Oracle® Solaris Trusted Extensions 構成ガイド

Part No: 820–4576–12
2010 年 9 月

ORACLE®

100901@24661

目次

はじめに 13

1 Trusted Extensions のセキュリティー計画 21
Trusted Extensions でのセキュリティー計画 21
Trusted Extensions について 22
サイトのセキュリティーポリシーについて 22
Trusted Extensions の管理ストラテジの作成 23
ラベルストラテジの作成 23
システムのハードウェアと Trusted Extensions の容量の計画 24
トラステッドネットワークの計画 25
Trusted Extensions でのゾーン計画 26
マルチレベルアクセスの計画 28
Trusted Extensions での LDAP ネームサービスの計画 28
Trusted Extensions での監査の計画 29
Trusted Extensions でのユーザーセキュリティーの計画 29
Trusted Extensions の構成ストラテジの作成 30
Trusted Extensions を有効にする前に行なう情報の収集 32
Trusted Extensions の有効化前に行うシステムのバックアップ 32
管理者の立場から見た Trusted Extensions の有効化の結果 33

2 Trusted Extensions の構成ロードマップ 35
作業マップ: Trusted Extensions 用 Solaris システムの準備 35
作業マップ: Trusted Extensions の準備と有効化 35
作業マップ: Trusted Extensions の構成 37

3 Solaris OS への Trusted Extensions ソフトウェアの追加 (手順) 41
初期設定チームの担当 41

Trusted Extensions 用 Solaris OS のインストールまたはアップグレード 42
▼ Solaris システムをインストールして Trusted Extensions をサポートする 42
▼ インストール済み Solaris システムを Trusted Extensions 用に準備する 43
Trusted Extensions の有効化前の情報収集と決定事項 46
▼ Trusted Extensions の有効化前にシステム情報を収集する 46
▼ Trusted Extensions の有効化前にシステムおよびセキュリティーに関する事項を決定する 47
Trusted Extensions サービスの有効化 49
▼ Trusted Extensions の有効化 49

4 Trusted Extensions の構成 (手順) 51
Trusted Extensions での大域ゾーンの設定 51
▼ ラベルエンコーディングファイルを検査およびインストールする 52
▼ Trusted Extensions で IPv6 ネットワーキングを有効にする 56
▼ 解釈ドメインの構成 57
▼ ゾーンのクローンを作成するために ZFS プールを作成する 59
▼ Trusted Extensions を再起動してログインする 60
▼ Trusted Extensions で Solaris 管理コンソールサーバーを初期化する 61
▼ Trusted Extensions で大域ゾーンを LDAP クライアントにする 65
ラベル付きゾーンの作成 68
▼ `txzonemgr` スクリプトを実行する 69
▼ Trusted Extensions でネットワークインタフェースを構成する 70
▼ ゾーンに名前およびラベルを付ける 75
▼ ラベル付きゾーンをインストールする 77
▼ ラベル付きゾーンを起動する 78
▼ ゾーンのステータスを確認する 80
▼ ラベル付きゾーンをカスタマイズする 81
▼ Trusted Extensions でゾーンのコピーまたはクローンを行う 83
ネットワークインタフェースをラベル付きゾーンに追加し、ルーティングする 85
▼ 既存のラベル付きゾーンを経路指定するためにネットワークインタフェースを追加する 85
▼ 既存のラベル付きゾーンを経路指定するために大域ゾーンを使用しないネットワークインタフェースを追加する 88
▼ ラベル付きゾーンごとにネームサービスキャッシュを構成する 92
Trusted Extensions での役割とユーザーの作成 93
▼ 責務分離を実施する権利プロファイルを作成する 94

▼ Trusted Extensions でセキュリティー管理者役割を作成する 97
▼ 制限されたシステム管理者役割を作成する 99
▼ Trusted Extensions で役割になれるユーザーを作成する 100
▼ Trusted Extensions の役割が機能することを確認する 103
▼ ユーザーがラベル付きゾーンにログインできるようにする 104
Trusted Extensions でのホームディレクトリの作成 105
▼ Trusted Extensions でホームディレクトリサーバーを作成する 105
▼ Trusted Extensions でユーザーがホームディレクトリにアクセスできるようにする 106
既存のトラステッドネットワークへのユーザーとホストの追加 108
▼ LDAP サーバーに NIS ユーザーを追加する 108
Trusted Extensions の構成のトラブルシューティング 110
Trusted Extensions の有効化後に `netservices limited` が実行された 110
ラベル付きゾーンでコンソールウィンドウが開かない 111
ラベル付きゾーンが X サーバーにアクセスできない 111
その他の Trusted Extensions 構成タスク 114
▼ Trusted Extensions でファイルをポータブルメディアにコピーする方法 114
▼ Trusted Extensions でポータブルメディアからファイルをコピーする方法 115
▼ Trusted Extensions をシステムから削除する 117

5 Trusted Extensions のための LDAP の構成 (手順) 119
Trusted Extensions ホストでの LDAP サーバーの構成 (作業マップ) 119
Trusted Extensions ホストでの LDAP プロキシサーバーの構成 (作業マップ) 120
Trusted Extensions システムでの Sun Java System Directory Server の構成 121
▼ LDAP 用に Directory Server の情報を収集する 121
▼ Sun Java System Directory Server をインストールする 122
▼ Directory Server 用の LDAP クライアントの作成 125
▼ Sun Java System Directory Server のログを構成する 127
▼ Sun Java System Directory Server のマルチレベルポートを設定する 128
▼ Sun Java System Directory Server にデータを入力する 129
既存の Sun Java System Directory Server のための Trusted Extensions プロキシの作成 . 131
▼ LDAP プロキシサーバーを作成する 132
LDAP のための Solaris 管理コンソールの設定 (作業マップ) 132
▼ LDAP の資格を Solaris 管理コンソールに登録する 133
▼ Solaris 管理コンソール でのネットワーク接続の受け付けを有効にする 134

▼ Solaris 管理コンソールの LDAP ツールボックスを編集する 135
▼ Solaris 管理コンソールに Trusted Extensions 情報が含まれていることを確認する 136

6 Trusted Extensions とヘッドレスシステムの構成 (タスク) 139
Trusted Extensions でのヘッドレスシステムの構成 (作業マップ) 139
▼ Trusted Extensions での root による遠隔ログインを有効にする 141
▼ Trusted Extensions での役割による遠隔ログインを有効にする 141
▼ ラベルなしシステムからの遠隔ログインを有効にする 143
▼ 遠隔の Solaris 管理コンソール を使用してファイルスコープで管理する 144
▼ 管理 GUI の遠隔表示を有効にする 145
▼ rlogin または ssh コマンドを使用して Trusted Extensions のヘッドレスシステムにログインする 145

A サイトのセキュリティーポリシー 149
セキュリティーポリシーの作成と管理 149
サイトのセキュリティーポリシーと Trusted Extensions 150
コンピュータのセキュリティーに関する推奨事項 151
物理的セキュリティーに関する推奨事項 152
個人のセキュリティーに関する推奨事項 153
よくあるセキュリティー違反 153
その他のセキュリティー関連資料 154
米国政府出版物 154
UNIX のセキュリティーに関する出版物 155
一般的なコンピュータセキュリティーに関する出版物 155
UNIX 全般に関する出版物 155

B Trusted Extensions での CDE アクションを使用したゾーンのインストール 157
CDE アクションを使用したネットワークインタフェースとゾーンの結合 (作業マップ) 157
▼ CDE アクションを使用してシステムに 2 つの IP アドレスを指定する 158
▼ CDE アクションを使用してシステムに 1 つの IP アドレスを指定する 159
CDE アクションを使用したゾーン作成の準備 (作業マップ) 160
▼ CDE アクションを使用してゾーン名とゾーンラベルを指定する 161
CDE アクションを使用したラベル付きゾーンの作成 (作業マップ) 163

▼CDE アクションを使用してラベル付きゾーンをインストール、初期化、および起動する 164
▼Trusted CDE でローカルゾーンを大域ゾーンルーティングに解決する 167
▼起動したゾーンを Trusted Extensions でカスタマイズする 168
▼ゾーンのコピー方法を Trusted Extensions で使用する 171
▼ゾーンのクローン作成方法を Trusted Extensions で使用する 171

C Trusted Extensions の構成チェックリスト 173
Trusted Extensions を構成するためのチェックリスト 173

用語集 177

索引 187

図目次

図 1–1 Trusted Extensions システムの管理: 役割によるタスク区分 32
図 4–1 Solaris 管理コンソール 初期ウィンドウ 62
図 4–2 Solaris 管理コンソールの Trusted Extensions ツール 64

表目次

表 1–1 Trusted Extensions のデフォルトのホストテンプレート 25
表 1–2 ユーザーアカウントに関する Trusted Extensions のセキュリティーデフォルト設定 29

はじめに

『Oracle Solaris Trusted Extensions 構成ガイド』ガイドでは、Solaris オペレーティングシステム (Solaris OS) 上で Trusted Extensions を構成する手順について説明します。また、Trusted Extensions を安全にインストールするための、Solaris システムの準備についても説明します。

注 – この Solaris のリリースでは、SPARC および x86 系列のプロセッサアーキテクチャーをサポートしています。サポートされるシステムについては、Solaris OS: Hardware Compatibility Lists (`http://www.sun.com/bigadmin/hcl`) を参照してください。本書では、プラットフォームにより実装が異なる場合は、それを特記します。

本書の x86 に関連する用語については、以下を参照してください。

- 「x86」は、64 ビットおよび 32 ビットの x86 互換製品系列を指します。
- 「x64」は、具体的には 64 ビット x86 互換 CPU を指します。
- 「32 ビット x86」は、x86 をベースとするシステムに関する 32 ビット特有の情報を指します。

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

対象読者

このマニュアルは、Trusted Extensions ソフトウェアを構成する熟練したシステム管理者およびセキュリティー管理者を対象にしています。サイトのセキュリティーポリシーによって求められる信頼度、および担当者の熟練度によって、構成タスクの実際の実行者が決まります。

サイトセキュリティーの実現

サイトに必要なセキュリティーに合わせた方法で、システムに対して Trusted Extensions を適切に構成するには、Trusted Extensions のセキュリティー機能とサイトのセキュリティーポリシーを理解する必要があります。作業を開始する前に、ソフトウェアの構成時の、サイトセキュリティーの確認方法については、第 1 章「Trusted Extensions のセキュリティー計画」を参照してください。

Trusted Extensions と Solaris オペレーティングシステム

Trusted Extensions は、Solaris OS の上で動作します。Trusted Extensions ソフトウェアは Solaris OS を変更する場合があるので、Trusted Extensions では、Solaris のインストールオプションに関して特定の設定が必要になることがあります。詳細については、第 3 章「Solaris OS への Trusted Extensions ソフトウェアの追加 (手順)」を参照してください。また、Trusted Extensions のマニュアルは Solaris のマニュアルを補足するものです。管理者は Solaris と Trusted Extensions のマニュアルを利用できる必要があります。

内容の紹介

第 1 章「Trusted Extensions のセキュリティー計画」では、1 つ以上の Solaris システムで Trusted Extensions ソフトウェアを構成する際に考慮する必要がある、セキュリティーの問題を説明します。

第 2 章「Trusted Extensions の構成ロードマップ」では、Solaris システムに Trusted Extensions ソフトウェアを追加するための作業マップを示します。

第 3 章「Solaris OS への Trusted Extensions ソフトウェアの追加 (手順)」では、Trusted Extensions ソフトウェアのために Solaris システムを準備する手順を説明します。また、Trusted Extensions を有効化する手順も説明します。

第 4 章「Trusted Extensions の構成 (手順)」では、モニターがあるシステムで Trusted Extensions ソフトウェアを構成する手順を説明します。

第 5 章「Trusted Extensions のための LDAP の構成 (手順)」では、Trusted Extensions のために LDAP を構成する手順を説明します。

第 6 章「Trusted Extensions とヘッドレスシステムの構成 (タスク)」では、ヘッドレスシステムでの Trusted Extensions ソフトウェアの構成方法および管理方法を説明します。

付録 A「サイトのセキュリティーポリシー」では、サイトのセキュリティーポリシーに触れ、より幅広い視野で組織およびサイトのセキュリティーに関連して Trusted Extensions を説明します。

付録 B 「Trusted Extensions での CDE アクションを使用したゾーンのインストール」では、Trusted CDE アクションを使用してラベル付きゾーンを構成する方法を説明します。

付録 C 「Trusted Extensions の構成チェックリスト」では、初期設定チームのための構成チェックリストを示します。

用語集は、このマニュアルで使用されている用語を選択して定義します。

Trusted Extensions マニュアルセットの構成

次の表は、Trusted Extensions のマニュアルで取り上げられるトピックと、各マニュアルの対象読者の一覧です。

マニュアルのタイトル	トピック	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 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
『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 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
『Oracle Solaris 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。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 リリース版)』	旧版。Solaris 10 11/06 と Solaris 10 8/07 リリースの Trusted Extensions における Trusted Extensions を計画、インストール、および構成する方法を説明しています。	管理者、開発者
『Oracle Solaris Trusted Extensions 構成ガイド』	Solaris 10 5/08 リリース以降において、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
『Oracle 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』	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

マニュアルのタイトル	トピック	対象読者
『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

関連するインストールガイド

次に示すマニュアルには、Trusted Extensions ソフトウェアを準備する際に役立つ情報が記載されています。

『Oracle Solaris 10 9/10 Installation Guide: Basic Installations 』 – Solaris OS のインストールオプションに関する説明が記述されています。

『Oracle Solaris 10 9/10 Installation Guide: Custom JumpStart and Advanced Installations 』 – インストール方法および構成オプションに関する説明が記述されています。

『Oracle Solaris 10 9/10 Installation Guide: Planning for Installation and Upgrade 』 – Solaris OS のアップグレードのインストールに関する説明が記述されています。

関連資料

自分のサイトのセキュリティーポリシーに関する文書 – 自分のサイトのセキュリティーポリシーおよびセキュリティー手順が説明されています。

Solaris Common Desktop Environment: Advanced User's and System Administrator's Guide – 共通デスクトップ環境 (CDE) が説明されています。

現在インストールされているオペレーティングシステムの管理者ガイド – システムファイルのバックアップ方法が説明されています。

関連する Sun 以外の Web サイト情報

このマニュアルでは、Sun 以外の URL を挙げ、関連する補足情報を示す場合があります。

注 – このマニュアル内で引用する第三者の Web サイトの可用性について Oracle は責任を負いません。こうしたサイトやリソース上の、またはこれらを通じて利用可能な、コンテンツ、広告、製品、その他の素材について、Oracle は推奨しているわけではなく、Oracle はいかなる責任も負いません。Oracle は、これらのサイトあるいはリソースを通じて、またはこれらの利用可能なコンテンツ、製品、サービスの利用、および信頼性によって、あるいはそれに関連して発生するいかなる損害、損失、申し立てに対する一切の責任を負いません。

マニュアル、サポート、およびトレーニング

追加情報については、以下の Web サイトを参照してください。

- マニュアル (http://docs.sun.com)
- サポート (http://www.oracle.com/us/support/systems/index.html)
- トレーニング (http://education.oracle.com) – 左のナビゲーションバーで「Sun」のリンクをクリックします。

Oracle へのご意見

Oracle はドキュメントの品質向上のために、お客様のご意見やご提案をお待ちしています。誤りを見つけたり、改善に向けた提案などがある場合は、http://docs.sun.com で「Feedback」をクリックしてください。可能な場合には、ドキュメントのタイトルやパート番号に加えて、章、節、およびページ番号を含めてください。返信を希望するかどうかもお知らせください。

Oracle Technology Network (http://www.oracle.com/technetwork/index.html) では、Oracle ソフトウェアに関する広範なリソースが提供されています。

- ディスカッションフォーラム (http://forums.oracle.com) で技術的な問題や解決策を話し合う。
- Oracle By Example (http://www.oracle.com/technology/obe/start/index.html) のチュートリアルで、手順に従って操作を体験する。
- サンプルコード (http://www.oracle.com/technology/sample_code/index.html) をダウンロードする。

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'`

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

- 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*]

- Bash シェル、Korn シェル、および Bourne シェル

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

- Bash シェル、Korn シェル、および Bourne 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。

◆ ◆ ◆ 第 1 章

Trusted Extensions のセキュリティー計画

Oracle Solaris Trusted Extensions の機能は、サイトのセキュリティーポリシーの一部をソフトウェアに実装します。この章では、セキュリティーに関する概要、およびこのソフトウェアの構成管理に関する概要を説明します。

- 21 ページの「Trusted Extensions でのセキュリティー計画」
- 33 ページの「管理者の立場から見た Trusted Extensions の有効化の結果」

Trusted Extensions でのセキュリティー計画

この節では、Trusted Extensions ソフトウェアの有効化と構成の前に必要な計画について概説します。

- 22 ページの「Trusted Extensions について」
- 22 ページの「サイトのセキュリティーポリシーについて」
- 23 ページの「Trusted Extensions の管理ストラテジの作成」
- 23 ページの「ラベルストラテジの作成」
- 24 ページの「システムのハードウェアと Trusted Extensions の容量の計画」
- 25 ページの「トラステッドネットワークの計画」
- 26 ページの「Trusted Extensions でのゾーン計画」
- 28 ページの「マルチレベルアクセスの計画」
- 28 ページの「Trusted Extensions での LDAP ネームサービスの計画」
- 29 ページの「Trusted Extensions での監査の計画」
- 29 ページの「Trusted Extensions でのユーザーセキュリティーの計画」
- 30 ページの「Trusted Extensions の構成ストラテジの作成」
- 32 ページの「Trusted Extensions を有効にする前に行なう情報の収集」
- 32 ページの「Trusted Extensions の有効化前に行うシステムのバックアップ」

Trusted Extensions の構成タスクのチェックリストについては、付録 C 「Trusted Extensions の構成チェックリスト」を参照してください。サイトのローカライズについては、24 ページの「英語以外のロケールで Trusted Extensions を使用するお客

様」を参照してください。評価された構成の実行については、22 ページの「サイトのセキュリティーポリシーについて」を参照してください。

Trusted Extensions について

Solaris Trusted Extensions の有効化および構成は、実行可能ファイルの読み込み、サイトのデータの指定、構成変数の設定などのタスクにとどまりません。高度な予備知識が必要です。Trusted Extensions ソフトウェアは、次の概念に基づいたラベル付き環境を実現します。

- ほとんどの UNIX 環境でスーパーユーザーに割り当てられる機能を、個別の管理役割で実行できます。
- UNIX のアクセス権のほかに、データへのアクセスが特別なセキュリティータグによって制御されます。このようなタグを「ラベル」と言います。ラベルはユーザー、プロセス、およびデータファイルやディレクトリなどのオブジェクトに割り当てられます。
- 特定のユーザーおよびアプリケーションがセキュリティーポリシーを上書きできるようにできます。

サイトのセキュリティーポリシーについて

Trusted Extensions では、サイトのセキュリティーポリシーを Solaris OS と効率的に統合できます。そのためには、ポリシーの範囲、およびそのポリシーに対応する Trusted Extensions ソフトウェアの機能について、適切に理解する必要があります。適切に計画された構成では、サイトのセキュリティーポリシーの一貫性とシステムにおけるユーザーの作業の利便性とのバランスを取るようにしてください。

Trusted Extensions は、デフォルトで、次の保護プロファイルに対して情報技術セキュリティー評価のための共通基準 (Common Criteria for Information Technology Security Evaluation) (ISO/IEC 15408) の認証レベル EAL4 に準拠するように構成されます。

- ラベル付きセキュリティー保護プロファイル
- 制御アクセス保護プロファイル
- 役割ベースアクセス制御保護プロファイル

これらの評価レベルに適合するために、LDAP をネームサービスとして設定する必要があります。次のいずれかを行なった場合、構成が評価に準拠しなくなる可能性があります。

- `/etc/system` ファイルのカーネルスイッチの設定の変更。
- 監査またはデバイス割り当てのオフ。
- 次の構成ファイルのデフォルトエントリの変更。

- /usr/openwin/server/etc/*
- /usr/dt/app-defaults/C/Dt
- /usr/dt/app-defaults/C/Dtwm
- /usr/dt/app-defaults/C/SelectionManager
- /usr/dt/bin/Xsession
- /usr/dt/bin/Xtsolsession
- /usr/dt/bin/Xtsolusersession
- /usr/dt/config/sel_config
- /usr/X11/lib/X11/xserver/TrustedExtensionsPolicy

詳細は、Common Criteria の Web サイト (http://www.commoncriteriaportal.org/)を参照してください。

Trusted Extensions の管理ストラテジの作成

Trusted Extensions を有効化する責任は、root ユーザーまたはシステム管理者役割にあります。役割を作成すると、複数の機能の領域で管理担当を分割することができます。

- セキュリティー管理者は、機密ラベルの設定と割り当て、監査の設定、パスワードポリシーの設定などのセキュリティー関連のタスクを担当します。
- システム管理者は、セキュリティー以外の設定、保守、および全般的な管理を担当します。
- 主管理者は、セキュリティー管理者の権利プロファイルの作成、およびセキュリティー管理者やシステム管理者が十分な特権を持たない問題の修正を担当します。
- さらに制限を持つ役割を設定することもできます。たとえば、あるオペレータがファイルのバックアップを担当する可能性もあります。

管理ストラテジの一環として、次の事項を決定する必要があります。

- どのユーザーがどの管理タスクを実行するか
- 管理者以外のどのユーザーがトラステッドアプリケーションを実行できるか、すなわち、必要なときにどのユーザーがセキュリティーポリシーを上書きできるか
- どのユーザーがデータのどのグループにアクセスできるか

ラベルストラテジの作成

ラベルを計画するには、機密ラベルの階層を定め、システム上の情報を分類する必要があります。ラベルエンコーディングファイルには、サイトについてのこの種の情報が含まれます。Trusted Extensions インストールメディアで提供されている label_encodings ファイルのいずれかを使用できます。あるいは、その提供ファイルの

いずれかを変更したり、サイト固有の label_encodings ファイルを新たに作成したりできます。このファイルには、Sun 固有のローカルな拡張機能、少なくとも COLOR NAMES セクションを組み込んでください。

注意 – label_encodings ファイルを提供する場合は、Trusted Extensions サービスを有効化してシステムをリブートする前に、このファイルの最終版を準備しておく必要があります。このファイルはリムーバブルメディアに置きます。

ラベルの計画には、そのラベル構成の計画も含まれます。Trusted Extensions サービスを有効化したあと、システムが 1 つのラベルでのみ実行できるか、または複数のラベルで実行できるかを決定する必要があります。管理を行わないすべてのユーザーが同じセキュリティーラベルで操作できる場合には、単一ラベルシステムを選択します。

また、ラベルを表示するかどうか、およびどのラベル名形式を表示するかも設定できます。詳細は、『Solaris Trusted Extensions ラベルの管理』を参照してください。『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』も参照してください。

英語以外のロケールで Trusted Extensions を使用するお客様

英語以外のロケールを使用するお客様が label_encodings ファイルをローカライズする場合は、ラベル名のみをローカライズしてください。管理ラベル名の ADMIN_HIGH および ADMIN_LOW をローカライズしてはいけません。いずれのベンダー製であれ、接続するラベル付きホストの名前はすべて、label_encodings ファイル内のラベル名と一致する必要があります。

Trusted Extensions でサポートされるロケールは Solaris OS より少ないです。Trusted Extensions でサポートされないロケールで作業する場合、ラベルに関するエラーメッセージなど、Trusted Extensions に固有のテキストは、そのロケールに翻訳されません。Solaris ソフトウェアは、使用中のロケールに翻訳されたまま、変化することはありません。

システムのハードウェアと Trusted Extensions の容量の計画

システムハードウェアには、システムそのものとそれに接続されるデバイスが含まれます。接続されるデバイスには、テープドライブ、マイクロフォン、CD-ROM ドライブ、およびディスクパックが含まれます。ハードウェアの容量には、システムメモリー、ネットワークインタフェース、およびディスク容量があります。

- Solaris リリースをインストールする場合、『Solaris 10 5/09 Installation Guide: Basic Installations』の「System Requirements and Recommendations」の推奨事項に従ってください。そこに示されるほかに、Trusted Extensions ではさらに追加される要件があります。

  次のシステムでは、推奨される最小容量よりも多くのメモリーが必要です。

  - 必要な管理 GUI である Solaris 管理コンソール を実行するシステム
  - 複数の機密ラベルで実行されるシステム
  - 管理役割になれるユーザーが使用するシステム
- 次のシステムではより多くのディスク容量が必要です。
  - 複数のラベルでファイルを格納するシステム
  - ユーザーが管理役割になれるシステム

トラステッドネットワークの計画

ネットワークハードウェアの計画の参考として、『System Administration Guide: IP Services』の第 2 章「Planning Your TCP/IP Network (Tasks)」を参照してください。

ほかのクライアントサーバーネットワークの場合と同様に、サーバーまたはクライアントという機能によってホストを区別し、それぞれ適切にソフトウェアを設定する必要があります。この計画の参考として、『Solaris 10 5/09 Installation Guide: Custom JumpStart and Advanced Installations』を参照してください。

Trusted Extensions ソフトウェアは、ラベル付きホストとラベルなしホストの 2 種類を識別します。どちらの種類のホストにも、表 1–1 に示すデフォルトのセキュリティーテンプレートがあります。

表 1–1　Trusted Extensions のデフォルトのホストテンプレート

ホストの種類	テンプレート名	目的
`unlabeled`	`admin_low`	初期起動時、大域ゾーンをラベル付けします。 初期起動後、ラベルなしパケットを送信するホストを特定します。
`cipso`	`cipso`	CIPSO パケットを送信するホストまたはネットワークを特定します。CIPSO パケットはラベル付けされます。

ネットワークにほかのネットワークによる到達性がある場合、アクセス可能なドメインおよびホストを指定する必要があります。また、どの Trusted Extensions のホストが、ゲートウェイとしての機能を果たすかも特定する必要があります。ゲートウェイ用のラベルの認可範囲と、ほかのホストのデータを表示できる機密ラベルを、指定する必要があります。

smtnrhtp(1M) のマニュアルページには、各種類のホストの詳細な説明と例があります。

Trusted Extensions でのゾーン計画

Trusted Extensions ソフトウェアは、Solaris OS の大域ゾーンに追加されます。そのあとで、ラベル付きの非大域ゾーンを設定します。重複しないすべてのラベルに対してそれぞれ 1 つのラベル付きゾーンを作成できますが、すべてのラベルに対してゾーンを作成する必要はありません。

ゾーン構成の一部がネットワークを構成しています。大域ゾーンおよびネットワーク上のほかのゾーンと通信するためには、ラベル付きゾーンを構成します。

- デスクトップディスプレイを実行する X サーバーは、大域ゾーンからのみ利用できます。Solaris 10 10/08 リリースから、ループバックインタフェース `lo0` を使用して大域ゾーンと通信できるようになりました。そのため、デスクトップディスプレイは、`lo0` 経由で非大域ゾーンから利用できます。
- デフォルトでは、非大域ゾーンは大域ゾーンを使用してネットワークに到達します。Solaris 10 10/08 リリースから、各非大域ゾーンに、大域ゾーンを使用しない固有のデフォルトルートを構成できます。

Trusted Extensions ゾーンと Solaris ゾーン

ラベル付きゾーンは、通常の Solaris のゾーンとは異なります。ラベル付きゾーンは、主にデータを分けるために使用されます。Trusted Extensions では、一般ユーザーはラベル付きゾーンに遠隔からログインすることはできません。ラベル付きゾーンに対する唯一の対話型インタフェースは、ゾーンコンソールにあります。root のみがゾーンコンソールにアクセスできます。

Trusted Extensions でのゾーン作成

ラベル付きゾーンを作成するには、Solaris OS 全体をコピーし、すべてのゾーンで Solaris OS のサービスを起動します。この手順は時間がかかります。1 つのゾーンを作成して、そのゾーンをコピーするかゾーンの内容のクローンを作成すると、それほど時間がかかりません。次の表は、Trusted Extensions でゾーンを作成するオプションを示します。

ゾーンの作成方法	必要な作業	この方法の特色
ラベル付きの各ゾーンを最初から作成します。	ラベル付きの各ゾーンを設定、初期化、インストール、カスタマイズ、および起動します。	■ この方法はサポートされています。1 つまたは 2 つの追加ゾーンを作成する場合に便利です。ゾーンをアップグレードできます。 ■ この方法は時間がかかります。

ゾーンの作成方法	必要な作業	この方法の特色
最初のラベル付きのゾーンのコピーから追加のラベル付きゾーンを作成します。	1 つのゾーンを設定、初期化、インストール、およびカスタマイズします。このゾーンを追加のラベル付きゾーンのテンプレートとして使用します。	■ この方法はサポートされています。最初からゾーンを作成する場合ほど時間がかかりません。ゾーンをアップグレードできます。ゾーンに問題がある場合に Sun のサポートを必要とする場合は、このゾーンのコピー方法を使用します。 ■ この方法は UFS を使用します。UFS には、Solaris ZFS で提供される追加のゾーンの切り離し機能はありません。
最初のラベル付きゾーンの ZFS スナップショットから追加のラベル付きゾーンを作成します。	Solaris のインストール時に確保したパーティションから ZFS プールを設定します。 1 つのゾーンを設定、初期化、インストール、およびカスタマイズします。このゾーンを ZFS スナップショットとして、追加のラベル付きゾーンに対して使用します。	■ この方法では Solaris ZFS を使用しますが、これがもっとも時間のかからない方法です。この方法は、すべてのゾーンをそれぞれファイルシステムにするため、UFS よりも高い分離性を提供します。ZFS では、はるかに少ないディスク容量を使用します。 ■ Trusted Extensions をテストし、ゾーンをアップグレードではなく再インストールできる場合に適している方法です。システムを再インストールしてすばやく使用可能な状態にできるので、コンテンツが揮発性ではないシステムでは、この方法が便利です。 ■ この方法はサポートされていません。この方法で作成されるゾーンは、Solaris OS の最新のバージョンがリリースされるときにアップグレードできません。

Solaris ゾーンは、パッケージのインストールおよびパッチの適用に影響します。詳細は、次のマニュアルページを参照してください。

- 『System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones』の第 25 章「About Packages and Patches on a Solaris System With Zones Installed (Overview)」
- Solaris のゾーンとコンテナについてのよく寄せられる質問 (FAQ) (`http://hub.opensolaris.org/bin/view/Community+Group+zones/faq`)

マルチレベルアクセスの計画

通常、印刷および NFS は、マルチレベルサービスとして設定されます。マルチレベルサービスにアクセスするには、適切に構成されたシステムで、すべてのゾーンが 1 つ以上のネットワークアドレスにアクセスできなければなりません。次の構成においてマルチレベルサービスが可能です。

- Solaris OS と同様に、大域ゾーンを含むすべてのゾーンに対してそれぞれの IP アドレスが割り当てられている。ゾーンごとに別々のネットワーク情報カード (NIC) を割り当てれば、この構成がさらに改善される。このような構成は、各 NIC に関連付けられている単一ラベルのネットワークを物理的に分離するために使用される。
- `all-zones` の 1 つのアドレスが割り当てられている。1 つ以上のゾーンがゾーン固有のアドレスを持つことができる。

次の 2 つの条件に合うシステムはマルチレベルサービスを行えません。

- 1 つの IP アドレスが割り当てられ、大域ゾーンとラベル付きゾーンが共有する。
- ゾーン固有のアドレスが 1 つも割り当てられていない。

ラベル付きゾーンのユーザーがローカルのマルチレベルプリンタにアクセスすることを想定しておらず、ホームディレクトリの NFS エクスポートも必要ない場合、Trusted Extensions が設定されたシステムに対して 1 つの IP アドレスを割り当てることができます。このようなシステムでは、マルチレベル印刷はサポートされず、ホームディレクトリを共有できません。この構成は、主としてラップトップコンピュータで使用します。

Trusted Extensions での LDAP ネームサービスの計画

ラベル付きシステムのネットワークの構成を計画していない場合、この節は省略できます。

システムのネットワーク上で Trusted Extensions を実行する予定の場合は、LDAP をネームサービスとして使用します。Trusted Extensions で、システムのネットワークを構成する場合、データ入力された Sun Java System Directory Server (LDAP サーバー) が必要です。サイトに既存の LDAP サーバーがある場合、Trusted Extensions データベースをそのサーバーに転送できます。そのサーバーにアクセスするには、Trusted Extensions システムに LDAP プロキシを設定します。

サイトに既存の LDAP サーバーがない場合、Trusted Extensions ソフトウェアを実行するシステムで LDAP サーバーを作成するようにします。手順については、第 5 章「Trusted Extensions のための LDAP の構成 (手順)」を参照してください。

Trusted Extensions での監査の計画

デフォルトでは、Trusted Extensions がインストールされるときに監査がオンに設定されます。したがって、デフォルトでは root ログインおよび root ログアウトが監査されます。システムを構成しようとするユーザーを監査するために、構成プロセスの最初の段階で役割を作成できます。手順については、93 ページの「Trusted Extensions での役割とユーザーの作成」を参照してください。

Trusted Extensions での監査の計画は、Solaris OS の場合と同じです。詳細は、『System Administration Guide: Security Services』のパート VII「OpenSolaris Auditing」を参照してください。Trusted Extensions は、クラス、イベント、および監査トークンを追加しますが、監査の管理方法は変更されません。監査に対する Trusted Extensions による追加については、『Oracle Solaris Trusted Extensions 管理の手順』の第 18 章「Trusted Extensions での監査 (概要)」を参照してください。

Trusted Extensions でのユーザーセキュリティーの計画

Trusted Extensions ソフトウェアでは、ユーザーに対して妥当なセキュリティーデフォルト設定を提供しています。このようなセキュリティーデフォルト設定を表 1–2 に示します。2 つの値が示されている場合、最初の値がデフォルト値です。セキュリティー管理者は、サイトのセキュリティーポリシーに合わせてデフォルト値を変更できます。セキュリティー管理者がデフォルト設定を行なったあと、システム管理者がすべてのユーザーを作成できます。それらのユーザーは設定されたデフォルト値を継承します。このようなデフォルト設定のキーワードや値については、label_encodings(4) および policy.conf(4) のマニュアルページを参照してください。

表 1–2　ユーザーアカウントに関する Trusted Extensions のセキュリティーデフォルト設定

ファイル名	キーワード	値
/etc/security/policy.conf	IDLECMD	lock|logout
	IDLETIME	30
	CRYPT_ALGORITHMS_ALLOW	1,2a,md5,5,6
	CRYPT_DEFAULT	_unix_
	LOCK_AFTER_RETRIES	no|yes
	PRIV_DEFAULT	basic
	PRIV_LIMIT	all
	AUTHS_GRANTED	solaris.device.cdrw

表 1–2 ユーザーアカウントに関する Trusted Extensions のセキュリティーデフォルト設定 (続き)

ファイル名	キーワード	値
	PROFS_GRANTED	Basic Solaris User
/etc/security/tsol/label_encodings の LOCAL DEFINITIONS セクション	Default User Clearance	CNF NEED TO KNOW
	Default User Sensitivity Label	PUBLIC

システム管理者は、すべてのユーザーに適切なシステムデフォルト値を設定するための標準ユーザーテンプレートを作成できます。たとえば、デフォルトでは各ユーザーの初期シェルは Bourne シェルです。システム管理者は、各ユーザーに対して C シェルを設定したテンプレートを作成できます。詳細は、Solaris 管理コンソール のオンラインヘルプで「ユーザーアカウント」を参照してください。

Trusted Extensions の構成ストラテジの作成

root ユーザーが Trusted Extensions ソフトウェアを構成できるようにするストラテジは、安全ではありません。次に、もっとも安全な構成ストラテジから順に示します。

- 2 人のチームでソフトウェアを構成します。構成プロセスは監査されます。

  ソフトウェアを有効化するとき、2 人でコンピュータに向かいます。構成プロセスの早い段階で、チームはローカルユーザーおよび役割を作成します。チームは、役割によって実行されるイベントを監査するための監査も設定します。役割がユーザーに割り当てられ、コンピュータが再起動されたあと、役割によるタスク区分をソフトウェアが実施します。監査証跡が構成プロセスの記録を提供します。安全な構成プロセスの図については、図 1–1 を参照してください。

  注 – サイトセキュリティーで責務分離が必要な場合は、ユーザーや役割を作成する前に、信頼できる管理者が、94 ページの「責務分離を実施する権利プロファイルを作成する」を完了します。このカスタマイズされた設定では、1 つの役割が、ユーザーのセキュリティー属性を含むセキュリティーを管理します。ほかの役割は、システムおよびユーザーのセキュリティー以外の属性を管理します。

- 1 人が適切な役割になり、ソフトウェアを有効化および構成します。構成プロセスは監査されます。

構成プロセスの早い段階で、root ユーザーがローカルユーザーおよび役割を作成します。同じユーザーが、役割によって実行されるイベントをチェックするための監査も設定します。役割がローカルユーザーに割り当てられ、コンピュータが再起動されると、役割によるタスク区分をソフトウェアが実施します。監査証跡が構成プロセスの記録を提供します。

- 1 人が適切な役割になり、ソフトウェアを有効化および構成します。構成プロセスは監査されません。

  このストラテジでは、構成プロセスは記録されません。

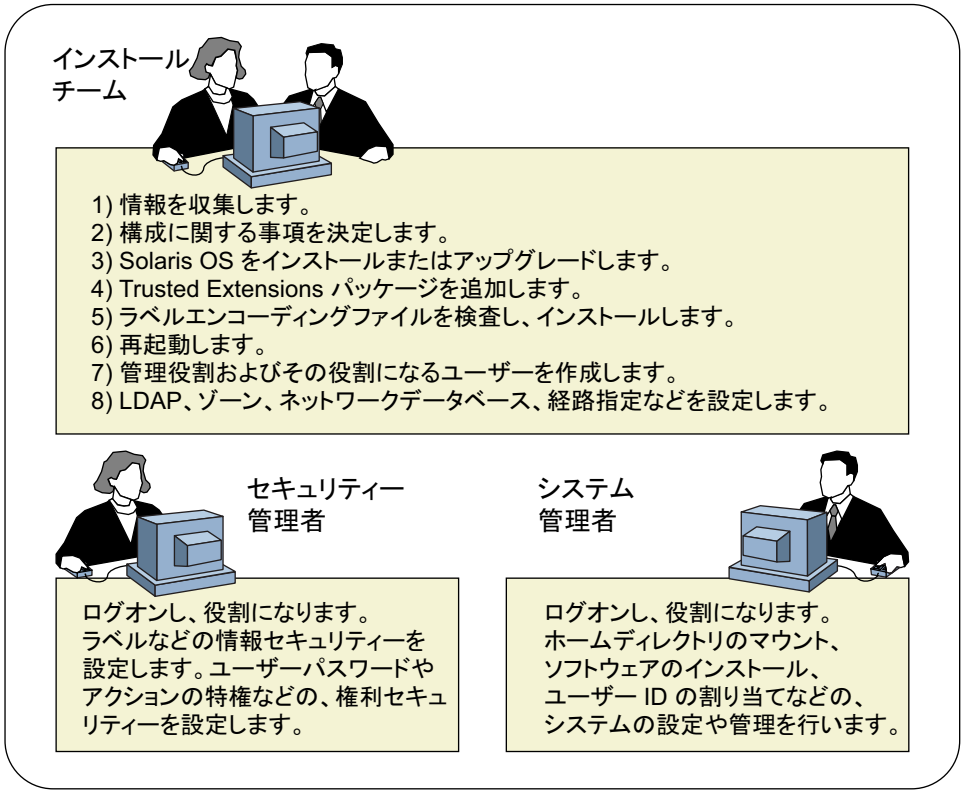
- root ユーザーがソフトウェアを有効化および構成します。構成プロセスは監査されます。

  チームは、構成時に root で実行されるすべてのイベントをチェックするための監査を設定します。このストラテジでは、監査するイベントを、そのチームが決定しなければなりません。監査証跡には root として操作するユーザーの名前は含まれません。

- root ユーザーがソフトウェアを有効化および構成します。

役割によるタスク区分を次の図に示します。セキュリティー管理者は、特に、監査の設定、ファイルシステムの保護、デバイスポリシーの設定、実行権を必要とするプログラムの決定、およびユーザーの保護を担当します。システム管理者は、特に、ファイルシステムの共有とマウント、ソフトウェアパッケージのインストール、およびユーザーの作成を担当します。

図 1–1　Trusted Extensions システムの管理: 役割によるタスク区分



Trusted Extensions を有効にする前に行なう情報の収集

Solaris OS を構成する場合と同様に、Trusted Extensions を構成する前に、システム、ユーザー、ネットワーク、およびラベルに関する情報を収集します。詳細は、46 ページの「Trusted Extensions の有効化前にシステム情報を収集する」を参照してください。

Trusted Extensions の有効化前に行うシステムのバックアップ

保存しなければならないファイルがシステムにある場合は、Trusted Extensions ソフトウェアを有効化する前にバックアップを実行します。ファイルをもっとも安全にバックアップする方法は、レベル 0 ダンプです。適切なバックアップ手順がわからない場合、現在のオペレーティングシステムの管理者ガイドを参照してください。

注 – Trusted Solaris 8 リリースから移行する場合、Trusted Extensions のラベルが Trusted Solaris 8 のラベルと同一であるときのみデータを復元できます。Trusted Extensions ではマルチレベルディレクトリが作成されないので、バックアップメディアの各ファイルおよびディレクトリは、バックアップのファイルラベルと同じラベルのゾーンに復元されます。バックアップは、Trusted Extensions を有効にしてシステムをリブートする前に、必ず完了してください。

管理者の立場から見た Trusted Extensions の有効化の結果

Trusted Extensions ソフトウェアの有効化とシステムのリブートが完了すると、次の各セキュリティー機能が使用可能になっています。多くの機能はセキュリティー管理者が変更できます。

