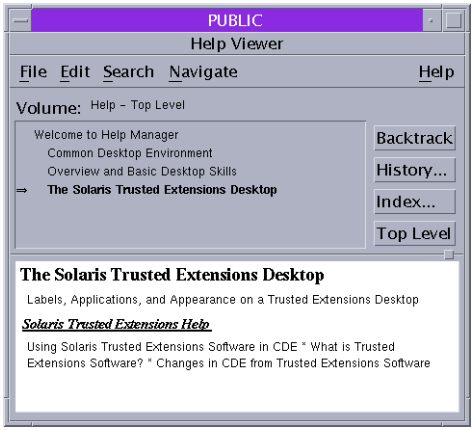


図 3–3 Trusted Extensions のオンラインヘルプ

a. 「索引 (**Index**)」ボタンをクリックします。

b. 「索引 (**Index**)」で、「全ボリューム (**All Volumes**)」から `Trusted` という言葉を検索します。

c. リンクをクリックして、**Trusted Extensions** 固有のヘルプを探します。

2 **Trusted JDS** では、トラステッドパスメニューの「**Help**」をクリックします。

- トラステッドパスメニューを開くには、トラステッドストライプの左側にあるトラステッドシンボルをクリックします。

- タスク固有のヘルプを検索するには、「デバイスマネージャー」など、現在使用しているトラステッドアプリケーションの「ヘルプ」ボタンをクリックします。

▼ CDE のワークスペースメニューをカスタマイズする

Trusted CDE では、ユーザーおよび役割が、ラベルごとにワークスペースメニューをカスタマイズできます。

1 現在のワークスペースで、ワークスペースメニューのカスタマイズを開始します。

- メニューに 1 つ以上の項目を追加するには、「メニューに項目を追加 (Add Item to Menu)」項目を選択します。
  「ブラウズ (Browse)」ボタンのあるダイアログボックスが表示されます。
- メニューまたはメニューのプロパティーを変更するには、「メニューをカスタマイズ (Customize Menu)」項目を選択します。
  ファイルマネージャーが表示されます。

2 ワークスペースメニューに項目を追加する場合は、次の操作を行います。

a. プログラムごとに、プログラムを検索して追加します。
   「ブラウズ (Browse)」ボタンをクリックすると、現在のワークスペースの現在のラベルで使用可能なファイルが表示されます。

b. プログラムを選択します。

c. ウィンドウを閉じます。
   選択した項目がワークスペースメニューの最上部に追加されます。

3 ワークスペースメニューを変更するには、次の手順を行います。

- メニュー項目を削除するには、項目の上でマウスボタン 3 をクリックし、「ごみ箱に捨てる (Put in Trash)」をクリックします。
- アクセス権などのプロパティーを変更するには、項目の上でマウスボタン 3 をクリックし、「属性 (Properties)」をクリックします。
  ここでアクセス権を変更できます。ファイルの情報と機密ラベルを確認することもできます。

4 メニューの変更を確定するか、取り消します。

- 変更を確定するには、「ファイル (File)」->「ワークスペースメニューの更新 (Update Workspace Menu)」の順に選択します。
  ワークスペースメニューに変更が反映されます。
- 変更を取り消すには、「ファイル (File)」->「閉じる (Close)」の順にクリックします。

▼ 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、『Solaris Trusted Extensions 管理の手順』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、システムがウィンドウ枠にラベルを表示するように設定されていない場合に便利です。

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 **(Query Window Label)**」を選択します。
   ポインタが疑問符に変わります。
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。

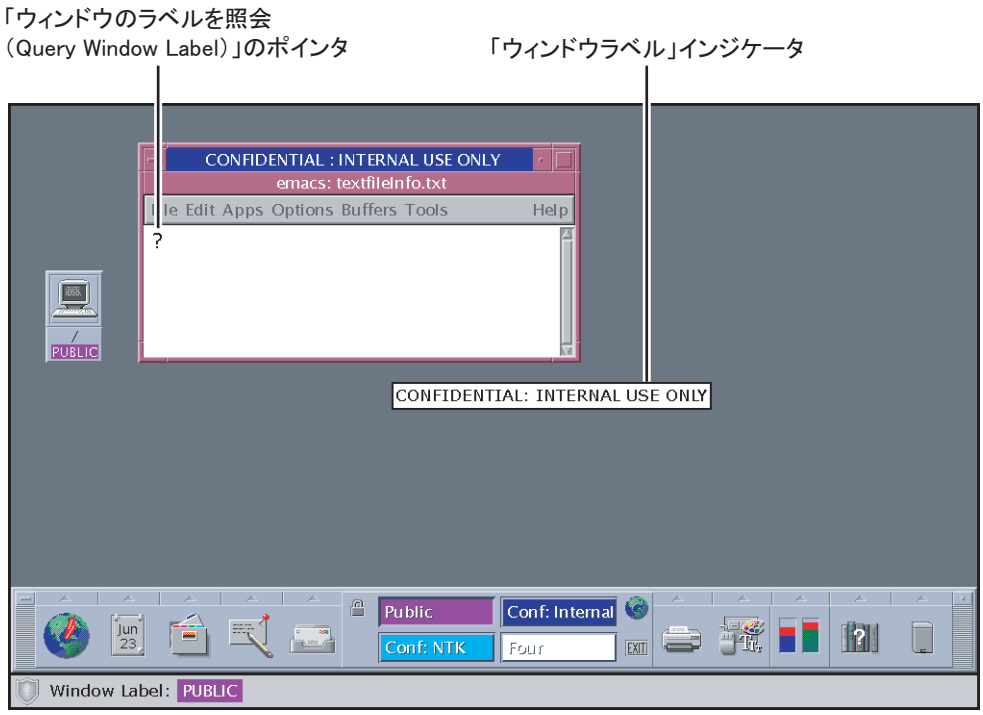


図 3–4 「ウィンドウのラベルを照会 (Query Window Label)」 の操作画面

3 マウスボタンをクリックして操作を終了します。

▼ 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
- Trusted CDE で、フロントパネルを復元し、スタイルマネージャーを使用する

1 ごみ箱を空にする。

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。

- **Trusted CDE** では、フロントパネルで「ごみ箱 **(Trash Can)**」を開きます。

  「ファイル (File)」->「すべてを選択 (Select All)」の順に選択してから、「ファイル (File)」->「廃棄 (Shred)」を選択します。その後、確定します。

- **Trusted JDS** では、デスクトップの「ごみ箱 **(Trash Can)**」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 (Empty Trash)」を選択してから確定します。

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、別のラベルの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 **Trusted CDE** で、トラステッドストライプをクリックしてフロントパネルを復元します。

アイコン化されているフロントパネルが復元されます。

4 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 **(**両方のデスクトップ**)**。

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

a. デスクトップを設定します。

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。

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

---

b. 現在のワークスペースを保存します。

- **Trusted CDE** で、スタイルマネージャーを開きます。「起動」アイコンの設定を選択します。

注 – スタイルマネージャーにはトラステッドパスが必要です。スタイルマネージャーは、フロントパネルまたはワークスペースメニューから実行します。この場合はスタイルマネージャーにトラステッドパスが与えられます。

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設定で復元されます。

- **Trusted JDS** では、ログアウトするときに、現在の設定を保存するように選択します。
  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設定で復元されます。

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。

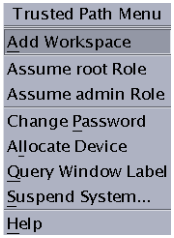
注意 – セキュリティー関連のアクションを実行しようとしたときにトラステッドシンボルが表示されない場合は、ただちにセキュリティー管理者に連絡してください。システムに重大な問題が起きている可能性があります。

▼ Trusted Extensions でパスワードを変更する

Solaris OS と異なり、Trusted Extensions では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中止するには、『Solaris Trusted Extensions 管理の手順』の「デスクトップの現在のフォーカスへの制御を取り戻す」を参照してください。

1 トラステッドパスメニューから「パスワード変更 **(Change Password)**」を選択します。
&TJDS で「パスワード変更 (Change Password)」メニュー項目を表示するには、トラステッドストライプで「トラステッドパス (`Trusted Path`)」をクリックします。

次の図は、Trusted CDE のトラステッドパスメニューを示しています。



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 (Change Password)」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。

▼ 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設定できます。

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。

詳細は、60 ページの「特定のラベルのワークスペースを追加する」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設定します。

3 ログインしたときに表示する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、51 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 (Allocate Device)」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 (Permission Denied)」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 **(Allocate Device)**」を選択します。

