Solaris Trusted Extensions 管理の手順

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

Part No: 819–7611–14
2009 年 10 月

原典: Solaris Trusted Extensions Administrator's Procedures

Part No: 819-0872–15

Revision A

090916@22749

目次

図目次

表目次

はじめに

『Solaris Trusted Extensions 管理の手順』ガイドでは、Solaris オペレーティングシステム上で Solaris™ Trusted Extensions を構成する手順について説明します。このマニュアルでは、Solaris Trusted Extensions ソフトウェアでラベル付けされるユーザー、ゾーン、デバイス、およびホストの管理手順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使用するシステムがサポートされます。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、特に 64 ビットの x86 互換 CPU に関連しています。
- 「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して管理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。

管理者は、Solaris の管理に精通していなければなりません。加えて、次の点も理解している必要があります。

- Trusted Extensions のセキュリティー機能およびサイトのセキュリティーポリシー
- Trusted Extensions が設定されたホストを使用する基本的な概念と手順 (『Solaris Trusted Extensions ユーザーズガイド』で説明)。

- 自サイトで、管理作業が複数の役割にどのように分担されるか。

Solaris Trusted Extensions の関連マニュアル

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

マニュアルのタイトル	内容	対象読者
『Solaris Trusted Extensions 移行ガイド』	旧版。Trusted Solaris 8 ソフトウェア、&Solaris 10; ソフトウェア、および Solaris Trusted Extensions ソフトウェア間の違いについて、概要を説明しています。 このリリースでは、Trusted Extensions の変更点を『Solaris OS の概要』のマニュアルで概説しています。	すべて
『Solaris Trusted Extensions リファレンスマニュアル』	旧版。Solaris 10 11/06 と Solaris 10 8/07 リリースの Trusted Extensions における Solaris Trusted Extensions マニュアルページが記載されています。 このリリースでは、Trusted Extensions のマニュアルページは Solaris のマニュアルページに含まれています。	すべて
『Solaris Trusted Extensions ユーザーズガイド』	Solaris Trusted Extensions の基本的な機能について説明しています。用語集も付属しています。	エンドユーザー、管理者、開発者
『Solaris Trusted Extensions インストールと構成 (Solaris 10 11/06 および Solaris 10 8/07 リリース版)』	旧版。Solaris 10 11/06 と Solaris 10 8/07 リリースの Trusted Extensions における Solaris Trusted Extensions を計画、インストール、および構成する方法について説明しています。	管理者、開発者
『Solaris Trusted Extensions 構成ガイド』	Solaris 10 5/08 リリース以降において、Solaris Trusted Extensions を有効化、および最初に構成する方法を説明しています。旧版の『Solaris Trusted Extensions インストールと構成』に替わるものです。	管理者、開発者
『Solaris Trusted Extensions 管理の手順』	具体的な管理業務の実行方法を示します。	管理者、開発者
『Solaris Trusted Extensions 開発ガイド』	Solaris Trusted Extensions を使ってアプリケーションを開発する方法について説明しています。	開発者、管理者
『Solaris Trusted Extensions ラベルの管理』	ラベルエンコーディングファイルでのラベル構成要素の指定方法について説明します。	管理者
『コンパートメントモードワークステーションのラベル作成: エンコード形式』	ラベルエンコーディングファイルで使用される構文について説明します。構文を使用することにより、適格な形式のラベルに関するさまざまな規則がシステムに適用されます。	管理者