- 監査が有効化されます。
- Sun label_encodings ファイルがインストールされて構成されます。
- 2 つのトラステッドデスクトップが追加されます。Solaris Trusted Extensions (CDE) は CDE のトラステッドバージョンです。Solaris Trusted Extensions (JDS) は Sun Java Desktop System のトラステッドバージョンです。各ウィンドウ表示の環境では、トラステッドパスのワークスペースが大域ゾーンに作成されます。
- Solaris OS と同様に、役割の権利プロファイルが定義されます。Solaris OS と同様に、役割が定義されません。

  役割を使用して Trusted Extensions を管理するためには、その役割を作成する必要があります。構成時に、セキュリティー管理者役割を作成します。
- 3 つの Trusted Extensions ネットワークデータベース `tnrhdb`、`tnrhtp`、および `tnzonecfg` が追加されます。これらのデータベースは、Solaris 管理コンソールの「セキュリティーテンプレート」ツールおよび「トラステッドネットワークゾーン」ツールを使用して管理します。
- Trusted Extensions に、システムを管理するための GUI が表示されます。一部の GUI は Solaris OS GUI の拡張機能です。
  - Trusted CDE で、管理アクションが Trusted_Extensions フォルダに提供されます。これらのアクションの一部は、Trusted Extensions を最初に構成するときに使用されます。ツールの概要は、『Oracle Solaris Trusted Extensions 管理の手順』の第 2 章「Trusted Extensions 管理ツール」で説明されています。
  - トラステッドエディタを使用すると、管理者はローカル管理ファイルを変更できます。Trusted CDE では、「管理エディタ」アクションでトラステッドエディタを起動します。
  - デバイス割り当てマネージャーが、接続されているデバイスを管理します。

- Solaris管理コンソールでは、ローカルおよびネットワーク管理のデータベースを管理するためにJavaベースのツールを用意しています。トラステッドネットワーク、ゾーン、およびユーザーを管理するために、このツールを使用する必要があります。

◆ ◆ ◆ 第 2 章

Trusted Extensions の構成ロードマップ

この章では、Trusted Extensions ソフトウェアの有効化および構成を行うための作業について説明します。

作業マップ: Trusted Extensions 用 Solaris システムの準備

Trusted Extensions 用 Solaris OS が、使用する Trusted Extensions の機能をサポートしていることを確認します。次の作業マップで説明する 2 つのタスクのいずれかを完了します。

作業	参照先
Trusted Extensions のために既存またはアップグレード済みの Solaris インストールを準備します。	43 ページの「インストール済み Solaris システムを Trusted Extensions 用に準備する」
Trusted Extensions の機能を考慮して Solaris OS をインストールします。	42 ページの「Solaris システムをインストールして Trusted Extensions をサポートする」

作業マップ: Trusted Extensions の準備と有効化

Trusted Extensions システムを構成する前にその準備を整えるには、次の作業マップで説明するタスクを完了してください。

作業	参照先
Solaris システムの準備を完了します。	35 ページの「作業マップ: Trusted Extensions 用 Solaris システムの準備」

作業	参照先
システムをバックアップします。	Trusted Solaris 8 システムの場合、使用しているリリースのマニュアルにある説明に従って、システムをバックアップします。ラベル付きバックアップは、それぞれ、同じラベルを持つゾーンに復元できます。
	Solaris システムの場合は、『Solaris のシステム管理 (基本編)』を参照してください。
システムおよび Trusted Extensions ネットワークに関する情報を収集し、必要な事項を決定します。	46 ページの「Trusted Extensions の有効化前の情報収集と決定事項」
Trusted Extensions を有効にします。	49 ページの「Trusted Extensions の有効化」
システムを構成します。	モニター付きのシステムの場合、37 ページの「作業マップ: Trusted Extensions の構成」を参照してください。
	ヘッドレスシステムの場合、139 ページの「Trusted Extensions でのヘッドレスシステムの構成 (作業マップ)」を参照してください。
	Sun Ray については、『Sun Ray Server Software 4.1 Installation and Configuration Guide for the Solaris Operating System 』を参照してください。Sun Ray 5 リリースについては、Sun Ray Server 4.2 および Sun Ray Connector 2.2 マニュアル (`http://wikis.sun.com/display/SRS/Home`)の Web サイトを参照してください。このサーバーとクライアントは、合わせて Sun Ray 5 パッケージを構成しています。 初期クライアントサーバー通信を設定するには、『Oracle Solaris Trusted Extensions 管理の手順』の「トラステッドネットワークデータベースの構成 (作業マップ)」を参照してください。
	ノートパソコンの場合、OpenSolaris Community: Security Web ページ (`http://hub.opensolaris.org/bin/view/Community+Group+security/`)を参照してください。「Trusted Extensions」をクリックします。「Trusted Extensions」ページの「Laptop Configurations」にある「`Laptop instructions`」をクリックします。
	ネットワークが大域ゾーンと通信しないようにするため、`vni0` インタフェースを構成します。例については、「`Laptop instructions`」を参照してください。 Solaris 10 10/08 リリースから、`vni0` インタフェースを構成する必要はありません。デフォルトでは、`lo0` インタフェースは `all-zones` インタフェースです。Trusted Extensions で DHCP を使用する場合、ノートパソコンに関するほかの手順も参照してください。

作業マップ:Trusted Extensions の構成

セキュリティー保護された構成プロセスを実現するには、早い段階で役割を作成してください。役割によってシステムを構成する際のタスクの順序を、次の作業マップに示します。

1. 大域ゾーンを構成します。	
タスク	参照先
ハードウェア設定を変更する際にパスワードの入力を求めることによって、マシンハードウェアを保護します。	『System Administration Guide: Security Services』の「Controlling Access to System Hardware」
ラベルを設定します。ラベルはサイトに合わせて設定する必要があります。デフォルトの `label_encodings` ファイルを使用する場合、このタスクは省略できます。	52 ページの「ラベルエンコーディングファイルを検査およびインストールする」
IPv6 ネットワークを実行する場合、ラベル付きパケットが IP によって認識されるように `/etc/system` ファイルを変更します。	56 ページの「Trusted Extensions で IPv6 ネットワーキングを有効にする」
ネットワークノードの CIPSO 解釈ドメイン (DOI) が 1 でない場合は、`/etc/system` ファイル内でその DOI を指定します。	57 ページの「解釈ドメインの構成」
ゾーンのクローンを作成するために Solaris ZFS スナップショットを使用する場合は、ZFS プールを作成します。	59 ページの「ゾーンのクローンを作成するために ZFS プールを作成する」
ラベル付きの環境をアクティブにするために起動します。ログインすると、大域ゾーンになります。システムの `label_encodings` ファイルによって必須アクセス制御 (MAC) を実施します。	60 ページの「Trusted Extensions を再起動してログインする 」
Solaris 管理コンソールを初期化します。この GUI は、いくつかあるほかのタスクの中で、ゾーンにラベルを付けるために使用します。	61 ページの「Trusted Extensions で Solaris 管理コンソールサーバーを初期化する」
セキュリティー管理者役割およびローカルに使用するその他の役割を作成します。これらの役割は Solaris OS の場合と同様に作成します。 このタスクは最後まで延期できます。その結果については、30 ページの「Trusted Extensions の構成ストラテジの作成」を参照してください。	93 ページの「Trusted Extensions での役割とユーザーの作成」 103 ページの「Trusted Extensions の役割が機能することを確認する」

ローカルファイルを使用してシステムの管理を行っている場合は、次の一連の手順を省略します。

2. ネームサービスを構成します。

	タスク	参照先
	ファイルを使用して Trusted Extensions を管理する場合、次のタスクを省略できます。	ファイルのネームサービスには、何も構成する必要はありません。
	既存の Sun Java System Directory Server (LDAP サーバー) がある場合、そのサーバーに Trusted Extensions データベースを追加します。次に、最初の Trusted Extensions システムを LDAP サーバーのプロキシにします。 LDAP サーバーがない場合、最初のシステムをサーバーとして構成します。	第 5 章「Trusted Extensions のための LDAP の構成 (手順)」
	Solaris 管理コンソールの LDAP ツールボックスを手動で設定します。このツールボックスを使用して、ネットワークオブジェクトに関する Trusted Extensions 属性を変更できます。	132 ページの「LDAP のための Solaris 管理コンソールの設定 (作業マップ)」
	LDAP サーバーでもプロキシサーバーでもないシステムの場合、それを LDAP クライアントにします。	65 ページの「Trusted Extensions で大域ゾーンを LDAP クライアントにする」
	LDAP スコープで、セキュリティー管理者役割および使用するつもりであるその他の役割を作成します。 このタスクは最後まで延期できます。その結果については、30 ページの「Trusted Extensions の構成ストラテジの作成」を参照してください。	93 ページの「Trusted Extensions での役割とユーザーの作成」 103 ページの「Trusted Extensions の役割が機能することを確認する」

3. ラベル付きゾーンを作成します。

	タスク	参照先
	`txzonemgr` コマンドを実行します。 ネットワークインタフェースを構成するメニューに従って、最初のラベル付きゾーンを作成し、カスタマイズします。次に、残りのゾーンをコピーするか、そのゾーンのクローンを作成します。	68 ページの「ラベル付きゾーンの作成」
	あるいは、Trusted CDE アクションを使用します。	付録 B 「Trusted Extensions での CDE アクションを使用したゾーンのインストール」
	(省略可能) すべてのゾーンが正常にカスタマイズされたあとで、ゾーン固有のネットワークアドレスおよびデフォルトのルーティングをラベル付きゾーンに追加します。	85 ページの「ネットワークインタフェースをラベル付きゾーンに追加し、ルーティングする」

使用する環境によっては、次のタスクが必要になる場合があります。

4. システムの設定を完了します。

	タスク	参照先
	ラベルを必要とする追加の遠隔ホスト、1 つ以上のマルチレベルのポート、または異なる制御メッセージポリシーを特定します。	『Oracle Solaris Trusted Extensions 管理の手順』の「トラステッドネットワークデータベースの構成 (作業マップ)」
	マルチレベルのホームディレクトリサーバーを作成し、インストールされたゾーンを自動マウントします。	105 ページの「Trusted Extensions でのホームディレクトリの作成」
	ユーザーによるシステムへのログインを有効にする前に、監査の設定、ファイルシステムのマウント、およびその他のタスクを実行します。	『Oracle Solaris Trusted Extensions 管理の手順』
	NIS 環境から LDAP サーバーにユーザーを追加します。	108 ページの「LDAP サーバーに NIS ユーザーを追加する」
	ホストとそのラベル付きゾーンを LDAP サーバーに追加します。	『Oracle Solaris Trusted Extensions 管理の手順』の「トラステッドネットワークデータベースの構成 (作業マップ)」

◆ ◆ ◆ 第 3 章

Solaris OS への Trusted Extensions ソフトウェアの追加 (手順)

この章では、Trusted Extensions ソフトウェア向けに Solaris OS を準備する方法を説明します。また、Trusted Extensions を有効化する前に必要な情報についても説明します。Trusted Extensions を有効化する手順についても説明します。

- 41 ページの「初期設定チームの担当」
- 42 ページの「Trusted Extensions 用 Solaris OS のインストールまたはアップグレード」
- 46 ページの「Trusted Extensions の有効化前の情報収集と決定事項」
- 49 ページの「Trusted Extensions サービスの有効化」

初期設定チームの担当

Trusted Extensions ソフトウェアは、別々のタスクを担当する 2 人によって有効化および構成されるように設計されています。しかし、Solaris インストールプログラムでは、この 2 つの役割によってタスクを区分できません。その代わり、タスクの区分は役割によって実行されます。Trusted Extensions のインストールが終了するまで役割とユーザーは作成されないので、有効化および構成は、少なくとも 2 人で構成される初期設定チームで行うことをお勧めします。

Trusted Extensions 用 Solaris OS のインストールまたはアップグレード

Solaris のインストールオプションの選択によっては、Trusted Extensions の使用方法およびセキュリティーに影響することがあります。

- Trusted Extensions を適切にサポートするには、基盤となる Solaris OS を確実にインストールする必要があります。Trusted Extensions に影響する Solaris のインストールオプションについては、42 ページの「Solaris システムをインストールして Trusted Extensions をサポートする」を参照してください。
- すでに Solaris OS を使用している場合は、現在の構成を Trusted Extensions の要件と比較してください。Trusted Extensions に影響する構成については、43 ページの「インストール済み Solaris システムを Trusted Extensions 用に準備する」を参照してください。

▼ Solaris システムをインストールして Trusted Extensions をサポートする

ここに示すタスクは、Solaris OS のフレッシュインストールの場合に該当します。アップグレードの場合は、43 ページの「インストール済み Solaris システムを Trusted Extensions 用に準備する」を参照してください。

- **Solaris OS をインストールする場合、次のインストールの選択に関して推奨アクションを実行します。**

  各選択は、Solaris インストール時の質問の順序に合わせて記載しています。この表に示されないインストールの質問は、Trusted Extensions に影響しません。

Solaris のオプション	Trusted Extensions の動作	推奨アクション
NIS ネームサービス NIS+ ネームサービス	Trusted Extensions は、ネームサービスのファイルおよび LDAP をサポートします。ホスト名解決には、DNS を使用できます。	NIS および NIS+ を選択しないでください。ファイルを意味する「なし」を選択できます。あとで、Trusted Extensions で機能するよう LDAP を構成できます。
アップグレード	Trusted Extensions は、特定のセキュリティー特性を持つラベル付きゾーンをインストールします。	アップグレードの場合は、43 ページの「インストール済み Solaris システムを Trusted Extensions 用に準備する」を参照してください。

Solaris のオプション	Trusted Extensions の動作	推奨アクション
root パスワード	Trusted Extensions の管理ツールにはパスワードが必要です。root ユーザーにパスワードがない場合、root はシステムを構成できません。	root パスワードを入力します。デフォルトの crypt_unix パスワード暗号化方式は変更しないでください。詳細は、『System Administration Guide: Security Services』の「Managing Password Information」を参照してください。
開発者グループ	Trusted Extensions は、ネットワークの管理のために Solaris 管理コンソールを使用します。エンドユーザーグループおよびそれより小さいグループは、Solaris 管理コンソールのパッケージをインストールしません。	ほかのシステムを管理するシステムには、エンドユーザーグループ、コアグループ、および限定ネットワークグループをインストールしないでください。
カスタムインストール	Trusted Extensions はゾーンをインストールするので、デフォルトインストールのパーティションより多くのディスク容量が必要になる場合があります。	カスタムインストールを選択し、パーティションを配置します。 役割用にスワップ空間の追加を検討します。ゾーンのクローンを作成する場合は、ZFS プール用に 2000M バイトのパーティションを作成します。 監査ファイルには、専用パーティションを作成するようにしてください。

▼ インストール済み Solaris システムを Trusted Extensions 用に準備する

ここに示すタスクは、すでに使用している Solaris システムがあり、その上で Trusted Extensions を実行する場合に該当します。また、アップグレード済みの Solaris システム上で Trusted Extensions を実行する場合も、この手順に従います。インストール済みの Solaris システムを変更する可能性のあるタスクは、Trusted Extensions 構成時に実行できます。

始める前に　Trusted Extensions は一部の Solaris 環境では有効化できません。

- システムがクラスタの一部である場合、Trusted Extensions をそのシステム上で有効化することはできません。
- 代替ブート環境 (BE) での Trusted Extensions の有効化はサポートされていません。Trusted Extensions は、現在のブート環境でのみ有効化できます。

1 非大域ゾーンがシステムにインストールされている場合は、削除してください。

または Solaris OS を再インストールします。Solaris OS を再インストールする場合、42 ページの「Solaris システムをインストールして Trusted Extensions をサポートする」の手順に従います。

Trusted Extensions はブランドゾーンを使用します。

2 システムに root パスワードがない場合は作成します。

Trusted Extensions の管理ツールにはパスワードが必要です。root ユーザーにパスワードがない場合、root はシステムを構成できません。

デフォルトの crypt_unix パスワード暗号化方式を root ユーザーに使用します。詳細は、『System Administration Guide: Security Services』の「Managing Password Information」を参照してください。

注 – ユーザーはパスワードをほかの人に知られないようにしてください。その人がユーザーのデータにアクセスすると、アクセスした人を特定できず、責任を追求できなくなります。パスワードがほかの人に知られるのは、ユーザーが故意に教えてしまうような直接的な場合と、書き留めておいたパスワードを見られたり、安全でないパスワードを設定したりするなど、間接的な場合があります。Solaris OS では安全でないパスワードが設定されないようにできますが、ユーザーがパスワードを教えたり、書き留めたりするのを防止することはできません。

---

3 サイトをこのシステムから管理する場合は、**Solaris** 管理コンソール用の **Solaris** パッケージを追加します。

Trusted Extensions は、ネットワークの管理のために Solaris 管理コンソールを使用します。エンドユーザーグループまたはそれより小さいグループでインストールされたシステムには、Solaris 管理コンソールのパッケージはありません。

4 xorg.conf ファイルを作成した場合、それを変更する必要があります。

/etc/X11/xorg.conf ファイルの Module セクションの最後に、次の行を追加します。

```
load "xtsol"
```

注 – デフォルトでは、xorg.conf ファイルはありません。このファイルがない場合は、何もする必要はありません。

---

5 **Solaris 10 9/09** および **Solaris 10 9/10** リリースでは、システムが **Oracle Solaris Cluster** 構成の一部になっている場合、クラスタ内で **Trusted Extensions** を有効にできます。

注 – アプリケーションは Oracle Solaris Cluster のゾーンクラスタでのみ実行する必要があります。

Trusted Extensions による Oracle Solaris Cluster のサポートの詳細については、『Oracle Solaris Cluster Software Installation Guide』の第 7 章「Creating Non-Global Zones and Zone Clusters」の「How to Prepare for Trusted Extensions Use With Zone Clusters」を参照してください。

6 **Trusted Extensions** システムをアップグレードする場合は、システムのアップグレード前に次の情報を参照してください。

- 『Solaris 10 の概要』の第 1 章「Solaris 10 10/08 リリースの新機能」
- 『Solaris 10 10/08 ご使用にあたって』

ヒント – 関連情報を見つけるには、文字列 `Trusted Extensions` を検索してください。

---

7 ゾーンのクローンを作成する場合、**ZFS** プール用のパーティションを作成します。

ゾーン作成方法を決定するには、26 ページの「Trusted Extensions でのゾーン計画」を参照してください。

8 このシステムにラベル付きゾーンをインストールする場合は、パーティションにゾーン用のディスク容量が十分にあることを確認します。

Trusted Extensions が設定されるほとんどのシステムには、ラベル付きゾーンをインストールします。ラベル付きゾーンでは、インストールされたシステムによって確保されたディスク容量よりも多くの容量が必要になることがあります。

ただし、一部の Trusted Extensions システムには、ラベル付きゾーンをインストールする必要がありません。たとえば、マルチレベルのプリンタサーバー、マルチレベルの LDAP サーバー、マルチレベルの LDAP プロキシサーバーなどでは、ラベル付きゾーンをインストールする必要はありません。このようなシステムでは、追加のディスク容量が不要な場合もあります。

9 (省略可能) 役割用のスワップ空間を追加します。

役割が Trusted Extensions を管理します。役割のプロセスのためにスワップの追加を検討します。

10 (省略可能) 監査ファイル専用のパーティションを作成します。

Trusted Extensions では、デフォルトで監査が有効になっています。監査ファイルには、専用パーティションを作成するようにしてください。

11 (省略可能) 強化された構成を実行するには、**Trusted Extensions** を有効化する前に `netservices limited` コマンドを実行します。

```
# netservices limited
```

Trusted Extensions の有効化前の情報収集と決定事項

Trusted Extensions を構成するシステムごとに、確認しておくべき情報、および構成に関して決定しておくべき事項があります。たとえば、ラベル付きゾーンを作成するには、ゾーンのクローンを Solaris ZFS ファイルシステムとして作成できるディスク容量を確保します。Solaris ZFS によって、ゾーン用の分離領域がさらに提供されます。

▼ Trusted Extensions の有効化前にシステム情報を収集する

1 システムのメインホスト名および IP アドレスを確認します。

このホスト名はネットワーク上のホストの名前であり、大域ゾーンです。Solaris システムでは、次のように getent コマンドを実行するとホスト名が返されます。

```
# getent hosts machine1
192.168.0.11   machine1
```

2 ラベル付きゾーンに対して IP アドレスの割り当てを決定します。

2 つの IP アドレスを持つシステムは、マルチレベルサーバーとして動作します。IP アドレスが 1 つのシステムは、印刷またはマルチレベルタスクを実行するためには、マルチレベルサーバーにアクセスする必要があります。IP アドレスのオプションについては、28 ページの「マルチレベルアクセスの計画」を参照してください。

ほとんどのシステムでは、ラベル付きゾーンのために 2 つめの IP アドレスが必要になります。ラベル付きゾーン用に 2 つめの IP アドレスを持つホストの場合の例を、次に示します。

```
# getent hosts machine1-zones
192.168.0.12   machine1-zones
```

3 LDAP 構成情報を収集します。

Trusted Extensions ソフトウェアを実行する LDAP サーバーの場合、次の情報が必要です。

- LDAP サーバーがサービスを提供する Trusted Extensions ドメインの名前
- LDAP サーバーの IP アドレス
- ロードする LDAP プロファイル名

LDAP プロキシサーバーの場合、LDAP プロキシのパスワードも必要です。

▼ Trusted Extensions の有効化前にシステムおよびセキュリティーに関する事項を決定する

Trusted Extensions を構成するシステムごとに、ソフトウェアの有効化に先立って、構成に関する決定を行います。

1 システムハードウェアをどれくらい安全に保護する必要があるかを決定します。

セキュリティー保護されたサイトでは、このステップはすべてのインストール済み Solaris システムに関して行われています。

- SPARC システムの場合、PROM セキュリティーレベルおよびパスワードが提供されています。
- x86 システムの場合は BIOS が保護されています。
- すべてのシステムで、`root` がパスワードで保護されています。

2 `label_encodings` ファイルを準備します。

サイト独自の `label_encodings` ファイルがある場合、その他の構成タスクを開始する前にファイルを確認してインストールします。サイト独自の `label_encodings` ファイルがない場合、Sun 提供のデフォルトファイルを使用できます。デフォルト以外の `label_encodings` ファイルも `/etc/security/tsol` ディレクトリにあります。Sun のファイルはデモファイルです。本番システムには適さないことがあります。

サイトに合わせてファイルをカスタマイズするには、『Solaris Trusted Extensions ラベルの管理』を参照してください。

3 `label_encodings` ファイルのラベルのリストから、作成する必要のあるラベル付きゾーンのリストを作成します。

次の表に、デフォルトの `label_encodings` ファイルでの、ラベル名と推奨されるゾーン名の一覧を示します。

ラベル	ゾーン名
`PUBLIC`	`public`
`CONFIDENTIAL : INTERNAL`	`internal`
`CONFIDENTIAL : NEED TO KNOW`	`needtoknow`
`CONFIDENTIAL : RESTRICTED`	`restricted`

NFS マウントを簡単にするため、特定のラベルのゾーン名はすべてのシステムで同じにする必要があります。マルチレベルのプリンタサーバーなどの一部のシステムでは、ラベル付きゾーンがインストールされている必要はありません。ただし、ラベル付きゾーンをプリンタサーバーにインストールする場合、そのゾーン名はネットワーク上のほかのシステムのゾーン名と同じにする必要があります。

4 役割をいつ作成するかを決定します。

役割になって Trusted Extensions を管理するようにサイトのセキュリティーポリシーで求められることがあります。このような場合、または、評価された構成の基準を満たすようにシステムを構成する場合、構成プロセスの早い段階で役割を作成してください。

役割を使用してシステムを構成する必要がない場合、スーパーユーザーとしてシステムを構成できます。この構成方法はあまり安全ではありません。構成時にどのユーザーがスーパーユーザーであったかは、監査レコードには示されません。スーパーユーザーはシステム上であらゆるタスクを実行できますが、役割が実行できるタスクは制限されます。したがって、役割によって構成を実行する場合、より細かく制御できます。

5 ゾーンの作成方法を選択します。

最初からのゾーンの作成、ゾーンのコピー、またはゾーンのクローンの作成があります。これらの方法は、作成にかかる時間、ディスク容量の要件、および堅牢性が異なります。それぞれの利点および欠点については、26 ページの「Trusted Extensions でのゾーン計画」を参照してください。

6 **LDAP 構成を計画します。**

ネットワーク接続されないシステムでは、ローカルファイルを使用した管理が実用的です。

LDAP は、ネットワーク接続された環境用のネームサービスです。複数のマシンを構成する場合、データ入力された LDAP サーバーが必要です。

- 既存の Sun Java System Directory Server (LDAP サーバー) がある場合、Trusted Extensions を実行するシステムに LDAP プロキシサーバーを作成できます。マルチレベルのプロキシサーバーは、ラベルなしの LDAP サーバーとの通信を取り扱います。
- LDAP サーバーがない場合、Trusted Extensions ソフトウェアを実行するシステムをマルチレベルの LDAP サーバーとして構成できます。

7 各システムおよびネットワークのセキュリティーに関するその他の問題を決定します。

たとえば、次のようなセキュリティーに関する問題を検討します。

- システムに接続し、使用のために割り当てることができるデバイスがどれかを指定します。
- どのラベルの、どのプリンタをシステムからアクセス可能にするかを決定します。
- ゲートウェイシステム、パブリックキオスクなど、制限されたラベル範囲を持つシステムを特定します。
- 特定のラベルなしシステムと通信できるラベル付きシステムを決定します。

Trusted Extensions サービスの有効化

Solaris 10 5/08 リリース以降の Trusted Extensions は、サービス管理機能 (Service Management Facility、SMF) によって管理されるサービスです。サービス名は `svc:/system/labeld:default` です。`labeld` サービスはデフォルトでは無効になっています。

▼ Trusted Extensions の有効化

`labeld` サービスは通信の終端にラベルを付加します。たとえば、次のものにラベルが付けられます。

- すべてのゾーン、および各ゾーン内のディレクトリとファイル
- ウィンドウプロセスも含む、すべてのプロセス
- すべてのネットワーク通信

始める前に　42 ページの「Trusted Extensions 用 Solaris OS のインストールまたはアップグレード」と 46 ページの「Trusted Extensions の有効化前の情報収集と決定事項」のタスクが完了しています。

1. **Solaris システム上で、`labeld` サービスを有効にします。**

   ```
   # svcadm enable -s svc:/system/labeld:default
   ```

   `labeld` サービスはシステムにラベルを追加し、Solaris 監査サービスとデバイス割り当てを開始します。プロンプトにカーソルが戻るまで、ほかのタスクを実行しないでください。

2. **サービスが使用可能になっていることを確認します。**

   ```
   # svcs -x labeld
   svc:/system/labeld:default (Trusted Extensions)
    State: online since weekday month date hour:minute:second year
      See: labeld(1M)
   Impact: None.
   ```

注 – システムをリブートしないとラベルは表示されません。51 ページの「Trusted Extensions での大域ゾーンの設定」には、リブート前に実行すべきタスクが含まれています。

注意事項　次のメッセージは、サービスとしての Trusted Extensions をサポートする Solaris リリースが実行されていないことを示します。 `svcs: Pattern 'labeld' doesn't match any instances.`

`labeld` サービスをサポートしない Solaris システム上で Trusted Extensions を実行するには、『Solaris Trusted Extensions インストールと構成』ガイドの手順に従います。

◆ ◆ ◆ 第 4 章

Trusted Extensions の構成 (手順)

この章では、モニターがあるシステムでの Trusted Extensions の構成方法について説明します。適切に作業するため、Trusted Extensions ソフトウェアで ラベル、ゾーン、ネットワーク、役割になれるユーザー、役割、およびツールを構成する必要があります。

- 51 ページの「Trusted Extensions での大域ゾーンの設定」
- 68 ページの「ラベル付きゾーンの作成」
- (省略可能) 85 ページの「ネットワークインタフェースをラベル付きゾーンに追加し、ルーティングする」
- 93 ページの「Trusted Extensions での役割とユーザーの作成」
- 105 ページの「Trusted Extensions でのホームディレクトリの作成」
- 108 ページの「既存のトラステッドネットワークへのユーザーとホストの追加」
- 110 ページの「Trusted Extensions の構成のトラブルシューティング」
- 114 ページの「その他の Trusted Extensions 構成タスク」

その他の構成タスクについては、『Oracle Solaris Trusted Extensions 管理の手順』を参照してください。

Trusted Extensions での大域ゾーンの設定

大域ゾーンを設定する前に、構成を決定してください。決定事項については、46 ページの「Trusted Extensions の有効化前の情報収集と決定事項」を参照してください。

作業	説明	参照先
ハードウェアを保護します。	ハードウェアの設定を変更する際にパスワードの入力を求めることによって、ハードウェアを保護できます。	『System Administration Guide: Security Services』の「Controlling Access to System Hardware」

作業	説明	参照先
ラベルを設定します。	ラベルはサイトに合わせて設定する必要があります。デフォルトの `label_encodings` ファイルを使用する場合、この手順は省略します。	52 ページの「ラベルエンコーディングファイルを検査およびインストールする」
IPv6 の場合、`/etc/system` ファイルを変更します。	IPv6 ネットワークを実行する場合、ラベル付きパケットが IP によって認識されるように `/etc/system` ファイルを変更します。	56 ページの「Trusted Extensions で IPv6 ネットワーキングを有効にする」
DOI の値が 1 でない場合は、`/etc/system` ファイルを変更します。	ネットワークノードの CIPSO 解釈ドメイン (DOI) が 1 でない場合は、`/etc/system` ファイル内でその DOI を指定します。	57 ページの「解釈ドメインの構成」
Solaris ZFS スナップショットのための領域を作成します。	ゾーンのクローンを作成するために Solaris ZFS スナップショットを使用する場合は、ZFS プールを作成します。 最初のゾーンのクローンを作成して、その他のラベル付きゾーンを作成する場合は、このタスクを実行します。	59 ページの「ゾーンのクローンを作成するために ZFS プールを作成する」
再起動してログインします。	ログインすると、大域ゾーンになり、その環境では必須アクセス制御 (MAC) が認識されて実施されます。	60 ページの「Trusted Extensions を再起動してログインする 」
Solaris 管理コンソールを初期化します。	Trusted Extensions で、ユーザー、役割、ゾーン、およびネットワークを管理するツールが Solaris 管理コンソールに追加されます。	61 ページの「Trusted Extensions で Solaris 管理コンソールサーバーを初期化する」
LDAP を構成します。	LDAP ネームサービスを使用している場合、LDAP サービスを設定します。	第 5 章「Trusted Extensions のための LDAP の構成 (手順)」
	LDAP サービスを設定している場合、このシステムを LDAP クライアントにします。	65 ページの「Trusted Extensions で大域ゾーンを LDAP クライアントにする」

▼ ラベルエンコーディングファイルを検査およびインストールする

エンコーディングファイルは、通信する相手の Trusted Extensions ホストと互換性がなければなりません。

注 – Trusted Extensions はデフォルトの label_encodings ファイルをインストールします。このデフォルトファイルは、デモンストレーションとして便利です。ただし、実際の使用に適しているとは限りません。デフォルトファイルを使用する場合、この手順は省略できます。

- エンコーディングファイルに慣れている場合、次に示す手順を使用します。
- エンコーディングファイルに慣れていない場合、要件、手順、および例について『Solaris Trusted Extensions ラベルの管理』を参照してください。

注意 – 続行する前に、ラベルを正しくインストールしてください。正しくインストールしていないと構成できません。

始める前に　セキュリティー管理者です。セキュリティー管理者は、label_encodings ファイルの編集、検査、および保守を担当します。label_encodings ファイルを編集する場合、ファイルが書き込み可能であることを確認してください。詳細は、label_encodings(4) のマニュアルページを参照してください。

1. label_encodings ファイルが含まれたメディアを適切なデバイスに挿入します。
2. label_encodings ファイルをディスクにコピーします。
3. ファイルの構文を検査し、それをアクティブな label_encodings ファイルにします。
   - **Trusted JDS** では、コマンド行からファイルの検査とインストールを行います。
     a. 端末ウィンドウを開きます。
     b. chk_encodings コマンドを実行します。
        ```
        # /usr/sbin/chk_encodings /full-pathname-of-label-encodings-file
        ```
     c. 出力を読み、次のいずれかを行います。
        - エラーを解決します。
          コマンドによってエラーが報告された場合、続行する前に、そのエラーを解決しなければなりません。参考として、『Solaris Trusted Extensions ラベルの管理』の第 3 章「ラベルエンコーディングファイルの作成 (手順)」を参照してください。
        - そのファイルをアクティブな label_encodings ファイルにします。
          ```
          # cp /full-pathname-of-label-encodings-file \
           /etc/security/tsol/label_encodings.site
          # cd /etc/security/tsol
          ```

```
# cp label_encodings label_encodings.tx.orig
# cp label.encodings.site label_encodings
```

注意 – 続行するには、label_encodings ファイルが chk_encodings テストに合格しなければなりません。

- **Trusted CDE** では、「エンコーディングの検査」アクションを使用します。

  a. **Trusted_Extensions** フォルダを開きます。
  背景をマウスボタン 3 でクリックします。

  b. ワークスペースメニューで、「アプリケーション」→「アプリケーション・マネージャ」を選択します。

  c. **Trusted_Extensions** フォルダのアイコンをダブルクリックします。

  d. 「エンコーディングの検査」アクションをダブルクリックします。
  ダイアログボックスで、ファイルのフルパス名を入力します
  /full-pathname-of-label-encodings-file
  chk_encodings コマンドを起動して、ファイルの構文を検査します。「エンコーディングの検査」ダイアログボックスに結果が表示されます。

  e. 「エンコーディングの検査」ダイアログボックスの内容を読み、次のいずれかを行います。

  - エラーを解決します。
    「エンコーディングの検査」アクションによってエラーが報告された場合、続行する前に、そのエラーを解決しなければなりません。参考として、『Solaris Trusted Extensions ラベルの管理』の第 3 章「ラベルエンコーディングファイルの作成 (手順)」を参照してください。

  - 「はい」をクリックすることで、そのファイルをアクティブな label_encodings ファイルにします。
    「エンコーディングの検査」アクションによって元のファイルのバックアップコピーが作成され、検査済みのバージョンが /etc/security/tsol/label_encodings にインストールされます。さらに、ラベルデーモンが再起動されます。

注意 – 続行するには、label_encodings ファイルがエンコーディングの検査テストに合格しなければなりません。

4 ファイルの構文を検査し、それをアクティブな label_encodings ファイルにします。コマンド行を使用します。

a. 端末ウィンドウを開きます。

b. chk_encodings コマンドを実行します。

```
# /usr/sbin/chk_encodings /full-pathname-of-label-encodings-file
```

c. 出力を読み、次のいずれかを行います。

- エラーを解決します。

  コマンドによってエラーが報告された場合、続行する前に、そのエラーを解決しなければなりません。参考として、『Solaris Trusted Extensions ラベルの管理』の第 3 章「ラベルエンコーディングファイルの作成 (手順)」を参照してください。

- そのファイルをアクティブな label_encodings ファイルにします。

```
# cp /full-pathname-of-label-encodings-file \
 /etc/security/tsol/label.encodings.site
# cd /etc/security/tsol
# cp label_encodings label_encodings.tx.orig
# cp label.encodings.site label_encodings
```

注意 – 続行するには、label_encodings ファイルがエンコーディングの検査テストに合格しなければなりません。

例 4–1 コマンド行での label_encodings 構文の検査

この例では、管理者がコマンド行を使用していくつかの label_encodings ファイルをテストします。

```
# /usr/sbin/chk_encodings /var/encodings/label_encodings1
No errors found in /var/encodings/label_encodings1
# /usr/sbin/chk_encodings /var/encodings/label_encodings2
No errors found in /var/encodings/label_encodings2
```

業務管理で label_encodings2 ファイルを使用することを決めたら、管理者はファイルの意味解析を実行します。

```
# /usr/sbin/chk_encodings -a /var/encodings/label_encodings2
No errors found in /var/encodings/label_encodings2
```

```
---> VERSION = MYCOMPANY LABEL ENCODINGS  2.0 10/10/2006

---> CLASSIFICATIONS <---

   Classification 1: PUBLIC
   Initial Compartment bits: 10
   Initial Markings bits: NONE

---> COMPARTMENTS AND MARKINGS USAGE ANALYSIS <---
...
---> SENSITIVITY LABEL to COLOR MAPPING <---
...
```

管理者は自分の記録用に意味解析のコピーを出力したのち、このファイルを `/etc/security/tsol` ディレクトリに移動します。

```
# cp /var/encodings/label_encodings2 /etc/security/tsol/label.encodings.10.10.06
# cd /etc/security/tsol
# cp label_encodings label_encodings.tx.orig
# cp label.encodings.10.10.06 label_encodings
```

最後に、管理者は `label_encodings` ファイルが会社ファイルであることを確認します。

```
# /usr/sbin/chk_encodings -a /etc/security/tsol/label_encodings | head -4
No errors found in /etc/security/tsol/label_encodings

---> VERSION = MYCOMPANY LABEL ENCODINGS  2.0 10/10/2006
```

▼ Trusted Extensions で IPv6 ネットワーキングを有効にする

CIPSO オプションは、パケットの IPv6 Option Type フィールドで使用すべき IANA (Internet Assigned Numbers Authority) 番号を持ちません。この手順で設定するエントリは、このオプションの番号を IANA が割り当てるまでローカルネットワークで使用する番号を提供します。この番号が定義されていないと、Trusted Extensions は IPv6 ネットワークを無効にします。

Trusted Extensions で IPv6 ネットワークを有効にするには、`/etc/system` ファイルにエントリを追加してください。

- `/etc/system` ファイルに次のエントリを入力します。

  ```
  set ip:ip6opt_ls = 0x0a
  ```

注意事項

- 起動中に IPv6 の構成が正しくないことを示すエラーメッセージが表示されたら、エントリを修正します。
  - エントリのスペルが正しいことを確認します。

- /etc/system ファイルに正しいエントリを追加したあとにシステムが再起動されたことを確認します。

- すでに IPv6 が有効になっている Solaris システムに Trusted Extensions をインストールして、/etc/system に IP エントリを追加できなかった場合、次のエラーメッセージが表示されます。 t_optmgmt: System error: Cannot assign requested address *time-stamp*
- IPv6 が有効ではない Solaris システムに Trusted Extensions をインストールして、/etc/system に IP エントリを追加できなかった場合、次のようなエラーメッセージが表示されます。
  - WARNING: IPv6 not enabled via /etc/system
  - Failed to configure IPv6 interface(s): hme0
  - rpcbind: Unable to join IPv6 multicast group for rpc broadcast *broadcast-number*

▼ 解釈ドメインの構成

Trusted Extensions で構成されたシステムとの間の通信はすべて、ある単一の CIPSO 解釈ドメイン (DOI) のラベル付け規則に従う必要があります。各メッセージ内で使用される DOI は、CIPSO IP Option ヘッダーの整数値によって識別されます。デフォルトで、Trusted Extensions の DOI は 1 になっています。

使用する DOI が 1 でない場合、/etc/system ファイルにエントリを追加し、デフォルトのセキュリティーテンプレートの doi 値を変更する必要があります。

1 /etc/system ファイルに次の **DOI** エントリを入力します。

```
set default_doi = n
```

このゼロでない正数は、使用するノードおよびそのノードと通信するシステムの tnrhtp データベースに含まれている DOI 番号に一致する必要があります。

2 tnrhtp データベースを **LDAP** サーバーに追加する前に、デフォルトエントリとローカルアドレスに対するすべてのエントリの doi 値を変更します。

Trusted Extensions の tnrhtp データベース内には、cipso と admin_low の 2 つのテンプレートが用意されています。ローカルアドレスのエントリを追加した場合には、それらのエントリも変更します。

a. tnrhtp データベースをトラステッドエディタで開きます。

```
# /usr/dt/bin/trusted_edit /etc/security/tsol/tnrhtp
```

Solaris Trusted Extensions (CDE) では代わりに、アプリケーションマネージャーの Trusted_Extensions フォルダ内の「管理エディタ」アクションを使用します。

b. cipso テンプレートエントリを別の行にコピーします。

```
cipso:host_type=cipso;doi=1;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH
cipso:host_type=cipso;doi=1;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH
```

c. いずれかの cipso エントリをコメントにします。

```
#cipso:host_type=cipso;doi=1;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH
cipso:host_type=cipso;doi=1;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH
```

d. コメントにされていない cipso エントリの doi 値を変更します。

この値を、/etc/system ファイル内の default_doi の値と同じにします。

```
#cipso:host_type=cipso;doi=1;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH
cipso:host_type=cipso;doi=n;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH
```

e. admin_low エントリの doi 値を変更します。

```
#admin_low:host_type=unlabeled;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH;doi=1;def_label=ADMIN_LOW
admin_low:host_type=unlabeled;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH;doi=n;def_label=ADMIN_LOW
```

tnrhtp データベース内のすべてのエントリのすべての doi 値が同じになったら作業は完了です。

注意事項 /etc/system ファイルで 1 以外の default_doi 値が設定されていて、かつこのシステムのセキュリティーテンプレートでその default_doi 値に一致しない値が設定されていた場合、インタフェースの構成時にシステムコンソール上に次のようなメッセージが表示されます。

- NOTICE: er10 failed: 10.17.1.12 has wrong DOI 4 instead of 1
- Failed to configure IPv4 interface(s): er10

インタフェースの構成に失敗した場合、次のようにログインが失敗する可能性があります。

- Hostname: unknown
- unknown console login: root
- Oct 10 10:10:20 unknown login: pam_unix_cred: cannot load hostname Error 0