または Trusted CDE で、フロントパネルの「ツール (Tools)」サブパネルから「デバイスの割り当て」を選択します。

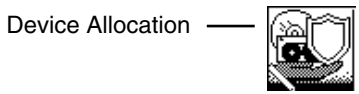


図 3–5　Trusted CDE の「デバイス割り当て (Device Allocation)」アイコン

「デバイス割り当てマネージャー」が表示されます。Solaris Trusted Extensions (JDS) では、この GUI はデバイスマネージャーと呼ばれます。

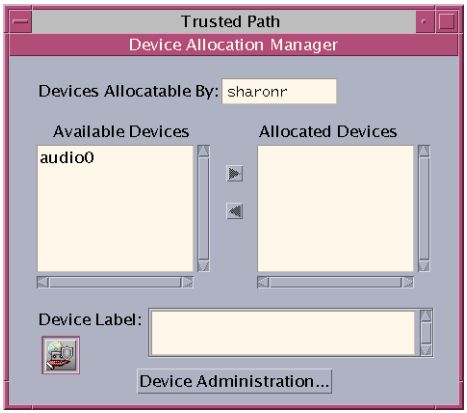


図 3–6 「デバイス割り当てマネージャー (Device Allocation Manager)」

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 (Available Devices)」に表示されます。

- `audio`*n* – マイクロフォンとスピーカを表します
- `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

3 デバイスを選択します。

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

- 「使用可能デバイス **(Available Devices)**」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。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 (Allocated Devices)」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。

例 3–3 ファイルシステムを読み取るためのリムーバブルメディアの読み込み

この例では、SECRET というラベルが付いた CD-ROM からシステムに情報を読み込みます。ユーザーは CD-ROM の割り当てを承認されています。

まず、SECRET というラベルでワークスペースを作成します。このワークスペースでデバイス割り当てマネージャーを開き、CD-ROM ドライブを割り当てます。次に CD を挿入し、マウントするかどうかの確認に対して yes を答えます。

ソフトウェアにより CD がマウントされ、ファイルマネージャーが表示されます。現在のディレクトリは、マウントポイントに設定されます。

例 3–4 メディアをフォーマットするためのリムーバブルメディアの読み込み

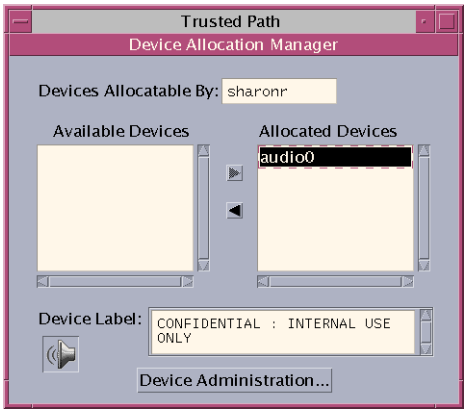
この例では、SECRET データを含むフロッピーディスクをフォーマットします。ユーザーは CD-ROM ドライブの割り当てを承認されています。

まず、SECRET というラベルでワークスペースを作成します。このワークスペースでデバイス割り当てマネージャーを開き、CD-ROM ドライブを割り当てます。次に CD を挿入し、マウントするかどうかの確認に対して no と答えます。これで、CD をフォーマットできます。

例 3–5 オーディオデバイスの割り当て

この例では、ユーザーがシステムにオーディオデバイスを割り当てます。オーディオデバイスを「割り当てられたデバイス (Allocated Devices)」リストに移動したところ、次のようなメッセージが表示されました。

このデバイスは、Confidential : Internal Use Only というラベルに割り当てられます。ラベルは、「割り当てられたデバイス (Allocated Devices)」リストでデバイスを選択したときに表示されます。



ユーザーは、オーディオデバイスの使用が終了したら、その割り当てを解除します。システムから、マイクロフォンのスイッチを切るように指示するメッセージが表示されます。

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。Trusted CDE では、ウィンドウメニューの「配置するワークスペース (Occupy Workspace)」コマンドを使用して、デバイス割り当てマネージャーを新しいワークスペースに移動すると、「使用可能デバイス (Available Devices)」リストと「割り当てられたデバイス (Allocated Devices)」リストの内容も、状況に合わせて変化します。Trusted JDS のデバイスマネージャーは、GUI を別のラベルのワークステーションに移動した場合も同様に機能します。

ファイルマネージャーまたは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、root ディレクトリ (/) に移動してください。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確認します。

▼ 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. デバイス割り当て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 「**Deallocation**」ダイアログボックスで、「了解 **(OK)**」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

Solaris OS と異なり、Trusted Extensions では役割を選択するための GUI が提供されます。

1 トラステッドパスメニューを開きます。

   - **Solaris Trusted Extensions (CDE)** では、フロントパネルの中央をクリックします。
     セキュリティー管理者から役割を割り当てられている場合は、トラステッドパスメニューに「役割になる: *rolename* (Assume rolename Role)」メニュー項目が表示されます。

     「役割になる: *rolename* (Assume rolename)」を選択します。

   - **Solaris Trusted Extensions (JDS)** では、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。
     メニューから役割名を選択します。

2 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 (Change Password)」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、役割のワークスペースに切り替わります。Trusted JDS では、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。Trusted CDE では、役割用に新しいワークスペースが作成されます。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、同じセッション内で複数の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、60 ページの「特定のラベルのワークスペースを追加する」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. ワークスペースボタンの上でマウスボタン **3** をクリックします。
2. メニューから「ワークスペースラベルを変更 **(Change Workspace Label)**」を選択します。
3. ラベルビルダーからラベルを選択します。

   ワークスペースラベルが新しいラベルに変更されます。ラベルの変更前に起動していたウィンドウやアプリケーションは、前のラベルで引き続き実行されます。トラステッドストライプには新しいラベルが表示されます。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。Trusted CDE では、ワークスペースボタンが色分けされています。

▼ 特定のラベルのワークスペースを追加する

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、同じセッション内で複数のラベルで作業するのに便利です。両方のデスクトップで、最

下位ラベルにワークスペースを追加できます。Trusted CDE では、既存のワークスペースのラベルでワークスペースを追加できます。

ヒント – Trusted CDE では、ワークスペースのラベルを反映するように、それぞれのワークスペースボタンの名前を変更します。

現在のワークスペースのラベルを変更するには、60 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 **Trusted JDS** で最下位ラベルにワークスペースを作成するには、次の手順に従います。

   a. パネル画面のワークスペース上でマウスボタン **3** をクリックします。

   b. メニューから「設定 **(Preferences)**」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。

   注 – Trusted JDS では、異なるラベルでワークスペースを追加するには、ワークスペースボックスを選択してそのラベルを変更します。詳細は、60 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。

   ---

2 **Trusted CDE** で最下位ラベルにワークスペースを作成するには、次の手順に従います。

   a. ワークスペーススイッチ領域でマウスボタン **3** をクリックします。

   b. メニューから、「ワークスペースの追加 **(Add Workspace)**」を選択します。
   ワークスペースが最下位ラベルで作成されます。

   c. **(**省略可能**)** ワークスペースの名前を変更します。

3 **Trusted CDE** で既存のワークスペースのラベルにワークスペースを作成するには、次の手順に従います。

   a. ワークスペースボタン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、「ワークスペースの追加 **(Add Workspace)**」を選択します。
   ワークスペースボタンのラベルでワークスペースが作成されます。

▼ 別のラベルのワークスペースに切り替える

1 **Trusted CDE** では、希望するラベルのワークスペーススイッチをクリックします。

図 3–7 異なるラベルのスイッチがあるフロントパネル

2 **Trusted JDS** では、パネル画面上のワークスペースボックスをクリックします。
これで、そのラベルのワークスペースに切り替わります。

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

別のワークスペースに移動したウィンドウは、元のラベルを維持します。このような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 **Trusted CDE** では、「配置するワークスペース **(Occupy Workspace)**」メニューを使用して、ウィンドウを別のワークスペースに移動します。

a. アプリケーションのウィンドウメニューから「配置するワークスペース **(Occupy Workspace)**」を選択します。

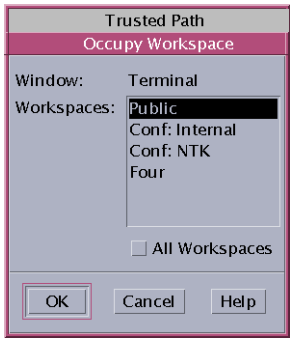


図 3–8 「配置するワークスペース (Occupy Workspace)」の選択

b. 別のラベルのワークスペースを選択し、「了解 (OK)」をクリックします。

これにより、異なるラベルを持つワークスペースにアプリケーションが移動します。「配置するワークスペース (Occupy Workspace)」ダイアログボックスのラベルは「トラステッドパス」です。このラベルは、ワークスペースへの配置がトラステッドコンピューティングベースに影響を与えることを示しています。