サン・マイクロシステムズ社のマニュアル

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

マニュアルのタイトル	トピック
『Solaris のシステム管理 (基本編)』	ユーザーアカウントとグループ、サーバーとクライアントのサポート、システムのシャットダウンとブート、管理サービス、およびソフトウェアの管理 (パッケージとパッチ)
『Solaris のシステム管理 (上級編)』	端末とモデム、システムリソース (ディスク割り当て、アカウンティング、および crontab)、システムプロセス、および Solaris ソフトウェアの障害追跡
『Solaris のシステム管理 (デバイスとファイルシステム)』	リムーバブルメディア、ディスクとデバイス、ファイルシステム、およびデータのバックアップと復元
『Solaris のシステム管理 (IP サービス)』	TCP/IP ネットワーク管理、IPv4 と IPv6 アドレス管理、DHCP、IPsec、IKE、Solaris IP フィルタ、モバイル IP、IP ネットワークマルチのパス化 (IPMP)、および IPQoS
『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)』	DNS、NIS、および LDAP のネーミングとディレクトリサービス (NIS から LDAP への移行、および NIS+ から LDAP への移行を含む)
『Solaris のシステム管理 (ネットワークサービス)』	Web キャッシュサーバー、時間関連サービス、ネットワークファイルシステム (NFS と Autofs)、メール、SLP、および PPP
『Solaris のシステム管理 (セキュリティサービス)』	監査、デバイス管理、ファイルセキュリティー、BART、Kerberos サービス、PAM、Solaris 暗号化フレームワーク、特権、RBAC、SASL、および Solaris Secure Shell
『Solaris のシステム管理 (Solaris コンテナ : 資源管理と Solaris ゾーン)』	リソース管理に関連する計画と作業、拡張アカウンティング、リソース制御、フェアシェアスケジューラ (FSS)、資源上限デーモン (rcapd) による物理メモリーの制御、および資源プール (Solaris Zones ソフトウェア区分技術と lx ブランドゾーンによる仮想化)
『Solaris ZFS 管理ガイド』	ZFS ストレージプールおよびファイルシステムの作成と管理、スナップショット、クローン、バックアップ、アクセス制御リスト (ACL) による ZFS ファイルの保護、ゾーンがインストールされた Solaris システム上での ZFS の使用、エミュレートされたボリューム、およびトラブルシューティングとデータ回復

マニュアルのタイトル	トピック
『Solaris のシステム管理 (印刷)』	Solaris の印刷に関するトピックと作業、印刷サービスやプリンタを設定して管理するためのサービス、ツール、プロトコル、およびテクノロジの使用方法

その他のマニュアル

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 Sun は責任を負いません。Sun は、これらのサイトあるいはリソースに関する、あるいはこれらのサイト、リソースから利用可能であるコンテンツ、広告、製品、あるいは資料に関して一切の責任を負いません。Sun 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

Sun の Web サイトでは、次のサービスに関する情報も提供しています。

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

表記上の規則

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

表 P–1 表記上の規則

字体または記号	意味	例
`AaBbCc123`	コマンド名、ファイル名、ディレクトリ名、画面上のコンピュータ出力、コード例を示します。	`.login` ファイルを編集します。 `ls -a` を使用してすべてのファイルを表示します。 `system%`
`AaBbCc123`	ユーザーが入力する文字を、画面上のコンピュータ出力と区別して示します。	`system%` **`su`** `password:`
AaBbCc123	変数を示します。実際に使用する特定の名前または値で置き換えます。	ファイルを削除するには、`rm` *filename* と入力します。
『 』	参照する書名を示します。	『コードマネージャ・ユーザーズガイド』を参照してください。
「 」	参照する章、節、ボタンやメニュー名、強調する単語を示します。	第 5 章「衝突の回避」を参照してください。 この操作ができるのは、「スーパーユーザー」だけです。
\	枠で囲まれたコード例で、テキストがページ行幅を超える場合に、継続を示します。	`sun%` **`grep '^#define \`** **`XV_VERSION_STRING'`**

コード例は次のように表示されます。

- C シェル

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

- C シェルのスーパーユーザー

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

- Bourne シェルおよび Korn シェル

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

- Bourne シェルおよび Korn シェルのスーパーユーザー

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

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

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

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

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

一般規則

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

◆ ◆ ◆ 第 1 章

Trusted Extensions の管理の概念

この章では、Solaris™ Trusted Extensions ソフトウェアが設定されたシステムの管理について紹介します。

Trusted Extensions ソフトウェアと Solaris OS

Trusted Extensions ソフトウェアは、Solaris オペレーティングシステム (Solaris OS) を実行しているシステムにラベルを追加します。ラベルは、「必須アクセス制御」(MAC) を実装します。MAC は任意アクセス制御 (DAC) とともに、システムのサブジェクト (プロセス) とオブジェクト (データ) を保護します。Trusted Extensions ソフトウェアには、ラベルの構成、ラベルの割り当て、およびラベルポリシーを処理するためのインタフェースが用意されています。