この問題を修正するには、システムをシングルユーザーモードでブートし、この手順で説明した方法でセキュリティーテンプレートを修正します。

参照 DOI の詳細については、『Oracle Solaris Trusted Extensions 管理の手順』の「Trusted Extensions のネットワークセキュリティー属性」を参照してください。

作成するセキュリティーテンプレートの doi 値を変更するには、『Oracle Solaris Trusted Extensions 管理の手順』の「遠隔ホストテンプレートを構築する」を参照してください。

ユーザーが選択したエディタを信頼できるエディタとして使用するには、『Oracle Solaris Trusted Extensions 管理の手順』の「トラステッドエディタとして任意のエディタを割り当てる」を参照してください。

▼ ゾーンのクローンを作成するために ZFS プールを作成する

Solaris ZFS スナップショットをゾーンテンプレートとして使用する場合、ZFS ファイルまたは ZFS デバイスから ZFS プールを作成する必要があります。このプールには、各ゾーンのクローンを作成するためのスナップショットが保持されます。ZFS プール用に /zone デバイスを使用します。

始める前に　Solaris のインストール時に、ZFS ファイルシステム用のディスク容量を確保しておきます。詳細は、26 ページの「Trusted Extensions でのゾーン計画」を参照してください。

1. /zone パーティションをアンマウントします。
   インストール時に、十分なディスク容量 (約 2000M バイト) の /zone パーティションを作成してあります。

   ```
   # umount /zone
   ```

2. /zone マウントポイントを削除します。

   ```
   # rmdir /zone
   ```

3. vfstab ファイルの /zone エントリをコメントにします。

   a. /zone エントリを読み取られないようにします。
      エディタで vfstab ファイルを開きます。/zone エントリの前にコメント記号を付けます。

      ```
      #/dev/dsk/cntndnsn  /dev/dsk/cntndnsn  /zone  ufs  2  yes  -
      ```

   b. ディスクスライス *cntndnsn* をクリップボードにコピーします。

   c. ファイルを保存し、エディタを閉じます。

4. ディスクスライスを使用して /zone を **ZFS** プールとして再作成します。

   ```
   # zpool create -f zone cntndnsn
   ```

   たとえば、/zone エントリがディスクスライス c0t0d0s5 を使用した場合、コマンドは次のようになります。

   ```
   # zpool create -f zone c0t0d0s5
   ```

5 **ZFS プールが正常であることを検証します。**

次のいずれかのコマンドを使用します。

```
# zpool status -x zone
pool 'zone' is healthy

# zpool list
NAME     SIZE     USED   AVAIL   CAP   HEALTH   ALTROOT
/zone    5.84G   80K    5.84G    7%   ONLINE   -
```

この例では、初期設定チームはゾーンのパーティション用に 6000M バイトを用意しました。詳細は、zpool(1M) のマニュアルページを参照してください。

▼ Trusted Extensions を再起動してログインする

ほとんどのサイトでは、初期設定チームの役割を果たす、2 人以上の管理者がシステムの構成を担当します。

始める前に 最初にログインする前に、Trusted Extensions のデスクトップおよびラベルのオプションを熟知しておいてください。詳細は、『Oracle Solaris Trusted Extensions ユーザーズガイド』の第 2 章「Trusted Extensions へのログイン (手順)」を参照してください。

1 **システムを再起動します。**

```
# /usr/sbin/reboot
```

システムにグラフィック表示用のディスプレイがない場合は、第 6 章「Trusted Extensions とヘッドレスシステムの構成 (タスク)」に進みます。

2 **Solaris Trusted Extensions (CDE) または Solaris Trusted Extensions (JDS) デスクトップにスーパーユーザーとしてログインします。**

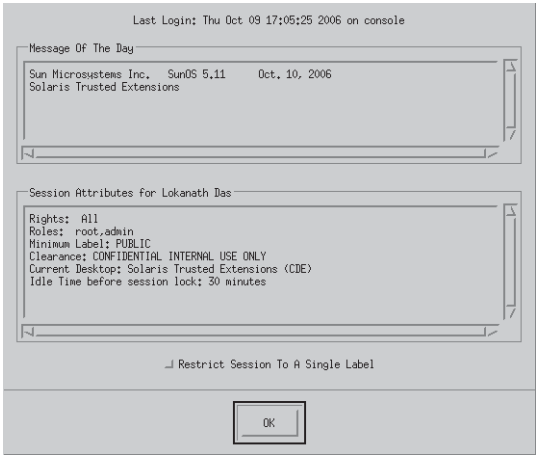
a. **ログインウィンドウで、いずれかのトラステッドデスクトップを選択します。**

Trusted CDE デスクトップには、システムの構成時に役立つアクションが含まれています。Solaris 10 10/08 リリースから、`txzonemgr` スクリプトがシステムを構成するために優先されるプログラムになりました。

b. **ログインダイアログボックスで、`root` および root パスワードを入力します。**

ユーザーはパスワードをほかの人に知られないようにしてください。その人がユーザーのデータにアクセスすると、アクセスした人を特定できず、責任を追求できなくなります。パスワードがほかの人に知られるのは、ユーザーが故意に教えてしまうような直接的な場合と、書き留めておいたパスワードを見られたり、安全でないパスワードを設定したりするなど、間接的な場合があります。Trusted Extensions ソフトウェアでは、安全でないパスワードが設定されないようにできますが、ユーザーがパスワードを教えたり、書き留めたりするのを防止することはできません。

3 「最後のログイン」ダイアログボックス内の情報を読みます。



「了解」をクリックしてボックスを閉じます。

4 ラベルビルダーを読みます。

「了解」をクリックしてデフォルトのラベルを受け入れます。

ログインプロセスが完了すると、Trusted Extensions 画面が短く表示され、4 つのワークスペースを持つデスクトップセッションになります。トラステッドストライプに `Trusted Path` のシンボルが表示されます。

注 – システムの前から離れるときは、ログオフするかまたは画面をロックしてください。これを怠ると、だれかが識別や認証を受けずにシステムにアクセスできてしまい、アクセスした人を特定できず、責任を追求できなくなります。

▼ Trusted Extensions で Solaris 管理コンソールサーバーを初期化する

この手順で、ユーザー、役割、ホスト、ゾーン、およびネットワークをこのシステム上で管理できるようになります。構成する最初のシステムでは、`files` スコープのみが使用可能です。

始める前に スーパーユーザーでなければなりません。

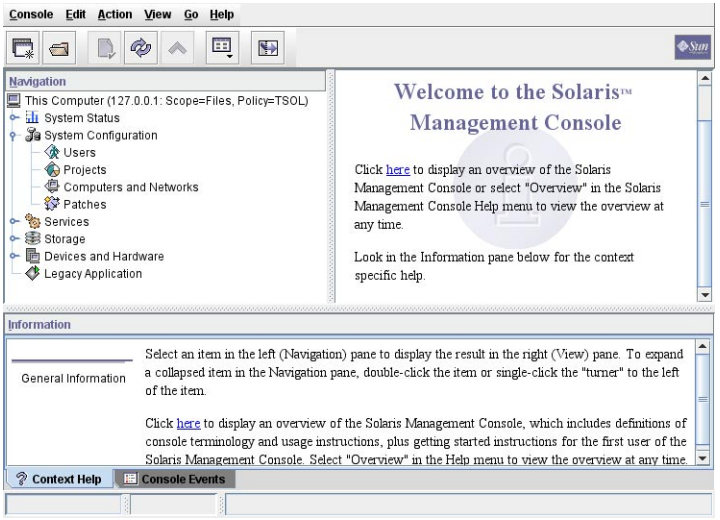
クライアントで動作する Solaris 管理コンソールから LDAP サーバー上の LDAP ツールボックスを使用するには、132 ページの「LDAP のための Solaris 管理コンソールの設定 (作業マップ)」のすべての作業を完了してください。

1 **Solaris 管理コンソールを起動します。**

```
# /usr/sbin/smc &
```

注 – Solaris 管理コンソールをはじめて起動するときには、登録タスクを実行します。このタスクには数分かかります。

図 4–1 Solaris 管理コンソール 初期ウィンドウ



2 **Solaris 管理コンソールでツールボックスのアイコンが表示されない場合、次のいずれかを実行します。**

- ナビゲーション区画が表示されない場合

  a. 表示されている「ツールボックスを開く」ダイアログボックスで、「サーバー」の下にあるシステムの名前の横の「読み込む」をクリックします。

  システムにメモリーおよびスワップの推奨容量がない場合、ツールボックスが表示されるまで数分かかる場合があります。推奨値については、42 ページの「Trusted Extensions 用 Solaris OS のインストールまたはアップグレード」を参照してください。

b. ツールボックスのリストから、`Policy=TSOL` であるツールボックスを選択します。

図 4–2 は、このコンピュータ (*this-host*: `Scope=Files, Policy=TSOL`) ツールボックスを示しています。Trusted Extensions で、「システムの構成」ノードにあるツールを変更します。

注意 – ポリシーがないツールボックスは選択しないでください。リストされているポリシーがないツールボックスは、Trusted Extensions をサポートしません。

影響を与えるスコープに応じて、ツールボックスの選択が決まります。

- ローカルファイルを編集するには、ファイルスコープを選択します。
- LDAP データベースを編集するには、LDAP スコープを選択します。

  132 ページの「LDAP のための Solaris 管理コンソールの設定 (作業マップ)」のすべての作業を完了すると、LDAP スコープが使用可能になります。

c. 「開く」をクリックします。

- ナビゲーション区画は表示されるが、ツールボックスのアイコンが停止標識である場合

  a. **Solaris** 管理コンソールを終了します。

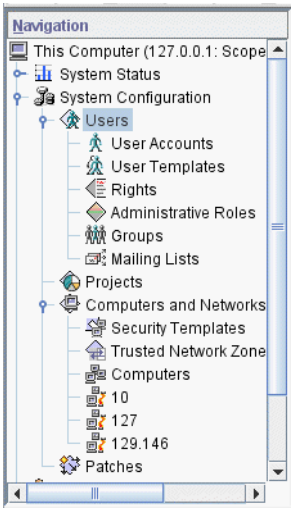
  b. **Solaris** 管理コンソールを再起動します。

  ```
  # /usr/sbin/smc &
  ```

3 `Policy=TSOL` のツールボックスをまだ選択していない場合は、それを選択します。

次の図は、このコンピュータ (*this-host*: `Scope=Files, Policy=TSOL`) ツールボックスを示しています。Trusted Extensions で、「システムの構成」ノードにあるツールを変更します。

図 4–2 Solaris 管理コンソールの Trusted Extensions ツール



4 (省略可能) 現在のツールボックスを保存します。

`Policy=TSOL` ツールボックスを保存すると、デフォルトで Trusted Extensions ツールボックスが読み込まれます。設定は役割ごと、ホストごとに保存されます。ホストは Solaris 管理コンソールサーバーです。

a. 「コンソール」メニューから「設定の変更」を選択します。

「ホーム」ツールボックスが選択されています。

b. `Policy=TSOL` ツールボックスを「ホーム」ツールボックスとして定義します。

「現在のツールボックスを使用」ボタンをクリックすることによって、現在のツールボックスを「場所」フィールドに入力します。

c. 「了解」をクリックして設定を保存します。

5 Solaris 管理コンソールを終了します。

参照 Solaris 管理コンソールに対する Trusted Extensions の追加事項の概要については、『Oracle Solaris Trusted Extensions 管理の手順』の「Solaris 管理コンソールツール」を参照してください。Solaris 管理コンソールを使用してセキュリティーテンプレートを作成するには、『Oracle Solaris Trusted Extensions 管理の手順』の「トラステッドネットワークデータベースの構成 (作業マップ)」を参照してください。

▼ Trusted Extensions で大域ゾーンを LDAP クライアントにする

LDAP では、この手順で大域ゾーンにネームサービス設定を構築します。LDAP を使用していない場合、この手順は省略できます。

Solaris 10 5/08 リリース以降、Solaris Trusted Extensions (CDE) ワークスペースにいるユーザーは、`txzonemgr` スクリプトまたは Trusted CDE アクションを使って LDAP クライアントを作成できます。Solaris Trusted Extensions (JDS) または Solaris Trusted Extensions (GNOME) ワークスペースにいるユーザーは、`txzonemgr` スクリプトを使用する必要があります。

注 – あるユーザーが各ラベル付きゾーン内でネームサーバーを設定することを計画している場合、各ラベル付きゾーンへの LDAP クライアント接続を確立する責任はそのユーザーにあります。

始める前に　Sun Java System Directory Server、つまり LDAP サーバーが存在しなければなりません。Trusted Extensions データベースのデータがサーバーに入力されていて、システムがサーバーと通信できなければなりません。そのため、構成しているシステムで、LDAP サーバー上の `tnrhdb` データベースへのエントリが必要です。あるいは、この手順を実行する前に、このシステムがワイルドカードエントリに含まれていなければなりません。

Trusted Extensions が設定された LDAP サーバーが存在しない場合、次に示す手順を実行する前に、第 5 章「Trusted Extensions のための LDAP の構成 (手順)」 の手順を完了します。

1 **DNS を使用している場合、`nsswitch.ldap` ファイルを変更します。**

a. 元の `nsswitch.ldap` ファイルのコピーを保存します。

LDAP 用の標準的なネームサービスのスイッチファイルは限定的であるため、Trusted Extensions には使用できません。

```
# cd /etc
# cp nsswitch.ldap nsswitch.ldap.orig
```

b. 次の各サービスの `nsswitch.ldap` ファイルエントリを変更します。

正しいエントリは次のとおりです。

```
hosts:    files dns ldap

ipnodes:    files dns ldap

networks:   ldap files
protocols:  ldap files
rpc:        ldap files
```

```
ethers:     ldap files
netmasks:   ldap files
bootparams: ldap files
publickey:  ldap files

services:   files
```

Trusted Extensions によって、次の 2 つのエントリが追加されます。

```
tnrhtp:    files ldap
tnrhdb:    files ldap
```

c. 変更した `nsswitch.ldap` ファイルを `nsswitch.conf` にコピーします。

```
# cp nsswitch.ldap nsswitch.conf
```

2 次の手順のいずれかを実行して **LDAP** クライアントを作成します。

- `txzonemgr` スクリプトを実行し、**LDAP** に関するプロンプトに答えます。
  「Create LDAP Client」メニュー項目によって構成されるのは、大域ゾーンだけです。

  a. 69 ページの「`txzonemgr` スクリプトを実行する」の手順に従います。
  このダイアログボックスのタイトルは「Labeled Zone Manager」です。

  b. 「**Create LDAP Client**」を選択します。

  c. 次の各プロンプトに答え、それぞれの回答のあとで「了解」をクリックします。

  ```
  Enter Domain Name:                          Type the domain name
  Enter Hostname of LDAP Server:              Type the name of the server
  Enter IP Address of LDAP Server servername:     Type the IP address
  Enter LDAP Proxy Password:                  Type the password to the server
  Confirm LDAP Proxy Password:                Retype the password to the server
  Enter LDAP Profile Name:                    Type the profile name
  ```

  d. 表示された値を確定するか取り消します。

  ```
  Proceed to create LDAP Client?
  ```

  確定した場合、`txzonemgr` スクリプトによって LDAP クライアントが追加されます。その後、コマンド出力がウィンドウに表示されます。

- **Trusted CDE** ワークスペースで、「**LDAP** クライアントを作成」アクションを検索して使用します。

  a. 背景でマウスボタン **3** をクリックして **Trusted_Extensions** フォルダに移動します。

b. ワークスペースメニューで、「アプリケーション」→「アプリケーション・マネージャ」を選択します。

c. **Trusted_Extensions** フォルダのアイコンをダブルクリックします。
このフォルダには、インタフェース、LDAP クライアント、およびラベル付きゾーンを設定するためのアクションが含まれています。

d. 「**LDAP** クライアントを作成」アクションをダブルクリックします。
次のプロンプトに答えます。

```
Domain Name:                    Type the domain name
Hostname of LDAP Server:        Type the name of the server
IP Address of LDAP Server:      Type the IP address
LDAP Proxy Password:            Type the password to the server
Profile Name:                   Type the profile name
```

e. 「了解 **(OK)**」をクリックします。
次の完了メッセージが表示されます。

```
global zone will be LDAP client of LDAP-server
System successfully configured.

*** Select Close or Exit from the window menu to close this window ***
```

f. アクションウィンドウを閉じます。

3 端末ウィンドウで、`enableShadowUpdate` パラメータに `TRUE` を設定します。

```
# ldapclient -v mod -a enableShadowUpdate=TRUE \
> -a adminDN=cn=admin,ou=profile,dc=domain,dc=suffix
System successfully configured
```

「LDAP クライアントを作成」アクションと `txzonemgr` スクリプトは `ldapclient init` コマンドのみを実行します。Trusted Extensions では、シャドウ更新を有効にするため、初期化された LDAP クライアントに変更を加える必要もあります。

4 サーバーに関する情報が正しいことを確認します。

a. 端末ウィンドウを開き、**LDAP** サーバーを照会します。

```
# ldapclient list
```

出力表示は次のようになります。

```
NS_LDAP_FILE_VERSION= 2.0
NS_LDAP_BINDDN= cn=proxyagent,ou=profile,dc=domain-name
...
NS_LDAP_BIND_TIME= number
```

b. エラーを修正します。

エラーが表示された場合は、もう一度 LDAP クライアントを作成し、正しい値を指定してください。たとえば、次のエラーが表示される場合、LDAP サーバーにシステムのエントリがない可能性があります。

```
LDAP ERROR (91): Can't connect to the LDAP server.
Failed to find defaultSearchBase for domain domain-name
```

このエラーを修正するには、LDAP サーバーを確認する必要があります。

例 4–2 resolv.conf ファイルの読み込み後にホスト名を使用する

この例では、管理者が、ある特定の DNS サーバー群をシステムから使用可能にします。管理者は、トラステッドネットワーク上のサーバーから resolv.conf ファイルをコピーします。DNS はまだアクティブになっていないため、管理者はサーバーの IP アドレスを使ってサーバーを特定します。

```
# cd /etc
# cp /net/10.1.1.2/export/txsetup/resolv.conf resolv.conf
```

resolv.conf ファイルがコピーされ、nsswitch.conf ファイルの hosts エントリに dns が含められると、管理者はホスト名を使ってシステムを特定できるようになります。

ラベル付きゾーンの作成

txzonemgr スクリプトを使用すると、ラベル付きゾーンを構成する次のタスクをすべて順に実行できます。

注意 – txzonemgr の手順を使用するには、Trusted Extensions の Solaris 10 8/07 リリース以降を実行している必要があります。または、Solaris 10 11/06 リリースのすべてのパッチをインストールしてください。

Solaris 10 11/06 リリースを現在のパッチを適用しないで実行している場合、付録 B 「Trusted Extensions での CDE アクションを使用したゾーンのインストール」の手順を使用してラベル付きゾーンを構成します。

この節の手順で、最大 2 つの IP アドレスに割り当てられているシステム上にラベル付きゾーンを構成します。その他の設定については、35 ページの「作業マップ: Trusted Extensions の準備と有効化」の構成オプションを参照してください。

作業	説明	参照先
1. txzonemgr スクリプトを実行します。	txzonemgr スクリプトで、ゾーンの構成時に適したタスクを提示する GUI を作成します。	69 ページの「txzonemgr スクリプトを実行する」

作業	説明	参照先
2. 大域ゾーンでネットワークインタフェースを管理します。	大域ゾーンでインタフェースを構成します。つまり、論理インタフェースを作成して、それらのインターフェースを大域ゾーンで構成します。	70 ページの「Trusted Extensions でネットワークインタフェースを構成する」
3. ゾーンに名前を付けてラベルを付けます。	ゾーンにそのラベルのバージョンを使って名前を付けて、ラベルに割り当てます。	75 ページの「ゾーンに名前およびラベルを付ける」
4. ゾーンをインストールして起動します。	パッケージをゾーンにインストールします。サービスをゾーンで構成します。ゾーン端末コンソールによって、ゾーンにアクティビティを表示できます。	77 ページの「ラベル付きゾーンをインストールする」 78 ページの「ラベル付きゾーンを起動する」
5. ゾーンのステータスを確認します。	ラベル付きゾーンが実行されており、そのゾーンが大域ゾーンと通信できることを確認します。	80 ページの「ゾーンのステータスを確認する」
6. ゾーンをカスタマイズします。	不要なサービスをゾーンから削除します。 ゾーンを使用してその他のゾーンを作成する場合は、このゾーンにのみ限定される情報を削除します。	81 ページの「ラベル付きゾーンをカスタマイズする」
7. その他のゾーンを作成します。	選択した方法を使用して、2 つめのゾーンを作成します。ゾーンの作成方法については、26 ページの「Trusted Extensions でのゾーン計画」を参照してください。	83 ページの「Trusted Extensions でゾーンのコピーまたはクローンを行う」
8. (省略可能) ゾーン固有のネットワークインタフェースを追加します。	ネットワークの遮断を行うには、1 つ以上のネットワークインタフェースをラベル付きゾーンに追加します。一般に、そのような構成はラベル付きサブネットを切り離すために使用します。	85 ページの「ネットワークインタフェースをラベル付きゾーンに追加し、ルーティングする」

▼ txzonemgr スクリプトを実行する

このスクリプトで、ラベル付きゾーンを適切に構成、インストール、初期化、および起動するタスクを順に実行します。このスクリプトでは、各ゾーンに名前を付けてその名前とラベルを関連付け、パッケージをインストールして仮想 OS を作成し、ゾーンを起動してそのゾーンでサービスを開始します。このスクリプトには、ゾーンのコピーおよびゾーンのクローン作成のタスクが含まれています。また、ゾーンの停止、ゾーンの状態の変更、ゾーン固有のネットワークインタフェースの追加もできます。

このスクリプトによって動的に決定されるメニューが提示され、現在の状況に有効な選択のみが表示されます。たとえば、ゾーンのステータスを設定する場合には、ゾーンをインストールするためのメニュー項目は表示されません。完了済みのタスクはリストに表示されません。

始める前に　スーパーユーザーになります。

ゾーンのクローンを作成する場合は、ゾーンのクローン作成の準備を完了しておきます。独自のセキュリティーテンプレートを使用する場合は、そのテンプレートを作成しておきます。

1 端末ウィンドウを大域ゾーンで開きます。

2 `txzonemgr` スクリプトを実行します。

```
# /usr/sbin/txzonemgr
```

このスクリプトで、「Labeled Zone Manager」ダイアログボックスが開きます。この「zenity」ダイアログボックスで、インストールの現在の状態に応じて、適切なタスクを実行するよう求められます。

タスクを実行するには、メニュー項目を選択してから、Return キーを押すかまたは「了解」をクリックします。テキストの入力を求められた場合は、テキストを入力してから Return キーを押すかまたは「了解」をクリックします。

ヒント – ゾーン完了の現在の状態を表示するには、Labeled Zone Manager の「Return to Main Menu」をクリックします。

▼ Trusted Extensions でネットワークインタフェースを構成する

注 – DHCP を使用するようにシステムを構成する場合、OpenSolaris Community: Security Web ページ (`http://hub.opensolaris.org/bin/view/Community+Group+security/`)の Trusted Extensions の節にあるノートパソコンに関する指示を参照してください。

Solaris 10 10/08 リリースから、各ラベル付きゾーンが独自のサブネットにあるシステムを構成する場合は、この手順を省略して、75 ページの「ゾーンに名前およびラベルを付ける」に進むことができます。ゾーンのインストールとカスタマイズを終えたら、85 ページの「既存のラベル付きゾーンを経路指定するためにネットワークインタフェースを追加する」で各ラベル付きゾーンのネットワークインタフェースを追加します。

このタスクで、ネットワーキングを大域ゾーンで構成します。all-zones インタフェースを 1 つだけ作成する必要があります。all-zones インタフェースは、ラベル付きゾーンと大域ゾーンで共有されます。この共有インタフェースは、ラベル付きゾーンと大域ゾーンの間のトラフィックの経路制御に使用されます。このインタフェースを構成するには、次のいずれかを実行します。

- 物理インタフェースから論理インタフェースを作成した後、物理インタフェースを共有します。

  この構成が、管理者にとって、もっとも簡単です。システムが 2 つの IP アドレスを割り当てられている場合に、この構成を選択します。この手順では、論理インタフェースは大域ゾーンの固有アドレスとなり、物理インタフェースは大域ゾーンとラベル付きゾーン間で共有されます。
- 物理インタフェースを共有します

  システムが 1 つの IP アドレスを割り当てられている場合に、この構成を選択します。この構成では、大域ゾーンとラベル付きゾーン間で物理インタフェースが共有されます。
- 仮想ネットワークインタフェース vni0 を共有します

  DHCP を構成する場合や、各サブネットワークのラベルが異なっている場合に、この構成を選択します。手順例については、OpenSolaris Community: Security Web ページ (http://hub.opensolaris.org/bin/view/Community+Group+security/)の Trusted Extensions 節にあるノートパソコンに関する指示を参照してください。

  Solaris 10 10/08 リリースから、Trusted Extensions のループバックインタフェースは all-zones インタフェースとして作成されます。そのため、vni0 共有インタフェースを作成する必要はありません。

ゾーン固有のネットワークインタフェースを追加するには、インタフェースを追加する前に、ゾーンの作成を終了して確認します。手順については、85 ページの「既存のラベル付きゾーンを経路指定するためにネットワークインタフェースを追加する」を参照してください。

始める前に　大域ゾーンでスーパーユーザーになります。

Labeled Zone Manager が表示されています。この GUI を開くには、69 ページの「txzonemgr スクリプトを実行する」を参照してください。

1 「**Labeled Zone Manager**」で、「**Manage Network Interfaces**」を選択して、「了解」をクリックします。

インタフェースのリストが表示されます。

注 – この例では、物理インタフェースにホスト名と IP アドレスがインストール時に割り当てられています。

---

2 物理インタフェースを選択します。

インタフェースが 1 つあるシステムには、次のようなメニューが表示されます。参考のために注記を追加しています。

```
vni0                          Down      Virtual Network Interface
eri0 global 10.10.9.9 cipso Up      Physical Interface
```

a. `eri0` インタフェースを選択します。

b. 「了解」をクリックします。

3 このネットワークインタフェースに適したタスクを選択します。

次の、3 つのオプションが提示されます。

```
View Template       Assign a label to the interface
Share       Enable the global zone and labeled zones to use this interface
Create Logical Interface       Create an interface to use for sharing
```

- システムが **1** つの **IP** アドレスを持つ場合は、手順 **4** に進みます。
- システムが **2** つの **IP** アドレスを持つ場合は、手順 **5** に進みます。

4 **1** つの **IP** アドレスを持つシステムでは、物理インタフェースを共有します。

この構成では、ホストの IP アドレスがすべてのゾーンに適用されます。したがって、ホストのアドレスは `all-zones` アドレスです。このホストをマルチレベルサーバーとして使用することはできません。たとえば、ユーザーはこのシステムからのファイルを共有することはできません。このシステムは、LDAP プロキシサーバー、NFS ホームディレクトリサーバー、プリンタサーバーとすることはできません。

a. 「**Share**」を選択して「了解」をクリックします。

b. 共有インタフェースが表示されたダイアログボックスで、「了解」をクリックします。

```
eri0  all-zones  10.10.9.8  cipso  Up
```

物理インタフェースが `all-zones` インタフェースになっていれば、手順は正常に完了しています。75 ページの「ゾーンに名前およびラベルを付ける」に進みます。

5 **2** つの **IP** アドレスを持つシステムでは、論理インタフェースを作成します。

その後、物理インタフェースを共有します。

これはもっともシンプルな Trusted Extensions ネットワーク構成です。 この構成では、メインの IP アドレスはほかのシステムがこのシステム上の任意のゾーンに到達

するために使用し、論理インタフェースは大域ゾーンに固有とすることができます。大域ゾーンはマルチレベルサーバーとして使用できます。

a. 「**Create Logical Interface**」を選択して「了解」をクリックします。
   新しい論理インタフェースの作成を確認するダイアログボックスを閉じます。

b. 「**Set IP address**」を選択して「了解」をクリックします。

c. プロンプトで論理インタフェースのホスト名を指定し、「了解」をクリックします。
   たとえば、論理インタフェースのホスト名として `machine1-services` を指定します。この名前は、このホストがマルチレベルサービスを提供することを示しています。

d. プロンプトで論理インタフェースの **IP** アドレスを指定し、「了解」をクリックします。
   たとえば、論理インタフェースの IP アドレスとして `10.10.9.2` を指定します。

e. 論理インタフェースをもう一度選択して、「了解」をクリックします。

f. 「**Bring Up**」を選択して「了解」をクリックします。
   インタフェースが `Up` として表示されます。

```
eri0    global       10.10.9.1   cipso   Up
eri0:1  global       10.10.9.2   cipso   Up
```

g. 物理インタフェースを共有します。

   i. 物理インタフェースを選択して「了解」をクリックします。

   ii. 「**Share**」を選択して「了解」をクリックします。

```
eri0    all-zones    10.10.9.1   cipso   Up
eri0:1  global       10.10.9.2   cipso   Up
```

少なくとも 1 つのインタフェースが `all-zones` インタフェースになっていれば、手順は正常に完了しています。

例 4–3 共有論理インタフェースがあるシステムでの /etc/hosts ファイルの表示

大域ゾーンに一意のインタフェースがあり、ラベル付きゾーンが別のインタフェースを大域ゾーンと共有するシステムでは、`/etc/hosts` ファイルは次のようになります。

```
# cat /etc/hosts
...
127.0.0.1  localhost
192.168.0.11 machine1 loghost
192.168.0.12 machine1-services
```

デフォルト構成では、tnrhdb ファイルは次のようになります。

```
# cat /etc/security/tsol/tnrhdb
...
127.0.0.1:cipso
192.168.0.11:cipso
192.168.0.12:cipso
0.0.0.0:admin_low
```

all-zones インタフェースが tnrhdb ファイル内にない場合、インタフェースはデフォルトの cipso になります。

例 4–4 IP アドレスが 1 つある Trusted Extensions システムでの共有インタフェースの表示

この例では、管理者がシステムをマルチレベルサーバーとして使用する計画はありません。IP アドレスを節約するため、すべてのラベル付きゾーンと IP アドレスを共有するように大域ゾーンが構成されます。

管理者は、システムの hme0 インタフェースとして「Share」を選択します。このソフトウェアにより、すべてのゾーンに論理 NIC があるよう設定されます。これらの論理 NIC は、大域ゾーンで 1 つの物理的な NIC を共有します。

管理者は **ifconfig -a** コマンドを実行して、ネットワークインタフェース 192.168.0.11 にある物理インタフェース hme0 が共有されることを確認します。all-zones の値が表示されます。

```
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        all-zones
        inet 192.168.0.11 netmask fffffe00 broadcast 192.168.0.255
```

Solaris 10 10/08 リリースから、Trusted Extensions のループバックインタフェースは all-zones インタフェースとして作成されます。

```
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
        all-zones
        inet 127.0.0.1 netmask ff000000
hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        all-zones
        inet 192.168.0.11 netmask fffffe00 broadcast 192.168.0.255
```

管理者は /etc/hostname.hme0 ファイルの内容も調べます。

```
192.168.0.11 all-zones
```

▼ ゾーンに名前およびラベルを付ける

label_encodings ファイル中のラベルごとにゾーンを作成する必要はありませんが、作成することもできます。管理 GUI により、このシステムで GUI 用に作成されたゾーンを持つことのできるラベルが列挙されます。

始める前に　大域ゾーンでスーパーユーザーになります。「Labeled Zone Manager」ダイアログボックスが表示されます。この GUI を開くには、69 ページの「txzonemgr スクリプトを実行する」を参照してください。ネットワークインタフェースを大域ゾーンに構成しています。

必要なセキュリティーテプレートを作成しています。セキュリティーテンプレートで、属性の中で特に、ネットワークインタフェースに割り当てることができるラベル範囲を定義します。デフォルトのセキュリティーテンプレートでも必要性は満たされることはあります。

- セキュリティーテンプレートの概要については、『Oracle Solaris Trusted Extensions 管理の手順』の「Trusted Extensions のネットワークセキュリティー属性」を参照してください。
- Solaris 管理コンソールを使用してセキュリティーテンプレートを作成するには、『Oracle Solaris Trusted Extensions 管理の手順』の「トラステッドネットワークデータベースの構成 (作業マップ)」を参照してください。

1 「**Labeled Zone Manager**」で、「**Create a new zone**」をクリックして、「了解」をクリックします。
プロンプトで名前の入力を求められます。

a. ゾーンの名前を入力します。

ヒント – ゾーンのラベルに似た名前をゾーンに付けます。たとえば、ラベルが CONFIDENTIAL: RESTRICTED であるゾーンには、restricted という名前を付けます。

たとえば、デフォルトの label_encodings ファイルには次のラベルが含まれています。

```
PUBLIC
CONFIDENTIAL: INTERNAL USE ONLY
CONFIDENTIAL: NEED TO KNOW
CONFIDENTIAL: RESTRICTED
SANDBOX: PLAYGROUND
MAX LABEL
```

ラベルごとにゾーンを 1 つ作成できますが、次のゾーンを作成することを検討してください。

- すべてのユーザーのシステムでは、PUBLIC ラベルに 1 つのゾーン、および CONFIDENTIAL ラベルに 3 つのゾーンを作成します。
- 開発者用のシステムでは、SANDBOX: PLAYGROUND ラベルにゾーンを 1 つ作成します。SANDBOX: PLAYGROUND は開発者用の不連続ラベルとして定義され、開発者が使用するシステムにのみ、このラベルにゾーンが必要です。
- MAX LABEL ラベルにはゾーンを作成しないでください。これは認可上限として定義されます。

b. 「了解 (OK)」をクリックします。
ダイアログボックスでは、タスクのリストの上に *zone-name* :configured が表示されます。

2 ゾーンにラベルを付けるには、次のいずれかを選択します。

- カスタマイズした label_encodings ファイルを使用している場合、トラステッドネットワークゾーンツールを使用してゾーンにラベルを付けます。

  a. トラステッドネットワークゾーンツールを **Solaris** 管理コンソールで開きます。

  i. **Solaris** 管理コンソールを起動します。

  ```
  # /usr/sbin/smc &
  ```

  ii. ローカルシステムの **Trusted Extensions** ツールボックスを開きます。

  「コンソール」→「ツールボックスを開く」を選択します。

  「このコンピュータ (*this-host*: Scope=Files, Policy=TSOL)」という名前のツールボックスを選択します。

  「開く」をクリックします。

  iii. 「システムの構成」にある「コンピュータとネットワーク」に移動します。
  求められたらパスワードを入力します。

  iv. トラステッドネットワークゾーンツールをダブルクリックします。

b. ゾーンごとに、適切なラベルとゾーン名を関連付けます。

i. 「アクション」→「ゾーン構成の追加」を選択します。
ダイアログボックスに、割り当てられているラベルがないゾーンの名前が表示されます。

ii. ゾーン名を確認してから「編集」をクリックします。

iii. ラベルビルダーで、ゾーン名に該当するラベルをクリックします。
間違ったラベルをクリックした場合、そのラベルをもう一度クリックして選択を解除し、正しいラベルをクリックします。

iv. 割り当てを保存します。
「トラステッドネットワークゾーンのプロパティー」ダイアログボックスで「了解」をクリックします。

必要なゾーンがすべてパネルに表示されたら終了です。あるいは、「ゾーン構成の追加」メニュー項目をクリックすると、ゾーン名の値がないダイアログボックスが開かれます。

- デフォルトの `label_encodings` ファイルを使用している場合、**Labeled Zone Manager** を使用します。
「Select Label」メニュー項目をクリックして「了解」をクリックし、使用可能なラベルのリストを表示します。

a. ゾーンのラベルを選択します。
`public` という名前のゾーンの場合、リストから `PUBLIC` ラベルを選択します。

b. 「了解 (OK)」をクリックします。
タスクのリストが表示されます。

▼ ラベル付きゾーンをインストールする

始める前に　大域ゾーンでスーパーユーザーになります。ゾーンが構成されており、割り当て済みのネットワークインタフェースがあります。

「Labeled Zone Manager」ダイアログボックスが表示され、*zone-name*`:configured` というサブタイトルが付いています。この GUI を開くには、69 ページの「`txzonemgr` スクリプトを実行する」を参照してください。

1 **Labeled Zone Manager** から「**Install**」を選択して「了解」をクリックします。

注意 – このプロセスが終了するまでしばらく時間がかかります。このタスクの実行中は、ほかのタスクを実行しないでください。

システムで、大域ゾーンから非大域ゾーンにパッケージがコピーされます。このタスクによって、ラベル付きの仮想オペレーティングシステムがゾーンにインストールされます。この例を続行するため、このタスクで `public` ゾーンがインストールされます。GUI に次のような出力が表示されます。

```
# Labeled Zone Manager: Installing zone-name zone
Preparing to install zone <zonename>
Creating list of files to copy from the global zone
Copying <total> files to the zone
Initializing zone product registry
Determining zone package initialization order.
Preparing to initialize <subtotal> packages on the zone.
Initializing package <number> of <subtotal>: percent complete: percent

Initialized <subtotal> packages on zone.
Zone <zonename> is initialized.
The file /zone/internal/root/var/sadm/system/logs/install_log
contains a log of the zone installation.
```

注 – `cannot create ZFS dataset zone/`*zonename*`: dataset already exists` のようなメッセージは、情報メッセージです。ゾーンは既存のデータセットを使用します。

インストールが完了すると、ホストの名前の入力を 要求するプロンプトが表示されます。名前が表示されます。

2 そのホストの名前をそのまま使用します。

ダイアログボックスでは、タスクのリストの上に *zone-name*`:installed` が表示されます。

注意事項 次のような警告が表示されます。 「`Installation of these packages generated errors: SUNW` *pkgname*」が表示された場合、インストールログを読み、パッケージのインストールを終了します。

▼ ラベル付きゾーンを起動する

始める前に 大域ゾーンでスーパーユーザーになります。ゾーンがインストールされており、割り当て済みのネットワークインタフェースがあります。

「Labeled Zone Manager」ダイアログボックスが表示され、 *zone-name*`:installed` というサブタイトルが付いています。この GUI を開くには、69 ページの「`txzonemgr` スクリプトを実行する」を参照してください。

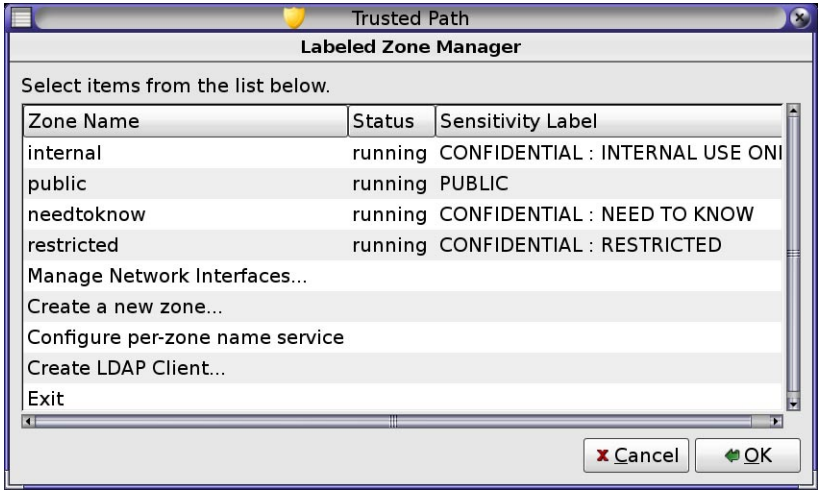
1 「**Labeled Zone Manager**」で「**Zone Console**」を選択して「了解」をクリックします。
現在のラベル付きゾーンに、別のコンソールウィンドウが表示されます。

2 「**Boot**」を選択します。
「ゾーン端末コンソール」は、ゾーン起動の進捗を追跡します。ゾーンを最初から作成する場合は、次のようなメッセージがコンソールに表示されます。

```
[Connected to zone 'public' console]

[NOTICE: Zone booting up]
...
Hostname: zone-name
Loading smf(5) service descriptions: number/total
Creating new rsa public/private host key pair
Creating new dsa public/private host key pair

rebooting system due to change(s) in /etc/default/init

[NOTICE: Zone rebooting]
```

注意 – このタスクの実行中は、ほかのタスクを実行しないでください。

4 つのデフォルトのゾーンが構成されて起動されると、Labeled Zone Manager では次のようにゾーンが表示されます。



注意事項 場合によっては、エラーメッセージが表示されてゾーンが再起動しないことがあります。ゾーン端末コンソールで Return キーを押します。再起動するために y の入力を求めるプロンプトが表示されたら、y を入力して Return キーを押します。ゾーンが再起動されます。

次の手順　このゾーンが別のゾーンからコピーされたかまたはクローン作成された場合は、80 ページの「ゾーンのステータスを確認する」に進みます。

このゾーンが最初のゾーンである場合は、81 ページの「ラベル付きゾーンをカスタマイズする」に進みます。

▼ ゾーンのステータスを確認する

注 – X サーバーが大域ゾーンで実行されます。それぞれのラベル付きゾーンがこの X サーバーを使用するには、大域ゾーンに接続できなければなりません。そのため、ゾーンネットワークが機能しなければ、ゾーンを使用することはできません。背景の説明については、28 ページの「マルチレベルアクセスの計画」を参照してください。

1 ゾーンが完全に起動されていることを確認します。

a. *zone-name*: ゾーン端末コンソールで、**root** としてログインします。

```
hostname console login: root
Password:       Type root password
```

b. ゾーン端末コンソールで、クリティカルサービスが実行されていることを確認します。

```
# svcs -xv
svc:/application/print/server:default (LP print server)
 State: disabled since Tue Oct 10 10:10:10 2006
Reason: Disabled by an administrator.
   See: http://sun.com/msg/SMF-8000-05
   See: lpsched(1M)
...
```