次の図は、1 つのワークスペースに配置された 2 つのラベルの異なる端末ウィンドウを示しています。

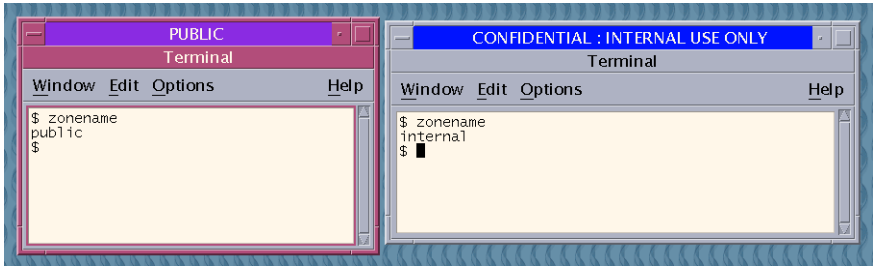


図 3–9 1 つのワークスペース内のラベルの異なるウィンドウ

2 **Trusted JDS** では、パネル画面で、ウィンドウを元のワークスペースボックスから別のワークスペースボックスにドラッグします。

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。

▼ 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。特に、ファイルのラベルがファイルマネージャーのラベルと異なる場合があります。

1. **Trusted CDE** では、ファイルマネージャーを使用してファイルのラベルを判断します。

   - ファイルマネージャーで、ファイルを選択し、「ファイル **(File)**」から「属性 **(Properties)**」メニュー項目を選択します。
     ファイルの機密ラベルプロパティーの値を確認します。
   - または、ファイルが表示されたファイルマネージャーからデスクトップにファイルをドラッグします。
     ファイルのアイコンにファイルのラベルが表示されます。

2. **Trusted JDS** では、ファイルブラウザを使用します。

ヒント – トラステッドパスメニューの「ウィンドウのラベルを照会 (Query Label)」メニュー項目を使用することもできます。

▼ ラベル間でデータを移動する

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、管理者は次の手順を完了している必要があります。

- 『Solaris Trusted Extensions 管理の手順』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」
- 『Solaris Trusted Extensions 管理の手順』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。
   詳細は、60 ページの「特定のラベルのワークスペースを追加する」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、63 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、62 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。次の図は、同じワークスペースに配置されたラベルの異なる 2 つのエディタを示しています。

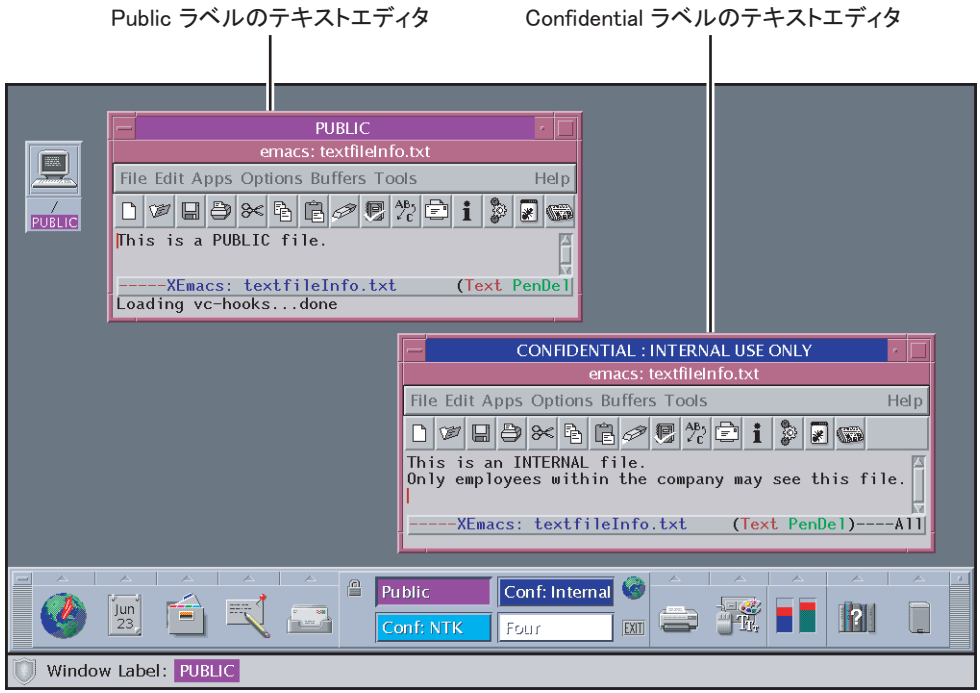


図 3–10 1 つのワークスペース内のラベルの異なるアプリケーション

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。

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、サイトの設定により異なります。

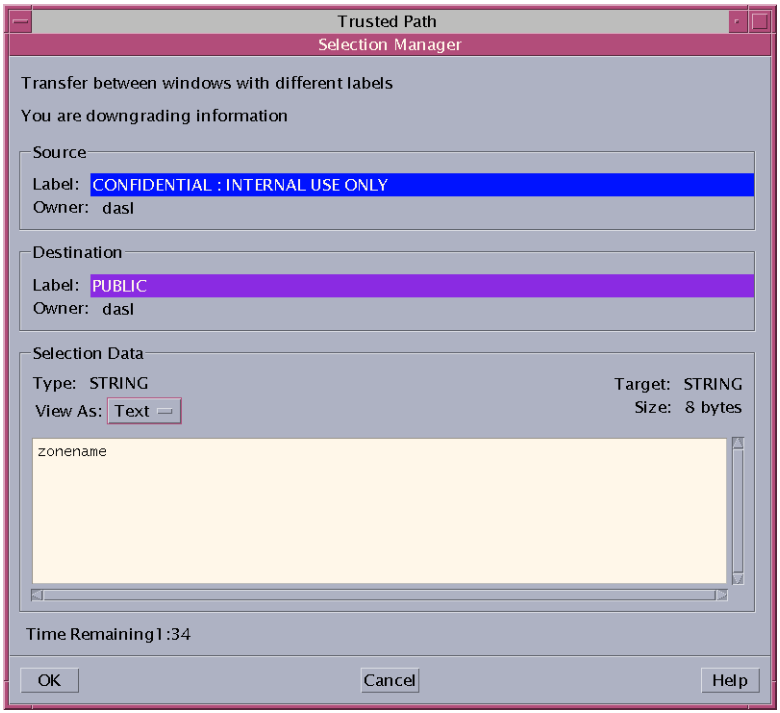


図 3–11 選択マネージャーの確認ダイアログボックス

6 (省略可能)「表示形式 (View As)」メニューで、ソース情報の表示方法を選択します。

- データを 16 進形式で表示する場合は、16 進数を選択します。
- データをすべて非表示にする場合は、「なし (None)」を選択します。

  「表示形式 (View As)」メニューの設定を変更すると、以降の転送データの表示に反映されます。判読不能なデータが含まれるファイルを選択した場合などは、「なし (None)」を選択してください。

7 データのラベルを変更するかどうかを確定します。

- トランザクションを中止するには「取り消し (Cancel)」をクリックします。
- それ以外の場合は「了解 (OK)」をクリックします。

▼ Trusted CDE でラベル間でファイルを移動する

標準的な Solaris システムの場合と同様に Trusted Extensions でファイルを移動できます。ファイルを別のラベルに移動するときは、ファイルに含まれる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ファイル移動を承認されている必要があります。

したがって、管理者は次の手順を完了している必要があります。

- 『Solaris Trusted Extensions 管理の手順』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」
- 『Solaris Trusted Extensions 管理の手順』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」

Trusted CDE の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。移動させるファイルは閉じておく必要があります。ほかにこのファイルを使用している人がいないことを確認します。