Trusted Extensions と Solaris OS の類似性

Trusted Extensions ソフトウェアは、権利プロファイル、役割、監査、特権、および Solaris OS のその他のセキュリティー機能を使用します。Solaris Secure Shell (SSH)、BART、Solaris 暗号フレームワーク、IPsec、および IPfilter を、Trusted Extensions で使用できます。

- Solaris OS の場合と同様、ユーザーが使用できるアプリケーションを、各自の職務を実行するために必要なアプリケーションだけに制限できます。ほかのユーザーには、その他の作業を承認することができます。
- Solaris OS の場合と同様、これまでスーパーユーザーに割り当てられていた機能を、個別の「役割」に割り当てられます。
- Solaris OS の場合と同様、特権でプロセスを保護します。プロセスを分離するため、ゾーンも使用されます。

- Solaris OS と同様に、システムのイベントを監査できます。
- Trusted Extensions は、`policy.conf` や `exec_attr` などの、Solaris OS のシステムの設定ファイルを使用します。

Trusted Extensions と Solaris OS の相違点

Trusted Extensions ソフトウェアは、Solaris OS を拡張します。次のリストに概要を示します。クイックリファレンスについては、付録 A 「Trusted Extensions 管理の手引き」を参照してください。

- Trusted Extensions は、「ラベル」という特別なセキュリティータグを使用して、データへのアクセスを制御します。ラベルでは「必須アクセス制御」(MAC) が使用されます。MAC 保護は、UNIX® のファイルアクセス権、つまり任意アクセス制御 (DAC) に追加されます。ラベルは、ユーザー、ゾーン、デバイス、ウィンドウ、およびネットワークの終端に直接割り当てられます。ラベルは、プロセス、ファイル、およびその他のシステムオブジェクトにも暗黙的に割り当てられます。

  一般ユーザーが MAC を上書きすることはできません。Trusted Extensions では、一般ユーザーはラベルが割り当てられたゾーンで作業する必要があります。デフォルトでは、ラベルが割り当てられたゾーンのユーザーまたはプロセスは MAC を上書きできません。

  Solaris OS と同様に、MAC の上書きを許可する場合は、セキュリティーポリシーを上書きできる機能を特定のプロセスまたはユーザーに割り当てます。たとえば、ファイルのラベルを変更できるようにユーザーを承認することができます。これらの処理は、ファイル内の情報の機密度をアップグレードまたはダウングレードします。
- Trusted Extensions は、既存の構成ファイルやコマンドを拡張します。たとえば、Trusted Extensions は監査イベント、承認、特権、権利プロファイルを追加します。
- Trusted Extensions システムでは、Solaris システムでオプションとされている機能の中に必要なものがあります。たとえば、Trusted Extensions が設定されたシステムではゾーンと役割が必要です。
- Trusted Extensions システムでは、Solaris システムでオプションとされている機能の中に推奨されるものがあります。たとえば、Trusted Extensions では、`root` ユーザーを `root` 役割に変更するようにしてください。
- Trusted Extensions では、Solaris OS のデフォルトの動作が変更される場合があります。たとえば、Trusted Extensions が設定されたシステムでは、監査がデフォルトで有効です。また、デバイス割り当てが必要です。
- Trusted Extensions では、利用できる選択肢が Solaris OS よりも制限される場合があります。たとえば、Trusted Extensions が設定されたシステムでは、NIS+ ネームサービスはサポートされません。また、Trusted Extensions では、すべてのゾーン

はラベル付きゾーンです。Solaris OS と異なり、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。Trusted Extensions では、複数のラベル付きゾーンで 1 つの IP アドレスを共有することもできます。