`sendmail` および `print` サービスは、クリティカルサービスではありません。

c. ゾーンに妥当な **IP** アドレスがあることを確認します。

```
# ifconfig -a
```

たとえば、次の出力には `hme0` インタフェースの IP アドレスが表示されます。

```
# ...
 hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
         all-zones
         inet 192.168.0.11 netmask fffffe00 broadcast 192.168.0.255
```

d. (省略可能) ゾーンが大域ゾーンと通信できることを確認します。

i. DISPLAY 変数が X サーバーをポイントするよう設定します。

```
# DISPLAY=global-zone-hostname:n.n
# export DISPLAY
```

ii. 端末ウィンドウから GUI を表示します。

たとえば、クロックを表示します。

```
# /usr/openwin/bin/xclock
```

ゾーンのラベルでクロックが表示されない場合は、ゾーンのネットワーキングが正しく構成されていません。デバックに関する提案事項は、111 ページの「ラベル付きゾーンが X サーバーにアクセスできない」を参照してください。

iii. GUI を閉じて続行します。

2 大域ゾーンから、ラベル付きゾーンのステータスを確認します。

```
# zoneadm list -v
ID NAME         STATUS         PATH                BRAND   IP
 0 global       running        /                   native  shared
 3 internal     running        /zone/internal      native  shared
 4 needtoknow   running        /zone/needtoknow    native  shared
 5 restricted   running        /zone/restricted    native  shared
```

次の手順 これでラベル付きゾーンの構成は完了です。ゾーン固有のネットワークインタフェースをゾーンに追加するか、ラベル付きゾーンごとにデフォルトルーティングを確立するには、85 ページの「ネットワークインタフェースをラベル付きゾーンに追加し、ルーティングする」に進みます。そうでない場合は、93 ページの「Trusted Extensions での役割とユーザーの作成」に進みます。

▼ ラベル付きゾーンをカスタマイズする

ゾーンのクローンを作成する、またはゾーンをコピーする場合、この手順によって、ゾーンがほかのゾーンのテンプレートになるように構成されます。さらに、この手順によって、使用するテンプレートから作成されていないゾーンを構成します。

始める前に 大域ゾーンでスーパーユーザーになります。80 ページの「ゾーンのステータスを確認する」を完了しておきます。

1 ゾーン端末コンソールで、ラベル付きゾーンで不要なサービスを無効にします。

このゾーンをコピーまたはクローンを作成する場合、無効にしたサービスは新しいゾーンで無効にされます。システムでオンラインであるサービスは、そのゾーンの

サービスマニフェストによって異なります。netservices limited コマンドを使用して、ラベル付きゾーンで必要としないサービスをオフにします。

a. 多数の不要なサービスを削除します。

```
# netservices limited
```

b. そのほかのサービスを一覧にします。

```
# svcs
...
STATE        STIME      FMRI
online       13:05:00   svc:/application/graphical-login/cde-login:default
...
```

c. グラフィカルログインを無効にします。

```
# svcadm disable svc:/application/graphical-login/cde-login
# svcs cde-login
STATE        STIME      FMRI
disabled     13:06:22   svc:/application/graphical-login/cde-login:default
```

サービス管理フレームワークの詳細は、smf(5) のマニュアルページを参照してください。

2 「**Labeled Zone Manager**」で「**Halt**」を選択してゾーンを停止します。

3 続行する前に、ゾーンがシャットダウンされていることを確認します。

zone-name: ゾーン端末コンソールで、次のメッセージによって、ゾーンがシャットダウンされていることが示されます。

```
[ NOTICE: Zone halted]
```

このゾーンをコピーまたはそのクローンを作成するのではない場合、この最初のゾーンを作成したのと同じ方法で残りのゾーンを作成します。そのほかの場合は、次の手順に進みます。

4 このゾーンをほかのゾーンのテンプレートとして使用する場合、次のとおりに実行します。

a. auto_home_*zone-name* ファイルを削除します。

大域ゾーンの端末ウィンドウで、*zone-name* ゾーンからこのファイルを削除します。

```
# cd /zone/zone-name/root/etc
# ls auto_home*
auto_home  auto_home_zone-name
# rm auto_home_zone-name
```

たとえば、public ゾーンがほかのゾーンのクローン作成元テンプレートである場合、auto_home_public ファイルを次のように削除します。

```
# cd /zone/public/root/etc
# rm auto_home_public
```

b. このゾーンのクローンを作成する場合、次の手順で **ZFS** スナップショットを作成してから、**83** ページの「**Trusted Extensions** でゾーンのコピーまたはクローンを行う」に進みます。

c. このゾーンをコピーする場合は、手順 **6** を完了してから**83** ページの「**Trusted Extensions** でゾーンのコピーまたはクローンを行う」に進みます。

5 その他のゾーンのクローンを作成するためのゾーンテンプレートを作成するには、「**Create Snapshot**」を選択して「了解」をクリックします。

注意 – スナップショットのゾーンは、ZFS ファイルシステム内になければなりません。59 ページの「ゾーンのクローンを作成するために ZFS プールを作成する」でゾーンに ZFS ファイルシステムが作成されます。

6 カスタマイズしたゾーンがまだ使用できることを確認するには、「**Labeled Zone Manager**」から「**Boot**」を選択します。

ゾーン端末コンソールは、ゾーン起動の進捗を追跡します。次のようなメッセージがコンソールに表示されます。

```
[Connected to zone 'public' console]

[NOTICE: Zone booting up]
...
Hostname: zonename
```

ログインプロンプトに対して Return キーを押します。root としてログインできます。

▼ Trusted Extensions でゾーンのコピーまたはクローンを行う

始める前に 81 ページの「ラベル付きゾーンをカスタマイズする」を完了しておきます。

「Labeled Zone Manager」ダイアログボックスが表示されます。この GUI を開くには、69 ページの「txzonemgr スクリプトを実行する」を参照してください。

1 ゾーンを作成します。

詳細は、75 ページの「ゾーンに名前およびラベルを付ける」を参照してください。

2 次の方法のいずれかを選択して、ゾーン作成ストラテジを続行します。
新規のゾーンごとに次の手順を繰り返します。

- ラベルを付けたゾーンをコピーします。

  a. 「**Labeled Zone Manager**」から「コピー」を選択して「了解」をクリックします。

  b. ゾーンテンプレートを選択して「了解」をクリックします。
  ウィンドウにコピーのプロセスが表示されます。プロセスが完了すると、ゾーンがインストールされます。

  「Labeled Zone Manager」に「*zone-name* :configured」と表示された場合は、次の手順に進みます。それ以外の場合は、手順 e に進みます。

  c. メニュー項目「**Select another zone**」を選択して「了解」をクリックします。

  d. 新規にインストールされたゾーンを選択して、「了解」をクリックします。

  e. 78 ページの「ラベル付きゾーンを起動する」を完了します。

  f. 80 ページの「ゾーンのステータスを確認する」を完了します。

- ラベルを付けたゾーンのクローンを作成します。

  a. 「**Labeled Zone Manager**」で「クローン」を選択して「了解」をクリックします。

  b. リストから **ZFS** スナップショットを選択して「了解」をクリックします。
  たとえば、`public` からスナップショットを作成した場合は、`zone/public@snapshot` を選択します。

  クローン作成のプロセスが完了すると、ゾーンがインストールされます。手順 c に進みます。

  c. ゾーンコンソールを開き、ゾーンを起動します。
  手順については、78 ページの「ラベル付きゾーンを起動する」を参照してください。

  d. 80 ページの「ゾーンのステータスを確認する」を完了します。

次の手順
- すべてのゾーンに対して 80 ページの「ゾーンのステータスを確認する」を完了していて、各ゾーンをそれぞれ別の物理ネットワークに配置する場合は、85 ページの「既存のラベル付きゾーンを経路指定するためにネットワークインタフェースを追加する」に進みます。
- まだ役割を作成していない場合は、93 ページの「Trusted Extensions での役割とユーザーの作成」に進みます。
- すでに役割を作成済みの場合は、105 ページの「Trusted Extensions でのホームディレクトリの作成」に進みます。

ネットワークインタフェースをラベル付きゾーンに追加し、ルーティングする

次の作業は、各ゾーンが個別の物理ネットワークに接続されている環境に対応します。

作業	説明	参照先
1a: ネットワークインタフェースを各ラベル付きゾーンに追加し、大域ゾーンを使用して外部ネットワークに到達します。	各ラベル付きゾーンを個別の物理ネットワークに接続します。ラベル付きゾーンは、大域ゾーンが提供するネットワークルーティングを使用します。	85 ページの「既存のラベル付きゾーンを経路指定するためにネットワークインタフェースを追加する」
または 1b: ネットワークインタフェースを、デフォルトルートを使用して各ラベル付きゾーンに追加します。	各ゾーンを個別の物理ネットワークに接続します。ラベル付きゾーンは、ルーティングで大域ゾーンを使用しません。	88 ページの「既存のラベル付きゾーンを経路指定するために大域ゾーンを使用しないネットワークインタフェースを追加する」
2. ネームサービスキャッシュを各ラベル付きゾーンに作成します。	各ゾーンに対してネームサービスデーモンを構成します。	92 ページの「ラベル付きゾーンごとにネームサービスキャッシュを構成する」

▼ 既存のラベル付きゾーンを経路指定するためにネットワークインタフェースを追加する

この手順で、ゾーン固有のネットワークインタフェースを既存のラベル付きゾーンに追加します。この構成は、各ラベル付きゾーンがそれぞれ別の物理ネットワークに接続される環境に対応します。ラベル付きゾーンは、大域ゾーンが提供するネットワークルーティングを使用します。

注 – 大域ゾーンでは、非大域ゾーンアドレスが構成される各サブネットに対して IP アドレスを構成する必要があります。

始める前に　大域ゾーンでスーパーユーザーになります。

すべてのゾーンに対し、68 ページの「ラベル付きゾーンの作成」の作業を完了します。

1 大域ゾーンで、追加のネットワークインタフェースの **IP** アドレスとホスト名を `/etc/hosts` ファイルに入力します。

ホストの名前に *-zone-name* を追加するなど、標準的な命名規則を使用してください。

```
## /etc/hosts in global zone
10.10.8.2    hostname-zone-name1
10.10.8.3    hostname-global-name1
10.10.9.2    hostname-zone-name2
10.10.9.3    hostname-global-name2
```

2 各インタフェースのネットワークで、`/etc/netmasks` ファイルにエントリを追加します。

```
## /etc/netmasks in global zone
10.10.8.0 255.255.255.0
10.10.9.0 255.255.255.0
```

詳細は、`netmasks(4)` のマニュアルページを参照してください。

3 大域ゾーンで、ゾーン固有の物理インタフェースを **plumb** します。

a. すでに **plumb** されている物理インタフェースを特定します。

```
# ifconfig -a
```

b. 各インタフェースの大域ゾーンアドレスを構成します。

```
# ifconfig interface-nameN1 plumb
# ifconfig interface-nameN1 10.10.8.3 up
# ifconfig interface-nameN2 plumb
# ifconfig interface-nameN2 10.10.9.3 up
```

c. 各大域ゾーンアドレスに対して `hostname.`*interface-nameN* ファイルを作成します。

```
# /etc/hostname.interface-nameN1
10.10.8.3
# /etc/hostname.interface-nameN2
10.10.9.3
```

大域ゾーンアドレスは、システムが起動するとただちに構成されます。ゾーン固有のアドレスは、ゾーンの起動時に構成されます。

4 それぞれのゾーン固有のネットワークインタフェースに、セキュリティーテンプレートを割り当てます。

ネットワークへのゲートウェイにラベルが構成されていない場合は、`admin_low` セキュリティーテンプレートを割り当てます。ネットワークへのゲートウェイにラベルが付いている場合は、`cipso` セキュリティーテンプレートを割り当てます。

各ネットワークのラベルを反映する、ホストタイプ `cipso` のセキュリティーテンプレートを作成できます。テンプレートの作成および割り当ての手順については、『Oracle Solaris Trusted Extensions 管理の手順』の「トラステッドネットワークデータベースの構成 (作業マップ)」を参照してください。

5 ゾーン固有のインタフェースに追加するすべてのラベル付きゾーンを停止します。

```
# zoneadm -z zone-name halt
```

6 **Labeled Zone Manager** を起動します。

```
# /usr/sbin/txzonemgr
```

7 ゾーン固有のインタフェースを追加させたい各ゾーンについては、次の操作を実行します。

a. ゾーンを選択します。

b. 「**Add Network**」を選択します。

c. ネットワークインタフェースに名前を付けます。

d. インタフェースの **IP** アドレスを入力します。

8 完了したすべてのゾーンの「**Labeled Zone Manager**」で、「**Zone Console**」を選択します。

9 「**Boot**」を選択します。

10 「**Zone Console**」で、インターフェスが作成されていることを確認します。

```
# ifconfig -a
```

11 サブネットのゲートウェイへのルートがゾーンにあることを確認します。

```
# netstat -rn
```

注意事項　ゾーン構成をデバッグするには、次を参照してください。

- 『System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones』の第 30 章「Troubleshooting Miscellaneous Solaris Zones Problems」
- 110 ページの「Trusted Extensions の構成のトラブルシューティング」
- 『Oracle Solaris Trusted Extensions 管理の手順』の「トラステッドネットワークのトラブルシューティング (作業マップ)」

▼ 既存のラベル付きゾーンを経路指定するために大域ゾーンを使用しないネットワークインタフェースを追加する

この手順では、既存のラベル付きゾーンに対して、ゾーン固有のデフォルトルートを設定します。この構成では、ラベル付きゾーンは、ルーティングで大域ゾーンを使用しません。

ラベル付きゾーンは、ゾーンを起動する前に大域ゾーンに plumb します。ただし、ラベル付きゾーンを大域ゾーンから切り離すために、ゾーンの起動時はインタフェースを down 状態にしてください。詳細は、『System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones』の第 17 章「Non-Global Zone Configuration (Overview)」.

注 – 起動するすべての非大域ゾーンに対し、固有のデフォルトルートを構成します。

始める前に　大域ゾーンでスーパーユーザーになります。

すべてのゾーンに対し、68 ページの「ラベル付きゾーンの作成」の作業を完了します。`vni0` インタフェースか `lo0` インタフェースを使用してラベル付きゾーンを大域ゾーンに接続しています。

1. すべてのネットワークインタフェースに対し、その **IP** アドレス、ネットマスク、デフォルトルートを調べます。

   IP アドレスとネットマスクを調べるには、`ifconfig -a` コマンドを使用します。デフォルトルートが割り当てられているかどうかを判定するには、`zonecfg -z zonename info net` コマンドを使用します。

2. 各ラベル付きゾーン用に、空の `/etc/hostname.`*interface* ファイルを作成します。

   ```
   # touch /etc/hostname.interface
   # touch /etc/hostname.interface:n
   ```

   詳細は、`netmasks(4)` のマニュアルページを参照してください。

3 ラベル付きゾーンのネットワークインタフェースを **plumb** します。

```
# ifconfig zone1-network-interface plumb
# ifconfig zone2-network-interface plumb
```

4 ラベル付きゾーンのインタフェースが down 状態になっていることを確認します。

```
# ifconfig -a
zone1-network-interface zone1-IP-address down
zone2-network-interface zone2-IP-address down
```

ゾーン固有のアドレスは、ゾーンの起動時に構成されます。

5 各インタフェースのネットワークで、/etc/netmasks ファイルにエントリを追加します。

```
## /etc/netmasks in global zone
192.168.2.0 255.255.255.0
192.168.3.0 255.255.255.0
```

詳細は、netmasks(4) のマニュアルページを参照してください。

6 それぞれのゾーン固有のネットワークインタフェースに、セキュリティーテンプレートを割り当てます。

各ネットワークのラベルを反映する、ホストタイプ cipso のセキュリティーテンプレートを作成します。テンプレートの作成および割り当てについては、『Oracle Solaris Trusted Extensions 管理の手順』の「トラステッドネットワークデータベースの構成 (作業マップ)」を参照してください。

7 txzonemgr スクリプトを実行し、別の端末ウィンドウを開きます。

Labeled Zone Manager で、ラベル付きゾーンのネットワークインタフェースを追加します。端末ウィンドウで、ゾーンに関する情報を表示し、デフォルトルートを設定します。

8 ゾーン固有のネットワークインタフェースとルーターを追加しようとしているすべてのゾーンに対し、次の手順を完了します。

a. 端末ウィンドウでゾーンを停止します。

```
# zoneadm -z zone-name halt
```

b. **Labeled Zone Manager** で、次の手順を実行します。

i. ゾーンを選択します。

ii. 「**Add Network**」を選択します。

iii. ネットワークインタフェースに名前を付けます。

iv. インタフェースの **IP** アドレスを入力します。

v. 端末ウィンドウで、ゾーン構成を確認します。

```
# zonecfg -z zone-name info net
net:    address: IP-address
        physical: zone-network-interface
        defrouter not specified
```

c. 端末ウィンドウで、ラベル付きゾーンのネットワークのデフォルトルートを構成します。

```
# zonecfg -z zone-name
zonecfg:zone-name > select net address=IP-address
zonecfg:zone-name:net> set defrouter=router-address
zonecfg:zone-name:net> end
zonecfg:zone-name > verify
zonecfg:zone-name > commit
zonecfg:zone-name > exit
#
```

詳細については、zonecfg(1M) のマニュアルページと『System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones』の「How to Configure the Zone」を参照してください。

d. ラベル付きゾーンを起動します。

```
# zoneadm -z zone-name boot
```

e. 大域ゾーンで、ラベル付きゾーンにサブネットのゲートウェイへの経路があることを確認します。

```
# netstat -rn
```

経路指定テーブルが表示されます。ラベル付きゾーンの宛先とインタフェースは、大域ゾーンのエントリと異なります。

9 デフォルトルートを削除するには、ゾーンのIPアドレスを選択し、削除します。

```
# zonecfg -z zone-name

zonecfg:zone-name > select net address=zone-IP-address
zonecfg:zone-name:net> remove net defrouter=zone-default-route
zonecfg:zone-name:net>  info net
net:
   address: zone-IP-address
   physical: zone-network-interface
   defrouter not specified
```

例 4–5 ラベル付きゾーンのデフォルトルートを設定する

この例では、管理者が Secret ゾーンを個別の物理サブネットに経路指定します。Secret ゾーンとの間のトラフィックは、大域ゾーン経由で経路指定されません。管理者は Labeled Zone Manager と zonecfg コマンドを使用し、ルーティングが機能することを確認します。

管理者は、qfe1 と qfe1:0 が現在使用中でないことを確認します。その後、2 つのラベル付きゾーンのマッピングを作成します。qfe1 は、Secret ゾーンに対して指定されたインタフェースです。

```
Interface IP Address    Netmask        Default Router
qfe1     192.168.2.22 255.255.255.0 192.168.2.2
qfe1:0   192.168.3.33 255.255.255.0 192.168.3.3
```

まず、管理者は /etc/hostname.qfe1 ファイルを作成し、/etc/netmasks ファイルを構成します。

```
# touch /etc/hostname.qfe1
```

```
# cat /etc/netmasks
## /etc/netmasks in global zone
192.168.2.0 255.255.255.0
```

次に、ネットワークインタフェースを plumb し、インタフェースが down 状態であることを確認します。

```
# ifconfig qfe1 plumb
# ifconfig -a
```

次に、Solaris 管理コンソール で、1 つのラベル Secret を持つセキュリティーテンプレートを作成し、インタフェースの IP アドレスをテンプレートに割り当てます。

ゾーンを停止します。

```
# zoneadm -z secret halt
```

txzonemgr スクリプトを実行し、Labeled Zone Manager を開きます。

```
# /usr/sbin/txzonemgr
```

Labeled Zone Manager で、Secret ゾーンを選択し、「Add Network」を選択して、ネットワークインタフェースを選択します。Labeled Zone Manager を閉じます。

コマンド行で、ゾーンの IP アドレスを選択し、そのデフォルトルートを設定します。コマンドを終了する前に、ルートを確認して確定します。

```
# zonecfg -z secret
zonecfg: secret > select net address=192.168.6.22
zonecfg: secret:net> set defrouter=192.168.6.2
zonecfg: secret:net> end
zonecfg: secret > verify
zonecfg: secret > commit
zonecfg: secret > info net
  net:
     address: 192.168.6.22
     physical: qfe1
     defrouter: 192.168.6.2
zonecfg: secret > exit
#
```

ゾーンを起動します。

```
# zoneadm -z secret boot
```

大域ゾーンの別の端末ウィンドウで、パケットの送受信を確認します。

```
# netstat -rn
Routing Table: IPv4
  Destination           Gateway           Flags  Ref     Use  Interface
-------------------- -------------------- ----- ----- ------- ---------
default              192.168.5.15         UG        1    2664 qfe0
192.168.6.2          192.168.6.22         UG        1     240 qfe1
192.168.3.3          192.168.3.33         U         1     183 qfe1:0
127.0.0.1            127.0.0.1            UH        1     380 lo0
...
```

▼ ラベル付きゾーンごとにネームサービスキャッシュを構成する

この手順では、各ラベル付きゾーンで、ネームサービスデーモン (nscd) を個別に構成できます。この構成がサポートする環境は、各ゾーンがそのゾーンのラベルで動作するサブネットワークに接続されており、そのサブネットワークにはそのラベル用の独自のネームサーバーがあります。

注 – この構成は、評価された構成の条件を満たしません。評価された構成では、nscd デーモンは大域ゾーンでのみ実行されます。各ラベル付きゾーン内の door は、そのゾーンを大域の nscd デーモンに接続します。

始める前に　大域ゾーンでスーパーユーザーになります。root はまだ役割になってはいけません。85 ページの「既存のラベル付きゾーンを経路指定するためにネットワークインタフェースを追加する」が正常に完了しています。

この構成では、高度なネットワークスキルが要求されます。LDAP をネームサービスとして使用するユーザーには、各ラベル付きゾーンへの LDAP クライアント接続を確立する責任があります。nscd デーモンは、ネームサービスの情報をキャッシュに書き込みますが、そのルーティングは行いません。

1. **LDAP を使用している場合、ラベル付きゾーンから LDAP サーバーへのルートを確認します。**

   各ラベル付きゾーンの端末ウィンドウで、次のコマンドを実行します。

   zone-name `# netstat -rn`

2. **大域ゾーンで Labeled Zone Manager を起動します。**

   ```
   # /usr/sbin/txzonemgr
   ```

3 「**Configure per-zone name service**」を選択し、「了解」をクリックします。
このオプションは、初期システム構成時に一度だけ使用されるように意図されています。

4 各ゾーンの nscd サービスを構成します。
参考として、nscd(1M) および nscd.conf(4) のマニュアルページを参照してください。

5 システムを再起動します。

6 ゾーンごとに、ルートとネームサービスデーモンを確認します。

a. ゾーンコンソールで nscd サービスを表示します。

```
zone-name # svcs -x name-service-cache
svc:/system/name-service-cache:default (name service cache)
 State: online since October 10, 2010  10:10:10 AM PDT
   See: nscd(1M)
   See: /etc/svc/volatile/system-name-service-cache:default.log
Impact: None.
```

b. サブネットワークへのルートを確認します。

```
zone-name # netstat -rn
```

7 ゾーン固有のネームサービスデーモンを削除するには、大域ゾーンで次の手順を実行します。

a. **Labeled Zone Manager** を開きます。

b. 「**Unconfigure per-zone name service**」を選択し、「了解」をクリックします。
この選択により、すべてのラベル付きゾーンで nscd デーモンが削除されます。

c. システムを再起動します。

Trusted Extensions での役割とユーザーの作成

すでに管理役割を使用している場合、セキュリティー管理者役割を追加できます。役割をまだ実装していないサイトにおいて、役割を作成する手順は Solaris OS の場合と同様です。Trusted Extensions ドメインを管理するためには、Trusted Extensions でセキュリティー管理役割を追加し、Solaris 管理コンソールを使用する必要があります。

サイトセキュリティーで、ユーザーと役割アカウントを作成するために 2 人の人が必要な場合は、カスタム権利プロファイルを作成し、役割に割り当てて、責務分離を実施します。

作業	説明	参照先
デフォルトのプロファイルよりも厳しい 3 つの権利プロファイルを作成します。	ユーザーを管理するための権利プロファイルを作成します。これらのプロファイルは、ユーザーを管理するデフォルトプロファイルよりも制限が厳しくなっています。	94 ページの「責務分離を実施する権利プロファイルを作成する」
セキュリティー管理者役割を作成します。	セキュリティー関連の作業を扱うセキュリティー管理者役割を作成します。	97 ページの「Trusted Extensions でセキュリティー管理者役割を作成する」
ユーザーパスワードを設定できないシステム管理者役割を作成します。	システム管理者役割を作成し、制限されたシステム管理者権利プロファイルに割り当てます。	99 ページの「制限されたシステム管理者役割を作成する」
管理役割になるユーザーを作成します。	役割になることができる 1 人または複数のユーザーを作成します。	100 ページの「Trusted Extensions で役割になれるユーザーを作成する」
役割が各自の作業を実行できることを確認します。	さまざまなシナリオで役割をテストします。	103 ページの「Trusted Extensions の役割が機能することを確認する」
ユーザーがラベル付きゾーンにログインできるようにします。	一般ユーザーがログインできるようにゾーンサービスを開始します。	104 ページの「ユーザーがラベル付きゾーンにログインできるようにする」

▼ 責務分離を実施する権利プロファイルを作成する

責務分離がサイトセキュリティー要件にない場合は、この手順を省略します。サイトで責務分離が必要な場合は、LDAP サーバーにデータを設定する前に、これらの権利プロファイルと役割を作成します。

この手順では、ユーザーを管理するための個別の機能を持つ権利プロファイルを作成します。これらのプロファイルを個々の役割に割り当てる場合、ユーザーを作成し構成するために 2 つの役割が必要です。一方の役割はユーザーを作成できますが、セキュリティー属性を割り当てることができません。もう一方の役割はセキュリティー属性を割り当てることができますが、ユーザーを作成できません。これらのプロファイルのいずれかが割り当てられた役割で Solaris 管理コンソール にログインすると、役割に該当するタブとフィールドだけが表示されます。

始める前に　スーパーユーザーになるか、`root` 役割または主管理者役割になる必要があります。この手順を開始する場合には、Solaris 管理コンソール を閉じます。

1 ユーザー構成に影響を与えるデフォルトの権利プロファイルのコピーを作成します。

a. `prof_attr` ファイルを `prof_attr.orig` ファイルにコピーします。

b. prof_attr ファイルをトラステッドエディタで開きます。

```
# /usr/dt/bin/trusted_edit /etc/security/prof_attr
```

c. 3 つの権利プロファイルをコピーし、コピーの名前を変更します。

```
System Administrator:::Can perform most non-security...
Custom System Administrator:::Can perform most non-security...

User Security:::Manage passwords...
Custom User Security:::Manage passwords...

User Management:::Manage users, groups, home...
Custom User Management:::Manage users, groups, home...
```

d. 変更を保存します。

e. 変更内容を確認します。

```
# grep ^Custom  /etc/security/prof_attr
Custom System Administrator:::Can perform most non-security...
Custom User Management:::Manage users, groups, home...
Custom User Security:::Manage passwords...
```

権利プロファイルを変更せずにコピーすることで、システムを新しい Solaris リリースにアップグレードしたときにも変更内容が保持されます。これらの権利プロファイルは複雑なため、デフォルトのプロファイルのコピーを変更したほうが、ゼロから制限の厳しいプロファイルを作成するよりも、誤りが起きにくくなります。

2 Solaris 管理コンソールを起動します。

```
# /usr/sbin/smc &
```

3 このコンピュータ (*this-host*: Scope=Files, Policy=TSOL) ツールボックスを選択します。

4 「システムの構成」をクリックして「ユーザー」をクリックします。
パスワードを入力するよう求められます。

5 適切なパスワードを入力します。

6 「権限」をダブルクリックします。

7 カスタムユーザーセキュリティー権利プロファイルを変更します。
ユーザーを作成できないようにこのプロファイルを制限します。

a. 「カスタムユーザーセキュリティー」をダブルクリックします。

b. 「認可」タブをクリックし、次の手順を実行します。

i. 「含む」リストから、「Manage Users and Roles」認可を削除します。
次のユーザーアカウント権限が残ります。

```
Audit Controls
Label and Clearance Range
Change Password
View Users and Roles
Modify Extended Security Attributes
```

ii. 「権限の管理」権限を「含む」リストに追加します。

c. 「了解」をクリックして変更内容を保存します。

8 カスタムユーザー管理プロファイルを変更します。
パスワードを設定できないようにこのプロファイルを制限します。

a. 「カスタムユーザー管理」をダブルクリックします。

b. 「認可」タブをクリックし、次の手順を実行します。

i. 「含む」リストのスクロールバーを「ユーザーアカウント」にドラッグします。

ii. 「含む」リストから、「Modify Extended Security Attributes」認可を削除します。
次のユーザーアカウント権限が残ります。

```
Manage Users and Roles
View Users and Roles
```

c. 変更を保存します。

9 カスタムシステム管理者権利プロファイルを変更します。
ユーザー管理者プロファイルは、このプロファイルの補助プロファイルです。システム管理者がパスワードを設定できないようにします。

a. 「カスタムシステム管理者」をダブルクリックします。

b. 「補助権限」タブをクリックし、次の手順を実行します。

i. ユーザー管理権利プロファイルを削除します。

ii. カスタムユーザー管理権利プロファイルを追加します。

iii. カスタムユーザー管理権利プロファイルを、すべての権利プロファイルの上に移動します。

c. 変更を保存します。

次の手順 デフォルトのプロファイルが使用されないようにするには、カスタムプロファイルによって責務分離が実施されることを確認したあと、103 ページの「Trusted Extensions の役割が機能することを確認する」の手順 7 を参照してください。

▼ Trusted Extensions でセキュリティー管理者役割を作成する

Trusted Extensions での役割作成は、Solaris OS での役割作成と同じです。ただし、Trusted Extensions では、セキュリティー管理者役割は必須です。ローカルのセキュリティー管理者役割を作成するには、例 4–6 のようにコマンド行インタフェースを使用することもできます。

始める前に スーパーユーザーになるか、`root` 役割または主管理者役割になる必要があります。

ネットワーク上に役割を作成するには、132 ページの「LDAP のための Solaris 管理コンソールの設定 (作業マップ)」を完了しておく必要があります。

1. **Solaris 管理コンソールを起動します。**

```
# /usr/sbin/smc &
```

2. 適切なツールボックスを選択します。

   - ローカルに役割を作成する場合、「このコンピュータ (*this-host*`: Scope=Files, Policy=TSOL`)」を使用します。
   - **LDAP** サービスに役割を作成する場合、「このコンピュータ (*ldap-server*`: Scope=LDAP, Policy=TSOL`)」を使用します。

3. 「システムの構成」をクリックして「ユーザー」をクリックします。
   パスワードを入力するよう求められます。

4. 適切なパスワードを入力します。

5. 「管理役割」をダブルクリックします。

6. 「アクション」メニューから「管理者役割を追加」を選択します。

7. セキュリティー管理者役割を作成します。

次の情報を参考にしてください。

- 「役割名」– `secadmin`
- 「役割の正式名」– `Security Administrator`
- 「備考欄」– サイトセキュリティー担当者 (ここには機密情報を入力しない)。
- 「役割の ID 番号」– ≥100
- 「役割シェル」– 管理者の Bourne (プロファイルシェル)
- 「役割メーリングリストを作成」– チェックボックスを選択されたままにしておきます。
- 「Password and confirm」– 6 文字以上の英数字のパスワードを割り当てます。

  セキュリティー管理者役割のパスワードをはじめとするすべてのパスワードは推測されにくいようにしなければなりません。パスワードが推測されて、悪意のある、承認されていないアクセスが行われる危険性を減らします。

  注 – すべての管理役割に対して、アカウントを常に有効にし、パスワード有効期限を設定しないでください。

- 「有効な権利」– 情報セキュリティー、ユーザーセキュリティー
  - サイトセキュリティーで責務分離が不要な場合は、情報セキュリティー権利プロファイルとデフォルトのユーザーセキュリティー権利プロファイルを選択します。
  - サイトセキュリティーで責務分離が必要な場合は、情報セキュリティー権利プロファイルとカスタムユーザーセキュリティー権利プロファイルを選択します。
- 「ホームディレクトリサーバー」– *home-directory-server*
- 「ホームディレクトリパス」– */mount-path*
- 「この役割にユーザーを割り当てます」– 役割をユーザーに割り当てると、このフィールドは自動的に入力されます。

8 役割を作成したら、設定が正しいことを確認します。

役割を選択してダブルクリックします。

次のフィールド内の値を確認します。

- 「有効なグループ」– 必要な場合にグループを追加します。
- 「Trusted Extensions 属性」– デフォルトが正しいです。

  単一ラベルのシステムでラベルを表示してはならない場合は、「ラベル: 表示/非表示」で「非表示」を選択してください。
- 「除外監査クラス/対象監査クラス」– 役割の監査フラグが `audit_control` ファイルのシステム設定に対する例外である場合のみ、監査フラグを設定します。

9 その他の役割を作成するには、セキュリティー管理者役割を参考にします。

例は、『System Administration Guide: Security Services』の「How to Create and Assign a Role by Using the GUI」を参照してください。各役割に一意の ID を指定し、その役割に正しい権利プロファイルを割り当てます。可能な役割は、次のとおりです。

- admin 役割 – `System Administrator` の付与権利
- primaryadmin 役割 – `Primary Administrator` の付与権利
- oper 役割 – `Operator` の付与権利

例 4–6 ローカルのセキュリティー管理者役割を作成するための roleadd コマンドの使用

この例では、root ユーザーが roleadd コマンドを使用して、セキュリティー管理者役割をローカルシステムに追加します。詳細は、roleadd(1M) のマニュアルページを参照してください。役割の作成の前に、root ユーザーは表 1–2 を確認します。このサイトでは、ユーザーを作成するために責務分離は不要です。

```
# roleadd -c "Local Security Administrator" -d /export/home1 \
-u 110 -P "Information Security,User Security" -K lock_after_retries=no \
-K idletime=5 -K idlecmd=lock -K labelview=showsl \
-K min_label=ADMIN_LOW -K clearance=ADMIN_HIGH secadmin
```

root ユーザーは、役割の初期パスワードを指定します。

```
# passwd -r files secadmin
New Password:             <Type password>
Re-enter new Password:    <Retype password>
passwd: password successfully changed for secadmin
#
```

役割をローカルユーザーに割り当てるには、例 4–7 を参照してください。

▼ 制限されたシステム管理者役割を作成する

責務分離がサイトセキュリティー要件でない場合は、この手順を省略します。

この手順では、より制限の厳しい権利プロファイルをシステム管理者役割に割り当てます。

始める前に スーパーユーザーになるか、root 役割または主管理者役割になる必要があります。

94 ページの「責務分離を実施する権利プロファイルを作成する」を完了しています。権利プロファイルを作成するために使用したのと同じツールボックスを使用します。

1. **Solaris** 管理コンソールで、システム管理者役割を作成します。
   詳細は、97 ページの「Trusted Extensions でセキュリティー管理者役割を作成する」を参照してください。
2. カスタムシステム管理者権利プロファイルを役割に割り当てます。
3. 変更を保存します。
4. **Solaris** 管理コンソールを閉じます。

▼ Trusted Extensions で役割になれるユーザーを作成する

ローカルユーザーを作成するには、次の手順の代わりに、例 4–7 のようにコマンド行インタフェースを使用することもできます。サイトのセキュリティーポリシーで許可されるなら、1 人で複数の管理役割になれるようなユーザーを作成することもできます。

セキュリティー保護されたユーザー作成を行うには、システム管理者役割がユーザーを作成し、セキュリティー管理者役割がパスワードなどのセキュリティー関連の属性を割り当てます。

始める前に スーパーユーザーになるか、`root` 役割、セキュリティー管理者役割、または主管理者役割になる必要があります。セキュリティー管理者役割には、ユーザー作成に必要な最低限の権限があります。

Solaris 管理コンソールが表示されます。詳細は、97 ページの「Trusted Extensions でセキュリティー管理者役割を作成する」を参照してください。

1. **Solaris** 管理コンソールで、「ユーザーアカウント」をダブルクリックします。
2. 「アクション」メニューから「ユーザーを追加」→「ウィザードを使用」を選択します。

注意 – 役割およびユーザーの名前と ID は、同じプールが元になります。追加するユーザーに既存の名前や ID を使用しないでください。

3. オンラインヘルプに従います。
   『System Administration Guide: Basic Administration』の「How to Add a User With the Solaris Management Console's Users Tool」の手順に従うこともできます。

4 ユーザーを作成したら、作成したユーザーをダブルクリックして設定を変更します。

注 – 役割になれるユーザーのユーザーアカウントは常に有効にし、パスワード有効期限を設定しないでください。

次のフィールドが正しく設定されていることを確認します。

- 「説明」 – ここには機密情報を入力しません。
- 「Password and confirm」 – 6 文字以上の英数字のパスワードを割り当てます。

注 – 初期設定チームは推測されにくいパスワードを選択しなければなりません。パスワードが推測されて、悪意のある、承認されていないアクセスが行われる危険性を減らします。

- 「アカウントの有効/無効」 – 常に有効です。
- 「Trusted Extensions 属性」 – デフォルトが正しいです。

  単一ラベルのシステムでラベルを表示してはならない場合は、「ラベル: 表示/非表示」で「非表示」を選択してください。
- 「アカウントの使用方法」 – アイドル時間およびアイドルアクションを設定します。

  「アカウントのロック」 – 役割になれるユーザーに対して「いいえ」を設定します。

5 Solaris 管理コンソールを閉じます。

6 ユーザーの環境をカスタマイズします。

a. 簡易認証の割り当て

サイトのセキュリティーポリシーを確認してから、簡易認証権利プロファイルを最初のユーザーに付与できます。このプロファイルによって、ユーザーはデバイスの割り当て、PostScript ファイルの印刷、ラベルなしの印刷、遠隔からのログイン、およびシステムのシャットダウンを行えます。プロファイルを作成するには、『Oracle Solaris Trusted Extensions 管理の手順』の「便利な承認のための権利プロファイルを作成する」を参照してください。

b. ユーザー初期設定ファイルをカスタマイズします。

『Oracle Solaris Trusted Extensions 管理の手順』の第 7 章「Trusted Extensions でのユーザー、権利、役割の管理 (手順)」を参照してください。

『Oracle Solaris Trusted Extensions 管理の手順』の「Solaris 管理コンソールでのユーザーと権利の管理 (作業マップ)」も参照してください。

c. マルチラベルのコピーおよびリンクファイルの作成

マルチラベルシステムで、ほかのラベルにコピーまたはリンクするユーザー初期化ファイルをリストするファイルによって、ユーザーおよび役割を設定できます。詳細は、『Oracle 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。

例 4–7 ローカルユーザーを作成するための useradd コマンドの使用

この例では、root ユーザーが、セキュリティー管理者役割になれるローカルユーザーを作成します。詳細は、useradd(1M) および atohexlabel(1M) のマニュアルページを参照してください。

最初に、root ユーザーは、ユーザーの最下位ラベルおよび認可上限ラベルの 16 進数形式を確認します。

```
# atohexlabel public
0x0002-08-08
# atohexlabel -c "confidential restricted"
0x0004-08-78
```

次に、root ユーザーは表 1–2 を確認してから、ユーザーを作成します。

```
# useradd -c "Local user for Security Admin" -d /export/home1 \
-K  idletime=10 -K idlecmd=logout -K lock_after_retries=no
-K min_label=0x0002-08-08 -K clearance=0x0004-08-78 -K labelview=showsl jandoe
```

root ユーザーは初期パスワードを指定します。

```
# passwd -r files jandoe
New Password:         <Type password>
Re-enter new Password:      <Retype password>
passwd: password successfully changed for jandoe
#
```

最後に、root ユーザーは、セキュリティー管理者役割をユーザーの定義に追加します。役割は、97 ページの「Trusted Extensions でセキュリティー管理者役割を作成する」で作成されました。

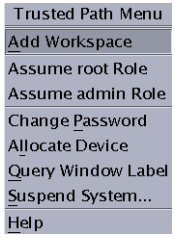
```
# usermod -R secadmin jandoe
```

▼ Trusted Extensions の役割が機能することを確認する

各役割を確認するには、その役割になります。その役割のみが実行できるタスクを実行します。

始める前に　DNS または経路指定を構成してある場合は、役割を作成したら再起動し、そのあとでその役割が機能することを確認してください。

1. 役割ごとに、その役割になれるユーザーとしてログインします。
2. トラステッドパスメニューを開きます。
   - **Trusted CDE** でワークスペーススイッチ領域をクリックします。

     メニューから役割になります。
   - **Trusted JDS** で、トラステッドストライプ内のユーザー名をクリックします。
     次のトラステッドストライプ内では、ユーザー名は `tester` です。

     割り当てられた役割の一覧から、役割を選択します。
3. 役割のワークスペースで、**Solaris** 管理コンソールを起動します。

   ```
   $ /usr/sbin/smc &
   ```
4. テストする役割の適切な範囲を選択します。
5. 「システムの構成」をクリックして、「ユーザー」に移動します。
   パスワードを入力するよう求められます。
   a. 役割のパスワードを入力します。
   b. 「ユーザーアカウント」をダブルクリックします。

6 ユーザーをクリックします。

- システム管理者役割では、「基本」、「ホームディレクトリ」、および「グループ」のタブの各フィールドを変更できます。

  責務分離を実施するための役割を構成した場合、システム管理者役割はユーザーの初期パスワードを設定できません。
- セキュリティー管理者役割では、すべてのタブの各フィールドを変更できます。