1 両方のラベルでワークスペースを作成します。

詳細は、60 ページの「特定のラベルのワークスペースを追加する」を参照してください。

2 両方のラベルでファイルマネージャーを開きます。

詳細は、45 ページの「ラベル付きワークスペースにファイルを表示する」を参照してください。

3 ソース側のファイルマネージャーで、ラベルを変更するファイルを表示します。

4 ターゲット側のファイルマネージャーで、ファイルの新しいディレクトリを表示します。

5 2 つのファイルマネージャーを 1 つのワークスペースに移動します。

詳細は、62 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。

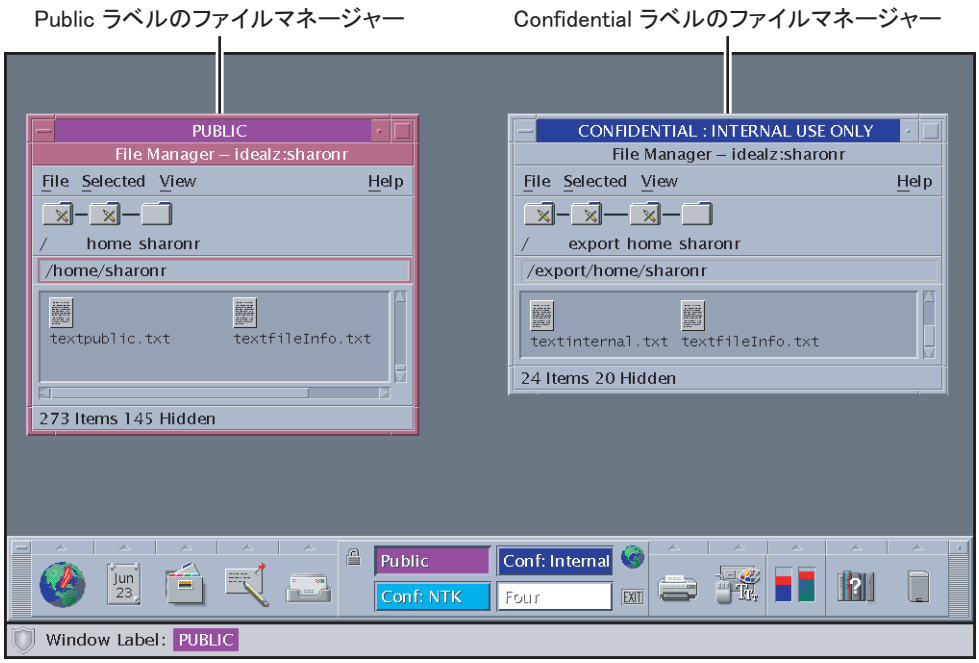


図 3–12　1 つのワークスペース内のラベルの異なるファイルマネージャー

6　ファイルをターゲットディレクトリにドラッグしてドロップします。

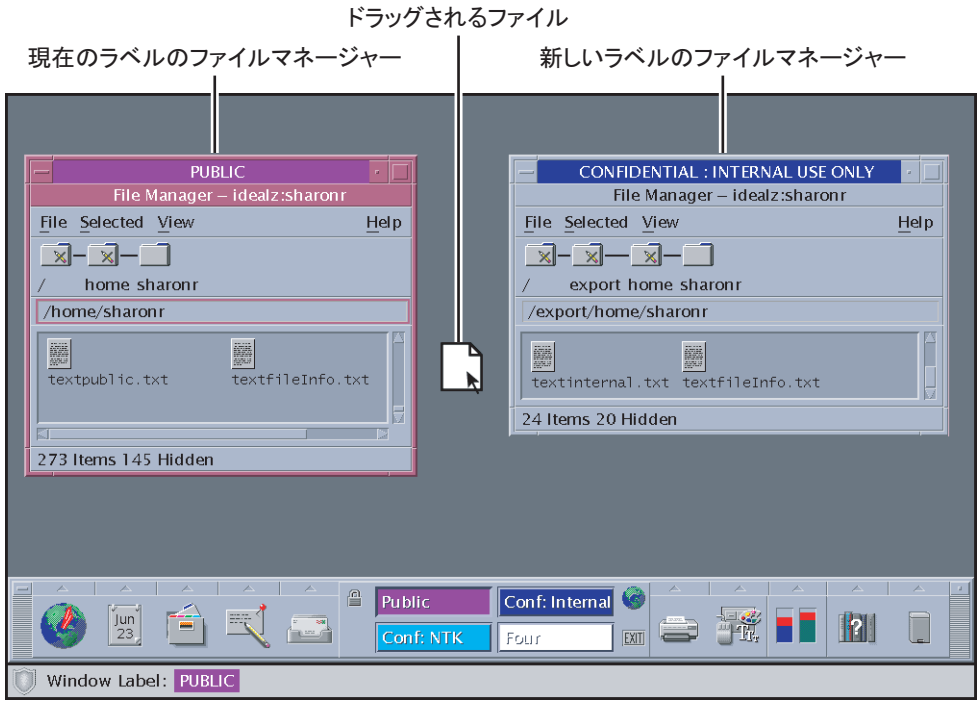


図 3–13　異なるラベルのファイルマネージャー間でのファイルのドラッグ

図 3–14 に示すように、ファイル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。

このダイアログボックスは選択マネージャーの確認ダイアログボックスと似ていますが、タイマーはありません。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)。

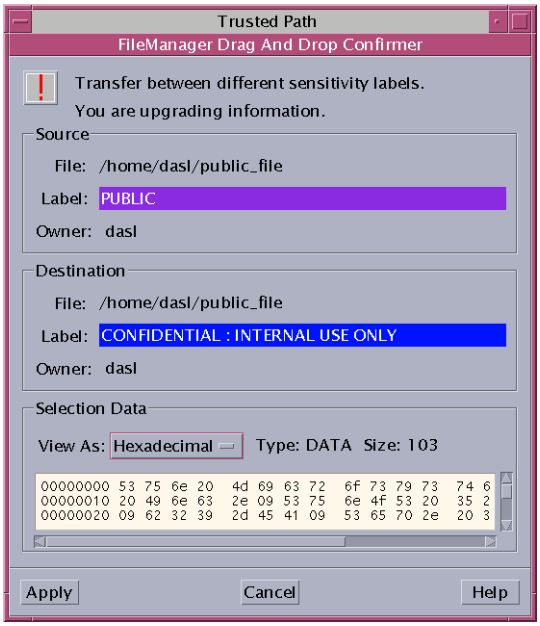


図 3–14 ファイルマネージャーの確認ダイアログボックス

7 ファイルのラベルを変更するかどうかを確定します。

- トランザクションを中止するには「取り消し (**Cancel**)」をクリックします。
- ファイルを新しいラベルに移動するには「適用 (**Apply**)」をクリックします。

例 3–6 別のラベルへのファイルのリンク

別のラベルにファイルをリンクする操作は、ラベルの低いファイルを高いラベルで表示するときに便利です。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。

ファイルをリンクするには、Shift キーと Control キーを押しながら、ソース側のファイルマネージャーからターゲット側のファイルマネージャーに、ファイルのアイコンをドラッグします。次に、リンクを確定するか、操作を取り消します。

注意事項 システムがラベルの昇格または降格を許可するように設定されていない場合は、転送が承認されないことを示すダイアログボックスが表示されます。このような場合は、管理者に確認してください。

◆ ◆ ◆ 第 4 章

Trusted Extensions の構成要素 (リファレンス)

この章では、Solaris 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。

- 71 ページの「Trusted Extensions の代表的な機能」
- 75 ページの「Trusted Extensions のファイルとアプリケーション」
- 76 ページの「Solaris OS のパスワードのセキュリティー」
- 77 ページの「フロントパネルのセキュリティー (Trusted CDE)」

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 (手順)」で説明したように、Trusted Extensions 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 が設定されたシステムは、4 つの特徴によって Solaris システムと区別できます。