- Trusted Extensions には、トラステッドバージョンの 2 つのデスクトップがあります。ラベル付き環境で作業するには、Trusted Extensions のデスクトップユーザーはこれらのデスクトップのいずれかを使用する必要があります。
  - **Solaris Trusted Extensions (CDE)** – トラステッドバージョンの共通デスクトップ環境 (CDE) です。この名称はTrusted CDE と略すことができます。
  - **Solaris Trusted Extensions (JDS)** – トラステッドバージョンの Java Desktop System, Release *number* です。この名称は Trusted JDS と略すことができます。
- Trusted Extensions には、グラフィカルユーザーインタフェース (GUI) とコマンド行インタフェース (CLI) が追加されています。たとえば、Trusted Extensions にはデバイスを管理するデバイス割り当てマネージャーが用意されています。また、`updatehome` コマンドは、一般ユーザーの各ラベルのホームディレクトリに、起動ファイルを配置するために使用します。
- Trusted Extensions では、管理に特定の GUI を使用する必要があります。たとえば、Trusted Extensions が設定されたシステムでは、Solaris 管理コンソールを使用してユーザー、役割、およびネットワークを管理します。同様に、Trusted CDE では、システムファイルを編集するには管理エディタを使用します。
- Trusted Extensions は、ユーザーが表示できる内容を制限します。たとえば、ユーザーが割り当てできないデバイスは、そのユーザーに対して表示されません。
- Trusted Extensions は、ユーザーのデスクトップオプションを制限します。たとえば、ユーザーがワークステーションを非活動のままにできる時間は制限されています。この時間を過ぎると、画面がロックされます。

マルチヘッドシステムと Trusted Extensions デスクトップ

マルチヘッドの Trusted Extensions システムのモニターが水平に設定されている場合、1 つのトラステッドストライプが複数のモニターにまたがって表示されます。モニターを垂直に設定すると、トラステッドストライプは一番下のモニターに表示されます。

さまざまなワークスペースがマルチヘッドシステムのモニターに表示される場合、Trusted CDE とTrusted JDS とではトラステッドストライプの表示の仕方が異なります。

- Trusted JDS デスクトップでは、各モニターにトラステッドストライプが表示されます。

- Trusted CDE デスクトップでは、1 つのトラステッドストライプが主モニターに表示されます。

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

ただちにセキュリティー管理者に連絡してください。正しいトラステッドストライプを確認するには、74 ページの「デスクトップの現在のフォーカスへの制御を取り戻す」を参照してください。

Trusted Extensions の基本概念

Trusted Extensions ソフトウェアにより、Solaris システムにラベルが追加されます。また、ラベル付きデスクトップと、ラベルビルダーやデバイス割り当てマネージャーなどのトラステッドアプリケーションも追加されます。この節で説明する概念は、ユーザーと管理者の両方にとって、Trusted Extensions を理解するために必要な知識です。『Solaris Trusted Extensions ユーザーズガイド』でも、これらの概念を説明しています。

Trusted Extensions が提供する保護

Trusted Extensions ソフトウェアは Solaris OS の保護を強化します。Solaris OS は、パスワードが必要なユーザーアカウントを使用して、システムへのアクセスを保護します。パスワードの定期的な変更を要求したり、パスワードの長さを指定することもできます。役割で管理タスクを実行するには、追加のパスワードが必要です。役割はログインアカウントとして使用できないため、認証を追加することで、root ユーザーのパスワードを推測した侵入者から受ける被害を小さくできます。Trusted Extensions ソフトウェアは、ユーザーと役割を承認されたラベル範囲にさらに限定します。このラベル範囲は、ユーザーと役割がアクセスできる情報を制限します。

Trusted Extensions ソフトウェアでは、トラステッドパスシンボルが表示されます。これは、トラステッドストライプの左に表示される、不正操作を防ぐための明白な目印です。Trusted CDE では、トラステッドストライプは画面の最下部に表示されます。Trusted JDS では、画面の最上部に表示されます。トラステッドパスシンボルは、システムのセキュリティーに影響する部分を使用していることをユーザーに通知します。ユーザーがトラステッドアプリケーションを実行しているときに、このシンボルが表示されていない場合は、実行中のアプリケーションが本物であることをただちに確認するようにしてください。トラステッドストライプが表示されない場合、デスクトップは信頼できません。デスクトップ表示の例については、図 1–1 を参照してください。