  責務分離を実施するための役割を構成した場合、セキュリティー管理者役割はユーザーを作成できません。
- 主管理者役割では、すべてのタブの各フィールドを変更できます。

7 (省略可能) 責務分離を実施する場合、デフォルトの権利プロファイルが使われないようにします。

注 – システムを新しいバージョンの Solaris OS にアップグレードすると、システム管理者、ユーザー管理、ユーザーセキュリティーのデフォルトプロファイルが置き換えられます。

トラステッドエディタで、次のいずれかの手順を実行します。

- **3** つの権利プロファイルを `prof_attr` ファイルから削除します。

  削除により、管理者がこれらのプロファイルを参照または割り当てできなくなります。また、`prof_attr.orig` ファイルも削除します。

- `prof_attr` ファイルの **3** つの権利プロファイルをコメントアウトします。

  権利プロファイルをコメントアウトすることにより、これらのプロファイルが Solaris 管理コンソール で表示されなくなり、ユーザーを管理するコマンドで使用できなくなります。プロファイルとその内容は、引き続き `prof_attr` ファイルで参照できます。

- `prof_attr` ファイルで、**3** つの権利プロファイルに別の説明を入力します。

  `prof_attr` ファイルを編集し、これらの権利プロファイルの説明フィールドを変更します。たとえば、説明を「`Do not use this profile`」に置き換えます。この変更により、管理者にこのプロファイルを使用しないよう警告しますが、プロファイルの使用は禁止されません。

▼ ユーザーがラベル付きゾーンにログインできるようにする

ホストが再起動されると、デバイスと基礎のストレージとの関連付けも再設定されなければなりません。

始める前に　少なくとも 1 つのラベル付きゾーンが作成されています。そのゾーンはクローンを作成中ではありません。

1. システムを再起動します。
2. root ユーザーとしてログインします。
3. ゾーンサービスを再起動します。

```
# svcs zones
STATE          STIME    FMRI
offline        -        svc:/system/zones:default

# svcadm restart svc:/system/zones:default
```

4. ログアウトします。

   これで、一般ユーザーがログインできます。そのセッションはラベル付きゾーンです。

Trusted Extensions でのホームディレクトリの作成

Trusted Extensions では、ユーザーは、ユーザーが作業するすべてのラベルでホームディレクトリにアクセスする必要があります。すべてのホームディレクトリをユーザーに使用可能にするには、マルチレベルのホームディレクトリサーバーを作成し、そのサーバー上でオートマウンタを実行し、ホームディレクトリをエクスポートする必要があります。クライアントサイドでは、ユーザーごとにすべてのゾーンのホームディレクトリを検索するスクリプトを実行したり、ホームディレクトリサーバーにユーザーログインしたりできます。

▼ Trusted Extensions でホームディレクトリサーバーを作成する

始める前に　スーパーユーザーになるか、root 役割または主管理者役割になる必要があります。

1. **Trusted Extensions** ソフトウェアを使用して、ホームディレクトリサーバーをインストールして構成します。
   - ゾーンのクローンを作成する場合、空のホームディレクトリがある Solaris ZFS スナップショットを必ず使用してください。
   - ユーザーはログインできるすべてのラベルのホームディレクトリが必要なので、ユーザーがログインできるすべてのゾーンを作成します。たとえば、デフォルトの label_encodings ファイルを使用する場合、PUBLIC ラベルのゾーンを作成します。

2 **Solaris ZFS** ではなく **UFS** を使用する場合、**NFS** サーバーが自身の機能を果たすようにします。

   a. 大域ゾーンで、`nsswitch.conf` ファイルの `automount` エントリを変更します。
      トラステッドエディタを使って `/etc/nsswitch.conf` ファイルを編集します。手順については、『Oracle Solaris Trusted Extensions 管理の手順』の「Trusted Extensions の管理ファイルを編集する」を参照してください。

      ```
      automount: files
      ```

   b. 大域ゾーンで `automount` コマンドを実行します。

3 ラベル付きゾーンごとに、『**Oracle Solaris Trusted Extensions** 管理の手順』の「ラベル付きゾーンでファイルを **NFS** マウントする」の自動マウント手順に従います。そのあと、この手順に戻ります。

4 ホームディレクトリが作成されていることを確認します。

   a. ホームディレクトリサーバーからログアウトします。

   b. 一般ユーザーとしてホームディレクトリサーバーにログインします。

   c. ログインゾーンで端末を開きます。

   d. 端末ウィンドウで、ユーザーのホームディレクトリが存在することを確認します。

   e. ユーザーが作業できるすべてのゾーンにワークスペースを作成します。

   f. 各ゾーンで端末ウィンドウを開き、ユーザーのホームディレクトリが存在することを確認します。

5 ホームディレクトリサーバーからログアウトします。

▼ Trusted Extensions でユーザーがホームディレクトリにアクセスできるようにする

最初にユーザーはホームディレクトリサーバーにログインして、その他のシステムと共有できるホームディレクトリを作成します。すべてのラベルでホームディレクトリを作成するには、各ユーザーはすべてのラベルでホームディレクトリサーバーにログインする必要があります。

あるいは、管理者は、ユーザーが最初にログインする前に、各ユーザーのホームシステムにホームディレクトリのマウントポイントを作成するスクリプトを作成しておくこともできます。このスクリプトは、ユーザーが作業できるすべてのラベルでマウントポイントを作成します。

始める前に　Trusted Extensions ドメインのホームディレクトリサーバーが構成されました。

- サーバーへの直接ログインを許可するか、スクリプトを実行するかを選択します。
  - ユーザーがホームディレクトリサーバーに直接ログインできるようにします。
    a. 各ユーザーに、ホームディレクトリサーバーにログインするように指示します。
       正常にログインできたユーザーは、ログアウトしてください。
    b. 各ユーザーに、再びログインして、今度は異なるログインラベルを選択するように指示します。
       ユーザーは、ラベルビルダーを使用して異なるログインラベルを選択します。正常にログインできたユーザーは、ログアウトしてください。
    c. 使用できるすべてのラベルに対してログインプロセスを繰り返すよう、各ユーザーに指示します。
    d. 通常のワークステーションからログインするよう、ユーザーに指示します。
       ユーザーのデフォルトラベルのホームディレクトリが使用可能です。ユーザーがセッションのラベルを変更するか、異なるラベルでワークスペースを追加すると、そのラベルのユーザーのホームディレクトリがマウントされます。
  - すべてのユーザーのホームディレクトリマウントポイントを作成するためのスクリプトを作成し、そのスクリプトを実行します。

```
#!/bin/sh
#
for zoneroot in `/usr/sbin/zoneadm list -p | cut -d ":" -f4` ; do
    if [ $zoneroot != / ]; then
        prefix=$zoneroot/root/export

        for j in `getent passwd|tr ' ' _` ; do
            uid=`echo $j|cut -d ":" -f3`
            if [ $uid -ge 100 ]; then
                gid=`echo $j|cut -d ":" -f4`
                homedir=`echo $j|cut -d ":" -f6`
                mkdir -m 711 -p $prefix$homedir
                chown $uid:$gid $prefix$homedir
            fi
        done
```

```
    fi
done
```

a. 大域ゾーンから、**NFS** サーバーでスクリプトを実行します。

b. 次に、ユーザーがログインするすべてのマルチレベルデスクトップでスクリプトを実行します。

既存のトラステッドネットワークへのユーザーとホストの追加

NIS マップで定義されているユーザーがいる場合、そのユーザーをネットワークに追加できます。

ホストおよびラベルをホストに追加するには、次の手順を参照してください。

- ホストを追加するには、Solaris 管理コンソールの 「コンピュータとネットワーク」ツールセットを使用します。詳細は、『Oracle Solaris Trusted Extensions 管理の手順』の「システムの既知のネットワークにホストを追加する」を参照してください。

  ホストを LDAP サーバーに追加するときには、そのホストに関連するすべての IP アドレスを追加します。ラベル付きゾーンのアドレスを含むすべてのゾーンのアドレスを LDAP サーバーに追加しなければなりません。
- ホストにラベルを付けるには、『Oracle Solaris Trusted Extensions 管理の手順』の「セキュリティーテンプレートをホストまたはホストのグループに割り当てる」を参照してください。

▼ LDAP サーバーに NIS ユーザーを追加する

始める前に　スーパーユーザーになるか、`root` 役割または主管理者役割になる必要があります。

1 **NIS** データベースから、必要な情報を収集します。

a. `aliases` データベースのユーザーのエントリからファイルを作成します。

```
% ypcat -k aliases | grep login-name > aliases.name
```

b. `passwd` データベースのユーザーのエントリからファイルを作成します。

```
% ypcat -k passwd | grep "Full Name" > passwd.name
```

c. `auto_home_` データベースのユーザーのエントリからファイルを作成します。

```
% ypcat -k auto_home | grep login-name > auto_home_label
```

2 **LDAP** および **Trusted Extensions** の情報の形式を再設定します。

a. sed コマンドを使用して aliases エントリの形式を再設定します。

```
% sed 's/ /:/g' aliases.login-name > aliases
```

b. nawk コマンドを使用して passwd エントリの形式を再設定します。

```
% nawk -F: '{print $1":x:"$3":"$4":"$5":"$6":"$7}' passwd.name > passwd
```

c. nawk コマンドを使用して shadow エントリを作成します。

```
% nawk -F: '{print $1":"$2":6445::::::"}' passwd.name > shadow
```

d. nawk コマンドを使用して user_attr エントリを作成します。

```
% nawk -F: '{print $1"::::lock_after_retries=yes-or-no;profiles=user-profile, ...;
labelview=int-or-ext,show-or-hide;min_label=min-label;
clearance=max-label;type=normal;roles=role-name,...;
auths=auth-name,..."}' passwd.name > user_attr
```

3 変更したファイルを **LDAP** サーバーの /tmp ディレクトリにコピーします。

```
# cp aliases auto_home_internal passwd shadow user_attr /tmp/name
```

4 手順 **3** のファイルのエントリを **LDAP** サーバーのデータベースに追加します。

```
# /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
-a simple -f /tmp/name/aliases aliases
# /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
-a simple -f /tmp/name/auto_home_internal auto_home_internal
# /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
-a simple -f /tmp/name/passwd passwd
# /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
-a simple -f /tmp/name/shadow shadow
# /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
-a simple -f /tmp/name/user_attr user_attr
```

例 **4–8** NIS データベースから LDAP サーバーへのユーザーの追加

次の例では、管理者が新しいユーザーをトラステッドネットワークに追加します。ユーザーの情報は、最初、NIS データベースに格納されています。LDAP サーバーパスワードを保護するため、管理者はサーバー上で ldapaddent コマンドを実行します。

Trusted Extensions で、新しいユーザーはデバイスを割り当てることができ、オペレータ役割になれます。このユーザーは役割になれるので、そのユーザーアカウントはロックアウトされません。ユーザーの最下位ラベルは PUBLIC です。ユーザーが作業するラベルは INTERNAL なので、jan が auto_home_internal データベースに追加されます。auto_home_internal データベースは、jan の読み取り/書き込みアクセス権のあるホームディレクトリを自動マウントします。

- LDAP サーバーで、管理者は NIS データベースからユーザー情報を取り出します。

```
# ypcat -k aliases | grep jan.doe > aliases.jan
# ypcat passwd | grep "Jan Doe" > passwd.jan
# ypcat -k auto_home | grep jan.doe > auto_home_internal
```

- 次に、管理者は LDAP のエントリの書式を再設定します。

```
# sed 's/ /:/g' aliases.jan > aliases
# nawk -F: '{print $1":x:"$3":"$4":"$5":"$6":"$7}' passwd.jan > passwd
# nawk -F: '{print $1":"$2":6445::::::"}' passwd.jan > shadow
```

- 次に、管理者は Trusted Extensions の `user_attr` エントリを作成します。

```
# nawk -F: '{print $1"::::lock_after_retries=no;profiles=Media User;
labelview=internal,showsl;min_label=0x0002-08-08;
clearance=0x0004-08-78;type=normal;roles=oper;
auths=solaris.device.allocate"}' passwd.jan > user_attr
```

- 次に、管理者はファイルを `/tmp/jan` ディレクトリにコピーします。

```
# cp aliases auto_home_internal passwd shadow user_attr /tmp/jan
```

- 最後に、管理者は `/tmp/jan` ディレクトリのファイルをサーバーに取り込みます。

```
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/aliases aliases
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/auto_home_internal auto_home_internal
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/passwd passwd
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/shadow shadow
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/user_attr user_attr
```

Trusted Extensions の構成のトラブルシューティング

Trusted Extensions では、ラベル付きゾーンが大域ゾーンを使って X サーバーと通信します。したがって、ラベル付きゾーンには大域ゾーンへの使用可能なルートが必要です。また、Solaris のインストール中に選択したオプションによっては、Trusted Extensions が大域ゾーンへのインタフェースを使用できなくなる可能性があります。

Trusted Extensions の有効化後に `netservices limited` が実行された

説明:
ユーザーは、Trusted Extensions の有効化前に `netservices limited` コマンドを実行すべきところを、有効化後にこのコマンドを大域ゾーンで実行しました。そのため、ラベル付きゾーンは大域ゾーン内の X サーバーに接続できません。

回避方法:
次のコマンドを実行して、Trusted Extensions がゾーン間で通信するために必要なサービスを開きます。

```
# svccfg -s x11-server setprop options/tcp_listen = true
# svcadm enable svc:/network/rpc/rstat:default
```

ラベル付きゾーンでコンソールウィンドウが開かない

説明:

ラベル付きゾーンでコンソールウィンドウを開こうとすると、次のようなエラーがダイアログボックスに表示されます。

```
Action:DttermConsole,*,*,*,0 [Error]
Action not authorized.
```

回避方法:

次の 2 行が、`/etc/security/exec_attr` ファイルの各ゾーンエントリに存在することを確認します。

```
All Actions:solaris:act:::*;*;*;*;*:
All:solaris:act:::*;*;*;*;*:
```

これらの行が存在しない場合は、これらのエントリを追加した Trusted Extensions パッケージがラベル付きゾーンにインストールされていません。この場合は、ラベル付きゾーンをもう一度作成してください。手順については、68 ページの「ラベル付きゾーンの作成」を参照してください。

ラベル付きゾーンが X サーバーにアクセスできない

説明:

ラベル付きゾーンが X サーバーにアクセスできない場合は、次のようなメッセージが表示されます。

- `Action failed. Reconnect to Solaris Zone?`
- `No route available`
- `Cannot reach globalzone-`*hostname*`:0`

原因:

ラベル付きゾーンが X サーバーにアクセスできない理由として次のものが考えられます。

- ゾーンが初期化されていないため、`sysidcfg` プロセスの完了を待機している。
- ラベル付きゾーンのホスト名が、大域ゾーンで実行中のネームサービスに認識されない。

- all-zones として指定されているインタフェースがない。
- ラベル付きゾーンのネットワークインタフェースがダウンしている。
- LDAP 名の検索が失敗する。
- NFS マウントが機能しない。

回避に向けての手順:

次の手順を実行してください。

1. ゾーンにログインします。

   zlogin コマンドまたは「ゾーン端末コンソール」アクションを使用できます。

   ```
   # zlogin -z zone-name
   ```

   スーパーユーザーとしてログインできない場合は、zlogin -S コマンドを使用して認証を省略してください。
2. ゾーンが実行中であることを確認します。

   ```
   # zoneadm list
   ```

   ゾーンの状態が running であれば、少なくとも 1 つのプロセスがゾーンで実行されています。
3. ラベル付きゾーンが X サーバーにアクセスするのを妨害しているすべての問題を解決します。
   - sysidcfg プロセスを完了することによってゾーンを初期化します。

     sysidcfg プログラムを対話式で実行します。ゾーン端末コンソール、または zlogin コマンドを実行した端末ウィンドウでプロンプトに答えます。

     sysidcfg プロセスを非対話式に実行するには、次のいずれかの方法があります。

     - /usr/sbin/txzonemgr スクリプトに対して初期化項目を指定します。

       初期化項目により、sysidcfg の質問にデフォルト値を入力できるようになります。
     - 独自の sysidcfg スクリプトを記述します。

       詳細は、sysidcfg(4) のマニュアルページを参照してください。
   - ゾーンから X サーバーにアクセスできることを確認します。

     ラベル付きゾーンにログインします。DISPLAY 変数が X サーバーをポイントするように設定し、ウィンドウを開きます。

     ```
     # DISPLAY=global-zone-hostname:n.n
     # export DISPLAY
     # /usr/openwin/bin/xclock
     ```

ラベル付きウィンドウが表示されない場合は、このラベル付きゾーンに対してゾーンネットワークが適切に構成されていません。

注 – Solaris 10 5/09 以降のリリースの Trusted CDE を実行している場合は、167 ページの「Trusted CDE でローカルゾーンを大域ゾーンルーティングに解決する」を参照してください。

- ネームサービスを使ってゾーンのホスト名を構成します。

  ゾーンのローカル `/etc/hosts` ファイルは使用しません。代わりに、同等の情報を大域ゾーンまたは LDAP サーバーに指定する必要があります。この情報には、ゾーンに割り当てられたホスト名の IP アドレスを含める必要があります。

- `all-zones` として指定されているインタフェースがない。

  すべてのゾーンに大域ゾーンと同じサブネット上の IP アドレスがある場合を除き、`all-zones` (共有) インタフェースを構成する必要のある場合があります。このように構成することによって、ラベル付きゾーンが大域ゾーンの X サーバーに接続できるようになります。大域ゾーンの X サーバーへのリモート接続を制限するには、`vni0` を `all-zones` アドレスとして使用します。

  `all-zones` インタフェースを構成しない場合は、それぞれのゾーンに大域ゾーンの X サーバーへのルートを指定する必要があります。これらのルートは大域ゾーン内で構成しなければなりません。

- ラベル付きゾーンのネットワークインタフェースがダウンしている。

  ```
  # ifconfig -a
  ```

  `ifconfig` コマンドを使用して、ラベル付きゾーンのネットワークインタフェースが `UP` と `RUNNING` の両方の状態であることを確認します。

- LDAP 名の検索が失敗する。

  `ldaplist` コマンドを使用して、各ゾーンが LDAP サーバーまたは LDAP プロキシサーバーと通信できることを確認します。LDAP サーバー上で、ゾーンが `tnrhdb` データベースに記載されていることを確認します。

- NFS マウントが機能しない。

  スーパーユーザーとして、ゾーンで `automount` を再起動します。または、`crontab` エントリを追加して、`automount` コマンドを 5 分ごとに実行します。

その他の Trusted Extensions 構成タスク

次の 2 つのタスクでは、構成ファイルの正確なコピーをサイトのすべての Trusted Extensions システムに転送することができます。最後のタスクでは、Trusted Extensions のカスタマイズを Solaris システムから削除できます。

▼ Trusted Extensions でファイルをポータブルメディアにコピーする方法

ポータブルメディアにコピーする場合、情報と同じ機密ラベルをメディアに付けます。

注 – Trusted Extensions の構成時に、スーパーユーザーまたは同等の役割が管理ファイルをポータブルメディアにコピーしたり、ポータブルメディアからコピーしたりします。このメディアには `Trusted Path` のラベルを付けます。

始める前に　管理ファイルをコピーするには、スーパーユーザーになるか、大域ゾーンで役割になります。

1. 適切なデバイスを割り当てます。

   デバイス割り当てマネージャーを使用し、何も記録されていないメディアを挿入します。詳細は、『Oracle Solaris Trusted Extensions ユーザーズガイド』の「Trusted Extensions でデバイスを割り当てる」を参照してください。

   - Solaris Trusted Extensions (CDE) では、「ファイルマネージャー」にポータブルメディアの内容が表示されます。
   - Solaris Trusted Extensions (JDS) では、「ファイルブラウザ」に内容が表示されます。

   以下の手順では、この GUI を指すのに「ファイルブラウザ」と記述します。

2. 別のファイルブラウザを開きます。

3. コピーするファイルがあるフォルダに移動します。

   たとえば、ファイルを `/export/clientfiles` フォルダにコピーしてあるとします。

4. 各ファイルに対して次の操作を実行します。

   a. ファイルのアイコンを強調表示します。

   b. ポータブルメディアのファイルブラウザにファイルをドラッグします。

5 デバイスの割り当てを解除します。

詳細は、『Oracle Solaris Trusted Extensions ユーザーズガイド』の「Trusted Extensions でデバイスの割り当てを解除する」を参照してください。

6 ポータブルメディアのファイルブラウザで、「ファイル」メニューから「取り出し」を選択します。

注 – コピーしたファイルの機密ラベルを示した物理的なラベルを、メディアに必ず貼り付けてください。

例 4–9 構成ファイルをすべてのシステムで同一にする

システム管理者は、同じ設定ですべてのマシンを確実に構成しようと思っています。そのためには、最初に構成するマシンで、再起動によって削除されないディレクトリを作成します。そのディレクトリに、管理者はすべてのシステムで同一のファイルまたはほとんど同じファイルを配置します。

たとえば、LDAP スコープ用に Solaris 管理コンソール が使用する Trusted Extensions ツールボックス `/var/sadm/smc/toolboxes/tsol_ldap/tsol_ldap.tbx` をコピーします。`tnrhtp` ファイルの遠隔ホストテンプレートをカスタマイズしてあり、DNS サーバーのリストおよび監査構成ファイルがあります。サイト向けに `policy.conf` ファイルも変更しました。これらのファイルを永続ディレクトリにコピーします。

```
# mkdir /export/commonfiles
# cp  /etc/security/policy.conf \
/etc/security/audit_control \
/etc/security/audit_startup \
/etc/security/tsol/tnrhtp \
/etc/resolv.conf \
/etc/nsswitch.conf \
/export/commonfiles
```

デバイス割り当てマネージャーを使用して大域ゾーンでフロッピーディスクを割り当て、ファイルをフロッピーディスクに転送します。`ADMIN_HIGH` のラベルを付けた別のフロッピーディスクに、サイト用の `label_encodings` ファイルを転送します。

システムにファイルをコピーする場合、システムの `/etc/security/audit_control` ファイルの `dir:` のエントリを変更します。

▼ Trusted Extensions でポータブルメディアからファイルをコピーする方法

ファイルを置き換える前に、元の Trusted Extensions ファイルの名前を変更しておくと安全です。システムを構成する際に、`root` 役割が管理ファイルの名前の変更およびコピーを行います。

始める前に　管理ファイルをコピーするには、スーパーユーザーになるか、大域ゾーンで役割になります。

1. 適切なデバイスを割り当てます。
   詳細は、『Oracle Solaris Trusted Extensions ユーザーズガイド』の「Trusted Extensions でデバイスを割り当てる」を参照してください。
   - Solaris Trusted Extensions (CDE) では、「ファイルマネージャー」にポータブルメディアの内容が表示されます。
   - Solaris Trusted Extensions (JDS) では、「ファイルブラウザ」に内容が表示されます。

   以下の手順では、この GUI を指すのに「ファイルブラウザ」と記述します。
2. 管理ファイルを含むメディアを挿入します。
3. システムに同じ名前のファイルがある場合、元のファイルを新しい名前でコピーします。
   たとえば、元のファイルの名前の後ろに `.orig` を追加します。
   ```
   # cp /etc/security/tsol/tnrhtp /etc/security/tsol/tnrhtp.orig
   ```
4. ファイルブラウザを開きます。
5. `/etc/security/tsol` などのコピー先ディレクトリに移動します。
6. コピーするそれぞれのファイルに対して、次の操作を実行します。
   a. マウントされたメディアのファイルブラウザで、ファイルのアイコンを強調表示します。
   b. 別のファイルブラウザのコピー先ディレクトリにファイルをドラッグします。
7. デバイスの割り当てを解除します。
   詳細は、『Oracle Solaris Trusted Extensions ユーザーズガイド』の「Trusted Extensions でデバイスの割り当てを解除する」を参照してください。
8. プロンプトが表示されたら、メディアを取り出します。

例 4–10 Trusted Extensions で監査構成ファイルを読み込む

この例では、システムにまだ役割が構成されていません。`root` ユーザーは、構成ファイルをポータブルメディアにコピーする必要があります。メディアの内容は、その他のシステムにコピーされます。これらのファイルは、Trusted Extensions ソフトウェアで構成される各システムにコピーされることになります。

root ユーザーは、デバイス割り当てマネージャーで floppy_0 デバイスを割り当てて、マウントのクエリーに対して yes と答えます。次に、root ユーザーは、構成ファイルが含まれたフロッピーディスクを挿入し、ディスクにコピーします。このフロッピーディスクには、Trusted Path というラベルが付けられています。

メディアから読み込むには、root ユーザーが受信ホストのデバイスを割り当てて、内容をダウンロードします。

構成ファイルがテープ上にある場合、root ユーザーは mag_0 デバイスを割り当てます。構成ファイルが CD-ROM 上にある場合、root ユーザーは cdrom_0 デバイスを割り当てます。

▼ Trusted Extensions をシステムから削除する

Trusted Extensions を Solaris システムから削除するには、特定の手順を実行して、Solaris システムに対する Trusted Extensions のカスタマイズを削除します。

1. **Solaris OS** の場合と同様に、ラベル付きゾーンのデータで残しておくものを保存します。

2. システムからラベル付きゾーンを削除します。
   詳細は、『System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones』の「How to Remove a Non-Global Zone」を参照してください。

3. **Trusted Extensions** サービスを無効化します。

   ```
   # svcadm disable labeld
   ```

4. bsmunconv コマンドを実行します。
   このコマンドの結果については、bsmunconv(1M) のマニュアルページを参照してください。

5. **(省略可能)** システムを再起動します。

6. システムを構成します。
   さまざまなサービスを Solaris システム用に構成する必要があります。その候補として、監査、基本的なネットワーキング、ネームサービス、およびファイルシステムのマウントがあります。

◆ ◆ ◆ 第 5 章

Trusted Extensions のための LDAP の構成 (手順)

この章では、Trusted Extensions で使用するために Sun Java System Directory Server および Solaris 管理コンソールを構成する方法について説明します。Directory Server は LDAP サービスを提供します。LDAP は、Trusted Extensions の対応ネームサービスです。Solaris 管理コンソールは、ローカルおよび LDAP データベースの管理 GUI です。

Directory Server の構成には、2 つの選択肢があります。Trusted Extensions システムに LDAP サーバーを構成するか、Trusted Extensions プロキシサーバーを使用して既存のサーバーに接続します。次の作業マップのいずれかの手順に従ってください。

- 119 ページの「Trusted Extensions ホストでの LDAP サーバーの構成 (作業マップ)」
- 120 ページの「Trusted Extensions ホストでの LDAP プロキシサーバーの構成 (作業マップ)」

Trusted Extensions ホストでの LDAP サーバーの構成 (作業マップ)

作業	説明	参照先
Trusted Extensions LDAP サーバーを設定します。	既存の Sun Java System Directory Server がない場合、最初の Trusted Extensions システムを Directory Server にします。このシステムにラベル付きゾーンはインストールされていません。 その他の Trusted Extensions システムは、このサーバーのクライアントになります。	121 ページの「LDAP 用に Directory Server の情報を収集する」 122 ページの「Sun Java System Directory Server をインストールする」 127 ページの「Sun Java System Directory Server のログを構成する」
Trusted Extensions データベースをサーバーに追加します。	Trusted Extensions システムファイルのデータを LDAP サーバーに入力します。	129 ページの「Sun Java System Directory Server にデータを入力する」

作業	説明	参照先
Solaris 管理コンソールが Directory Server で機能するように構成します。	Solaris 管理コンソールの LDAP ツールボックスを手動で設定します。このツールボックスを使用して、ネットワークオブジェクトに関する Trusted Extensions 属性を変更できます。	132 ページの「LDAP のための Solaris 管理コンソールの設定 (作業マップ)」
その他のすべての Trusted Extensions システムを、このサーバーのクライアントとして構成します。	別のシステムに Trusted Extensions を構成する場合、そのシステムをこの LDAP サーバーのクライアントにします。	65 ページの「Trusted Extensions で大域ゾーンを LDAP クライアントにする」

Trusted Extensions ホストでの LDAP プロキシサーバーの構成 (作業マップ)

Solaris システムで実行されている既存の Sun Java System Directory Server がある場合、この作業マップを使用します。

作業	説明	参照先
Trusted Extensions データベースをサーバーに追加します。	Trusted Extensions ネットワークデータベースの `tnrhdb` および `tnrhtp` は、LDAP サーバーに追加する必要があります。	129 ページの「Sun Java System Directory Server にデータを入力する」
LDAP プロキシサーバーを設定します。	1 つの Trusted Extensions システムをその他の Trusted Extensions システムのプロキシサーバーにします。その他の Trusted Extensions システムは、このプロキシサーバーを使用して LDAP サーバーにアクセスします。	132 ページの「LDAP プロキシサーバーを作成する」
プロキシサーバーに LDAP 用のマルチレベルポートを構成します。	Trusted Extensions プロキシサーバーが特定ラベルで LDAP サーバーと通信できるようにします。	128 ページの「Sun Java System Directory Server のマルチレベルポートを設定する」
Solaris 管理コンソールが LDAP プロキシサーバーで機能するように構成します。	Solaris 管理コンソールの LDAP ツールボックスを手動で設定します。このツールボックスを使用して、ネットワークオブジェクトに関する Trusted Extensions 属性を変更できます。	132 ページの「LDAP のための Solaris 管理コンソールの設定 (作業マップ)」
その他のすべての Trusted Extensions システムを LDAP プロキシサーバーのクライアントとして構成します。	別のシステムに Trusted Extensions を構成する場合、そのシステムを LDAP プロキシサーバーのクライアントにします。	65 ページの「Trusted Extensions で大域ゾーンを LDAP クライアントにする」

Trusted Extensions システムでの Sun Java System Directory Server の構成

LDAP ネームサービスは、Trusted Extensions の対応ネームサービスです。サイトで LDAP ネームサービスがまだ実行されていない場合、Trusted Extensions が構成されているシステムで Sun Java System Directory Server (Directory Server) を構成します。

サイトですでに Directory Server が実行されている場合、Trusted Extensions データベースをサーバーに追加する必要があります。Directory Server にアクセスするために、Trusted Extensions システムで LDAP プロキシを設定します。

注 – この LDAP サーバーを NFS サーバーまたは Sun Ray クライアント用のサーバーとして使用しない場合は、このサーバーにラベル付きゾーンをインストールする必要はありません。

▼ LDAP 用に Directory Server の情報を収集する

- 次の項目の値を決定します。

  各項目は、Sun Java Enterprise System のインストールウィザードに表示される順序で記載されています。

インストールウィザードのプロンプト	対応または情報
Sun Java System Directory Server *version*	
「管理者ユーザー ID」	デフォルト値は「`admin`」です。
「管理者ユーザーパスワード」	「`admin123`」のようなパスワードを作成します。
「ディレクトリマネージャ DN」	デフォルト値は「`cn=Directory Manager`」です。
「ディレクトリマネージャパスワード」	「`dirmgr89`」のようなパスワードを作成します。
「Directory Server ルート」	デフォルト値は「`/var/opt/mps/serverroot`」です。プロキシソフトウェアをインストールする場合、このパスはあとでも使用されます。
「サーバー識別子」	デフォルト値はローカルシステムです。

インストールウィザードのプロンプト	対応または情報
「サーバーポート」	Directory Server を使用して標準的な LDAP ネームサービスをクライアントシステムに提供する場合は、デフォルト値「389」を使用します。 Directory Server を使用してプロキシサーバーの今後のインストールをサポートする場合は、「10389」など標準以外のポートを入力します。
「サフィックス」	「dc=example-domain,dc=com」のように、ドメイン構成要素を含めます。
「管理ドメイン」	「example-domain.com」のように、サフィックスに対応させて作成します。
「システムユーザー」	デフォルト値は「root」です。
「システムグループ」	デフォルト値は「root」です。
「データの保存場所」	デフォルト値は「このサーバーに設定データを保存します。」です。
「データの保存場所」	デフォルト値は「このサーバーにユーザー/グループデータを保存します。」です。
「Administration Port」	デフォルト値はサーバーポートです。デフォルトを変更するために推奨される慣例は、ソフトウェアバージョンに 1000 を掛けた数値です。ソフトウェアバージョン 5.2 の場合、この慣例ではポート 5200 になります。

▼ Sun Java System Directory Server をインストールする

Directory Server パッケージは、Sun Software Gateway web site (http://www.oracle.com/solaris)から入手できます。

始める前に　大域ゾーンが 1 つだけインストールされた Trusted Extensions システムで作業しているとします。システムにラベル付きゾーンはありません。

Trusted Extensions LDAP サーバーは、pam_unix を使用して LDAP リポジトリに対する認証を行うクライアントのために構成されています。pam_unix を使用する場合、パスワード操作と、その結果としてのパスワードポリシーは、クライアントによって決定されます。すなわち、LDAP サーバーによって設定されたポリシーは使用されません。クライアントで設定できるパスワードパラメータについては、『Solaris のシステム管理 (セキュリティサービス)』の「パスワード情報の管理」を参照してください。pam_unix の詳細については、pam.conf(4) のマニュアルページを参照してください。

注 – LDAP クライアントで pam_ldap を使用する構成は、Trusted Extensions では評価されていません。

1 **Directory Server** パッケージをインストールする前に、システムのホスト名エントリに **FQDN** を追加します。

FQDN とは「完全指定のドメイン名 (Fully Qualified Domain Name)」のことです。この名前は、次のようにホスト名と管理ドメインの組み合わせになります。

```
## /etc/hosts
...
192.168.5.5 myhost myhost.example-domain.com
```

Solaris 10 8/07 リリースより前のリリースを実行しているシステムでは、/etc/inet/ipnodes ファイルに IPv4 と IPv6 のエントリを追加します。次のように、1 つのシステムのエントリは連続してそのファイルに入力します。

実行しているのが Solaris OS の最新リリースではない場合、以下のパッチがインストールされている必要があります。最初の番号は SPARC のパッチです。次の番号は X86 のパッチです。

- 138874–05、138875–05: ネイティブ LDAP、PAM、name-service-switch パッチ
- 119313-35、119314-36: WBEM パッチ
- 121308-21、121308-21: Solaris 管理コンソールパッチ
- 119315-20、119316-20: Solaris 管理アプリケーションパッチ

2 **Oracle Sun Web** サイトで **Sun Java System Directory Server** パッケージを検索します。

a. **Sun Software Gateway (**http://www.oracle.com/solaris**)** のページで、「**Get It**」タブをクリックします。

b. 「**Sun Java Identity Management Suite**」の前のチェックボックスをクリックします。

c. 「**Submit**」ボタンをクリックします。

d. 登録していない場合は、登録します。

e. ログインしてこのソフトウェアをダウンロードします。

f. 画面左上の「**Download Center**」をクリックします。

g. 「**Identity Management**」領域で、使用しているプラットフォームに適切な最新のソフトウェアをダウンロードします。

3 **Directory Server** パッケージをインストールします。

121 ページの「LDAP 用に Directory Server の情報を収集する」からの情報を使って質問に答えます。質問、デフォルト値、推奨される回答の詳細な一覧については、『Solaris のシステム管理 (ネーミングとディレクトリサービス : DNS、NIS、LDAP 編)』の第 11 章「LDAP クライアントと Sun Java System Directory Server の設定 (手順)」と『Solaris のシステム管理 (ネーミングとディレクトリサービス : DNS、NIS、LDAP 編)』の第 12 章「LDAP クライアントの設定 (手順)」を参照してください。

4 (省略可能) 自身のパスに **Directory Server** の環境変数を追加します。

```
# $PATH
/usr/sbin:.../opt/SUNWdsee/dsee6/bin:/opt/SUNWdsee/dscc6/bin:/opt/SUNWdsee/ds6/bin:
/opt/SUNWdsee/dps6/bin
```

5 (省略可能) MANPATH に **Directory Server** のマニュアルページを追加します。

```
/opt/SUNWdsee/dsee6/man
```

6 cacaoadm プログラムを有効にして、プログラムが有効になったことを確認します。

```
# /usr/sbin/cacaoadm enable
# /usr/sbin/cacaoadm start
start: server (pid n) already running
```

7 起動するたびに **Directory Server** も起動されるようにします。

Directory Server 用の SMF サービスのテンプレートが、Sun Java System Directory Server パッケージ内に含まれています。

- **Trusted Extensions Directory Server** で、サービスを有効にします。

  ```
  # dsadm stop /export/home/ds/instances/your-instance
  # dsadm enable-service -T SMF /export/home/ds/instances/your-instance
  # dsadm start /export/home/ds/instances/your-instance
  ```

  dsadm コマンドについては、dsadm(1M) のマニュアルページを参照してください。

- プロキシ **Directory Server** で、サービスを有効にします。

  ```
  # dpadm stop /export/home/ds/instances/your-instance
  # dpadm enable-service -T SMF /export/home/ds/instances/your-instance
  # dpadm start /export/home/ds/instances/your-instance
  ```

  dpadm コマンドについては、dpadm(1M) のマニュアルページを参照してください。

8 インストールを確認します。

```
# dsadm info /export/home/ds/instances/your-instance
Instance Path:          /export/home/ds/instances/your-instance
Owner:                  root(root)
Non-secure port:        389
Secure port:            636
Bit format:             32-bit
State:                  Running
```

```
Server PID:             298
DSCC url:               -
SMF application name:   ds--export-home-ds-instances-your-instance
Instance version:       D-A00
```

注意事項　LDAP 構成の問題解決のストラテジについては、『System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)』の第 13 章「LDAP Troubleshooting (Reference)」を参照してください。

▼ Directory Server 用の LDAP クライアントの作成

このクライアントを使用して、LDAP 用の Directory Server にデータを入力します。このタスクは、Directory Server にデータを入力する前に実行する必要があります。

一時的に Trusted Extensions Directory Server 上にクライアントを作成してからサーバー上のクライアントを移動することも、独立したクライアントを作成することもできます。

1 システムに **Trusted Extensions** をインストールします。

Trusted Extensions Directory Server を使用することも、別個のシステムに Trusted Extensions をインストールすることもできます。

注 – 実行しているのが Solaris OS の最新リリースではない場合、以下のパッチがインストールされている必要があります。最初の番号は SPARC のパッチです。次の番号は X86 のパッチです。

- 138874–05、138875–05: ネイティブ LDAP、PAM、name-service-switch パッチ
- 119313-35、119314-36: WBEM パッチ
- 121308-21、121308-21: Solaris 管理コンソールパッチ
- 119315-20、119316-20: Solaris 管理アプリケーションパッチ

---

2 クライアントで、デフォルトの `/etc/nsswitch.ldap` ファイルを変更します。

太字のエントリは、変更部分を示しています。ファイルは次のようになります。

```
# /etc/nsswitch.ldap
#
# An example file that could be copied over to /etc/nsswitch.conf; it
# uses LDAP in conjunction with files.
#
# "hosts:" and "services:" in this file are used only if the
# /etc/netconfig file has a "-" for nametoaddr_libs of "inet" transports.

# LDAP service requires that svc:/network/ldap/client:default be enabled
# and online.

# the following two lines obviate the "+" entry in /etc/passwd and /etc/group.
passwd:     files ldap
```

```
group:      files ldap

# consult /etc "files" only if ldap is down.
hosts:      files ldap dns [NOTFOUND=return] files

# Note that IPv4 addresses are searched for in all of the ipnodes databases
# before searching the hosts databases.
ipnodes:    files ldap [NOTFOUND=return] files

networks:   files ldap [NOTFOUND=return] files
protocols:  files ldap [NOTFOUND=return] files
rpc:        files ldap [NOTFOUND=return] files
ethers:     files ldap [NOTFOUND=return] files
netmasks:   files ldap [NOTFOUND=return] files
bootparams: files ldap [NOTFOUND=return] files
publickey:  files ldap [NOTFOUND=return] files

netgroup:   ldap

automount:  files ldap
aliases:    files ldap

# for efficient getservbyname() avoid ldap
services:   files ldap

printers:   user files ldap

auth_attr:  files ldap
prof_attr:  files ldap

project:    files ldap

tnrhtp:     files ldap
tnrhdb:     files ldap
```

3 大域ゾーンで ldapclient init コマンドを実行します。

このコマンドは、nsswitch.ldap ファイルを nsswitch.conf ファイルにコピーします。

この例では、LDAP クライアントは example-domain.com ドメイン内にあります。サーバーの IP アドレスは 192.168.5.5 です。

```
# ldapclient init -a domainName=example-domain.com -a profileNmae=default \
> -a proxyDN=cn=proxyagent,ou=profile,dc=example-domain,dc=com \
> -a proxyDN=cn=proxyPassword={NS1}ecc423aad0 192.168.5.5
System successfully configured
```

4 サーバーの enableShadowUpdate パラメータに TRUE を設定します。

```
# ldapclient -v mod -a enableShadowUpdate=TRUE \
> -a adminDN=cn=admin,ou=profile,dc=example-domain,dc=com
System successfully configured
```

enableShadowUpdate パラメータについては、『Solaris のシステム管理 (ネーミングとディレクトリサービス : DNS、NIS、LDAP 編)』の「enableShadowUpdate スイッチ」と、ldapclient(1M) のマニュアルページを参照してください。

▼ Sun Java System Directory Server のログを構成する

この手順では次の 3 種類のログを構成します。 アクセスログ、監査ログ、およびエラーログです。次のデフォルト設定は変更されません。

- すべてのログが有効化およびバッファリングされます。
- 各ログは対応する `/export/home/ds/instances/`*your-instance*`/logs/`*LOG_TYPE* ディレクトリ内に配置されます。
- イベントはログレベル 256 でロギングされます。
- ログは `600` ファイルアクセス権で保護されます。
- アクセスログは毎日ローテーションされます。
- エラーログは毎週ローテーションされます。