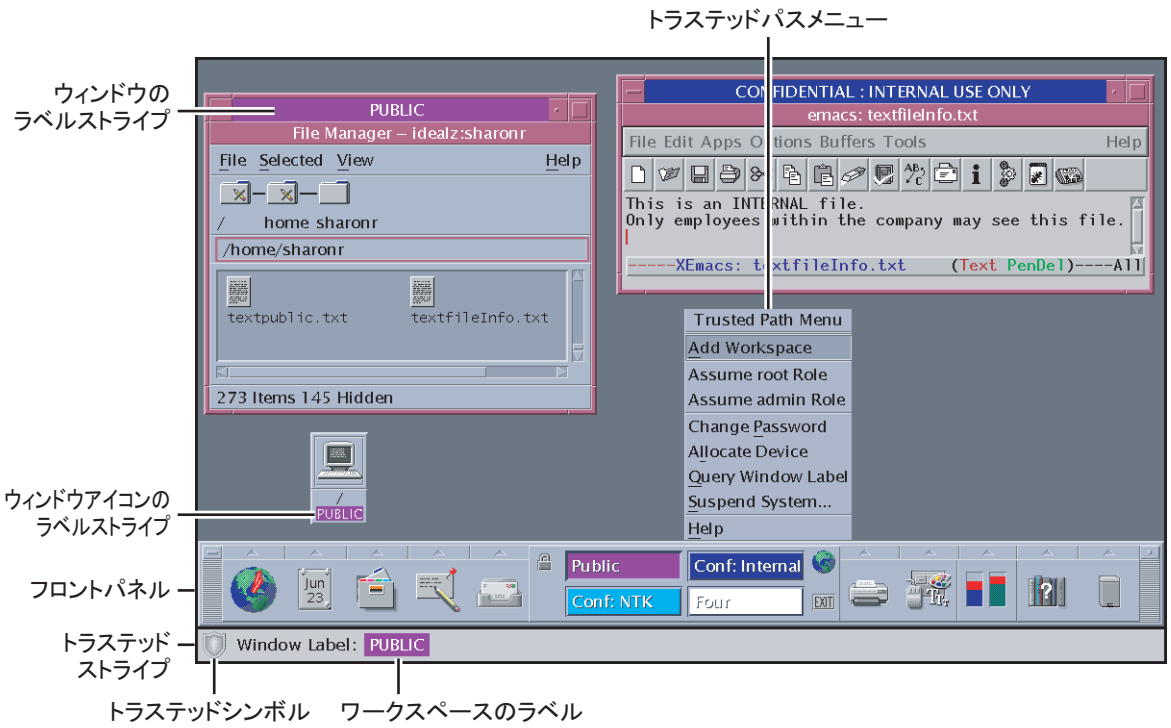


図 4–1 マルチレベルの Trusted CDE デスクトップ

- 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、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 – 特殊なグラフィカルセキュリティー機構です。Solaris Trusted Extensions (CDE) では、トラステッドストライプは常に画面の最下部に表示されます。Solaris Trusted Extensions (JDS) では、ストライプを画面の最上部に表示できます。
- 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 – ユーザー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 – Trusted CDE では、フロントパネルのスイッチ領域からトラステッドパスメニューにアクセスできます。トラステッドパスメニューは、セキュリティー関連のタスクの実行に使用されます。Trusted JDS では、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
- ウィンドウアイコンのラベルストライプ: アイコン化されたウィンドウの下
- 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
- トラステッドパスメニュー項目の「ウィンドウのラベルを照会 (Query Window Label)」インジケータ: ポインタが置かれたウィンドウまたはアイコンのラベルを表示します

図 4–1 は、ラベルを表示するように設定されたシステムでラベルが表示される方法を示しています。このシステムでは、デスクトップに Trusted CDE を使用しています。ラベルを表示しないようにサイトを設定することもできます。管理者がラベルを表示しないようにシステムを設定している場合でも、ラベル機能は有効です。この場合は、「ウィンドウのラベルを照会 (Query Window Label)」メニュー項目を使用して、ウィンドウのラベルを表示できます。説明図は、図 3–4 を参照してください。

トラステッドストライプ

Trusted CDE では、すべての Trusted Extensions セッションで、トラステッドストライプが画面最下部の予約領域に表示されます。Trusted JDS では、トラステッドストライプを画面の最上部に表示できます。

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。

Trusted CDE では、トラステッドストライプに次の 2 つ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関連にあるときに表示されます。
- ウィンドウラベル – 省略可能。アクティブウィンドウのラベルが表示されます。

Trusted JDS では、トラステッドストライプにさらに次の 2 つの構成要素があります。

- 現在のユーザー名または役割名 – トラステッドシンボルのすぐ右に、ワークスペース内での新しいプロセスの所有者の名前が表示されます。
- ラベルの付いたウィンドウ – ワークスペース内のすべてのウィンドウのラベルを表示します。

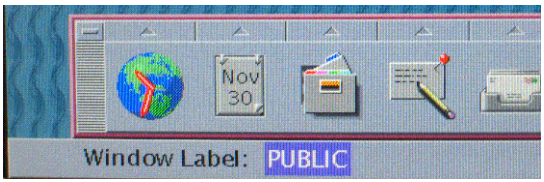


図 4–2 トラステッドストライプに表示された PUBLIC ウィンドウラベル

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。構成によってラベルが非表示にされている場合、トラステッドシンボルはトラステッドストライプとともに表示されます。Trusted CDE では、トラステッドシンボルはフロントパネルの左側に表示されます。Trusted JDS では、トラステッドシンボルはトラステッドストライプの左側に表示されます。

トラステッドシンボルは、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ません。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、「Trusted Path」という表示がトラステッドストライプに表示されます。

図 4–3 トラステッドストライプ内の Trusted Path 表示

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設定します。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初めて移動するときに、そのファイルがコピーされます。.copy_files 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 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。.link_files は、最下位ラベルのホームディレクトリに格納されます。このファイルは、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。

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。Solaris OS では、パスワードの内容に関する条件を設定したり、パスワードの再設定の条件を強制したりできます。再設定の条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。Solaris OS のパスワードは、少なくとも次の基準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 (Change Password)」メニュー項目を使用して変更できます。手順については、53 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。

フロントパネルのセキュリティー (Trusted CDE)

Solaris Trusted Extensions (CDE) のフロントパネルは、標準の CDE で使用されるフロントパネルとよく似ています。Trusted Extensions のフロントパネルでは、ユーザーが使用を許可されているアプリケーション、ファイル、およびユーティリティーのみにアクセスが制限されます。ワークスペーススイッチ領域内の任意の場所でマウスボタン 3 をクリックすると、トラステッドパスメニューが表示されます。

リムーバブルメディアマネージャーでデバイスにアクセスできるようにするには、デバイス割り当てマネージャーを使ってそのデバイスを割り当てておく必要があります。デバイス割り当てマネージャーには、フロントパネルのスタイルマネージャーアイコンの上にある「ツール (Tools)」サブパネルからアクセスします。

ヒント – フロントパネルがアイコン化されている場合は、トラステッドストライプの任意の場所をクリックすることで、パネルを元のサイズに戻すことができます。

Trusted Extensions では、「アイコンのインストール (Install Icon)」ドロップサイトは、現在のワークスペースのラベルで使用が許可されているアプリケーションおよびファイルに制限されています。

標準の CDE に関する詳細は、『Solaris 共通デスクトップ環境 ユーザーズ・ガイド』を参照してください。

ワークスペーススイッチ領域

Trusted Extensions のワークスペースボタンは、個別のワークスペースを定義するだけでなく、特定ラベルでの作業をユーザーに義務付けます。マルチレベルセッションを開始すると、それぞれのワークスペースは、使用可能な最下位のラベルに設定されます。管理者がサイトのラベルを色分けしている場合は、各ラベルの色がワークスペースボタンに表示されます。ワークスペーススイッチ領域から、トラステッドパスメニューにアクセスできます。

トラステッドパスメニュー

トラステッドパスメニューには、次の図に示すような、セキュリティーに影響を与えるメニュー項目が表示されます。

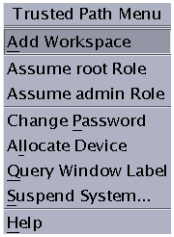


図 4–4 トラステッドパスメニュー – 基本バージョン

たとえば、このメニューを使用してパスワードを変更したり、デバイスを割り当てたりします。詳細は、53 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。

Trusted CDE では、トラステッドパスメニューに 、もう 1 つのバージョンがあります。ワークスペース 名バージョンには、追加のワークスペースのオプションが含まれます。メニューに表示される選択肢は、管理者によるアカウントの設定によって異なります。

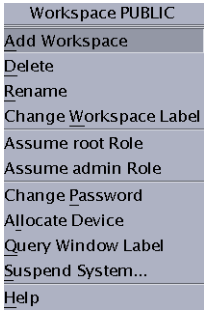


図 4–5　トラステッドパスメニュー – ワークスペース名 (Workspace Name)バージョン

クロックのセキュリティー

Trusted Extensions では、管理者だけがワークステーションに設定された日時を変更できます。

カレンダのセキュリティー

カレンダには、現在のワークスペースのラベルのアポイントメントだけが表示されます。別のラベルのアポイントメントを表示するには、そのラベルでカレンダを開く必要があります。

ファイルマネージャーのセキュリティー

Trusted Extensions では、現在のワークスペースのラベルのファイルがファイルマネージャーによって表示されます。複数のラベルのファイルを一度に表示するには、異なるラベルを持つ複数のワークスペースで、ファイルマネージャーをそれぞれに実行します。次に、「配置するワークスペース (Occupy Workspace)」コマンドを使用して、同じワークスペースに複数のファイルマネージャーウィンドウを表示します。

ファイルマネージャーを使用すると、ファイルやフォルダの基本的なアクセス権およびアクセス制御リスト (ACL) を変更できます。承認があれば、異なるラベルのファイルマネージャー間でファイルの移動やリンクを実行することもできます。ファイルマネージャーの使い方の詳細は、45 ページの「ラベル付きワークスペースにファイルを表示する」および 53 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。

テキストエディタのセキュリティー

テキストエディタは、現在のワークスペースのラベルのファイルを編集する場合にのみ使用できます。承認があれば、異なるラベルのテキストエディタ間で情報をコピーできます。

個人アプリケーションサブパネル

「個人アプリケーション (Personal Applications)」サブパネルに組み込まれているデフォルトのアプリケーションは、標準の CDE 環境のものと同様に動作します。端末アイコンをクリックすると、管理者によって割り当てられたデフォルトのシェルが開きます。Web サーバーにアクセスするには、ブラウザのラベルを Web サーバーと同じにする必要があります。