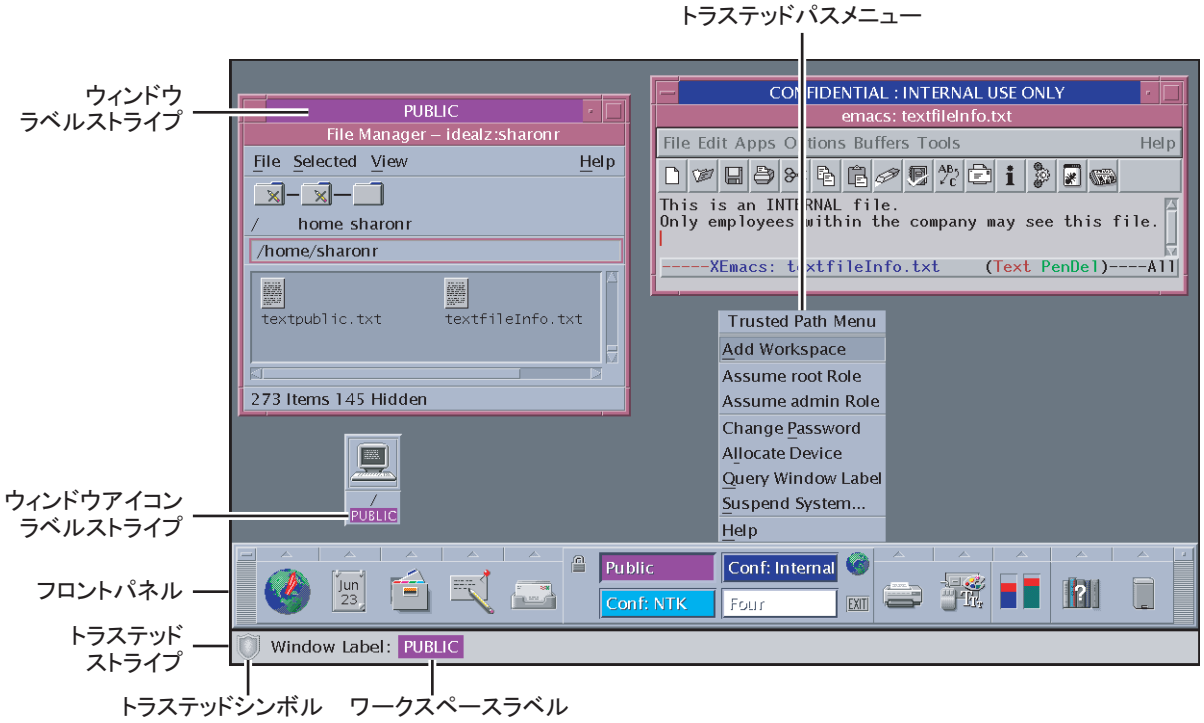


図 1-1 Trusted Extensions マルチレベル CDE デスクトップ

セキュリティーにもっとも関連するソフトウェアであるトラステッドコンピューティングベース (TCB) は、大域ゾーンで動作します。一般ユーザーは、大域ゾーンに入ったり、大域ゾーンのリソースを表示することはできません。パスワードを変更する場合など、ユーザーは TCB ソフトウェアを対話的に実行できます。トラステッドパスシンボルは、ユーザーが TCB と対話するときに常に表示されます。

Trusted Extensions とアクセス制御

Trusted Extensions ソフトウェアは、任意アクセス制御 (DAC) と必須アクセス制御 (MAC) を通じて、情報とほかのリソースを保護します。DAC は、所有者が自由に設定する、従来の UNIX のアクセス権ビットとアクセス制御リストです。MAC は、システムが自動的に実施するメカニズムです。MAC は、トランザクション中のプロセスとデータのラベルを確認することで、すべてのトランザクションを制御します。

ユーザーの「ラベル」は、ユーザーが許可された操作および選択する操作の機密レベルを表します。標準ラベルは `Secret` または `Public` です。ラベルによ

り、ユーザーがアクセスできる情報が決定されます。MAC と DAC のどちらも、Solaris OS で設定された特殊なアクセス権で上書きできます。「特権」は、プロセスに付与される特殊なアクセス権です。「承認」は、管理者によってユーザーと役割に付与される特殊なアクセス権です。