この手順の設定は次の要件を満たします。

- 監査ログは毎日ローテーションされます。
- 3 か月よりも古いログファイルは期限切れになります。
- すべてのログファイルで最大 20,000M バイトのディスク容量を使用します。
- 各ファイル最大 500M バイトの、最大 100 のログファイルが保持されます。
- ディスク容量の空きが 500M バイトを下回ると古いログから削除されます。
- エラーログでは追加情報が収集されます。

1 アクセスログを構成します。

アクセスの *LOG_TYPE* は `ACCESS` です。ログを構成するための構文は、次のとおりです。

`dsconf set-log-prop` *LOG_TYPE property*:*value*

```
# dsconf set-log-prop ACCESS max-age:3M
# dsconf set-log-prop ACCESS max-disk-space-size:20000M
# dsconf set-log-prop ACCESS max-file-count:100
# dsconf set-log-prop ACCESS max-size:500M
# dsconf set-log-prop ACCESS min-free-disk-space:500M
```

2 監査ログを構成します。

```
# dsconf set-log-prop AUDIT max-age:3M
# dsconf set-log-prop AUDIT max-disk-space-size:20000M
# dsconf set-log-prop AUDIT max-file-count:100
# dsconf set-log-prop AUDIT max-size:500M
# dsconf set-log-prop AUDIT min-free-disk-space:500M
# dsconf set-log-prop AUDIT rotation-interval:1d
```

監査ログのローテーション間隔は、デフォルトで 1 週間です。

3 エラーログを構成します。

この構成では、エラーログで追加データが収集されるように指定します。

```
# dsconf set-log-prop ERROR max-age:3M
# dsconf set-log-prop ERROR max-disk-space-size:20000M
```

```
# dsconf set-log-prop ERROR max-file-count:30
# dsconf set-log-prop ERROR max-size:500M
# dsconf set-log-prop ERROR min-free-disk-space:500M
# dsconf set-log-prop ERROR verbose-enabled:on
```

4 **(省略可能) さらにログを構成します。**

ログごとに次の設定を行うことも可能です。

```
# dsconf set-log-prop LOG_TYPE rotation-min-file-size:undefined
# dsconf set-log-prop LOG_TYPE rotation-time:undefined
```

`dsconf` コマンドについては、`dsconf(1M)` のマニュアルページを参照してください。

▼ Sun Java System Directory Server のマルチレベルポートを設定する

Trusted Extensions で作業するには、Directory Server のサーバーポートを大域ゾーンのマルチレベルポート (MLP) として設定する必要があります。

1 **Solaris 管理コンソールを起動します。**

```
# /usr/sbin/smc &
```

2 **このコンピュータ (*this-host*: `Scope=Files, Policy=TSOL`) ツールボックスを選択します。**

3 **「システムの構成」をクリックしてから「コンピュータとネットワーク」をクリックします。**

パスワードを入力するよう求められます。

4 **適切なパスワードを入力します。**

5 **「トラステッドネットワークゾーン」をダブルクリックします。**

6 **大域ゾーンをダブルクリックします。**

7 **TCP プロトコルのマルチレベルポートを追加します。**

a. **「ゾーンの IP アドレスに対するマルチレベルポートの追加」をクリックします。**

b. **ポート番号として 389 と入力し、「了解」をクリックします。**

8 **UDP プロトコルのマルチレベルポートを追加します。**

a. **「ゾーンの IP アドレスに対するマルチレベルポートの追加」をクリックします。**

b. ポート番号として **389** と入力します。

c. **udp** プロトコルを選択して、「了解」をクリックします。

9 「了解」をクリックして設定を保存します。

10 カーネルを更新します。

```
# tnctl -fz /etc/security/tsol/tnzonecfg
```

▼ Sun Java System Directory Server にデータを入力する

ラベル構成、ユーザー、および遠隔システムに関する Trusted Extensions データを保持するために、複数の LDAP データベースが作成および変更されています。この手順では、Directory Server データベースに Trusted Extensions 情報を取り込みます。

始める前に シャドウ更新が有効になっている LDAP クライアントからデータベースにデータを入力する必要があります。前提条件については、125 ページの「Directory Server 用の LDAP クライアントの作成」を参照してください。

サイトセキュリティーで責務分離が必要な場合は、ディレクトリサーバーにデータを設定する前に、次の手順を実行します。

- 94 ページの「責務分離を実施する権利プロファイルを作成する」
- 97 ページの「Trusted Extensions でセキュリティー管理者役割を作成する」
- 99 ページの「制限されたシステム管理者役割を作成する」

1 ネームサービスデータベースにデータを入力するために使用するファイルのステージング領域を作成します。

```
# mkdir -p /setup/files
```

2 サンプルの /etc ファイルをステージング領域にコピーします。

```
# cd /etc
# cp aliases group networks netmasks protocols /setup/files
# cp rpc services auto_master /setup/files

# cd /etc/security
# cp auth_attr prof_attr exec_attr /setup/files/
#
# cd /etc/security/tsol
# cp tnrhdb tnrhtp /setup/files
```

Solaris 10 11/06 リリースをパッチを適用しないで実行している場合、ipnodes ファイルをコピーします。

```
# cd /etc/inet
# cp ipnodes /setup/files
```

3 /setup/files/auto_master ファイルから +auto_master エントリを削除します。

4 ?:::::? エントリを /setup/files/auth_attr ファイルから削除します。

5 /setup/files/prof_attr ファイルから :::: エントリを削除します。

6 ステージング領域にゾーン自動マップを作成します。

次の自動マップのリストで、各ペアの最初の行はファイルの名前を示します。2 行めはファイルの内容を示します。ゾーン名は、Trusted Extensions ソフトウェアに含まれているデフォルトの label_encodings ファイルからのラベルを特定します。

- ここに示された行のゾーン名を実際のゾーン名に置き換えてください。
- *myNFSserver* でホームディレクトリの NFS サーバーを特定します。

```
/setup/files/auto_home_public
 * myNFSserver_FQDN:/zone/public/root/export/home/&

/setup/files/auto_home_internal
 * myNFSserver_FQDN:/zone/internal/root/export/home/&

/setup/files/auto_home_needtoknow
 * myNFSserver_FQDN:/zone/needtoknow/root/export/home/&

/setup/files/auto_home_restricted
 * myNFSserver_FQDN:/zone/restricted/root/export/home/&
```

7 ネットワーク上のすべてのシステムを /setup/files/tnrhdb ファイルに追加します。

ここではワイルドカードは使用できません。通信を行うすべてのシステムの IP アドレスは、ラベル付きゾーンの IP アドレスも含めてこのファイル内に存在する必要があります。

a. トラステッドエディタを開き、/setup/files/tnrhdb を編集します。

b. **Trusted Extensions** ドメインのラベル付きシステムのすべての **IP** アドレスを追加します。

ラベル付きシステムのタイプは cipso です。また、ラベル付きシステムのセキュリティーテンプレートの名前も cipso です。したがって、デフォルト構成では cipso エントリは次のようになります。

```
192.168.25.2:cipso
```

注 – このリストには、大域ゾーンおよびラベル付きゾーンの IP アドレスが含まれます。

c. ドメインが通信できるラベルなしシステムをすべて追加します。

ラベルなしシステムのタイプは `unlabeled` です。ラベルなしシステムのセキュリティーテンプレートの名前は `admin_low` です。したがって、デフォルト構成ではラベルなしシステムのエントリは次のようになります。

```
192.168.35.2:admin_low
```

d. ファイルを保存し、エディタを終了します。

e. ファイルの構文を検査します。

```
# tnchkdb -h /setup/files/tnrhdb
```

f. エラーを修正してから作業を続行します。

8 `/setup/files/tnrhdb` ファイルを `/etc/security/tsol/tnrhdb` ファイルにコピーします。

9 `ldapaddent` コマンドを使用して、ステージング領域のすべてのファイルを利用して **Directory Server** にデータを入力します。

たとえば、次のコマンドでは、ステージング領域の `hosts` ファイルからサーバーにデータが入力されます。

```
# /usr/sbin/ldapaddent -D "cn=directory manager" \
-w dirmgr123 -a simple -f /setup/files/hosts hosts
```

10 **Trusted Extensions Directory Server** で `ldapclient` コマンドを実行する場合は、システム上のクライアントを無効にします。

大域ゾーンで `ldapclient uninit` コマンドを実行します。詳細出力を使用して、そのシステムが LDAP クライアントではなくなっていることを確認します。

```
# ldapclient -v uninit
```

詳細については、`ldapclient(1M)` のマニュアルページを参照してください。

既存の Sun Java System Directory Server のための Trusted Extensions プロキシの作成

最初に、Solaris システムの既存の Directory Server に Trusted Extensions データベースを追加する必要があります。次に、Trusted Extensions システムが Directory Server にアクセスできるように、Trusted Extensions システムが LDAP プロキシサーバーになるよう構成する必要があります。

▼ LDAP プロキシサーバーを作成する

サイトに LDAP サーバーがすでに存在する場合、Trusted Extensions システムにプロキシサーバーを作成します。

始める前に　`enableShadowUpdate` パラメータに `TRUE` を設定するように変更したクライアントから、LDAP サーバーにデータを入力しました。要件については、125 ページの「Directory Server 用の LDAP クライアントの作成」を参照してください。

また、`enableShadowUpdate` パラメータに `TRUE` を設定したクライアントから、Trusted Extensions の情報を含むデータベースを LDAP サーバーに追加しました。詳細は、129 ページの「Sun Java System Directory Server にデータを入力する」を参照してください。

1. **Trusted Extensions が設定されているシステムで、プロキシサーバーを作成します。**

   注 – 2 つの `ldapclient` コマンドを実行する必要があります。`ldapclient init` コマンドを実行したら、`ldapclient modify` コマンドを実行して、`enableShadowUpdate` パラメータに `TRUE` を設定します。

   詳細は、『Solaris のシステム管理 (ネーミングとディレクトリサービス : DNS、NIS、LDAP 編)』の第 12 章「LDAP クライアントの設定 (手順)」を参照してください。

2. **Trusted Extensions データベースがプロキシサーバーで表示できることを確認します。**

   ```
   # ldaplist -l database
   ```

注意事項　LDAP 構成の問題解決のストラテジについては、『System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)』の第 13 章「LDAP Troubleshooting (Reference)」を参照してください。

LDAP のための Solaris 管理コンソールの設定 (作業マップ)

Solaris 管理コンソールは、Trusted Extensions を実行しているシステムのネットワークを管理するための GUI です。

作業	説明	参照先
Solaris 管理コンソールを初期化します。	Solaris 管理コンソールを初期化します。この手順は、大域ゾーンのシステムごとに 1 回実行します。	61 ページの「Trusted Extensions で Solaris 管理コンソールサーバーを初期化する」

作業	説明	参照先
資格を登録します	LDAP サーバーによって Solaris 管理コンソールを認証します。	133 ページの「LDAP の資格を Solaris 管理コンソールに登録する」
システムで遠隔管理を有効にします。	デフォルトでは、Solaris 管理コンソール クライアントは別のシステムにあるコンソールサーバーと通信できません。明示的に遠隔管理を有効にしてください。	134 ページの「Solaris 管理コンソールでのネットワーク接続の受け付けを有効にする」
LDAP ツールボックスを作成します	Trusted Extensions 用の Solaris 管理コンソールに LDAP ツールボックスを作成します。	135 ページの「Solaris 管理コンソールの LDAP ツールボックスを編集する」
通信を確認します。	Trusted Extensions ホストが LDAP クライアントになれることを確認します。	136 ページの「Solaris 管理コンソールに Trusted Extensions 情報が含まれていることを確認する」

▼ LDAP の資格を Solaris 管理コンソールに登録する

始める前に　Trusted Extensions を実行している LDAP サーバーで `root` ユーザーになります。このサーバーはプロキシサーバーでもかまいません。

Sun Java System Directory Server が構成されている必要があります。次のいずれかの構成を完了しています。

- 119 ページの「Trusted Extensions ホストでの LDAP サーバーの構成 (作業マップ)」
- 120 ページの「Trusted Extensions ホストでの LDAP プロキシサーバーの構成 (作業マップ)」

1. **LDAP 管理資格を登録します。**

```
LDAP-Server # /usr/sadm/bin/dtsetup storeCred
Administrator DN:       Type the value for cn on your system
Password:       Type the Directory Manager password
Password (confirm):       Retype the password
```

2. ディレクトリサーバー上のスコープを一覧表示します。

```
LDAP-Server # /usr/sadm/bin/dtsetup scopes
Getting list of manageable scopes...
Scope 1 file:       Displays name of file scope
Scope 2 ldap:       Displays name of ldap scope
```

サーバー設定によって、表示される LDAP スコープが決定されます。LDAP スコープは、LDAP ツールボックスを編集するまで一覧表示されません。ツールボックスは、サーバーを登録するまで編集できません。

例 5–1 LDAP 資格の登録

この例で、LDAP サーバーの名前は LDAP1 であり、cn の値はデフォルトの Directory Manager です。

```
# /usr/sadm/bin/dtsetup storeCred
Administrator DN:cn=Directory Manager
Password:abcde1;!
Password (confirm):abcde1;!
# /usr/sadm/bin/dtsetup scopes
Getting list of manageable scopes...
Scope 1 file:/LDAP1/LDAP1
Scope 2 ldap:/LDAP1/cd=LDAP1,dc=example-domain,dc=com
```

▼ Solaris 管理コンソールでのネットワーク接続の受け付けを有効にする

デフォルトでは、Solaris システムはセキュリティー上の危険があるポートでは待機しないように設定されます。そのため、遠隔で管理するシステムは、ネットワーク通信を受け付けるように明示的に構成します。たとえば、LDAP サーバー上のネットワークデータベースをクライアントから管理するには、LDAP サーバー上の Solaris 管理コンソール サーバーがネットワーク通信を受け付けるようにします。

LDAP サーバーがあるネットワークのための Solaris 管理コンソール の構成要件については、『Oracle Solaris Trusted Extensions 管理の手順』の「Solaris 管理コンソール を使用したクライアントサーバー通信」を参照してください。

始める前に Solaris 管理コンソール サーバーシステム上で大域ゾーンのスーパーユーザーでなくてはなりません。この手順では、そのシステムを遠隔システムと呼びます。また、スーパーユーザーとしてクライアントシステムにコマンド行からアクセスできることも必要です。

1 遠隔システムで、遠隔接続を受け付けるようにシステムを設定します。

smc デーモンは wbem サービスによって制御されます。wbem サービスの options/tcp_listen プロパティーが true に設定されている場合、Solaris 管理コンソール サーバーは遠隔接続を受け付けます。

```
# /usr/sbin/svcprop -p options wbem
options/tcp_listen boolean false
# svccfg -s wbem setprop options/tcp_listen=true
```

2 wbem サービスの再表示と再起動を行います。

```
# svcadm refresh wbem
# svcadm restart wbem
```

3 wbem サービスが遠隔接続を受け付けるように設定されていることを確認します。

```
# svcprop -p options wbem
options/tcp_listen boolean true
```

4 遠隔システムおよび **Solaris** 管理コンソールにアクセスするすべてのクライアントで、smcserver.config ファイルで遠隔接続が有効になっていることを確認します。

a. smcserver.config ファイルをトラステッドエディタで開きます。

```
# /usr/dt/bin/trusted_edit /etc/smc/smcserver.config
```

b. remote.connections パラメータに true を設定します。

```
## remote.connections=false
remote.connections=true
```

c. ファイルを保存し、トラステッドエディタを終了します。

注意事項 wbem サービスを再起動または有効にする場合、smcserver.config ファイルの remote.connections パラメータが true のままであることを確認します。

▼ Solaris 管理コンソールの LDAP ツールボックスを編集する

始める前に LDAP サーバー上のスーパーユーザーでなくてはなりません。LDAP 資格を Solaris 管理コンソールに登録する必要があり、/usr/sadm/bin/dtsetup scopes コマンドの出力について知っている必要があります。詳細は、133 ページの「LDAP の資格を Solaris 管理コンソールに登録する」を参照してください。

1 **LDAP** ツールボックスを探します。

```
# cd /var/sadm/smc/toolboxes/tsol_ldap
# ls *tbx
tsol_ldap.tbx
```

2 **LDAP** サーバー名を入力します。

a. トラステッドエディタを開きます。

b. tsol_ldap.tbx ツールボックスのフルパス名をコピーして、引数としてエディタにペーストします。

たとえば、次のパスが LDAP ツールボックスのデフォルトの位置です。

```
/var/sadm/smc/toolboxes/tsol_ldap/tsol_ldap.tbx
```

c. スコープ情報を置き換えます。

<Scope> タグと </Scope> タグの間にある server タグを、ldap:/..... 行の出力 (/usr/sadm/bin/dtsetup scopes コマンドから) で置き換えます。

```
<Scope>ldap:/<ldap-server-name>/<dc=domain,dc=suffix></Scope>
```

d. <?server?> または <?server ?> のすべてのインスタンスを **LDAP** サーバーと置き換えます。

```
<Name>This Computer (ldap-server-name: Scope=ldap, Policy=TSOL)</Name>
services and configuration of ldap-server-name.</Description>
and configuring ldap-server-name.</Description>
...
```

e. ファイルを保存し、エディタを終了します。

3 wbem サービスの再表示と再起動を行います。

```
# svcadm refresh wbem
# svcadm restart wbem
```

例 **5–2** LDAP ツールボックスの設定

この例では、LDAP サーバーの名前は LDAP1 です。ツールボックスを設定するには、管理者が <?server ?> のインスタンスを LDAP1 と置き換えます。

```
# cd /var/sadm/smc/toolboxes/tsol_ldap
# /usr/dt/bin/trusted_edit /tsol_ldap.tbx
<Scope>ldap:/LDAP1/cd=LDAP1,dc=example-domain,dc=com</Scope

...
<Name>This Computer (LDAP1: Scope=ldap, Policy=TSOL)</Name>
services and configuration of LDAP1.</Description>
and configuring LDAP1.</Description>
...
```

▼ Solaris 管理コンソールに Trusted Extensions 情報が含まれていることを確認する

LDAP サーバーがあるネットワークと LDAP サーバーがないネットワークのための Solaris 管理コンソール の構成要件については、『Oracle Solaris Trusted Extensions 管理の手順』の「Solaris 管理コンソール を使用したクライアントサーバー通信」を参照してください。

始める前に 管理役割になって、またはスーパーユーザーとして LDAP クライアントにログインします。システムを LDAP クライアントにする場合は、65 ページの「Trusted Extensions で大域ゾーンを LDAP クライアントにする」を参照してください。

ローカルシステムを管理するには、61 ページの「Trusted Extensions で Solaris 管理コンソールサーバーを初期化する」を完了してください。

ローカルシステムから遠隔システム上のコンソールサーバーに接続するには、両方のシステムで61 ページの「Trusted Extensions で Solaris 管理コンソールサーバーを初期化する」を完了してください。また、遠隔システムで、134 ページの「Solaris 管理コンソール でのネットワーク接続の受け付けを有効にする」を完了してください。

LDAP ネームサービス中のデータベースを LDAP クライアントから管理するには、LDAP サーバーで、上の手順に加えて135 ページの「Solaris 管理コンソールの LDAP ツールボックスを編集する」完了してください。

1 **Solaris 管理コンソールを起動します。**

```
# /usr/sbin/smc &
```

2 **Trusted Extensions ツールボックスを開きます。**

Trusted Extensions ツールボックスの値は `Policy=TSOL` です。

- **LDAP** をネームサービスとして使用するトラステッドネットワークでは、次のテストを実行します。

  a. ローカル管理データベースにアクセスできることを確認するには、次のツールボックスを開きます。

  このコンピュータ (*this-host*: `Scope=Files, Policy=TSOL`)

  b. **LDAP** サーバーのローカル管理データベースにアクセスできることを確認するには、次のツールボックスを指定します。

  このコンピュータ (*ldap-server*: `Scope=Files, Policy=TSOL`)

  c. **LDAP** サーバー上のネームサービスデータベースにアクセスできることを確認するには、次のツールボックスを指定します。

  このコンピュータ (*ldap-server*: `Scope=LDAP, Policy=TSOL`)

- **LDAP** をネームサービスとして使用しないトラステッドネットワークでは、次のテストを実行します。

  a. ローカル管理データベースにアクセスできることを確認するには、次のツールボックスを開きます。

  このコンピュータ (*this-host*: `Scope=Files, Policy=TSOL`)

  b. 遠隔システムのローカル管理データベースにアクセスできることを確認するには、次のツールボックスを指定します。

  このコンピュータ (*remote-system*: `Scope=Files, Policy=TSOL`)

3 「システムの構成」領域で、「コンピュータとネットワーク」、「セキュリティーテンプレート」と移動します。

4 正しいテンプレートおよびラベルが遠隔システムに適用されていることを確認します。

注 – LDAP サーバーではないシステムからネットワークデータベース情報にアクセスしようとしても、処理に失敗します。コンソールを使用すると、遠隔ホストにログインしてツールボックスを開くことができます。ただし、情報にアクセスしたり情報を変更したりしようとした場合、LDAP サーバーではないシステム上で `Scope=LDAP` を選択したことを示す、次のエラーメッセージが表示されます。

```
Management server cannot perform the operation requested.
...
Error extracting the value-from-tool.
The keys received from the client were machine, domain, Scope.
Problem with Scope.
```

注意事項 LDAP 構成をトラブルシューティングするには、『System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)』の第 13 章「LDAP Troubleshooting (Reference)」を参照してください。

◆ ◆ ◆ 第 6 章

Trusted Extensions とヘッドレスシステムの構成 (タスク)

Netra シリーズなどのヘッドレスシステム上の Trusted Extensions ソフトウェアを構成および管理するには、そのヘッドレスシステムのセキュリティー設定を変更して遠隔アクセスを可能にする必要があります。遠隔 Trusted Extensions システムを管理する場合にも同様の設定が必要になります。管理 GUI を実行するには、そのプロセスを遠隔システム上で実行し、その GUI をデスクトップシステム上で表示する必要がある場合があります。

要件の説明については、『Oracle Solaris Trusted Extensions 管理の手順』の第 8 章「Trusted Extensions での遠隔管理 (手順)」を参照してください。

注 – ヘッドレスシステムや遠隔システムで必要とされる構成方法は、評価された構成の基準を満たしません。詳細は、22 ページの「サイトのセキュリティーポリシーについて」を参照してください。

Trusted Extensions でのヘッドレスシステムの構成 (作業マップ)

ヘッドレスシステムでは、コンソールはシリアル回線によって端末エミュレータウィンドウに接続されます。この回線は、通常、`tip` コマンドによって保護されます。利用可能な増設システムのタイプに応じて、次の方法のいずれかを使用してヘッドレスシステムを構成できます。次の表では、安全性が高い方法から順に示します。これらの手順は遠隔システムにも適用されます。

作業	説明	参照先
root ユーザーによる遠隔ログインを有効にします。	LDAP を使用していない場合、最初に root としてヘッドレスシステムにログインします。LDAP を使用している場合、この手順は省略できます。	141 ページの「Trusted Extensions での root による遠隔ログインを有効にする」
遠隔ログインを有効にします。	root 役割または別の管理役割になれるユーザーの遠隔ログインを有効にします。	141 ページの「Trusted Extensions での役割による遠隔ログインを有効にする」
	ラベルなしシステムから Trusted Extensions システムの管理を有効にします。	143 ページの「ラベルなしシステムからの遠隔ログインを有効にする」
	ヘッドレスシステム上の大域ゾーンにユーザーがアクセスできるようにします。	『Oracle Solaris Trusted Extensions 管理の手順』の「特定のユーザーが Trusted Extensions の大域ゾーンに遠隔でログインできるようにする」
(省略可能) 管理 GUI の表示を有効にします。	ヘッドレスシステム上で実行されている管理 GUI をデスクトップシステム上で表示できるようにします。	145 ページの「管理 GUI の遠隔表示を有効にする」
(省略可能) 仮想ネットワークコンピューティング (virtual network computing、vnc) を有効にします。	任意のクライアントから、遠隔 Trusted Extensions で Xvnc サーバーを使用して、クライアントにマルチレベルセッションを表示します。	『Oracle 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」
ヘッドレスシステムを設定するための構成と管理の方法を選択します。	遠隔システムを管理するための、スーパーユーザーまたは役割になります。	145 ページの「rlogin または ssh コマンドを使用して Trusted Extensions のヘッドレスシステムにログインする」
	ヘッドレスシステム上で Solaris 管理コンソールを使用します。	144 ページの「遠隔の Solaris 管理コンソール を使用してファイルスコープで管理する」
	ウィンドウ表示システムがない場合、シリアルログインをスーパーユーザーとして使用できます。この手順は安全ではありません。	構成は不要です。

注 – セキュリティーポリシーを確認して、サイトで許可されている遠隔管理の方法を判定します。

▼ Trusted Extensions での root による遠隔ログインを有効にする

Solaris OS の場合と同じように、CONSOLE エントリが無効なとき、root はラベル付きシステムから遠隔でログインできます。

ローカルファイルを編集して遠隔システムを管理する場合、次の手順に従います。

1 トラステッドエディタで、/etc/default/login ファイルの CONSOLE= 行をコメントアウトします。

```
# /usr/dt/bin/trusted_edit /etc/default/login
```

編集した行は次のようになります。

```
#CONSOLE=/dev/console
```

2 ssh 接続での root ユーザーログインを許可します。

/etc/ssh/sshd_config ファイルを変更します。デフォルトでは、ssh は Solaris システムで有効です。

```
# /usr/dt/bin/trusted_edit /etc/ssh/sshd_config
```

編集した行は次のようになります。

```
PermitRootLogin yes
```

次の手順 また、ラベルなしシステムから root ユーザーとしてログインするには、143 ページの「ラベルなしシステムからの遠隔ログインを有効にする」を完了してください。

役割による遠隔ログインを有効にするには、引き続き141 ページの「Trusted Extensions での役割による遠隔ログインを有効にする」を実行してください。

▼ Trusted Extensions での役割による遠隔ログインを有効にする

rlogin または ssh コマンドを使用してヘッドレスシステムを管理する必要がある場合のみ、この手順に従ってください。

構成エラーは遠隔でデバッグできます。

始める前に ローカルファイルを使用して遠隔システムを管理している場合、141 ページの「Trusted Extensions での root による遠隔ログインを有効にする」を完了しておきます。次に、root ユーザーとして、次のタスクを両方のシステム上で実行します。

1 両方のシステム上で、互いのシステムをラベル付きシステムとして認識します。

デスクトップシステムおよびヘッドレスシステムは、同じセキュリティーテンプレートを使用して互いに相手を特定する必要があります。手順については、『Oracle Solaris Trusted Extensions 管理の手順』の「セキュリティーテンプレートをホストまたはホストのグループに割り当てる」を参照してください。

一時ラベルを割り当てるには、例 6–1 を参照してください。

2 両方のシステム上で、同一のユーザーと役割を作成します。

両方のシステム上で、名前と ID を同じにして、役割をユーザーに割り当てます。ユーザーと役割を作成するには、93 ページの「Trusted Extensions での役割とユーザーの作成」を参照してください。

3 遠隔の **Solaris** 管理コンソールにアクセスするには、両方のシステム上で次の手順を実行します。

a. 互いのシステムのホスト名および **IP** アドレスを `/etc/hosts` ファイルに追加します。

```
# /usr/dt/bin/trusted_edit /etc/hosts

127.0.0.1    localhost
192.168.66.66    local-system-name    loghost
192.168.66.12    remote-system-name
```

b. 遠隔役割の引き受けを許可するには、`pam.conf` ファイルを変更して **PAM** ポリシーを緩和します。

i. `/etc/pam.conf` ファイルを `/etc/pam.conf.orig` にコピーします。

```
# cp /etc/pam.conf /etc/pam.conf.orig
```

ii. トラステッドエディタで、`pam.conf` ファイルを開きます。

```
# /usr/dt/bin/trusted_edit /etc/pam.conf
```

iii. デフォルトエントリをアカウントの管理にコピーします。

iv. 互いのコピーされたエントリで、`other` を `smcconsole` に変更します。

v. コピーされた `pam_roles.so.1` エントリに、`allow_remote` を追加します。

Tab キーを使用してフィールドを移動します。このセクションは次のようになります。

```
# Solaris Management Console definition for Account management
#
smcconsole   account requisite   pam_roles.so.1   allow_remote
smcconsole   account required    pam_unix_account.so.1
smcconsole   account required    pam_tsol_account.so.1
```

```
# Default definition for Account management
# Used when service name is not explicitly mentioned for account management
#
other   account requisite    pam_roles.so.1
other   account required     pam_unix_account.so.1
other   account required     pam_tsol_account.so.1
```

vi. ファイルを保存し、エディタを終了します。

vii. (省略可能) ファイルを /etc/pam.conf.site にコピーします。

```
# cp /etc/pam.conf /etc/pam.conf.site
```

システムを新しいリリースにアップグレードする場合、変更内容を /etc/pam.conf.site から pam.conf ファイルにコピーするべきかどうかを評価してください。

例 6–1 Trusted Extensions ホストタイプの一時的な定義の作成

この例では、管理者は、ホストタイプの定義が設定される前に遠隔 Trusted Extensions システムの構成を開始します。管理者はそのために、次のように遠隔システム上で tnctl コマンドを使用して、デスクトップシステムのホストタイプを一時的に定義します。

```
remote-TX# tnctl -h desktop-TX:cipso
```

その後、管理者は、Trusted Extensions が構成されていないデスクトップシステムから遠隔 Trusted Extensions システムにアクセスします。この場合、管理者は次のように遠隔システム上で tnctl コマンドを使用して、デスクトップシステムのホストタイプを ADMIN_LOW ラベルで動作するラベルなしシステムとして一時的に定義します。

```
remote-TX# tnctl -h desktop-TX:admin_low
```

▼ ラベルなしシステムからの遠隔ログインを有効にする

始める前に この手順は安全ではありません。

141 ページの「Trusted Extensions での役割による遠隔ログインを有効にする」の説明に従って、遠隔役割の引き受けを許可するよう PAM ポリシーを緩和しておきます。

1 トラステッドシステム上で、適切なセキュリティーテンプレートをラベルなしシステムに適用します。

注意 – デフォルトの設定では、別のラベルなしシステムが遠隔システムにログインしてその管理を行える可能性があります。したがって、`0.0.0.0` ネットワークのデフォルトを `ADMIN_LOW` から別のラベルに変更してください。手順については、『Oracle Solaris Trusted Extensions 管理の手順』の「トラステッドネットワーク上で接続できるホストを制限する」を参照してください。

2 トラステッドエディタで、`/etc/pam.conf` ファイルを開きます。

```
# /usr/dt/bin/trusted_edit /etc/pam.conf
```

3 `smcconsole` エントリを検索します。

4 `allow_unlabeled` を `tsol_account` モジュールに追加します。

Tab キーを使用してフィールドを移動します。

```
smcconsole   account required  pam_tsol_account.so.1 allow_unlabeled
```

編集後のこのセクションは、次のようになります。

```
# Solaris Management Console definition for Account management
#
smcconsole  account  requisite      pam_roles.so.1    allow_remote
smcconsole  account  required       pam_unix_account.so.1
smcconsole  account  required       pam_tsol_account.so.1 allow_unlabeled
```

▼ 遠隔の Solaris 管理コンソールを使用してファイルスコープで管理する

LDAP を使用せずに、遠隔システム上で Solaris 管理コンソール を使用する場合は、コンソールへの遠隔接続を有効にします。ただし、次の手順では、LDAP スコープのアクセスを有効にすることはできません。

LDAP スコープのアクセスを有効にするには、132 ページの「LDAP のための Solaris 管理コンソールの設定 (作業マップ)」の手順をすべて完了してください。

始める前に システムは両方ともラベル付きシステムです。

次の手順を完了しておきます。

- 61 ページの「Trusted Extensions で Solaris 管理コンソールサーバーを初期化する」
- 141 ページの「Trusted Extensions での役割による遠隔ログインを有効にする」

1 134 ページの「Solaris 管理コンソールでのネットワーク接続の受け付けを有効にする」を完了します。

2 デスクトップシステムで、両方のシステム上で同じように定義されている ユーザーになります。

3 デスクトップシステムで、両方のシステム上で同じように定義されている役割になります。

4 デスクトップシステムで **Solaris** 管理コンソールを起動します。

```
# /usr/sbin/smc &
```

5 「サーバー」ダイアログボックスで、ヘッドレスシステムの名前を入力します。

次に、Scope=Files ツールボックスを選択します。

このコンピュータ (*remote-system*: Scope=Files, Policy=TSOL)

▼ 管理 GUI の遠隔表示を有効にする

デスクトップ上での遠隔表示の手順は、Trusted Extensions が構成されていない Solaris システム上での手順と同じです。この手順は、利便性を考慮して記載されています。

1 デスクトップシステムで、ヘッドシステムからのプロセスが表示されるようにします。

a. ヘッドレスシステムがデスクトップシステム上の **X** サーバーにアクセスできるようにします。

```
desktop $ xhost + headless-host
```

b. デスクトップの DISPLAY 変数の値を指定します。

```
desktop $ echo $DISPLAY
:n.n
```

2 ヘッドレスシステム上で、DISPLAY 変数をデスクトップシステムに設定します。

```
headless $ DISPLAY=desktop:n.n
headless $ export DISPLAY=n:n
```

▼ rlogin または ssh コマンドを使用して Trusted Extensions のヘッドレスシステムにログインする

この手順では、コマンド行および txzonemgr GUI を使用してスーパーユーザーまたは役割としてヘッドレスシステムを管理できます。

注 – rlogin コマンドを使用した遠隔ログインは、ssh コマンドを使用した遠隔ログインよりも安全性が低くなります。

Solaris 管理コンソール を使用して遠隔システムを管理する場合、遠隔ログインコマンドを使用する必要はありません。手順については、『Oracle Solaris Trusted Extensions 管理の手順』の「Trusted Extensions システムから Solaris 管理コンソールを使ってシステムを遠隔管理する」を参照してください。

始める前に　141 ページの「Trusted Extensions での役割による遠隔ログインを有効にする」を完了しました。

あなたは、通常と同じユーザー名とユーザー ID でヘッドレスシステムにログインすることを許可されたユーザーであり、ヘッドレスシステム上でもデスクトップシステム上でなれるのと同じ役割になることができます。

1. デスクトップシステムで、ヘッドシステムからのプロセスが表示されるようにします。

```
desktop $ xhost + headless-host
desktop $ echo $DISPLAY
:n.n
```

2. 両方のシステムで同じように定義されているユーザーになっている必要があります。

3. 端末ウィンドウから遠隔にヘッドレスシステムにログインします。

   - 次のように ssh コマンドを使用してログインします。

```
desktop $ ssh -l identical-username  headless
Password:       Type the user's password
headless $
```

   - 次のように rlogin コマンドを使用してログインします。

```
desktop # rlogin headless
Password:       Type the user's password
headless $
```

4. 両方のシステムで同じように定義されている役割になります。

   同じ端末ウィンドウを使用します。たとえば、root の役割になります。

```
headless $ su - root
Password:       Type the root password
```

   大域ゾーンになります。これで、この端末を使用してコマンド行からヘッドレスシステムを管理できるようになりました。

5 ヘッドレスシステム上のプロセスがデスクトップシステム上に表示されるようにします。

注 – また、ssh -X コマンドでログインして、遠隔 GUI を表示することもできます。詳細は、ssh(1) のマニュアルページを参照してください。例については、例 6–2 を参照してください。

```
headless $  DISPLAY desktop:n.n
headless $ export DISPLAY=n:n
```

Trusted Extensions の GUI を使用してヘッドレスシステムを管理できるようになります。たとえば、次のようにして txzonemgr GUI を起動します。

```
headless $ /usr/sbin/txzonemgr
```

Labeled Zone Manager は遠隔システム上で実行され、デスクトップシステム上に表示されます。

6 **(省略可能) Trusted CDE アクションにアクセスします。**

アプリケーションマネージャーのオープンと安全なクローズを行うには、『Oracle Solaris Trusted Extensions 管理の手順』の「dtappsession で Trusted Extensions を遠隔管理する」を参照してください。

例 6–2 ヘッドレスシステムでのラベル付きゾーンの設定

この例では、管理者が txzonemgr GUI を使用して、ラベル付きデスクトップシステムからラベル付きヘッドレスシステム上のラベル付きゾーンを設定します。Solaris OS と同様に、管理者は ssh コマンドに -X オプションを使用して、デスクトップシステムへの X サーバーのアクセスを許可します。ユーザー install1 は両方のシステムで同じように定義されているので、役割 remoterole になることができます。

```
TXdesk1 $ xhost + TXnohead4
TXdesk1 $ whoami
install1

TXdesk1 $ ssh -X -l install1 TXnohead4
Password: Ins1PwD1
TXnohead4 $
```

大域ゾーンに到達するには、管理者は役割 remoterole になります。この役割は、両方のシステムで同じように定義されています。

```
TXnohead4 # su - remoterole
Password: abcd1EFG
```

次に、管理者は txzonemgr GUI を起動します。

```
TXnohead4 $ /usr/sbin/txzonemgr &
```

Labeled Zone Manager はヘッドレスシステム上で実行され、デスクトップシステム上に表示されます。

◆ ◆ ◆ 付 録 A

サイトのセキュリティーポリシー

この付録では、サイトのセキュリティーポリシーについて解説し、詳細についての参考文書や Web サイトを紹介します。

- 150 ページの「サイトのセキュリティーポリシーと Trusted Extensions」
- 151 ページの「コンピュータのセキュリティーに関する推奨事項」
- 152 ページの「物理的セキュリティーに関する推奨事項」
- 153 ページの「個人のセキュリティーに関する推奨事項」
- 153 ページの「よくあるセキュリティー違反」
- 154 ページの「その他のセキュリティー関連資料」

セキュリティーポリシーの作成と管理

各 Solaris Trusted Extensions サイトは固有であるので、それぞれ独自のセキュリティーポリシーを作成します。セキュリティーポリシーを作成および管理する場合は、次のタスクを実行してください。

- セキュリティーチームの設置。セキュリティーチームは、トップレベルの経営、人事管理、コンピュータシテム管理と管理者、および設備管理からの代表者で構成する必要があります。チームは、Trusted Extensions 管理者のポリシーと手順を検討し、すべてのシステムユーザーに適用される一般セキュリティーポリシーを勧告する必要があります。
- 経営管理担当者に対するサイトセキュリティーポリシーについての教育。サイトの経営管理に携わる担当者は全員、セキュリティーポリシーに関する教育を受ける必要があります。ポリシーの情報はコンピュータシステムのセキュリティーに直接関係するので、一般ユーザーがセキュリティーポリシーに触れることができないようにする必要があります。
- ユーザーに対する Trusted Extensions ソフトウェアおよびセキュリティーポリシーについての教育。すべてのユーザーは『Oracle Solaris Trusted Extensions ユーザーズガイド』を読まなければなりません。システムが正常に動作していない場合、通常、これを最初に知るのはユーザーであるため、ユーザーはシステム

に関する知識を持ち、発生した問題をシステム管理者に報告する必要があります。セキュリティー保護された環境では、次のような異常に気が付いたら、ただちにシステム管理者に報告する必要があります。

- 各セッションの初めに報告される前回のログイン時間が間違っている
- ファイルデータに異常な変更がある
- 人間が理解できる形式の印刷出力をなくしたり盗まれたりした
- ユーザー機能が実行できない

- セキュリティーポリシーの施行。セキュリティーポリシーが施行されていなかったり遵守されていない場合、Trusted Extensions が設定されたシステムに格納されるデータは保護されません。問題を記録する手順、および問題解決のために行なった措置を記録する手順を決定しなければなりません。
- セキュリティーポリシーの定期的な検討。セキュリティーチームは、セキュリティーポリシーの評価と、前回のポリシー評価のあとに発生したすべてのできごとの評価を定期的に行わなければなりません。これによってポリシーを修正することによって、セキュリティーを向上させることができます。

サイトのセキュリティーポリシーと Trusted Extensions

セキュリティー管理者は、サイトのセキュリティーポリシーに基づいて Trusted Extensions ネットワークを設計しなければなりません。セキュリティーポリシーが次のような構成上の決定の基準になります。

- すべてのユーザーについてどの程度の監査が行われるか、また、どのイベントクラスについて行われるか
- 役割を持つユーザーについてどの程度の監査が行われるか、また、どのイベントクラスについて行われるか
- 監査データをどのように管理、保管、および評価するか
- システムでどのラベルを使用するか、また、一般ユーザーが `ADMIN_LOW` ラベルおよび `ADMIN_HIGH` ラベルを表示できるか
- 各ユーザーにどのユーザー認可上限が割り当てられるか
- デバイスがある場合、どの一般ユーザーによってどのデバイスを割り当てることができるか
- システム、プリンタ、その他のデバイスにどのラベル範囲が定義されるか
- 評価された構成で Trusted Extensions が使用されるかどうか

コンピュータのセキュリティーに関する推奨事項

サイトのセキュリティーポリシーを構築するときには、次のガイドラインのリストを検討してください。

- Trusted Extensions が設定されたシステムの最上位ラベルは、サイトで実行される作業のセキュリティーレベルの上限を超えないように割り当ててください。
- システムのリブート、停電、およびシャットダウンは、手動でサイトログに記録します。
- ファイルシステムの損傷を文書化して、影響を受けたすべてのファイルについて、潜在的なセキュリティーポリシー違反がないか分析します。
- 操作マニュアルと管理者マニュアルは、その情報を使用する正当な理由のある人員以外が読めないようにします。
- Trusted Extensions ソフトウェアの異常な動作または予期しない動作は、報告および文書化して、原因を突き止めます。
- Trusted Extensions が設定されたシステムは、可能であれば 2 人以上で管理します。セキュリティー関連の決定に関するセキュリティー管理権限を、1 人に割り当てます。システム管理タスクに関するシステム管理権限を、それとは別の人に割り当てます。
- 定期的なバックアップルーチンを定めます。
- 承認は、それを必要とし、適切に使用すると信頼できるユーザーのみに割り当てます。
- プログラムに特権を割り当てるのは、作業を行うために特権が必要な場合、また、プログラムを精査して特権の使用についての信頼性が証明された場合のみです。新しいプログラムに特権を設定する際は、その基準として、既存の Trusted Extensions プログラムの特権を確認します。
- 監査情報は定期的に確認および分析を行います。異常なイベントがないか調査して、そのイベントの原因を判別します。
- 管理 ID の数は最小限にします。
- setuid および setgid プログラムの数を最小限にします。承認、特権、役割を使用して、プログラムを実行し、誤使用を回避します。
- 管理者は、一般ユーザーが妥当なログインシェルを持っていることを、定期的に確認します。
- 管理者は、一般ユーザーがシステム管理の ID の値ではなく、妥当なユーザー ID の値を持っていることを定期的に確認してください。