メールプログラムのセキュリティー

Trusted Extensions では、すべてのメールメッセージにラベルが付きます。メッセージを送信する場合、メッセージはメールアプリケーションのラベルで送信されます。そのラベルの認可を受けているホストおよびユーザーのみがメッセージを受信します。そのラベルで作業しているユーザーのみがメッセージを表示できます。

メールプログラムの不在返信メッセージオプションを使う必要がある場合は、通常メールを受信しているラベルのそれぞれについて、不在返信メッセージの送付を明示的に設定しなければなりません。不在返信メッセージに関するサイトのセキュリティーポリシーについては、セキュリティー管理者に確認してください。

プリンタのセキュリティー

「個人プリンタ (Personal Printers)」サブパネルの印刷マネージャーには、ユーザーの認可上限の範囲で認可されているすべてのプリンタのアイコンが表示されます。ただし、これらのプリンタの中で使用できるのは、現在のワークスペースのラベルで文書を印刷する認可を受けているものだけです。

Trusted Extensions での一般的な印刷ジョブには、次のようなラベルや追加ページが含まれます。

- 印刷ジョブの最初に出力されるバナーページ。サイトに応じた印刷ジョブ、取り扱い指示、ラベルが印刷されます。
- ヘッダーおよびフッターにラベルの付いた本文ページ。
- 印刷ジョブの最後に出力されるトレーラページ。ジョブの最後であることを示します。

一般的なバナーページを次の図に示します。JOB START という語句が、バナーページであることを示しています。

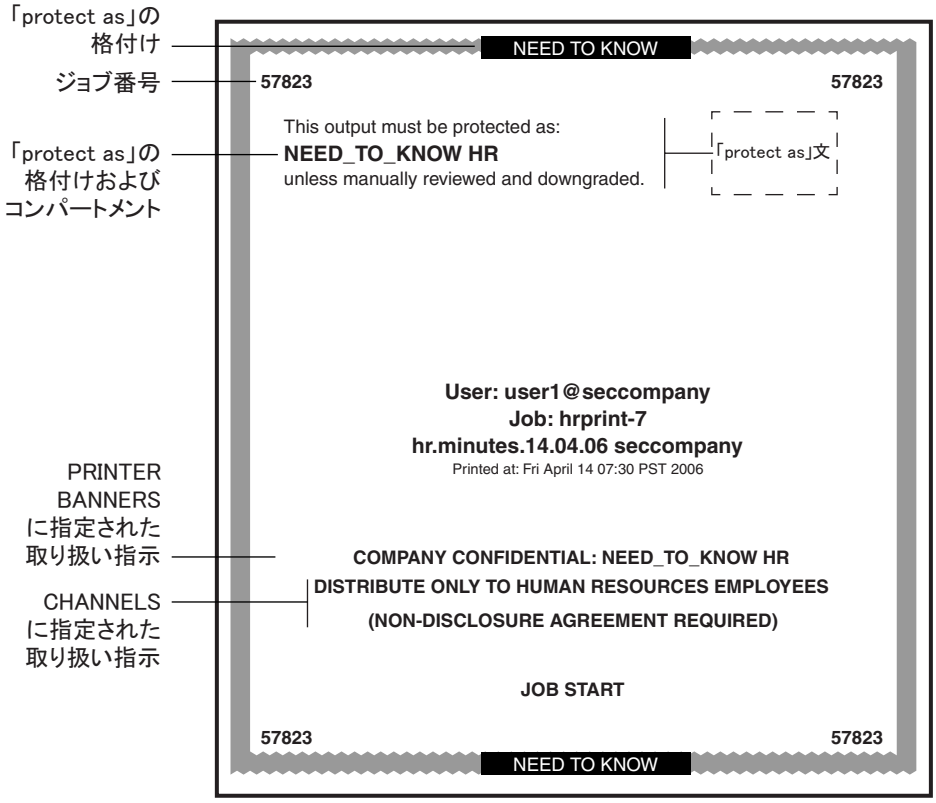


図 4–6 ラベル付き印刷ジョブの一般的なバナーページ

サイトでの印刷に関する厳密なセキュリティー情報については、管理者に確認してください。

スタイルマネージャーのセキュリティー

次に挙げる 3 つの例外を除き、スタイルマネージャーの操作は Solaris システムの場合と同じです。

- スタイルマネージャーをアプリケーションマネージャーから実行できない。これは、Trusted Extensions が設定されているときは、スタイルマネージャーがトラステッドパスを必要とするためです。スタイルマネージャーはフロントパネルと

ワークスペースメニューから実行してください。この場合はスタイルマネージャーにトラステッドパスが与えられます。

- スクリーンセーバーと画面ロックオプションは制限される。ロックされるまでのシステムの最大アイドル時間が管理者によって設定されます。ユーザーはアイドル時間を短くできます。最大値を超えてアイドル時間を増やすことはできません。ただし、画面のロックパターンは選択可能です。サイトのセキュリティーポリシーの詳細は、管理者に確認してください。
- ユーザーの起動セッション設定は、ログイン時に指定したラベルまたは認可上限に応じて起動制御によって設定される。したがって、使用するアカウントラベル範囲内の各ラベルに対して異なるワークスペース設定を保存できます。

アプリケーションマネージャーのセキュリティー

アプリケーションマネージャーでは、管理者がユーザーに割り当てたアプリケーションおよびユーティリティーのみにアクセスできます。ユーザーは役割の中で、別のアプリケーションや機能にアクセスできます。ファイル上で操作できる機能は、現在のワークスペースのラベルによって異なります。

同様に、アイコンを「アイコンのインストール (Install Icon)」ドロップサイトにドロップすると、そのアプリケーションは「個人アプリケーション (Personal Application)」サブメニューに追加されますが、実行できるアプリケーションは、管理者が指定したものに限られます。

ごみ箱のセキュリティー

Trusted Extensions のごみ箱には、削除するファイルをラベルごとに格納できます。どのラベルのファイルもごみ箱に入れることができますが、表示されるのは現在のラベルのファイルのみです。機密情報は、ごみ箱に入れた直後に削除する必要があります。

ワークスペースのセキュリティー (Trusted JDS)

Trusted Extensions では、Trusted JDS は Trusted CDE と同等のセキュリティーを備えていますが、見た目と使い心地が異なります。Trusted CDE では、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。

セキュリティー機能の場所が Trusted JDS と Trusted CDE では異なります。動作も異なる場合があります。

- Trusted JDS では、トラステッドストライプから Trusted Path メニューが使用可能です。
- ウィンドウの上にマウスを移動すると、パネル上のタスクの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のユーザー名または役割名をクリックし、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。
- 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、デスクトップを設定できます。

用語集

Trusted JDS 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グラフィカルなデスクトップ。Trusted JDS は完全なアクセシビリティーを備えたデスクトップです。

アカウントラベル範囲 Trusted Extensions が設定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。

アクション CDE (Common Desktop Environment、共通デスクトップ環境) のグラフィカルユーザーインタフェースからアクセスされるアプリケーション。アクションはアイコンで表現され、1 つ以上のコマンドと任意のユーザープロンプトで構成されます。Trusted Extensions でユーザーが実行できるアクションは、そのユーザーのアカウントに割り当てられる権利プロファイルにセキュリティー管理者が設定したものに限られます。同様に、アクションの特定の機能も、セキュリティー管理者が適切な承認と特権を権利プロファイルに割り当てた場合にのみ使用できます。

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)** Solaris OS のセキュリティー機能の 1 つ。 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構成要素。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
: Solaris OS のセキュリティー機能の 1 つ。 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)
: Solaris OS のセキュリティー機能の 1 つ。 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。

共通デスクトップ環境 (CDE)
: 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グラフィカルなデスクトップ。Trusted Extensions では、ラベルビルダー、デバイス割り当てマネージャー、選択マネージャーなどのトラステッドアプリケーションがデスクトップに追加されます。Trusted JDS も参照してください。

グループ ID (GID)
: Solaris OS のセキュリティー機能の 1 つ。 共通のアクセス権を持つユーザーのグループの識別に使用される整数。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
: Solaris OS のセキュリティー機能の 1 つ。サイトのセキュリティー管理者が、コマンドや CDE のアクションをセキュリティー属性でまとめるために使用します。ユーザーの承認や特権などの属性に応じて、コマンドやアクションが正常に処理されます。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
: ラベルを構成する階層的ではない要素で、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) の文書 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 のセッションを初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。Trusted Extensions 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プロセスの代理として実行される役割を指します。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
: Solaris OS のセキュリティー機能の 1 つ。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作業を実行する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、サイトの管理ラベルとセキュリティー管理者が使用できるシステム管理者が含まれます。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 Solaris OS のセキュリティー機能の 1 つ。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 に代わって有効になる 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 GID 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 Solaris OS のセキュリティー機能の 1 つ。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。