管理者はサイトのセキュリティーポリシーに従って、ファイルとディレクトリをセキュリティーで保護する適切な手順について、ユーザーにトレーニングを実施する必要があります。また、ラベルのアップグレードまたはダウングレードを許可されたユーザーには、どのような場合にラベルの変更が適切かについて指示するようにしてください。

役割と Trusted Extensions

Solaris ソフトウェアだけを実行して Trusted Extensions を使用していないシステムでは、役割の使用は任意です。Trusted Extensions が設定されたシステムでは、役割は必須です。システムは、システム管理者役割とセキュリティー管理者役割で管理されます。一部では、`root` 役割を使用する場合もあります。

Solaris OS と同様、権利プロファイルは役割の機能の基本です。Trusted Extensions では、Information Security と User Security の 2 つの権利プロファイルを使用します。これらの 2 つのプロファイルによって、セキュリティー管理者役割が定義されます。

Trusted Extensions の役割で利用できるプログラムには、「トラステッドパス属性」という特殊なプロパティーが与えられます。この属性は、プログラムが TCB の一部であることを表します。トラステッドパス属性は、プログラムが大域ゾーンから起動された場合に利用できます。

役割については、『System Administration Guide: Security Services』 のパート III「Roles, Rights Profiles, and Privileges」 を参照してください。

Trusted Extensions ソフトウェアのラベル

ラベルと認可上限は、Trusted Extensions の必須アクセス制御 (MAC) で中心的な機能を果たします。これらは、各ユーザーがアクセスできるプログラム、ファイル、およびディレクトリを決定します。ラベルと認可上限は、1 つの「格付け」構成要素と任意の数の「コンパートメント」構成要素から構成されます。格付けコンポーネントは、`TOP SECRET` や `CONFIDENTIAL` などの、セキュリティーの階層レベルを表します。コンパートメントコンポーネントは、共通な情報へのアクセスを必要とするユーザーのグループを表します。コンパートメントの一般的な例として、プロジェクト、部署、物理的な場所などがあります。承認されたユーザーには、ラベルは読みやすい形式で表示されますが、内部的にはラベルは数値として処理されます。数値によるラベルと人が読みやすい形式のラベルは、`label_encodings` ファイルで定義されます。

Trusted Extensions は、試行されるセキュリティー関連トランザクションのすべてを仲介します。このソフトウェアは、アクセス元のエンティティー (一般的にはプロセス) のラベルと、アクセス先のエンティティー (通常はファイルシステムオブジェクト) のラベルを比較します。このソフトウェアは、どちらのラベルが「優位」であるかに応じて、トランザクションを許可または拒否します。ラベルは、割り当て可能なデバイス、ネットワーク、フレームバッファー、別のホストなど、ほかのシステムリソースへのアクセスを決定する場合にも使用されます。

ラベル間の優位関係

次の 2 つの条件を満たす場合、一方のエンティティーのラベルが、他方のエンティティーのラベルよりも優位であると言います。

- 一方のエンティティーのラベルの格付け構成要素が、他方のエンティティーの格付けと同等かそれよりも高い。セキュリティー管理者は、`label_encodings` ファイルで格付けに数値を割り当てます。ソフトウェアはこれらの数値を比較して、優位性を決定します。
- 一方のエンティティーのコンパートメントセットに、他方のエンティティーのコンパートメントがすべて含まれる。

2 つのラベルの格付けが同じで、コンパートメントのセットも同じである場合、これらのラベルは「同等」であるとされます。ラベルが同等であれば、相互に優位となり、アクセスは許可されます。

一方のラベルのコンパートメントに他方のラベルのコンパートメントがすべて含まれ、このラベルの格付けが他方よりも高いか、両方のラベルの格付けが同等である場合、最初のラベルは他方のラベルより「完全に優位」であると言います。

どちらのラベルにも優位が付けられない場合、これらのラベルは「無関係」または「比較不可能」とみなされます。

次の表に、ラベルの優位の比較例を示します。この例では、`NEED_TO_KNOW` の格付けは `INTERNAL` よりも上位にあります。3 つのコンパートメントとして Eng、Mkt、および Fin があります。