物理的セキュリティーに関する推奨事項

サイトのセキュリティーポリシーを構築するときには、次のガイドラインのリストを検討してください。

- Trusted Extensions が設定されたシステムへのアクセスを制限します。もっとも安全な場所は、通常、1 階以外の屋内です。
- Trusted Extensions が設定されたシステムへのアクセスを監視および文書化します。
- コンピュータ装置は、盗難を防ぐために、テーブルや机などの大きな室内用具に固定します。木製用具に固定する場合は、金属プレートを付けて強度を上げます。
- 機密度の高い情報にはリムーバブルストレージメディアの使用を検討します。使用していないメディアは適切に保管します。
- システムのバックアップおよびアーカイブは、システムとは別の安全な場所に保管します。
- バックアップメディアおよびアーカイブメディアへの物理的なアクセスは、システムへのアクセスと同じ方法で制限します。
- コンピュータ施設に高温アラームを設置し、温度が製造元の仕様の範囲外になったらわかるようにします。推奨範囲は 10 ～ 32°C です。
- コンピュータ施設は水検知器を設置し、床、下張り床の隙間、天井の水漏れなどがわかるようにします。
- 火災を知らせる煙探知機、および防火システムを設置します。
- 湿度アラームを設置し、湿度が高すぎたり低すぎたりするとわかるようにします。
- コンピュータに TEMPEST シールドがない場合は、使用を検討します。TEMPEST シールドは、施設の壁、床、天井などに使用できます。
- TEMPEST を使用した装置の開閉は認定された技術者のみに許可し、電磁放射を確実に防護します。
- コンピュータ装置が置かれている施設や部屋に侵入できる物理的な不備がないか確認します。上げ床、吊り天井、通風口、元の壁と対隣壁の間などを調べます。
- コンピュータ施設内またはコンピュータ装置の近くでの飲食および喫煙を禁止します。コンピュータ装置に影響を与えずにこれらの行為が可能な区域を設けます。
- コンピュータ施設の設計図を保護します。
- コンピュータ施設の建物の設計図、間取り図、写真などの使用を制限します。

個人のセキュリティーに関する推奨事項

サイトのセキュリティーポリシーを構築するときには、次のガイドラインのリストを検討してください。

- パッケージ、文書、およびストレージメディアは、入手した時点およびセキュリティー保護されたサイトから外部へ持ち出す前に検査します。
- 訪問者を含むすべての人に ID カードを常時身に着けるように求めます。
- 複製や偽造が困難な ID カードを使用します。
- 訪問者の立ち入りを禁止する領域を決め、標識によって明らかにわかるようにします。
- 訪問者には常にだれかが付き添います。

よくあるセキュリティー違反

コンピュータを完全にセキュリティー保護することはできません。コンピュータ施設のセキュリティーの限界は、その施設の使用者次第です。セキュリティー違反のほとんどのアクションは、ユーザーの注意や装置の追加によって簡単に解決できます。次に、発生する可能性のある問題の例を示します。

- ユーザーが、システムへのアクセスを許可されていない人にパスワードを教える。
- ユーザーがパスワードを書き留め、それを失くしたり、安全でない場所に放置したりする。
- ユーザーが、簡単に推測できる語や名前をパスワードに設定する。
- パスワードを入力しているのをほかのユーザーに見られ、パスワードを知られる。
- 承認されていないユーザーがハードウェアの取り外しや交換を行なったり、ハードウェアに不正な変更を加える。
- ユーザーが画面をロックしないでシステムを放置する。
- ユーザーがファイルのアクセス権を変更し、ほかのユーザーがそのファイルを読み取れるようにする。
- ユーザーがファイルのラベルを変更し、ほかのユーザーがそのファイルを読み取れるようにする。
- 機密の印刷文書をシュレッダーにかけないで処分したり、安全でない場所に放置したりする。
- 施設のドアに施錠をしない。
- 鍵を紛失する。
- リムーバブルストレージメディアを適切に保管しない。

- 外部に面した窓からコンピュータ画面が見える。
- ネットワークケーブルが盗聴される。
- 電子的な傍受によって、コンピュータ装置から放射される信号が捕捉される。
- 停電、過電流、スパイクによってデータが破壊される。
- 地震、洪水、竜巻、台風、落雷によってデータが破壊される。
- 太陽の黒点の活動など、外部の電磁放射の干渉によってファイルが解読できなくなる。

その他のセキュリティー関連資料

米国政府発行の出版物では、コンピュータセキュリティーに関する標準、ポリシー、方法、および用語が詳細に説明されています。さらに、UNIX システムのシステム管理者向けのガイドもここに示されています。UNIX のセキュリティー上の問題と解決策を十分に理解するのに役立ちます。

インターネットを通じても資料を入手できます。特に、CERT (`http://www.cert.org`) の Web サイトには、企業やユーザー向けにソフトウェアのセキュリティーホールに関する警告が掲載されています。SANS 協会 (`http://www.sans.org/`)では、トレーニング、詳細な用語集、インターネットからの主な脅威の最新リストが提供されています。

米国政府出版物

米国政府は、多数の出版物を Web 上で提供しています。米国国立標準技術研究所 (NIST) の コンピュータセキュリティーリソースセンター (CSRC) が、コンピュータセキュリティーに関する情報を発表しています。NIST のサイト (`http://csrc.nist.gov/index.html`)からダウンロードできる出版物の一部を次に示します。

- An Introduction to Computer Security: The NIST Handbook.SP 800-12, October 1995.
- Standard Security Label for Information Transfer.FIPS-188, September 1994.
- Swanson, Marianne and Barbara Guttman.Generally Accepted Principles and Practices for Securing Information Technology Systems.SP 800-14, September 1996.
- Tracy, Miles, Wayne Jensen, and Scott Bisker.Guidelines on Electronic Mail Security.SP 800-45, September 2002. セクション E.7 では、メール用の LDAP の安全な設定について解説。
- Wilson, Mark and Joan Hash.Building an Information Technology Security Awareness and Training Program.SP 800-61, January 2004.便利な用語集を収録。
- Grace, Tim, Karen Kent, and Brian Kim.Computer Security Incident Handling Guidelines.SP 800-50, September 2002. セクション E.7 では、メール用の LDAP の安全な設定について解説。

- Scarfone, Karen,Wayne Jansen, and Miles Tracy. Guide to General Server Security SP 800-123, July 2008.
- Souppaya, Murugiah, John Wack, and Karen Kent.Security Configuration Checklists Program for IT Products. SP 800-70, May 2005.

UNIXのセキュリティーに関する出版物

Chirillo, John and Edgar Danielyan.Sun Certified Security Administration for Solaris 9 & 10 Study Guide.McGraw-Hill/Osborne, 2005.

Garfinkel, Simson, Gene Spafford, and Alan Schwartz.Practical UNIX and Internet Security, 3rd Edition.O'Reilly & Associates, Inc, Sebastopol, CA, 2006.

一般的なコンピュータセキュリティーに関する出版物

Brunette, Glenn M. and Christoph L. Toward Systemically Secure IT Architectures. Sun Microsystems, Inc, June 2005.

Kaufman, Charlie, Radia Perlman, and Mike Speciner.Network Security: Private Communication in a Public World, 2nd Edition.Prentice-Hall, 2002.

Pfleeger, Charles P. and Shari Lawrence Pfleeger. Security in Computing.Prentice Hall PTR, 2006.

Privacy for Pragmatists: A Privacy Practitioner's Guide to Sustainable Compliance.Sun Microsystems, Inc, August 2005.

Rhodes-Ousley, Mark, Roberta Bragg, and Keith Strassberg.Network Security: The Complete Reference.McGraw-Hill/Osborne, 2004.

Stoll, Cliff. The Cuckoo's Egg.Doubleday, 1989. (『カッコウはコンピュータに卵を産む(上・下)』、草思社発行、1991)

UNIX全般に関する出版物

Bach, Maurice J. The Design of the UNIX Operating System. Prentice Hall, Englewood Cliffs, NJ, 1986. (『UNIXカーネルの設計』、共立出版発行、1991)

Nemeth, Evi, Garth Snyder, and Scott Seebas.UNIX System Administration Handbook.Prentice Hall, Englewood Cliffs, NJ, 1989. (『UNIXシステム管理入門』、ソフトバンククリエイティブ発行、1992)

◆ ◆ ◆ 付 録 B

Trusted Extensions での CDE アクションを使用したゾーンのインストール

この付録では、Trusted CDE アクションを使用して Trusted Extensions にラベル付きゾーンを構成する方法について説明します。Solaris 10 11/06 リリースをパッチを適用せずに実行しているか、またはこれらのアクションに精通している場合は、Trusted CDE アクションを使用します。`txzonemgr` スクリプトを使用するには、68 ページの「ラベル付きゾーンの作成」を参照してください。

- 157 ページの「CDE アクションを使用したネットワークインタフェースとゾーンの結合 (作業マップ)」
- 160 ページの「CDE アクションを使用したゾーン作成の準備 (作業マップ)」
- 163 ページの「CDE アクションを使用したラベル付きゾーンの作成 (作業マップ)」

CDE アクションを使用したネットワークインタフェースとゾーンの結合 (作業マップ)

次のタスクをいずれか 1 つのみを実行します。それぞれの利点と欠点については、28 ページの「マルチレベルアクセスの計画」を参照してください。

作業	説明	参照先
論理インタフェースを共有します。	大域ゾーンを 1 つの IP アドレスにマップし、ラベル付きゾーンを別の IP アドレスにマップします。	158 ページの「CDE アクションを使用してシステムに 2 つの IP アドレスを指定する」
物理インタフェースを共有します。	すべてのゾーンを 1 つの IP アドレスにマップします。	159 ページの「CDE アクションを使用してシステムに 1 つの IP アドレスを指定する」

▼ CDE アクションを使用してシステムに 2 つの IP アドレスを指定する

この構成では、ホストのアドレスは大域ゾーンにのみ適用されます。ラベル付きゾーンは、別の IP アドレスを大域ゾーンと共有します。

始める前に　大域ゾーンでスーパーユーザーになります。システムにはすでに 2 つの IP アドレスが割り当てられています。Trusted CDE ワークスペースにアクセスします。

1. **Trusted_Extensions フォルダに移動します。**

   a. 背景をマウスボタン 3 でクリックします。

   b. ワークスペースメニューで、「アプリケーション」→「アプリケーション・マネージャ」を選択します。

   c. **Trusted_Extensions** フォルダのアイコンをダブルクリックします。
   このフォルダには、インタフェース、LDAP クライアント、およびラベル付きゾーンを設定するためのアクションが含まれています。

2. 「論理インタフェースの共有」アクションをダブルクリックして、プロンプトに応答します。

注 – システムにはすでに 2 つの IP アドレスが割り当てられていなければなりません。このアクションのために、2 つめのアドレスとそのアドレスのホスト名を入力します。2 つめのアドレスが共有アドレスです。

```
Hostname:       Type the name for your labeled zones interface
IP Address:     Type the IP address for the interface
```

このアクションによって、複数の IP アドレスを持つホストが構成されます。大域ゾーンの IP アドレスが、そのホストの名前です。ラベル付きゾーンの IP アドレスは、別のホスト名です。さらに、ラベル付きゾーンの IP アドレスが大域ゾーンと共有されます。この構成を使用すると、ラベル付きゾーンがネットワークプリンタにアクセスできます。

ヒント – ラベル付きゾーンには標準的な命名規則を使用してください。たとえば、ホスト名に -zones を追加します。

---

3. (省略可能) 端末ウィンドウでこのアクションの結果を確認します。

```
# ifconfig -a
```

たとえば、次の出力は、ラベル付きゾーンのネットワークインタフェース 192.168.0.12 の共有論理インタフェース hme0:3 を示しています。hme0 インタフェースは、大域ゾーンの一意の IP アドレスです。

```
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
        ether 0:0:00:00:00:0
hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 192.168.0.11 netmask fffffe00 broadcast 192.168.0.255
hme0:3 flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        all-zones
        inet 192.168.0.12 netmask fffffe00 broadcast 192.168.0.255
```

Solaris 10 10/08 リリースから、ループバックインタフェースの lo0 も all-zones インタフェースです。

```
 lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
        all-zones
        inet 127.0.0.1 netmask ff000000
        ether 0:0:00:00:00:0
...
```

▼ CDE アクションを使用してシステムに 1 つの IP アドレスを指定する

この構成では、ホストのアドレスが、ラベル付きゾーンを含むすべてのゾーンに適用されます。

始める前に　大域ゾーンでスーパーユーザーになります。Trusted CDE ワークスペースにアクセスします。

1. **Trusted_Extensions** フォルダに移動します。
   a. 背景をマウスボタン **3** でクリックします。
   b. ワークスペースメニューで、「アプリケーション」→「アプリケーション・マネージャ」を選択します。
   c. **Trusted_Extensions** フォルダのアイコンをダブルクリックします。
      このフォルダには、インタフェース、LDAP クライアント、およびラベル付きゾーンを設定するためのアクションが含まれています。
2. 「物理インタフェースの共有」アクションをダブルクリックします。
   このアクションによって、1 つの IP アドレスを持つホストが構成されます。大域ゾーンには一意のアドレスはありません。このシステムは、マルチレベルプリンタサーバーまたは NFS サーバーとして使用できません。

3 (省略可能) 端末ウィンドウでこのアクションの結果を確認します。

```
# ifconfig -a
```

「物理インタフェースの共有」アクションで、すべてのゾーンに論理 NIC を構成します。これらの論理 NIC は、大域ゾーンで 1 つの物理的な NIC を共有します。

たとえば、次の出力は、すべてのゾーンのネットワークインタフェース `192.168.0.11` の共有物理インタフェース `hme0` を示しています。

```
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
       inet 127.0.0.1 netmask ff000000
       ether 0:0:00:00:00:0
hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
       all-zones
       inet 192.168.0.11 netmask fffffe00 broadcast 192.168.0.255
```

Solaris 10 10/08 リリースから、ループバックインタフェースの `lo0` も `all-zones` インタフェースです。

```
  lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
         all-zones
         inet 127.0.0.1 netmask ff000000
         ether 0:0:00:00:00:0
...
```

CDE アクションを使用したゾーン作成の準備 (作業マップ)

次の作業マップは、システムでのゾーン作成を準備するタスクについて示しています。ゾーンの作成方法については、26 ページの「Trusted Extensions でのゾーン計画」を参照してください。

作業	説明	参照先
1. 各ゾーンに名前を付け、ゾーン名とゾーンラベルをリンクします。	各ラベル付きゾーンにラベルのバージョンが入った名前を付け、Solaris 管理コンソール で名前とラベルを関連付けます。	161 ページの「CDE アクションを使用してゾーン名とゾーンラベルを指定する」
2. ゾーンを作成する前にネットワークを構成します。	すべてのホストで、ラベルをネットワークインタフェースに割り当て、さらに構成を行います。	『Oracle Solaris Trusted Extensions 管理の手順』の「トラステッドネットワークデータベースの構成 (作業マップ)」

▼ CDE アクションを使用してゾーン名とゾーンラベルを指定する

label_encodings ファイル中のラベルごとにゾーンを作成する必要はありませんが、作成することもできます。tnzonecfg データベースには、そのシステムでゾーンを作成できるラベルが列挙されます。

1 **Trusted_Extensions** フォルダに移動します。

   a. 背景をマウスボタン **3** でクリックします。

   b. ワークスペースメニューで、「アプリケーション」→「アプリケーション・マネージャ」を選択します。

   c. **Trusted_Extensions** フォルダのアイコンをダブルクリックします。

2 ゾーンごとにゾーンの名前を付けます。

   a. 「ゾーンを構成」アクションをダブルクリックします。

   b. プロンプトに対して名前を入力します。

   ヒント – ゾーンのラベルと似た名前をゾーンに付けます。たとえば、ラベルが CONFIDENTIAL : INTERNAL USE ONLY であるゾーンに、internal という名前を付けます。

3 ゾーンごとに「ゾーンを構成」アクションを繰り返します。

   たとえば、デフォルトの label_encodings ファイルには次のラベルが含まれています。

```
PUBLIC
CONFIDENTIAL: INTERNAL USE ONLY
CONFIDENTIAL: NEED TO KNOW
CONFIDENTIAL: RESTRICTED
SANDBOX: PLAYGROUND
MAX LABEL
```

   「ゾーンを構成」アクションを 6 回実行してラベルごとにゾーンを 1 つ作成した場合でも、次のゾーンを作成することを検討します。

   - すべてのユーザーのシステムでは、PUBLIC ラベルに 1 つのゾーン、および CONFIDENTIAL ラベルに 3 つのゾーンを作成します。
   - 開発者用のシステムでは、SANDBOX: PLAYGROUND ラベルにゾーンを 1 つ作成します。SANDBOX: PLAYGROUND は開発者用の不連続ラベルとして定義され、開発者が使用するシステムにのみ、このラベルにゾーンが必要です。

- MAX LABEL ラベルにはゾーンを作成しないでください。これは認可上限として定義されます。

4 トラステッドネットワークゾーンツールを開きます。

Solaris 管理コンソールのツールは、ユーザーエラーを防ぐように設計されています。これらのツールは、構文エラーを検査し、自動的に正しい順序でコマンドを実行してデータベースを更新します。

a. **Solaris** 管理コンソールを起動します。

```
# /usr/sbin/smc &
```

b. ローカルシステムの **Trusted Extensions** ツールボックスを開きます。

i. 「コンソール」→「ツールボックスを開く」を選択します。

ii. 「このコンピュータ (*this-host*: Scope=Files, Policy=TSOL)」という名前のツールボックスを選択します。

iii. 「開く」をクリックします。

c. 「システムの構成」にある「コンピュータとネットワーク」に移動します。
求められたらパスワードを入力します。

d. トラステッドネットワークゾーンツールをダブルクリックします。

5 ゾーンごとに、適切なラベルとゾーン名を関連付けます。

a. 「アクション」→「ゾーン構成の追加」を選択します。
ダイアログボックスに、割り当てられているラベルがないゾーンの名前が表示されます。

b. ゾーン名を確認してから「編集」をクリックします。

c. ラベルビルダーで、ゾーン名に該当するラベルをクリックします。
間違ったラベルをクリックした場合、そのラベルをもう一度クリックして選択を解除し、正しいラベルをクリックします。

d. 割り当てを保存します。
「トラステッドネットワークゾーンのプロパティー」ダイアログボックスで「了解」をクリックします。

必要なゾーンがすべてパネルに表示されたら終了です。あるいは、「ゾーン構成の追加」メニュー項目をクリックすると、ゾーン名の値がないダイアログボックスが開かれます。

注意事項 「トラステッドネットワークゾーンのプロパティー」ダイアログボックスで、作成するゾーンが表示されない場合、ゾーンネットワーク構成ファイルが存在しないか、すでに作成されています。

- ゾーンネットワーク構成ファイルが存在しないことを確認します。パネルで名前を探します。
- ファイルが存在しない場合、「ゾーンを構成」アクションを実行してゾーン名を指定します。次に、手順 5 を繰り返してファイルを作成します。

CDE アクションを使用したラベル付きゾーンの作成 (作業マップ)

トラステッドネットワークゾーン構成データベースのエントリごとに、ゾーンを 1 つ作成できます。161 ページの「CDE アクションを使用してゾーン名とゾーンラベルを指定する」の手順で「ゾーンを構成」アクションを実行することにより、エントリを作成しました。

アプリケーションマネージャーの Trusted_Extensions フォルダには、ラベル付きゾーンを作成する次のアクションが含まれています。

- ゾーンを構成 – すべてのゾーン名に対してゾーン構成ファイルを作成します
- ゾーンのインストール – 正しいパッケージとファイルシステムをゾーンに追加します
- ゾーン端末コンソール – ゾーンのイベントを表示するためのウィンドウです
- LDAP 用ゾーンを初期化 – ゾーンを LDAP クライアントにして、ゾーンの起動の準備をします
- ゾーンを起動 – ゾーンを起動し、サービス管理フレームワーク (SMF) のすべてのサービスを起動します
- ゾーンのシャットダウン – ゾーンの状態を起動から停止に変更します

タスクを次の順序で完了します。

作業	説明	参照先
1. 1 つのゾーンをインストールして起動します。	最初のラベル付きゾーンを作成します。パッケージをインストールし、ゾーンを LDAP クライアントにし、ゾーンのすべてのサービスを起動します。	164 ページの「CDE アクションを使用してラベル付きゾーンをインストール、初期化、および起動する」
2. ゾーンをカスタマイズします。	不要なサービスを削除します。ゾーンをコピーまたはゾーンのクローンを作成する場合、ゾーン固有の情報を削除します。	168 ページの「起動したゾーンを Trusted Extensions でカスタマイズする」

作業	説明	参照先
3. その他のゾーンを作成します。	次のいずれかの方法を使用してその他のゾーンを作成します。方法の選択については、47 ページの「Trusted Extensions の有効化前にシステムおよびセキュリティーに関する事項を決定する」を参照してください。	
	各ゾーンを最初から作成します。	164 ページの「CDE アクションを使用してラベル付きゾーンをインストール、初期化、および起動する」 167 ページの「Trusted CDE でローカルゾーンを大域ゾーンルーティングに解決する」 168 ページの「起動したゾーンを Trusted Extensions でカスタマイズする」
	最初のラベル付きゾーンを別のラベルにコピーします。すべてのゾーンで繰り返します。	171 ページの「ゾーンのコピー方法を Trusted Extensions で使用する」
	ZFS スナップショットを使用して、最初のラベル付きゾーンからほかのゾーンのクローンを作成します。	171 ページの「ゾーンのクローン作成方法を Trusted Extensions で使用する」

▼ CDE アクションを使用してラベル付きゾーンをインストール、初期化、および起動する

ゾーン作成ではオペレーティングシステム全体をコピーしなければならないので、このプロセスには時間がかかります。時間がかからない方法として、1 つのゾーンを作成し、それをほかのゾーンのテンプレートにして、そのゾーンテンプレートをコピーまたはクローンを作成します。

始める前に　161 ページの「CDE アクションを使用してゾーン名とゾーンラベルを指定する」を完了しています。

LDAP をネームサービスとして使用している場合は、65 ページの「Trusted Extensions で大域ゾーンを LDAP クライアントにする」を完了しています。

ゾーンのクローンを作成する場合は、59 ページの「ゾーンのクローンを作成するために ZFS プールを作成する」を完了しています。次の手順で、準備したゾーンをインストールします。

1 **Trusted_Extensions** フォルダで「ゾーンのインストール」アクションをダブルクリックします。

   a. インストールするゾーンの名前を入力します。

      このアクションによって、ラベル付き仮想オペレーティングシステムが作成されます。この手順が終了するまでしばらくお待ちください。ゾーンのインストールの実行中は、システムでその他のタスクを実行しないでください。

```
# zone-name: Install Zone
Preparing to install zone <zone-name>
Creating list of files to copy from the global zone
Copying <total> files to the zone
Initializing zone product registry
Determining zone package initialization order.
Preparing to initialize <subtotal> packages on the zone.
Initializing package <number> of <subtotal>: percent complete: percent

Initialized <subtotal> packages on zone.
Zone <zone-name> is initialized.
The file /zone/internal/root/var/sadm/system/logs/install_log
contains a log of the zone installation.

*** Select Close or Exit from the window menu to close this window ***
```

   b. コンソールを開いて、インストールされたゾーンのイベントを監視します。

      i. 「ゾーン端末コンソール」アクションをダブルクリックします。

      ii. インストールしたばかりのゾーンの名前を入力します。

2 ゾーンを初期化します。

   - **LDAP** を使用している場合は、「**LDAP** 用ゾーンを初期化」アクションをダブルクリックします。

```
Zone name:                  Type the name of the installed zone
Host name for the zone:     Type the host name for this zone
```

     たとえば、共有論理インタフェースがあるシステムでは、値は次のようになります。

```
Zone name:              public
Host name for the zone: machine1-zones
```

     このアクションによって、ラベル付きゾーンが、大域ゾーンで動作する同じ LDAP サーバーの LDAP クライアントになります。次の情報が表示されたらこのアクションは完了です。

```
zone-name zone will be  LDAP client of IP-address
zone-name is ready for booting
Zone label is LABEL
```

```
*** Select Close or Exit from the window menu to close this window ***
```

- **LDAP を使用していない場合は、次の手順のいずれかを実行して手動でゾーンを初期化します。**

  Trusted Extensions での手動の手順は、Solaris OS の手順と同一です。システムに少なくとも 1 つの `all-zones` インタフェースがある場合は、すべてのゾーンに対するホスト名が、大域ゾーンのホスト名に一致する必要があります。一般に、ゾーンの初期化中に発生する質問の回答は、大域ゾーンに対する回答と同じです。

  次のいずれかを実行してホスト情報を入力します。

  - 手順 **3** でゾーンを起動したあと、ゾーン端末コンソールでシステム特性に関する質問に答えます。

    この回答を使用してゾーンに `sysidcfg` ファイルが生成されます。

    注 – ラベル付きゾーンから大域ゾーンへの Trusted CDE デスクトップのルートが存在するようにしてください。手順については、167 ページの「Trusted CDE でローカルゾーンを大域ゾーンルーティングに解決する」を参照してください。

  - `Step 3` でゾーンを起動する前に、このゾーンの `/etc` ディレクトリに 手順 **3** カスタムファイルを置きます。

3 「ゾーンを起動」アクションをダブルクリックします。

プロンプトに答えます。

`Zone name:` *Type the name of the zone that you are configuring*

このアクションによってゾーンが起動されると、そのゾーンで実行されるすべてのサービスが起動されます。サービスの詳細は、`smf(5)` のマニュアルページを参照してください。

ゾーン端末コンソールは、ゾーン起動の進捗を追跡します。次のようなメッセージがコンソールに表示されます。

```
[Connected to zone 'public' console]

[NOTICE: Zone booting up]
...
Hostname: zonename
Loading smf(5) service descriptions: number/total
Creating new rsa public/private host key pair
Creating new dsa public/private host key pair

rebooting system due to change(s) in /etc/default/init

[NOTICE: Zone rebooting]
```

4 コンソール出力を監視します。

168 ページの「起動したゾーンを Trusted Extensions でカスタマイズする」に進む前に、ゾーンが再起動されていることを確認します。次のコンソールログインプロンプトは、ゾーンが再起動されたことを示しています。

hostname `console login:`

注意事項 ゾーンのインストールで、警告「`Installation of these packages generated errors: SUNW` *pkgname*」が表示された場合、インストールログを読み、パッケージのインストールを終了します。

▼ Trusted CDE でローカルゾーンを大域ゾーンルーティングに解決する

すべてのゾーンが Trusted CDE にアクセスできるようにするには、`DISPLAY` 変数を解決してください。Trusted CDE でこの変数を解決するには、ラベル付きゾーンのノード名、大域ゾーンのノード名、および all-zones インタフェースのノード名を同一の名前に解決します。

始める前に Trusted CDE を使用して、ラベル付きゾーンを手動で初期化します。

1 次の方法のいずれかを使用して、**Trusted CDE** をゾーンのラベルに表示できるようにします。

- 方法 **1:** ほかのシステムとの **X** サーバーのトラフィックを有効にします。
  この設定では、ラベル付きゾーンは、大域ゾーンの X サーバーを経由してほかのシステムに到達できます。

  a. `/etc/nodename` ファイルでシステムの名前を指定する必要があります。

  ```
  ## /etc/nodename
  machine1
  ```

  b. `/etc/hosts` ファイルでシステムの名前を指定する必要があります。

  ```
  ## /etc/hosts
  192.168.2.3  machine1 loghost
  ```

  ToolTalk サービスを機能させるには、システムの名前が `loghost` と同じ行にあるようにしてください。

c. `/etc/hostname.`*interface* ファイルでシステムの名前を指定する必要があります。

この設定では、`machine1` は Trusted CDE の all-zones インタフェースになります。

```
## /etc/hostname.bge0
machine1 all-zones
```

- 方法 2: X サーバーのトラフィックをローカルシステムに制限します。

この設定では、ラベル付きゾーンはローカルシステム上の X サーバーと通信できます。ただし、ローカルの X サーバーからネットワーク上のほかのシステムへのルートは存在しません。このルートでは、別のインタフェースを使用します。

a. `/etc/nodename` ファイルでシステムの名前を指定する必要があります。

```
## /etc/nodename
machine1
```

b. `/etc/hosts` ファイルでシステムの名前を指定する必要があります。

Solaris 10 10/08 リリースから、`lo0` は all-zones インタフェースです。この場合、このファイルは次のようになります。

```
## /etc/hosts
127.0.0.1  localhost  machine1 loghost
```

また、`vni0` インタフェースも使用できます。

ToolTalk サービスを機能させるには、システムの名前を `loghost` と同じ行に指定してください。

- 方法 3: ゾーンごとの論理インタフェースでの経路指定可能なアドレスなど、別の方法で `DISPLAY` 変数を解決します。

この手順については、85 ページの「ネットワークインタフェースをラベル付きゾーンに追加し、ルーティングする」を参照してください。

2 ゾーンを起動するには、手順 3 の 164 ページの「CDE アクションを使用してラベル付きゾーンをインストール、初期化、および起動する」 に戻ります。

▼ 起動したゾーンを Trusted Extensions でカスタマイズする

ゾーンのクローンを作成する場合、この手順によって、ゾーンがほかのゾーンのテンプレートになるように構成します。さらに、この手順でゾーンを使用するよう構成します。

1 ゾーンが完全に起動されていることを確認します。

a. *zone-name*: ゾーン端末コンソールで、**root** としてログインします。

```
hostname console login: root
Password:       Type root password
```

b. ゾーンが実行されていることを確認します。

STATUS が `running` の場合は、ゾーン内で少なくとも 1 つのプロセスが実行中であることを示します。

```
# zoneadm list -v
ID NAME         STATUS         PATH
 2 public       running        /
```

c. ゾーンが大域ゾーンと通信できることを確認します。

X サーバーが大域ゾーンで実行されます。それぞれのラベル付きゾーンがこのサービスを使用するには、大域ゾーンに接続できなければなりません。そのため、ゾーンネットワークが機能しなければ、ゾーンを使用することはできません。詳細は、111 ページの「ラベル付きゾーンが X サーバーにアクセスできない」を参照してください。

2 ゾーン端末コンソールで、ラベル付きゾーンで不要なサービスを無効にします。

このゾーンをコピーまたはクローンを作成する場合、無効にしたサービスは新しいゾーンで無効にされます。システムでオンラインであるサービスは、そのゾーンのサービスマニフェストによって異なります。`netservices limited` コマンドを使用して、ラベル付きゾーンで必要としないサービスをオフにします。

a. 多数の不要なサービスを削除します。

```
# netservices limited
```

b. そのほかのサービスを一覧にします。

```
# svcs
...
STATE        STIME      FMRI
online       13:05:00   svc:/application/graphical-login/cde-login:default
...
```

c. グラフィカルログインを無効にします。

```
# svcadm disable svc:/application/graphical-login/cde-login
# svcs cde-login
STATE        STIME      FMRI
disabled     13:06:22   svc:/application/graphical-login/cde-login:default
```

サービス管理フレームワークの詳細は、`smf(5)` のマニュアルページを参照してください。

3 ゾーンをシャットダウンします。
次の方法のいずれかを選択します。

- 「ゾーンのシャットダウン」アクションを実行します。
  ゾーンの名前を入力します。
- 大域ゾーンの端末ウィンドウで、zlogin コマンドを使用します。

  ```
  # zlogin zone-name init 0
  ```

  詳細は、zlogin(1) のマニュアルページを参照してください。

4 ゾーンがシャットダウンされたことを確認します。
zone-name: ゾーン端末コンソールで、次のメッセージによって、ゾーンがシャットダウンされていることが示されます。

```
[ NOTICE: Zone halted]
```

このゾーンをコピーまたはそのクローンを作成するのではない場合、この最初のゾーンを作成したのと同じ方法で残りのゾーンを作成します。

5 このゾーンをほかのゾーンのテンプレートとして使用する場合、次のとおりに実行します。

a. auto_home_*zone-name* ファイルを削除します。
大域ゾーンの端末ウィンドウで、*zone-name* ゾーンからこのファイルを削除します。

```
cd /zone/zone-name/root/etc
# ls auto_home*
auto_home  auto_home_zone-name
# rm auto_home_zone-name
```

たとえば、public ゾーンをほかのゾーンのクローン作成元にした場合、その auto_home ファイルを次のように削除します。

```
# cd /zone/public/root/etc
# rm auto_home_public
```

次の手順
- ゾーンをコピーしている場合は、171 ページの「ゾーンのコピー方法を Trusted Extensions で使用する」に進みます。
- ゾーンのクローンを作成している場合は、171 ページの「ゾーンのクローン作成方法を Trusted Extensions で使用する」に進みます。

▼ ゾーンのコピー方法を Trusted Extensions で使用する

始める前に
- 161 ページの「CDE アクションを使用してゾーン名とゾーンラベルを指定する」を完了しています。
- 163 ページの「CDE アクションを使用したラベル付きゾーンの作成 (作業マップ)」でクローンを作成するためのテンプレートとなるゾーンをカスタマイズしています。
- クローン作成用のテンプレートであるゾーンが、現在実行されていません。
- Trusted_Extensions フォルダが表示されています。

1 作成したいゾーンごとに、「ゾーンをコピー」アクションをダブルクリックします。

プロンプトに答えます。

```
New Zone Name:          Type name of target zone
From Zone Name:         Type name of source zone
```

注意 – このタスクの実行中は、ほかのタスクを実行しないでください。

2 ゾーンが作成されたら、すべてのゾーンのステータスをチェックします。

a. 「ゾーン端末コンソール」アクションをダブルクリックします。

b. 各ゾーンにログインします。

c. 80 ページの「ゾーンのステータスを確認する」を完了します。

▼ ゾーンのクローン作成方法を Trusted Extensions で使用する

始める前に
- 161 ページの「CDE アクションを使用してゾーン名とゾーンラベルを指定する」を完了しています。
- 59 ページの「ゾーンのクローンを作成するために ZFS プールを作成する」を完了しています。
- 59 ページの「ゾーンのクローンを作成するために ZFS プールを作成する」を完了して、ゾーンテンプレートを作成しています。
- 163 ページの「CDE アクションを使用したラベル付きゾーンの作成 (作業マップ)」でクローン作成用のテンプレートとなるゾーンをカスタマイズしています。
- クローン作成用のテンプレートとなるゾーンは、シャットダウンされています。
- Trusted_Extensions フォルダが表示されています。

1 ゾーンテンプレートの **Solaris ZFS** スナップショットを作成します。

```
# cd /
# zfs snapshot zone/zone-name@snapshot
```

このスナップショットを使用して、そのほかのゾーンのクローンを作成します。`public` という名前の構成済みゾーンの場合、スナップショットコマンドは次のようになります。

```
# zfs snapshot zone/public@snapshot
```

2 作成したいゾーンごとに、「ゾーンのクローンを作成」アクションをダブルクリックします。

プロンプトに答えます。

```
New Zone Name:          Type name of source zone
ZFS Snapshot:             Type name of snapshot
```

3 ダイアログボックスの情報を読みます。

```
Zone label is <LABEL>
zone-name is ready for booting

*** Select Close or Exit from the window menu to close this window ***
```

4 ゾーンごとに「ゾーンを起動」アクションを実行します。

別のゾーンに対するアクションを実行する前に、それぞれのゾーンを起動します。

5 ゾーンが作成されたあと、すべてのゾーンのステータスをチェックします。

a. 「ゾーン端末コンソール」アクションをダブルクリックします。

b. **80** ページの「ゾーンのステータスを確認する」を完了します。

◆ ◆ ◆ 付録 C

Trusted Extensions の構成チェックリスト

このチェックリストでは、Trusted Extensions. の主な構成タスクの概要を示します。これらの主なタスクに、細かいタスクの概略が含まれています。このチェックリストだけでは、このマニュアルに記述されている各手順を実行することはできません。

Trusted Extensions を構成するためのチェックリスト

次のリストは、サイトで Trusted Extensions を有効化および構成するために必要な事項を示します。ほかの場所に記載されているタスクは、相互参照されます。

1. 次を参照します。
   - 『Oracle Solaris Trusted Extensions 管理の手順』の最初の 5 つの章を読みます。
   - サイトのセキュリティー要件を把握します。
   - 150 ページの「サイトのセキュリティーポリシーと Trusted Extensions」を読みます。
2. 次の準備をします。
   - `root` パスワードを決定します。
   - PROM または BIOS のセキュリティーレベルを決定します。
   - PROM または BIOS のパスワードを決定します。
   - 周辺機器の接続を許可するかを決定します。
   - 遠隔プリンタへのアクセスを許可するかを決定します。
   - ラベルなしネットワークへのアクセスを許可するかを決定します。
   - ゾーン作成方法を決定します。
3. Trusted Extensions を有効にします。
   a. Solaris OS をインストールします。
      - 遠隔管理の場合、開発者グループか、それより大きなグループの Solaris パッケージをインストールします。

- ゾーンのクローン作成メソッドの場合、カスタムインストールを選択し、/zone パーティションを配置します。

b. Trusted Extensions サービス svc:/system/labeld を有効にします。

4. Trusted Extensions の IPv6 を有効化します (IPv6 を使用する場合)。
5. 1 以外の DOI を使用する場合には、/etc/system および /etc/security/tsol/tnrhtp ファイル内にその DOI を設定します。
6. (省略可能) ゾーンのクローン作成用の ZFS プールを作成します。
7. ラベルを設定します。
   a. サイトの label_encodings ファイルをファイナライズします。
   b. ファイルをチェックしてインストールします。
   c. 再起動します。
8. 大域ゾーン用およびラベル付きゾーン用のインタフェースを設定します。
9. Solaris 管理コンソールを設定します。
10. ネームサービスを設定します。
    - ファイルネームサービスを使用します。これに必要な設定はありません。
    - または、LDAP を設定します。
      a. Trusted Extensions プロキシサーバーまたは Trusted Extensions LDAP サーバーを作成します。
      b. Solaris 管理コンソール サーバーがネットワーク接続を受け付けるようにします。
      c. Solaris 管理コンソール を LDAP に登録します。
      d. Solaris 管理コンソール 用の LDAP ツールボックスを作成します。
11. LDAP 用のネットワーク接続を設定します。
    - LDAP サーバーまたはプロキシサーバーを遠隔ホストテンプレートの cipso ホストタイプに割り当てます。
    - ローカルシステムを遠隔ホストテンプレートの cipso ホストタイプに割り当てます。
    - ローカルシステムを LDAP サーバーのクライアントにします。
12. ラベル付きゾーンを作成します。
    - オプション 1: txzonemgr スクリプト を使用します。
    - オプション 2: Trusted CDE アクションを使用します。
      a. ラベル付きゾーンの設定
         i. Solaris 管理コンソール で、ゾーン名を特定のラベルに関連付けます。
         ii. 「ゾーンを構成」アクションを実行します。
      b. 「ゾーンのインストール」アクションを実行します。
      c. 「LDAP 用ゾーンを初期化」アクションを実行します。

d. 「ゾーンを起動」アクションを実行します。
e. 実行中のゾーンをカスタマイズします。
f. 「ゾーンのシャットダウン」アクションを実行します。
g. ゾーンのシャットダウン中にゾーンをカスタマイズします。
h. (省略可能) ZFS スナップショットを作成します。
i. 残りのゾーンを最初から作成するか、「ゾーンをコピー」アクションまたは「ゾーンのクローンを作成」アクションを使用して作成します。

13. ネットワークを設定します。『Oracle Solaris Trusted Extensions 管理の手順』の「トラステッドネットワークデータベースの構成 (作業マップ)」を参照してください。
    - 単一ラベルのホストおよび制限範囲のホストを特定します。
    - ラベルなしホストからの受信データに適用するラベルを決定します。
    - 遠隔ホストテンプレートをカスタマイズします。
    - 各ホストをテンプレートに割り当てます。
    - サブネットをテンプレートに割り当てます。
14. 静的経路指定を設定します。『Oracle Solaris Trusted Extensions 管理の手順』の「Trusted Extensions での経路の構成とネットワーク情報のチェック (作業マップ)」を参照してください。
15. ローカルユーザーおよびローカル管理役割を設定します。
    - 責務分離を強制するには、カスタマイズした権利プロファイルを作成します。
    - セキュリティー管理者役割を作成します。
    - セキュリティー管理者役割になれるローカルユーザーを作成します。
    - その他の役割を作成し、場合によって、その役割になるローカルユーザーを作成します。
16. NFS サーバーにホームディレクトリを作成します。
    - ユーザーがアクセスできるすべてのラベルでユーザーごとにホームディレクトリを作成します。
    - (省略可能) 下位レベルのホームディレクトリをユーザーが読み取れないようにします。
17. 印刷を設定します。『Oracle Solaris Trusted Extensions 管理の手順』の「Trusted Extensions での印刷の管理 (作業マップ)」を参照してください。
18. デバイスを設定します。『Oracle Solaris Trusted Extensions 管理の手順』の「Trusted Extensions でのデバイスの扱い (作業マップ)」を参照してください。
    a. デバイス管理プロファイルまたはシステム管理者プロファイルを役割に割り当てます。
    b. デバイスを使用可能にするには、次のいずれかを実行します。
        - システムごとに、デバイスを割り当て可能にします。