シングルラベル設定 1 つのラベルだけで操作するように設定されたユーザーアカウント。シングルレベル設定とも呼ばれます。

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 が設定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設定されます。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 Solaris OS のセキュリティー機能の 1 つ。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示します。

セッション認可上限　ログイン時に設定され、Trusted Extensions 認可上限のラベルの上限を定義するセッション。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設定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。

代替機構　`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　Solaris OS のセキュリティー機能の 1 つ。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機構。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割り当てマネージャーによって処理されます。

デバイス割り当てマネージャー　Trusted Extensions のトラステッドアプリケーションの 1 つ。デバイスの設定、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。デバイスの設定には、デバイスへの承認条件の追加などがあります。

特権　Solaris OS のセキュリティー機能の 1 つ。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上書き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　Solaris OS のセキュリティー機能の 1 つ。特権プロセスは、割り当てられたユーザーに特権がある場合に実行されます。

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 が設定されたシステムの、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、文書、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示します。サイトの設定に応じ、トラステッドストライプには 1 つまたは 2 つの構成要素があります。 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 つ目は任意表示のラベルで、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機構。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機構。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。認可条件には 1 つの格付けと任意の数のコンパートメントという 2 つの構成要素があります。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)
: システムが強制的に実施するアクセス制御機構で、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てから、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、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
: Solaris OS のセキュリティー機能の 1 つ。 Bourne シェルの一種で、ユーザーはセキュリティー属性を使って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
: `tnrhtp` データベースのレコードの 1 つで、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の定義に使用されます。

無関係なラベル
: 優位なラベルを参照してください。

役割
: Solaris OS のセキュリティー機能の 1 つ。 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、特定の処理を実行するために必要なセキュリティー属性を使用して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要素を持ち、 他方のラベルのコンパートメント要素をすべて持ち合わせているラベル。これらの要素が同じである場合、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)**	Solaris OS のセキュリティー機能の 1 つ。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 つの構成要素があります。1 つはセキュリティーの階層的なレベルを示す格付けであり、もう 1 つは特定の格付けの実体にだれがアクセスできるかを定義するコンパートメントで、コンパートメントがない場合や複数ある場合もあります。ラベルエンコーディングファイルも参照してください。
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。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	Solaris Trusted Extensions (CDE) または Solaris Trusted Extensions (JDS) 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。
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	Solaris OS のセキュリティー機能の 1 つ。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	Solaris OS のセキュリティー機能の 1 つ。 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

A

admin 役割, 「システム管理者の役割」を参照

C

CDE, フロントパネルのトラステッドアプリケーション, 77
`.copy_files` ファイル
　作成, 49-50
　説明, 76
　トラブルシューティング, 50

L

`.link_files` ファイル
　作成, 49-50
　説明, 76
　トラブルシューティング, 50

N

`Not Found` エラーメッセージ, 29
`Not in Profile` エラーメッセージ, 29

O

oper 役割, 「オペレータの役割」を参照

P

`pfsh` コマンド, 「プロファイルシェル」を参照
Trusted Extensions でのアプリケーションマネージャーのセキュリティー, 82
Trusted Extensions でのカレンダのセキュリティー, 79
Trusted Extensions でのクロックのセキュリティー, 79
Trusted Extensions でのごみ箱のセキュリティー, 82
Trusted Extensions でのテキストエディタのセキュリティー, 80
Trusted Extensions でのプリンタツールのセキュリティー, 80-81
Trusted Extensions でのメールのセキュリティー, 80
Trusted Extensions のヘルプ
　オンラインヘルプ, 47-48
　マニュアルページ, 46-47
Trusted Extensions のマニュアルページ, 46-47

R

root の役割, 責任, 29

S

secadmin 役割, 「セキュリティー管理者の役割」を参照
Solaris Trusted Extensions (CDE), 「CDE」を参照

Stop-A (L1-A) キーの組み合わせ，45

T

Trusted CDE
  Trusted Extensions デスクトップ，31
  Trusted Extensions のオンラインヘルプの検索，47
  スタイルマネージャーの使用，53
  デスクトップのカスタマイズ，52
  デスクトップの選択，34
  ワークスペースメニューのカスタマイズ，48-49
Trusted Extensions
  概要，15-16
  代表的な機能，71-75
Trusted JDS
  Trusted Extensions デスクトップ，31
  オンラインヘルプ，47
  デスクトップのカスタマイズ，52
  デスクトップの選択，34
  ワークスペースのセキュリティー，82-83

あ
アクセシビリティー, Trusted JDS，31
アクセス
  Trusted Extensions のマニュアルページ，46-47
  あらゆるラベルの初期設定ファイル，49-50
  遠隔マルチレベルデスクトップ，38-39
  書き込み，23
  読み取り/書き込み，23
  読み取り専用，23
  レベルが低いホームディレクトリ，21
アクセス権
  ファイル所有者による選択，18
  ユーザーの責任，24
アクセス制御
  アクセス権ビット，18
  アクセス制御リスト (ACL)，18
  任意アクセス制御 (DAC)，18
  必須アクセス制御 (MAC)，18-24
アクセス制御リスト (ACL)，18

い
移動
  ウィンドウを別のラベルのワークスペースに，62-63
  データを別のラベルに，64-67
  ファイルを別のラベルに，67-70
印刷, 一般的なラベル付きバナーページ，81

う
「ウィンドウのラベルを照会 (Query Window Label)」メニュー項目，50-51
ウィンドウラベルインジケータ，75

え
遠隔ログイン, マルチレベルデスクトップに，38-39

お
オブジェクト
  再使用，27
  定義，20
オペレータの役割, 責任，29

か
書き込みアクセス, ラベル付き環境，23
カスタマイズ
  デスクトップ，52
  ワークスペースメニュー，48-49

き
キーの組み合わせ, 占有が信頼できるかをテスト，53-54
機密ラベル
  「ラベル」を参照
  ラベルの種類，19

け
決定, ウィンドウのラベル, 50-51
検索
  Trusted Extensions のオンラインヘルプ, 47-48
  あらゆるラベルのカレンダイベント, 52
  トラステッドパスメニュー, 59, 72
権利プロファイル, 定義, 28-29

こ
降格情報, 24
異なるラベルのファイルのリンク, 70
コピー＆ペースト, ラベルへの影響, 24
コンテナ, 「ゾーン」を参照

さ
作業, 「ユーザー」を参照
作成
  $HOME/.copy_files ファイル, 49-50
  $HOME/.link_files ファイル, 49-50
サブジェクト, 定義, 20

し
システム管理者, Trusted Extensions, 27-29
システム管理者の役割, 責任, 29
「システム保存停止 (Suspend System)」メニュー項目, 44-45
周辺装置, 「デバイス」を参照
昇格情報, 24
承認
  データのラベル変更に必要, 64-67
  ラベルの変更, 24
情報, 「データ」を参照
初期化ファイル, カスタマイズ時のトラブルシューティング, 38
初期設定ファイル, あらゆるラベルのアクセス, 49-50
シングルレベルセッション, 定義, 25
シングルレベルのログイン, Trusted CDE または Trusted JDS, 34
信頼できる占有, キーの組み合わせ, 53-54

す
スタイルマネージャー
  Solaris Trusted Extensions (CDE) での制限, 81-82
  セッション特性の変更, 54
  トラステッドパスが必要, 53
スプーフィング
  定義, 17, 88

せ
責任
  管理者, 29
  データ保護に関するユーザーの責任, 24-25
  パスワードのセキュリティーに関するユーザーの責任, 76-77
  ユーザーによるメディアのクリア, 27
  ログアウトするユーザー, 43-44
セキュリティー管理者の役割
  責任, 29
  トラステッドインジケータが表示されないことを報告, 75
  トラステッドストライプが表示されないことを連絡, 42
セキュリティー設定の確認
  「最後のログイン (Last Login)」ダイアログボックス, 33
  ログイン時の手順, 35-37
セキュリティーの実践, 定義, 15
セキュリティーポリシー
  定義, 15, 88
セッション
  シングルレベルとマルチレベル, 25
  認可上限の選択, 25
  レベル選択の影響, 25-26
  レベルの設定, 37
セッション認可上限, 定義, 25
選択
  デスクトップ, 33, 34
  ラベルの変更, 64-67
  ログイン中のラベルまたは認可上限, 36