表 1–1　ラベル関係の例

ラベル 1	関係	ラベル 2
`NEED_TO_KNOW Eng Mkt`	ラベル 1 はラベル 2 より (完全に) 優位	`INTERNAL Eng Mkt`
`NEED_TO_KNOW Eng Mkt`	ラベル 1 はラベル 2 より (完全に) 優位	`NEED_TO_KNOW Eng`
`NEED_TO_KNOW Eng Mkt`	ラベル 1 はラベル 2 より (完全に) 優位	`INTERNAL Eng`

表 1–1 ラベル関係の例 (続き)

ラベル 1	関係	ラベル 2
NEED_TO_KNOW Eng Mkt	ラベル 1 はラベル 2 より優位 (または同等)	NEED_TO_KNOW Eng Mkt
NEED_TO_KNOW Eng Mkt	無関係	NEED_TO_KNOW Eng Fin
NEED_TO_KNOW Eng Mkt	無関係	NEED_TO_KNOW Fin
NEED_TO_KNOW Eng Mkt	無関係	INTERNAL Eng Mkt Fin

管理ラベル

Trusted Extensions には、 ADMIN_HIGH と ADMIN_LOW の 2 つの特殊な管理ラベルがあり、ラベルまたは認可上限として使用されます。これらのラベルは、システムリソースを保護するために使用され、一般ユーザーではなく管理者用のラベルです。

ADMIN_HIGH は最大のラベルです。ADMIN_HIGH は、システム中のすべてのラベルに対して優位であり、管理データベースや監査証跡などのシステムデータが読み取られるのを防ぎます。ADMIN_HIGH ラベルが付いたデータを読み取るには、大域 ゾーンで操作する必要があります。

ADMIN_LOW は最小のラベルです。一般ユーザーのラベルも含め、システム内のその他すべてのラベルは、ADMIN_LOW に対して優位になります。必須アクセス制御では、ユーザーはユーザーのラベルよりも低いラベルのファイルにデータを書き込むことができません。したがって、一般ユーザーは ADMIN_LOW ラベルのファイルを読み取ることはできますが、修正することはできません。一般的に ADMIN_LOW は、/usr/bin のファイルなど、共有されている誰でも実行可能なファイルを保護するために使用されます。

ラベルエンコーディングファイル

システムのラベルコンポーネント (格付け、コンパートメント、および関連規則) はすべて、ADMIN_HIGH ファイルの label_encodings ファイルに保存されます。このファイルは、/etc/security/tsol ディレクトリに保存されます。セキュリティー管理者は、サイトの label_encodings ファイルを設定します。ラベルエンコーディングファイルには、次の内容が含まれます。

- コンポーネントの定義 – 格付け、コンパートメント、ラベル、および認可上限を、必要な組み合わせと制約の規則を含めて定義します
- 認可範囲の定義 – システム全体と一般ユーザーが利用できるラベルのセットを定義する、認可上限と最小ラベルを指定します
- 印刷の指定 – プリンタ出力の印刷バナー、トレーラ、ヘッダー、フッター、およびその他のセキュリティー機能で使用される、識別情報と取り扱い情報です
- カスタマイズ – ラベルのカラーコードなどのローカルな定義と、その他のデフォルトです

詳細は、label_encodings(4) のマニュアルページを参照してください。詳しい情報は、『Solaris Trusted Extensions ラベルの管理』と『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。

ラベル範囲

「ラベル範囲」は、ユーザーが操作を実行できる使用可能なラベルのセットです。ユーザーとリソースは、どちらにもラベル範囲があります。ラベル範囲で保護可能なリソースには、割り当て可能なデバイス、ネットワーク、インタフェース、フレームバッファー、コマンドやアクションなどが含まれます。ラベル範囲は、上限が認可上限によって、下限が最小ラベルによって定められます。

範囲は必ずしも、最大ラベルと最小ラベル間のすべてのラベルの組み合わせを含む必要はありません。label_encodings ファイルの規則で、特定の組み合わせを無効にできます。ラベルが範囲に含まれるためには、ラベルエンコーディングファイルの適用可能なすべての規則で許可される、「適格な形式」である必要があります。