- 選択したユーザーおよび役割にデバイスの割り当て承認を割り当てます。

19. Solaris 機能を構成します。
    - 監査を設定します。
    - セキュリティーの設定を設定します。
    - 特定の LDAP クライアントが LDAP 管理システムになるようにします。
    - LDAP でユーザーを設定します。
    - LDAP でネットワークの役割を設定します。
    - ファイルシステムをマウントおよび共有します。『Oracle Solaris Trusted Extensions 管理の手順』の第 11 章「Trusted Extensions でのファイルの管理とマウント (手順)」を参照してください。

用語集

CDE 共通デスクトップ環境を参照。

CIPSO ラベル 共通 IP セキュリティーオプション (Common IP Security Option)。CIPSO は、Trusted Extensions が実装するラベル標準です。

.copy_files ファイル マルチラベルシステムに関する任意の設定ファイル。このファイルには、システムまたはアプリケーションが正常に動作するためにユーザー環境またはユーザーアプリケーションで必要とされる `.cshrc`、`.mozilla` などの起動ファイルのリストが含まれます。ユーザーのホームディレクトリが高いラベルで作成されると、`.copy_files` に含まれるファイルがそのディレクトリにコピーされます。.link_files ファイルも参照。

DAC 任意アクセス制御を参照。

GFI 政府提供情報 (Government Furnished Information の略)。このマニュアルでは、米国政府提供の label_encodings ファイルを指します。Trusted Extensions ソフトウェアで GFI を使用するには、Sun 固有の `LOCAL DEFINITIONS` セクションを GFI の末尾に追加します。詳細は、『Solaris Trusted Extensions ラベルの管理』の第 5 章「LOCAL DEFINITIONS のカスタマイズ」を参照してください。

IP アドレス インターネットプロトコル (Internet Protocol、IP) アドレス。インターネットプロトコルによって通信が可能になるための、ネットワークに接続されたシステムを識別する一意の数字。IPv4 のアドレスは、ピリオドで区切られた 4 つの数字です。通常、IP アドレスの各部は 0 から 225 です。ただし、最初の数字は 224 未満とし、最後の数字は 0 以外にしてください。

IP アドレスは、論理的に、ネットワークの部分と ネットワーク上のsystemの部分に分けられます。ネットワーク番号は電話番号の市外局番、システム番号はそれ以外の電話番号に相当します。

label オブジェクトに割り当てられるセキュリティー識別子。ラベルは、オブジェクトの情報を保護するレベルを基準にします。セキュリティー管理者がどのようにユーザーを設定したかによって、ユーザーは機密ラベルを参照できたりできなかったりします。ラベルはlabel_encodings ファイルで定義されます。

label_encodings ファイル 認可範囲、ラベルビュー、デフォルトのラベル表示/非表示、デフォルトのユーザー認可上限、およびその他のラベルに関する事項を含む完全な機密ラベルを定義するファイル。

.link_files ファイル　マルチラベルシステムに関する任意の設定ファイル。このファイルには、システムまたはアプリケーションが正常に動作するためにユーザー環境またはユーザーアプリケーションで必要とされる `.cshrc`、`.mozilla` などの起動ファイルのリストが含まれます。ユーザーのホームディレクトリが高いラベルで作成されると、`.link_files` に含まれるファイルがそのディレクトリにリンクされます。.copy_files ファイルも参照。

MAC　必須アクセス制御を参照。

process　コマンドを呼び出したユーザーに代わってコマンドを実行するアクション。プロセスは、ユーザー ID (UID)、グループ ID (GID)、補助グループリスト、ユーザーの監査 ID (AUID) などの多数のセキュリティー属性をユーザーから受け取ります。プロセスが受け取るセキュリティー属性には、実行されるコマンドが使用可能な特権、および現在のワークスペースの機密ラベルも含まれます。

Solaris 管理コンソール　管理プログラムのツールボックスを含む Java ベースの管理 GUI。このコンソールのツールボックスを使用することによって、システム、ネットワーク、およびユーザーのほとんどの管理を行えます。

system　コンピュータの総称。インストール後、ネットワーク上のシステムはホストとも呼ばれます。

tnrhdb データベース　トラステッドネットワークの遠隔ホストデータベース。このデータベースは、ラベル特性のセットを遠隔ホストに割り当てます。アクセスは、`/etc/security/tsol/tnrhdb` のファイルとして、または LDAP サーバーから可能です。

tnrhtp データベース　トラステッドネットワークの遠隔ホストテンプレート。このデータベースは、遠隔ホストに割り当てることができるラベル特性のセットを定義します。アクセスは、`/etc/security/tsol/tnrhtp` のファイルとして、または LDAP サーバーから可能です。

txzonemgr スクリプト　`/usr/sbin/txzonemgr` スクリプトは、ラベル付きゾーンを管理するための簡単な GUI を提供します。また、このスクリプトはネットワークオプションやネームサービスオプションのメニュー項目、および大域ゾーンを既存の LDAP サーバーのクライアントにするためのメニュー項目も提供します。`txzonemgr` は、root ユーザーによって大域ゾーンで実行されます。

アクセス権ビット　ファイルやディレクトリをだれが読み取り、書き込み、または実行できるかを表すために、所有者が一連のビットを指定する任意アクセス制御の一種。各ファイルまたはディレクトリに割り当てられるアクセス権には、所有者に設定されるセット、所有者のグループに設定されるセット、その他のすべてに設定されるセットの 3 つがあります。

アプリケーション検索パス　CDE で、systemがアプリケーションや特定の構成情報を見つけるために使用する検索パス。アプリケーション検索パスはトラステッド役割によって制御されます。

遠隔ホスト　ローカルシステムとは異なるシステム。遠隔ホストは、ラベルなしホストまたはラベル付きホストになります。

オープンネットワーク　ほかのネットワークと物理的に接続され、Trusted Extensions ソフトウェアを使用して Trusted Extensions 以外のホストと通信する Trusted Extensions ホストのネットワーク。閉じたネットワークと比較。

解釈ドメイン (DOI)
: Trusted Extensions が構成された Solaris システム上で、解釈ドメインは、類似のラベルが定義される可能性のある label_encodings ファイル同士を区別するために使用されます。DOI は、ネットワークパケット上のセキュリティー属性をローカルの label_encodings ファイルによる表現に変換するための規則セットです。同一の DOI を持つシステムはその規則セットを共有しており、ラベル付きのネットワークパケットを変換できます。

格付け
: 認可上限またはlabelの階層構成要素。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。

管理役割
: 役割が管理タスクを実行できるように、必要な承認、特権コマンド、特権アクション、およびトラステッドパスのセキュリティー属性を付与する役割。役割は、バックアップ、監査など、Solaris スーパーユーザーの権限のサブセットを実行します。

機密ラベル
: オブジェクトまたはプロセスに割り当てられるセキュリティーlabel。このラベルは、含まれるデータのセキュリティーレベルに従ってアクセスを制限するために使用します。

共通デスクトップ環境
: Trusted Extensions ソフトウェアの管理用に以前から使用されているウィンドウ表示環境。Trusted Extensions で環境を変更して Trusted CDE を作成します。Trusted JDS を作成するには、Sun Java Desktop System も変更します。

クライアント
: ネットワークに接続されているシステム。

権利プロファイル
: コマンドとCDE アクションのバンドルのための、および実行可能ファイルに割り当てられているセキュリティー属性のバンドルのためのメカニズム。権利プロファイルによって、Solaris 管理者は、だれがどのコマンドを実行できるかを制御でき、また、コマンドが実行されるときのコマンドの属性を制御できます。ユーザーはログインすると、ユーザーに割り当てられているすべての権利が有効になり、ユーザーのすべての権利プロファイルで割り当てられているすべてのコマンド、CDE アクション、および承認にアクセスできます。

コンパートメント
: label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labelを形成します。コンパートメントは、技術部署や学際的プロジェクトチームなどに使用される、情報の集合を表すために使われます。

最下位ラベル
: ユーザーの機密ラベルの下限とシステムの機密ラベルの下限。ユーザーのセキュリティー属性の指定の際にセキュリティー管理者によって設定される最下位ラベルは、ユーザーが最初にログインするときの最初のワークスペースの機密ラベルです。label_encodings ファイルの最下位ラベルのフィールドでセキュリティー管理者によって指定される機密ラベルがシステムの下限を設定します。

システム管理者
: Trusted Extensions において、ユーザーアカウントの設定のうちセキュリティーに関連しない部分など、標準的なシステム管理タスクの実行を担当するユーザーに割り当てられるトラステッド役割。セキュリティー管理者と比較。

システム認可範囲
: セキュリティー管理者が label_encodings ファイルで定義する規則に従って作成されるすべての有効なlabelのセットと、Trusted Extensions が設定されたすべてのシステムで使用される 2 つの管理labelを含ませたもの。その 2 つの管理ラベルは ADMIN_LOW と ADMIN_HIGH です。

主管理者	組織に対する新しい権利プロファイルの作成を任せられ、セキュリティー管理者とシステム管理者が一緒になっても困難なマシンの問題の解決を任せられる管理者。この役割が使用されることはほとんどありません。最初のセキュリティー構成のあとで、サイトをより安全にするためには、この役割の作成をやめたり、主管理者プロファイルをいずれの役割にも割り当てないようにします。
承認	セキュリティーポリシーによって許可されないアクションを実行できるように、ユーザーまたは役割に付与する権利。承認は権利プロファイルで付与されます。特定のコマンドが成功するには、ユーザーに特定の承認が必要です。たとえば、PostScript ファイルを印刷するには、Postscript 印刷の承認が必要です。
初期設定チーム	Trusted Extensions ソフトウェアの有効化および構成を監督する、最低 2 人のチーム。セキュリティーに関する決定とシステム管理に関する決定を別々のチームメンバーが担当します。
初期ラベル	ユーザーまたは役割に割り当てられる最下位ラベルであり、ユーザーの初期ワークスペースのラベル。 初期ラベルは、ユーザーまたは役割が作業できる最下位ラベルです。
責務分離	ユーザーの作成および認証に 2 人の管理者または 2 つの役割を必要とするセキュリティーポリシー。一方の管理者または役割には、ユーザー、ユーザーのホームディレクトリ、およびその他の基本的な管理を作成する責任があります。もう一方の管理者または役割には、パスワードおよびラベル範囲など、ユーザーのセキュリティー属性に対して責任があります。
セキュリティー管理者	機密情報を保護しなければならない組織において、サイトのセキュリティーポリシーを定義および実施する人員。この人物は、サイトで処理されているすべての情報へのアクセスが認められています。ソフトウェアで、適切な認可上限を持つ 1 人以上に対してセキュリティー管理者の管理役割が割り当てられます。この管理者は、ソフトウェアによってサイトのセキュリティーポリシーが実施されるように、すべてのユーザーおよびホストのセキュリティー属性を設定します。システム管理者と比較。
セキュリティー属性	Trusted Extensions セキュリティーポリシーを実施するために使用される属性。さまざまなセットのセキュリティー属性が、process、ユーザー、ゾーン、ホスト、割り当て可能なデバイス、およびその他のオブジェクトに割り当てられます。
セキュリティーポリシー	Trusted Extensions ホスト上の、DAC、MAC、および情報へのアクセス方法を定義するラベル付け規則のセット。また、顧客サイトについて、そのサイトで処理される情報の機密度と、承認されていないアクセスから情報を保護する手段を定義する規則のセット。
セキュリティーラベルセット	tnrhtp データベースエントリに対して個別セットのセキュリティーラベルを指定します。セキュリティーラベルセットとともにテンプレートに割り当てられているホストは、そのラベルセットのいずれかのラベルに一致するパケットを送受信できます。

ツールボックス　Solaris 管理コンソールのプログラムの集まり。Trusted Extensions ホストで、管理者が Policy=TSOL のツールボックスを使用します。各ツールボックスには、ツールボックスのスコープで使用可能なプログラムがあります。たとえば、システムの tnzonecfg データベースを処理するトラステッドネットワークゾーンツールは、スコープが常にローカルであるため、Files ツールボックスにのみあります。ユーザーアカウントプログラムはすべてのツールボックスにあります。ローカルユーザーを作成するには、管理者は Files ツールボックスを使用し、ネットワークユーザーを作成するには、LDAP ツールボックスを使用します。

デバイス　デバイスには、プリンタ、コンピュータ、テープドライブ、フロッピードライブ、CD-ROM ドライブ、DVD ドライブ、オーディオデバイス、および内蔵擬似端末デバイスがあります。デバイスは、「同位読み取り、同位書き込み」の MAC ポリシーに従います。DVD ドライブなどのリムーバブルデバイスへのアクセスはデバイスの割り当てによって制御されます。

デバイスの割り当て　割り当て可能なデバイスの情報を、そのデバイスを割り当てたユーザー以外の者がアクセスできないように保護するメカニズム。デバイスが割り当て解除されるまで、デバイスを割り当てたユーザー以外の者がデバイスに関連付けられている情報にアクセスすることはできません。ユーザーがデバイスを割り当てるには、セキュリティー管理者によってデバイス割り当ての承認がユーザーに付与されている必要があります。

閉じたネットワーク　Trusted Extensions が設定されているシステムのネットワーク。このネットワークは Trusted Extensions 以外のホストから切り離されています。Trusted Extensions ネットワークの外へ配線せずに物理的に切り離すことができます。あるいは、Trusted Extensions ホストが Trusted Extensions ホストのみを認識するようにソフトウェアで切り離すことができます。ネットワークの外側からのデータ入力は、Trusted Extensions ホストに接続された周辺機器に制限されます。オープンネットワークと比較。

特権　コマンドを実行中のプロセスに付与される権限。完全セットの特権は、基本機能から管理機能に至るまでのシステムの完全機能です。システムクロックの設定などのセキュリティーポリシーをバイパスする特権は、サイトのセキュリティー管理者が付与できます。

ドメイン　インターネットのネーミング階層の一部。ローカルネットワーク上の system のグループであり、管理ファイルを共有します。

ドメイン名　ローカルネットワーク上の system のグループを識別します。ドメイン名は、ピリオドで区切られた一連の構成要素名から構成されます (たとえば、example1.town.state.country.org)。ドメイン名内で右側にある構成要素名ほど、より大きな管理権限領域 (通常は遠隔) を表します。

トラステッドエディタ　Trusted Extensions が設定された Solaris システムでは、管理ファイルの作成および変更にトラステッドエディタが使用されます。このエディタではファイル名を変更できません。また、エディタの使用は監査され、シェルエスケープコマンドは無効になっています。Trusted CDE では、「管理エディタ」アクションでトラステッドエディタを起動します。Trusted JDS では、/usr/dt/bin/trusted_edit コマンドでトラステッドエディタを起動します。

トラステッドストライプ	なりすましができない領域。トラステッドストライプは、Trusted CDE では画面下部にあり、Trusted JDS では上部にあります。このストライプには、トラステッドパスインジケータとウィンドウ機密ラベルによって、ウィンドウシステムの状態に関するフィードバックが視覚的に表示されます。機密ラベルがユーザーに表示されないように設定されている場合、トラステッドストライプはアイコンになって、トラステッドパスインジケータのみが表示されます。
トラステッドネットワークデータベース	`tnrhtp` (トラステッドネットワークの遠隔ホストテンプレート) および `tnrhdb` (トラステッドネットワークの遠隔ホストデータベース) によって、Trusted Extensions システムが通信できる遠隔ホストが定義されます。
トラステッドパス	Trusted Extensions が構成された Solaris システム上のトラステッドパスは、システムと対話するための、改ざん耐性を備えた信頼できる方法です。トラステッドパスを使えば、管理機能が損なわれることがなくなります。パスワードの変更など、保護する必要のあるユーザー機能でもトラステッドパスが使用されます。トラステッドパスがアクティブになっていると、改ざん耐性インジケータがデスクトップに表示されます。
トラステッド役割	管理役割を参照。
任意アクセス制御	ファイルまたはディレクトリの所有者の判断によって付与または拒否されるアクセスのタイプ。Trusted Extensions には、UNIX アクセス権ビット と ACL の 2 種類の任意アクセス制御 (discretionary access control、DAC) があります。
認可上限	ユーザーが作業可能なラベルのセットの上限。下限はセキュリティー管理者が割り当てる最下位ラベルです。認可上限は、セッション認可上限とユーザー認可上限の 2 種類があります。
認可範囲	ユーザーまたはリソースのクラスに認可された機密ラベルのセット。有効なlabelのセット。システム認可範囲とユーザー認可範囲も参照。
ネームサービス	ネットワーク上の全systemに関する重要なシステム情報が収められている分散型ネットワークデータベース。ネットワーク上のシステムは、これを利用して相互通信を行います。ネームサービスを使用することによって、ネットワーク全域にわたるシステム情報を保守、管理、または取得できます。Sun は LDAP ネームサービスをサポートします。ネームサービスを使用しないと、各systemはローカルの `/etc` ファイルにシステム情報のコピーを保持しなければなりません。
ネットワークに接続されたシステム	ハードウェアとソフトウェアによって接続され、ローカルエリアネットワーク (LAN) とも呼ばれるシステムのグループ。システムをネットワークに接続するには、通常、1 台以上のサーバーが必要です。
ネットワークに接続されていないシステム	ネットワークに接続されていない、またはほかのホストに依存しないコンピュータ。
必須アクセス制御	ファイル、ディレクトリ、またはデバイスの機密ラベルとそれにアクセスしようとするプロセスの機密ラベルとの比較に基づくアクセス制御。あるラベルのプロセスが下位のラベルのファイルを読み取ろうとする場合、MAC 規則の「同位読み取り、下位読み取り」が適用されます。あるラベルのプロセスが別のラベルのディレクトリに書き込もうとする場合、MAC 規則の「同位書き込み、下位読み取り」が適用されます。

評価外の構成
: 評価された構成の基準を満たすと認められているソフトウェアがセキュリティーの基準を満たさない設定で構成される場合、そのソフトウェアは「評価外の構成」と呼ばれます。

評価された構成
: 認証局によって特定の基準に適合すると認定された構成で実行されている 1 つ以上の Trusted Extensions ホスト。米国での基準は TCSEC です。評価と認定を行うのは NSA です。

  - Solaris 10 11/06 リリースで設定されている Trusted Extensions ソフトウェアでは、多数の保護プロファイルが、ISO 標準である共通基準 v2.3 (2005 年 8 月) の評価保証レベル (EAL) 4 に認定されます。
  - NSA に認定された Trusted Extensions ソフトウェアは保証継続 (Assurance Continuity) を通して Solaris 10 5/09 リリースに設定されます。

  共通基準 v2 (CCv2) と保護プロファイルによって、以前の TCSEC U.S. 標準はレベル B1+ まで廃止されます。CCv2 に関する相互認証協定が米国、英国、カナダ、デンマーク、オランダ、ドイツ、およびフランスで調印されています。

  Trusted Extensions 構成ターゲットは、TCSEC C2 レベルと B1 レベルと同様の機能および一部の追加機能を示します。

ファイルシステム
: 論理的階層に編成および構成した情報のセットをなすファイルおよびディレクトリの集まり。ファイルシステムはローカル system または遠隔システムからマウントできます。

プロファイルシェル
: 特権、承認、特殊な UID や GID などのセキュリティー属性を認識する特別なシェル。通常、プロファイルシェルは、ユーザーが使用できるコマンドを制限しますが、より多くの権限がある場合にはそれらのコマンドを実行できるようにすることも可能です。プロファイルシェルは、トラステッド役割のデフォルトのシェルです。

ホスト名
: ネットワーク上のその他の system によって認識される、システムの名前。この名前は、ドメイン内のすべての system で一意です。通常、ドメインは単一の組織を表します。ホスト名は、文字、数字、マイナス符号 (–) を任意に組み合わせて作成できますが、先頭と末尾にマイナス符号は使用できません。

マルチレベルデスクトップ
: Trusted Extensions が構成された Solaris システムでは、ユーザーはある特定のラベルでデスクトップを実行できます。複数ラベルでの作業を承認されたユーザーは、各ラベルで作業するためのワークスペースを、ラベルごとに 1 つずつ作成できます。このマルチレベルデスクトップでは、承認済みユーザーは、異なるラベルのウィンドウ間でカット & ペーストを行なったり、さまざまなラベルでメールを受信したり、異なるラベルのワークスペース内でラベル付きウィンドウを表示して使用したりできます。

マルチレベルポート **(MLP)**
: Trusted Extensions が構成された Solaris システムでは、MLP は、あるゾーン内でマルチレベルサービスを提供するために使用されます。デフォルトでは、X サーバーは大域ゾーン内で定義されたマルチレベルサービスです。MLP はポート番号とプロトコルで指定されます。たとえば、マルチレベルデスクトップ用の X サーバーの MLP は、6000-6003 と TCP によって指定されます。

役割
: 役割は、ログインできないことを除いて、ユーザーと同じです。通常、管理機能を割り当てるために役割が使用されます。役割は、コマンド、承認、および CDE アクションの特定セットに制限されます。管理役割を参照。

ユーザー認可上限　セキュリティー管理者によって割り当てられる認可上限で、ユーザーが常に作業可能なlabelのセットの上限を設定します。ユーザーは、ログインセッション時にデフォルトを受け入れたり、認可上限をさらに制限したりできます。

ユーザー認可範囲　一般ユーザーがsystemで作業できるすべての可能なラベルのセット。サイトのセキュリティー管理者が label_encodings ファイルで範囲を指定します。システム認可範囲を定義する適格な形式のlabelに関する規則は、このファイルの ACCREDITATION RANGE セクションの値 (上限、下限、組み合わせ制約など) によってさらに制限されます。

ラベル間の関係　Trusted Extensions が構成された Solaris システムでは、あるラベルは、別のラベルよりも上位である、別のラベルと等しい、別のラベルから切り離されている、のいずれかになります。たとえば、ラベル Top Secret はラベル Secret よりも上位です。2 つのシステムが同じ解釈ドメイン (DOI) を持つ場合、一方のラベル Top Secret は他方のラベル Top Secret と等しくなります。

ラベル構成　単一ラベルまたはマルチラベルの機密ラベルに関する Trusted Extensions インストール時の選択。ほとんどの環境では、サイトのすべてのシステムでラベル構成は同一です。

ラベルセット　セキュリティーラベルセットを参照。

ラベル付きシステム　ラベル付きシステムとは、Trusted Extensions や MLS が有効化された SELinux など、マルチレベルオペレーティングシステムが実行されているシステムのことです。このシステムは、共通 IP セキュリティーオプション (CIPSO) でラベル付けされたヘッダーを含むネットワークパケットを送受信できます。

ラベル付きゾーン　Trusted Extensions が構成された Solaris システムでは、すべてのゾーンに一意のラベルが割り当てられます。大域ゾーンもラベル付けされますが、ラベル付きゾーンは通常、 ラベルが割り当てられた非大域ゾーンを指します。ラベル付きゾーンは、ラベルが構成されていない Solaris システム上の非大域ゾーンとは異なる特性を 2 つ備えています。第 1 に、ラベル付きゾーンは同じプールのユーザー ID とグループ ID を使用する必要があります。第 2 に、ラベル付きゾーンは IP アドレスを共有できます。

ラベル付きホスト　複数のラベル付きシステムから成るトラステッドネットワークの一部をなすラベル付きシステム。

ラベルなしシステム　Trusted Extensions が構成された Solaris システムにとって、ラベルなしシステムとは、Trusted Extensions や MLS が有効化された SELinux などのマルチレベルオペレーティングシステムが実行されていないシステムのことです。ラベルなしシステムはラベル付きパケットを送信しません。通信中の Trusted Extensions システムがある単一のラベルをラベルなしシステムに割り当てた場合、その Trusted Extensions システムとラベルなしシステムとの間のネットワーク通信は、そのラベルで行われます。ラベルなしシステムは「シングルレベルシステム」とも呼ばれます。

ラベルなしホスト　Solaris OS を実行するシステムなど、ラベルなしネットワークパケットを送信する、ネットワークに接続されたシステム。

ラベル範囲	コマンド、ゾーン、および割り当て可能デバイスに割り当てられている機密ラベルのセット。最上位ラベルと最下位ラベルを指定することによってこの範囲を指定します。コマンドの場合、最上位ラベルと最下位ラベルは、コマンドが実行されるラベルを制限します。ラベルを認識しない遠隔ホストには、セキュリティー管理者が 1 つのラベルに制限するその他のホストと同様に、1 つの機密ラベルが割り当てられます。ラベル範囲は、デバイスが割り当てられるラベルを制限し、そのデバイスを使用する場合に情報が格納または処理されるラベルを制限します。
割り当て	デバイスへのアクセスを制御するメカニズム。デバイスの割り当てを参照。

索引

A

Action failed. Reconnect to Solaris Zone?，111-113

C

Cannot reach global zone，111-113
CDE アクションを使用したゾーン作成の準備 (作業マップ)，160-163
CDE アクションを使用したネットワークインタフェースとゾーンの結合 (作業マップ)，157-160
CDE アクションを使用したラベル付きゾーンの作成 (作業マップ)，163-172
chk_encodings コマンド，55-56
「Create a new zone」メニュー項目，75, 83-85

D

dpadm サービス，124
dsadm サービス，124

E

/etc/system ファイル
  1 でない DOI に対する変更，57-58
  IPv6 ネットワークのための変更，56-57

I

IPv6
  /etc/system ファイルへのエントリ，56-57
  トラブルシューティング，56

L

label_encodings ファイル
  インストール，52-56
  検査，52-56
  変更，52-56
  ローカライズ，24
labeld サービス，49
  トラブルシューティング，49
  無効化，117
Labeled Zone Manager，「txzonemgr スクリプト」を参照
LDAP
  クライアントからの管理の有効化，134-135
  計画，28
「LDAP クライアントの作成」アクション，65-68
LDAP 構成
  Sun Ray サーバー、および，121
  クライアントの作成，65-68
LDAP サーバー
  Trusted Extensions クライアントのためのプロキシの構成，131-132
  Trusted Extensions クライアントのためのプロキシの作成，132
  Trusted Extensions へのインストール，122-125
  資格を Solaris 管理コンソールに登録，133-134

LDAP サーバー (続き)
情報の収集，121-122
責務分離の計画，129
ネームサービスの構成，122-125
マルチレベルポートの設定，128-129
ログファイルの保護，127-128
LDAP の構成, Trusted Extensions のための，121-131
LDAP のための Solaris 管理コンソールの設定 (作業マップ)，132-138
「LDAP 用ゾーンを初期化」アクション，165
lpaddent コマンド，108-110

N

No route available，111-113
nscd デーモン, すべてのラベル付きゾーンへの追加，92-93

P

Solaris がインストールされたシステム, Trusted Extensions の要件，43-45
Solaris のインストールオプション, 要件，42-43
Trusted Extensions 構成, ラベル付きゾーン，157-172
Trusted Extensions でのヘッドレスシステムの構成 (作業マップ)，139-148
Trusted Extensions ネットワーク
IPv6 の有効化，56-57
ゾーン固有の nscd デーモンの削除，93
ゾーン固有の nscd デーモンの追加，92-93
ゾーン固有のインタフェースの追加，85-88
ラベル付きゾーンに対するデフォルトルートの指定，88-92
Trusted Extensions の構成
LDAP，121-131
LDAP のためのデータベース，121-131
インストールチームのためのチェックリスト，173-176
最初の手順，51-117
作業マップ，35-39
初期設定チームの担当，41
タスクの区分，41
Trusted Extensions の構成 (続き)
デフォルトの DOI 値の変更，57-58
トラブルシューティング，110-113
ネットワークデータベースの LDAP サーバーへの追加，129-131
評価された構成，22
ヘッドレスアクセス，139-148
ヘッドレスシステム，139-148
ラベル付きゾーン，68-85, 157-172
ラベルをアクティブにするための再起動，60-61
Trusted Extensions のネットワーク, 計画，25-26
Trusted Extensions の無効化，「無効化」を参照
Trusted Extensions の要件
Solaris がインストールされたシステム，43-45
Solaris のインストール，42-43
Solaris のインストールオプション，42-43
root パスワード，44
Trusted Extensions ホストでの LDAP サーバーの構成 (作業マップ)，119-120
Trusted Extensions ホストでの LDAP プロキシサーバーの構成 (作業マップ)，120-121

R

resolv.conf ファイル, 構成時の読み込み，68
roleadd コマンド，99
root パスワード, Trusted Extensions で必要，44

S

Solaris Trusted Extensions，「Trusted Extensions」を参照
Solaris 管理コンソール
LDAP 資格の登録，133-134
LDAP ツールボックスの設定，135-136
LDAP ツールボックスを使用できるようにする，134-135
Sun Java System Directory Server で機能，132-138
LDAP のための設定，132-138
Trusted Extensions ツールボックスの読み込み，61-64
初期化，61-64

Solaris 管理コンソール *(続き)*
トラステッドネットワークゾーン構成ツールの使用，76, 162
トラブルシューティング，61-64
Sun Java System Directory Server，「LDAP サーバー」を参照
Sun Ray システム
LDAP サーバー、および，121
マニュアルの Web サイト，36
`svcs: Pattern 'labeld' doesn't match any instances`，49

T

`tcp_listen=true` LDAP 設定，134-135
Trusted Extensions
「Trusted Extensions の計画」も参照
2 つの役割による構成のストラテジ，31
Solaris の管理者の立場から見た違い，33-34
計画，21-33
構成ストラテジの計画，30-31
構成前の結果，33-34
準備，42-45, 46-48
責務分離，30-31
ネットワークの計画，25-26
ハードウェアの計画，24-25
無効化，117
メモリー要件，25
有効化，49
有効化前に行うべき決定，47-48
有効化前の情報収集，46
`tsol_ldap.tbx` ファイル，135-136
`txzonemgr` スクリプト，69-70, 112

U

`useradd` コマンド，102
`/usr/sbin/txzonemgr` スクプト，163
`/usr/sbin/txzonemgr` スクリプト，69-70, 112

X

X サーバーへのアクセス，111-113

Z

`zenity` スクリプト，69-70
ZFS, サポートされていないが、時間がかからないゾーンの作成方法，27
ZFS プール, ゾーンのクローンを作成するための作成，59-60
Zone Console, 出力，79

あ

アカウント
計画，29
作成，93-105
アクション，「管理アクション」を参照
アドレス
システムごとに 1 つの IP アドレスを指定，74, 159-160
大域ゾーンとラベル付きゾーンでの共有，158-159

い

印刷, 計画，28
インストール
`label_encodings` ファイル，52-56
Trusted Extensions 用に Solaris OS をインストールする，41-49
Sun Java System Directory Server，121-131
ゾーン，77-78, 164-167
インストールメニュー
Create a new zone，75, 83-85
Zone Console，79

え

エラーメッセージ
トラブルシューティング，49, 111-113

遠隔ログイン, 役割に対して可能にする，141-143
「エンコーディングの検査」アクション，52-56
エンコーディングファイル，「label_encodings ファイル」を参照

お
行うべき決定, Trusted Extensions の有効化前，47-48

か
開始, ゾーン，78-80
解釈ドメイン (DOI), /etc/system ファイル内のエントリ，57-58
確認
ゾーンのステータス，80-81
役割が機能すること，103-104
画面, 初期表示，61
監査, 計画，29
監査の計画，29
管理, 役割による遠隔の，141-143
管理アクション
LDAP クライアントの作成，65-68
LDAP 用ゾーンを初期化，165
エンコーディングの検査，52-56
ゾーン端末コンソール，83, 165, 166
ゾーンのインストール，165
ゾーンのクローンを作成，171-172
ゾーンのシャットダウン，170
ゾーンを起動，166
ゾーンを構成，161
ゾーンをコピー，171
物理インタフェースの共有，159
論理インタフェースの共有，158

き
起動
ゾーン，78-80, 166

け
計画
「Trusted Extensions の使用」も参照
LDAP ネームサービス，28
NFS サーバー，28
Trusted Extensions の構成ストラテジ，30-31
Trusted Extensions，21-33
アカウント作成，29
印刷，28
監査，29
管理ストラテジ，23
ゾーン，26-27
データ移送，32-33
ネットワーク，25-26
ハードウェア，24-25
ラベル，23-24
決定
Sun 提供のエンコーディングファイルの使用，47
役割としてまたはスーパーユーザーとして構成，48
決定する事項, サイトのセキュリティーポリシーに基づく，150
検査
label_encodings ファイル，52-56
役割が機能すること，103-104
権利プロファイル, 責務分離のためのカスタマイズ，94-97

こ
構成
Trusted Extensions クライアントのための LDAP プロキシサーバー，131-132
Trusted Extensions ソフトウェア，51-117
Trusted Extensions のための LDAP，121-131
Trusted Extensions ラベル付きゾーン，68-85, 157-172
ネットワークインタフェース，70-74
ヘッドレス Trusted Extensions へのアクセス，139-148
役割としてか、スーパーユーザーとしてか，48
構成Trusted Extensions, ラベル付きゾーン，68-85
構成ファイル, コピー，114-115

コンソールウィンドウ, 開かない場合のトラブルシューティング, 111

さ

サービス管理フレームワーク (SMF)
dpadm, 124
dsadm, 124
labeld サービス, 49
再起動
ラベル付きゾーンへのログインの有効化, 104-105
ラベルの有効化, 60-61
サイトのセキュリティーポリシー
Trusted Extensions 構成の決定, 150
関連タスク, 149-155
個人に関する推奨事項, 153
推奨事項, 151
物理的アクセスに関する推奨事項, 152
よくある違反, 153-154
～の理解, 22-23
作業と作業マップ, ラベル付きゾーンの作成, 68-85
作業マップ: Solaris 用 Solaris システムの準備, 35
作業マップ: Trusted Extensions の構成, 37-39
作業マップ: Trusted Extensions の準備と有効化, 35-37
削除
ゾーン固有の nscd デーモン, 93
ラベル付きゾーン, 117
作成
LDAP クライアント, 65-68
LDAP ツールボックス, 135-136
Trusted Extensions クライアントのための LDAP プロキシサーバー, 132
roleadd によるローカル役割, 99
useradd によるローカル役割, 102
アカウント, 93-105
構成時または構成後のアカウント, 48
ゾーン, 68-85, 164-167
ホームディレクトリ, 105-108
ホームディレクトリサーバー, 105-106
役割, 93-105
役割になれるユーザー, 100-102
作成 (続き)
ラベル付きゾーン, 68-85

し

資格, LDAP を Solaris 管理コンソールに登録, 133-134
システム管理者役割, 制限, 99-100
出版物, セキュリティーと UNIX, 154-155
情報の収集
LDAP サービス, 121-122
Trusted Extensions の構成の計画, 32
Trusted Extensions の有効化前, 46
初期化
LDAP のゾーン, 164-167
Solaris 管理コンソール, 61-64
ゾーン, 165
初期設定チーム, Trusted Extensions を構成するためのチェックリスト, 173-176
初期設定チームのためのチェックリスト, 173-176

せ

責務分離
LDAP のための計画, 129
計画, 30-31
権利プロファイルの作成, 94-97
セキュリティー
root パスワード, 44
サイトのセキュリティーポリシー, 149-155
出版物, 154-155
初期設定チーム, 41
セキュリティー管理者役割, 作成, 97-99
設定, LDAP のための Solaris 管理コンソール, 132-138

そ

ゾーン
LDAP 用の初期化, 164-167
txzonemgr スクリプト, 112
/usr/sbin/txzonemgr スクリプト, 69-70, 163

ゾーン (続き)
アクセスのトラブルシューティング，111-113
インストール，77-78, 164-167
インストールに関するトラブルシューティング，78
各ラベル付きゾーンへの nscd デーモンの追加，92-93
カスタマイズ，81-83
起動，78-80, 166
共有 IP アドレスの指定，158-159
クローン作成のための ZFS プールの作成，59-60
削除，117
作成，164-167
作成方法の決定，26-27
シャットダウン，170
初期化，165
ステータスの確認，80-81
すべてのゾーンに 1 つの IP アドレスを指定，74, 159-160
ゾーンアクティビティーの表示，83, 166
ゾーンアクティビティの表示，79
ゾーン名とラベルの関連付け，76, 162
停止，82
デフォルトルートによる切り離し，88-92
デフォルトルートの指定，88-92
名前の指定，75-77, 161-163
ネットワークインタフェースの追加，85-88
有効化するログイン先，104-105
ラベル付きゾーンからの nscd デーモンの削除，93
ラベルの指定，75-77, 161-163
「ゾーン端末コンソール」アクション
出力，83, 166
～を使用した，165
「ゾーンのインストール」アクション，165
「ゾーンのインストール」アクション, トラブルシューティング，167
「ゾーンのクローンを作成」アクション，171-172
「ゾーンのシャットダウン」アクション，170
「ゾーンを起動」アクション，166
「ゾーンを構成」アクション，161
「ゾーンをコピー」アクション，171
その他の Trusted Extensions 構成タスク，114-117

た

タスクと作業マップ
CDE アクションを使用したゾーン作成の準備 (作業マップ)，160-163
CDE アクションを使用したネットワークインタフェースとゾーンの結合 (作業マップ)，157-160
CDE アクションを使用したラベル付きゾーンの作成 (作業マップ)，163-172
LDAP のための Solaris 管理コンソールの設定 (作業マップ)，132-138
Trusted Extensions でのヘッドレスシステムの構成 (作業マップ)，139-148
Trusted Extensions ホストでの LDAP サーバーの構成 (作業マップ)，119-120
Trusted Extensions ホストでの LDAP プロキシサーバーの構成 (作業マップ)，120-121
その他の Trusted Extensions 構成タスク，114-117

つ

追加
LDAP ツールボックス，135-136
lpaddent を使用してユーザーを，108-110
Solaris システムへの Trusted Extensions の追加，49
roleadd によるローカル役割，99
useradd によるローカル役割，102
共有ネットワークインタフェース，70-74
すべてのラベル付きゾーンへの nscd デーモンの追加，92-93
ゾーン固有の nscd デーモン，92-93
ゾーン固有のネットワークインタフェース，85-88
ネットワークデータベースの LDAP サーバーへの，129-131
役割，93-105
役割になれるユーザー，100-102
ラベル付きゾーンに対するデフォルトルート，88-92
ツールボックス
Trusted Extensions で読み込み，61-64
Scope=LDAP，133-134

ツールボックス (続き)
tsol_ldap.tbx への LDAP サーバーの追加，135-136

て
ディレクトリ, ネームサービス設定，129
テープデバイス, 割り当て，117
デバイスの割り当て
データのコピー，114-115
テープドライブ，117
デフォルトルート, ラベル付きゾーンに対する指定，88-92

と
登録, Solaris 管理コンソールでの LDAP の資格，133-134
トラステッドネットワークゾーンツール
トラブルシューティング，163
名前付きゾーンへのラベルの割り当て，76, 162
トラブルシューティング
Installation of these packages generated errors: SUNW*pkgname*，78, 167
IPv6 の構成，56
labeld サービスをサポートする Solaris リリース，49
Trusted Extensions の構成，110-113
Solaris 管理コンソール，61-64
X サーバーへのアクセス，111-113
コンソールウィンドウが開かない，111
トラステッドネットワークゾーンのプロパティー，163

な
名前
ゾーンに対する指定，75-77, 161-163
名前を付ける
ゾーン，75-77, 161-163

ね
ネームサービスキャッシュデーモン，「nscd デーモン」を参照
ネットワーク，「Trusted Extensions のネットワーク」を参照

は
ハードウェアの計画，24-25
バックアップ, インストールする前のシステム，32-33

ふ
ファイル
resolv.conf，68
リムーバブルメディアからのコピー，115
「物理インタフェースの共有」アクション，159

へ
変更, label_encodings ファイル，52-56

ほ
ホームディレクトリ
サーバーの作成，105-106
作成，105-108
ログインと取得，106-108

ま
マルチレベルサーバー, 計画，28

む
無効化, Trusted Extensions，117

め
メディア, ポータブルメディアからのファイルのコピー, 115

や
役割
roleadd によるローカル役割の追加, 99
遠隔のログイン, 141-143
機能することを確認, 103-104
作成する時期の決定, 48
責務分離, 94-97, 99-100
セキュリティー管理者の作成, 97-99

ゆ
有効化
1 ではない DOI, 57-58
dpadm サービス, 124
dsadm サービス, 124
IPv6 ネットワーク, 56-57
labeld サービス, 49
Solaris システム上の Trusted Extensions, 49
クライアントからの LDAP 管理, 134-135
ラベル付きゾーンへのログイン, 104-105
ユーザー
NIS サーバーからの追加, 108-110
useradd によるローカル役割の追加, 102
初期ユーザーの作成, 100-102
ユーザーを作成するために 2 つの役割が必要, 94-97, 99-100

ら
ラベル
計画, 23-24
ゾーンに対する指定, 75-77, 161-163
トラステッドストライプ上, 61
名前付きゾーンへの割り当て, 76, 162
ラベル付きゾーンの作成, 68-85
ラベル付け
ゾーン, 75-77, 161-163
ラベル付け (続き)
ラベルのオン, 60-61

る
ルーティング, ラベル付きゾーンに対するデフォルトルートの指定, 88-92

ろ
ロードマップ
作業マップ: Trusted Extensions の構成, 37-39
作業マップ: Trusted Extensions の準備と有効化, 35-37
作業マップ: Trusted Extensions 用 Solaris システムの準備, 35
ログイン
rlogin コマンドの使用, 145-148
遠隔, 141-143
ホームディレクトリサーバーへの, 106-108
ログファイル, Directory Server のログの保護, 127-128
「論理インタフェースの共有」アクション, 158

わ
ワークスペース, 初期表示, 61