選択マネージャー，65

そ
ゾーン
　ホームディレクトリの表示/非表示，21
　ラベル付き，21

つ
追加
　ラベル付きワークスペース，60-61
　ワークスペース，60-61

て
ディレクトリ
　ホームディレクトリの表示/非表示，21
　ラベルの変更，67-70
データ
　MAC による保護，18-24
　ラベルの判断，63-64
　ラベルの変更，64-67
手順，「ユーザー」を参照
デスクトップ
　Trusted Extensions，31-32
　遠隔でログインする，38-39
　キーボードフォーカス，53-54
　共通タスク，51-53
デバイス
　再使用前にクリア，27
　使用，55-58
　トラブルシューティング，58
　保護，17
　リムーバブルメディアの使用，57
　割り当て，55-58
デバイスの使用，「デバイスの割り当て」を参照
デバイスの割り当て，55-58
　トラブルシューティング，58
デバイスの割り当て解除，基本的な手順，59
デバイス割り当てマネージャー，デバイスの割り当て解除，59
「デバイスを割り当てる (Allocate Device)」メニュー項目，55-58
電子メール，ラベルの実施，27
電子メール指示，ユーザーの責任，24

と
トラステッドアプリケーション
　権利プロファイルの使用，28-29
　フロントパネル，77
トラステッドインジケータ，表示されない，75
トラステッドインジケータが表示されない，トラブルシューティング，75
トラステッドコンピューティングベース (TCB)
　TCP と対話する手順，53-70
　対話中を示すシンボル，74
　対話のシンボル，17
　定義，16
トラステッドシンボル
　Trusted CDE ワークスペースでの表示，41
　説明，74
　不正操作防止アイコン，17
トラステッドストライプ
　CDE での場所，20，72
　Trusted JDS での場所，72
　説明，73
　表示されない場合の措置，42
　マルチヘッドのシステム，41
　ロック画面には表示されない，43
トラステッドデスクトップの使用，シングルレベルまたはマルチレベル，34
トラステッドパスメニュー
　「ウィンドウのラベルを照会 (Query Window Label)」，50-51
　使用，47
　説明，78
　「デバイスを割り当てる (Allocate Device)」，55-58
　場所，72
　パスワードの変更，53-54
　「役割になる: *rolename* (Assume rolenama role)」，59-60
　「ワークスペースラベルを変更 (Change Workspace Label)」，60

ドラッグ＆ドロップ, ラベルへの影響，24
トラブルシューティング
  $HOME/.copy_files ファイル，50
  $HOME/.link_files ファイル，50
  アイコン化されたフロントパネル，77
  コマンド行のエラーメッセージ，29
  デバイスの割り当て，58
  トラステッドインジケータが表示されない，75
  トラステッドストライプが表示されない，42
  パスワードの失敗，35
  ファイルのラベルの付け直し，70
  ファイルマネージャーが表示されない，58
  ログイン，37-38

に

任意アクセス制御l (DAC), 定義，18
認可上限
  セッションの設定，37
  ラベルの種類，19
  ログイン時に設定，25
  ログイン時の設定，37
認証, デバイスの割り当て，17

は

パスワード, ユーザーの責任，76-77
「パスワード変更 (Change Password)」メニュー項目，53-54
判断, ファイルのラベル，63-64

ひ

必須アクセス制御 (MAC)
  定義，18-24
  電子メールに実施，27
表示/非表示
  デスクトップセキュリティー，41-42
  トラステッドストライプ，20, 42, 72
  レベルが低いホームディレクトリの読み取り，21
  ログイン後のラベル，31-32
表示されないトラステッドストライプ, トラブルシューティング，42

ふ

ファイル
  $HOME/.copy_files，49-50, 76
  $HOME/.link_files，49-50, 76
  あらゆるラベルの初期設定ファイルへのアクセス，49-50
  異なるラベルのファイルマネージャー間のリンク，70
  ファイルマネージャー間の移動，67-70
  ラベルの変更，67-70
  ワークスペースに表示，45-46
ファイルの保護
  DAC，18
  MAC，18-24
  ユーザーの責任，24
  ラベルを使用，25-27
ファイルブラウザ
  内容の表示，46
  表示されない場合のトラブルシューティング，58
  ファイルのラベルの表示，64
ファイルマネージャー
  Trusted Extensions でのセキュリティー，79
  内容の表示，45
  表示されない場合のトラブルシューティング，58
  ファイルのラベル変更，70
  ラベルの変更，67-70
フォーマット, リムーバブルメディア，57
復旧ログイン，37-38
プロファイル，「権利プロファイル」を参照
プロファイルシェル, 定義，28
フロントパネル
  アイコンから元に戻す，77
  トラステッドアプリケーションの説明，77

へ

別のラベルのファイルをリンク, `.link_files` の使用, 49-50
別のラベルのワークスペースに切り替える, 62
変更
  承認されたユーザーによるラベル, 67-70
  データのセキュリティーレベル, 64-67, 67-70
  パスワード, 53-54
  ワークスペースラベル, 60

ほ

ホームディレクトリ, レベルが高いゾーンからの表示, 21
ホットキー, デスクトップフォーカスの再取得, 53-54
ポリシー, 「セキュリティーポリシー」を参照

ま

マウント, リムーバブルメディア, 57
マルチヘッドのシステム, トラステッドストライプ, 41
マルチレベルセッション, 定義, 25
マルチレベルのログイン, Trusted CDE または Trusted JDS, 34
マルチレベルログイン, 遠隔で, 38-39

や

役割
  共通の役割, 29
  責任, 29
  特殊なユーザーアカウント, 27-29
  ラベル付きワークスペースの追加, 60-61
  ワークスペースラベルの変更, 60
「役割になる: *rolename* (Assume rolename role)」メニュー項目, 59-60
役割になる, 59-60

ゆ

ユーザー
  Trusted Extensions のオンラインヘルプの検索, 47-48
  あらゆるラベルの初期設定ファイルへのアクセス, 49-50
  ウィンドウを別のラベルのワークスペースに移動, 62-63
  オンラインヘルプの使用, 46-47
  画面のロック, 42-43
  画面のロック解除, 43
  異なるラベルのファイルのリンク, 70
  責任
    データ保護, 24-25
    デバイスのクリア, 27
    パスワードのセキュリティー, 76-77
    ワークステーションから離れるとき, 43-44
  データのセキュリティーレベル変更の承認, 64-67
  デバイスの割り当て, 55-58
  パスワードの変更, 53-54
  ファイルのラベルの判断, 63-64
  ファイルのラベル変更の承認, 67-70
  別のラベルにログイン, 54
  別のラベルのワークスペースに切り替える, 62
  役割になる, 59-60
  ラベル間でデータを移動, 64-67
  ラベル間でファイルを移動, 67-70
  ラベル付きワークスペースの追加, 60-61
  ログアウト, 43-44
  ワークステーションのシャットダウン, 44-45
  ワークスペースにファイルを表示, 45-46
  ワークスペースメニューのカスタマイズ, 48-49
  ワークスペースラベルの変更, 60
ユーザー認可上限, 定義, 19
ユーザーの責任
  データ保護, 24-25
  パスワードのセキュリティー, 76-77
  ワークステーションから離れるとき, 42

よ

読み取りアクセス, ラベル付き環境, 23

ら

ラベル
「認可上限」も参照
Trusted Extensions での表示，73
ウィンドウの照会で決定，50-51
関係，22-24
構成要素，19-20
産業界のラベルサンプル，19
種類，19
情報のラベルを変更，24
政府のラベルの例，22
セッションラベルの設定，37
データの保護手段，25-27
データのラベルの変更，64-67
デスクトップでの表示，20, 41
範囲，19
ファイルのラベル変更，67-70
優位性，22-24
ラベル関係のサンプル，23
ラベル付きゾーン，21
ログイン時に認可上限を設定，25
ログイン時の設定，37
ラベル間の優位性，22-24
ラベルの格付け要素, 定義，19
ラベルのコンパートメント要素, 定義，19
ラベルの種類，19
ラベルのない画面
ログイン画面，32
ロック画面，43
ラベルの変更, トラブルシューティング，70
ラベル範囲
説明，19
範囲が制限されたワークステーションのトラブルシューティング，38

ろ

ログアウト
手順，43-44
ユーザーの責任，42
ログイン
5 つの手順，32
セキュリティー設定の確認，35-37
デスクトップの選択，33, 34
ログイン (続き)
トラブルシューティング，35, 37-38
復旧，37-38
別のラベル，54
マルチレベルデスクトップに遠隔で，38-39
ラベルまたは認可上限の選択，36
ログインプロセス，「ログイン」を参照

わ

ワークステーションのシャットダウン，44-45
ワークスペース
デフォルトラベルの設定，54
ラベル付き，26-27
ワークスペーススイッチ領域
Trusted Extensions CDE，78
説明図，26
ワークスペースメニュー
カスタマイズ，48-49
「システム保存停止 (Suspend System)」，44-45
「ワークスペースラベルを変更 (Change Workspace Label)」メニュー項目，60
割り当て
メディアのフォーマット，57
リムーバブルメディア，57