ただし、認可上限は適格な形式である必要はありません。たとえば、label_encodings ファイルで、ラベルでコンパートメント Eng、Mkt、および Fin の組み合わせが禁止されている場合を考えます。 INTERNAL Eng Mkt Fin は、有効な認可上限ですが、有効なラベルではありません。認可上限として、この組み合わせはユーザーが INTERNAL Eng、INTERNAL Mkt、および INTERNAL Fin のラベルのファイルにアクセスすることを許可します。

アカウントラベル範囲

ユーザーに認可上限と最小ラベルを割り当てると、ユーザーが操作の実行を許可される「アカウントラベル範囲」の上限と下限が決まります。次の式は、アカウントラベル範囲を表しています。≤ は、「前者より後者が優位であるか、両者が同等」であることを表します。

最小ラベル ≤ 許可されたラベル ≤ 認可上限

ユーザーは、認可上限を超えず、最小ラベルよりも優位なラベルで操作が許可されます。ユーザーの認可上限または最小ラベルが明示的に設定されていない場合は、label_encodings ファイルで定義されたデフォルトが有効になります。

ユーザーが複数ラベルまたは単一ラベルで操作を実行できるよう、認可上限と最小ラベルを割り当てることができます。ユーザーの許可上限と最小ラベルが等しい場合、このユーザーは 1 つのラベルだけで操作できます。

セッション範囲

「セッション範囲」は、Trusted Extensions のセッション中にユーザーが利用可能なラベルのセットです。セッション範囲は、ユーザーのアカウントラベル範囲内であり、かつシステムに設定されたラベル範囲内である必要があります。ログイン時に

ユーザーがシングルラベルのセッションモードを選択する場合、セッション範囲はそのラベルに制限されます。ユーザーが複数ラベルのセッションモードを選択する場合、ユーザーによって選択されたラベルがセッションの認可上限になります。セッションの認可上限は、セッション範囲の上限を定義します。ユーザーの最小ラベルは、下限を定義します。ユーザーは、最小ラベルのワークスペースでセッションを開始します。ユーザーはセッション中に、セッション範囲内の別のラベルのワークスペースに切り替えることができます。

ラベルの保護対象とラベルの表示場所

ラベルは、デスクトップに表示されるほか、プリンタ出力など、デスクトップで実行される出力にも表示されます。

- アプリケーション – アプリケーションはプロセスを開始します。これらのプロセスは、アプリケーションが起動されたワークスペースのラベルで動作します。ラベル付きゾーンのアプリケーションには、ファイルとしてゾーンのラベルでラベルが付けられます。
- デバイス – デバイスを通過するデータは、デバイス割り当てとデバイスのラベル範囲で制御されます。デバイスを使用するユーザーは、デバイスのラベル範囲内にあり、デバイスを割り当てるために承認される必要があります。
- ファイルシステムのマウントポイント – すべてのマウントポイントにはラベルが設定されます。ラベルは `getlabel` コマンドを使用して表示できます。
- ネットワークインタフェース – IP アドレス (ホスト) には、ラベル範囲を記述するテンプレートがあります。ラベルなしのホストにも、デフォルトのラベルがあります。
- プリンタと印刷 – プリンタにはラベル範囲があります。ラベルは本文ページに印刷されます。ラベル、取り扱い情報、およびその他のセキュリティー情報が、バナーとトレーラページに印刷されます。Trusted Extensions で印刷を構成するには、第 15 章「ラベル付き印刷の管理 (手順)」と『Solaris Trusted Extensions ラベルの管理』の「印刷出力のラベル」を参照してください。
- プロセス – プロセスはラベル付けされています。プロセスは、プロセスが開始されたワークスペースのラベルで動作します。プロセスのラベルは、`plabel` コマンドを使用して表示できます。
- ユーザー – ユーザーはデフォルトラベルとラベルの範囲を割り当てられています。ユーザーのワークスペースのラベルは、ユーザーのプロセスのラベルを表します。
- ウィンドウ – ラベルは、デスクトップのウィンドウ上部に表示されます。デスクトップのラベルは、色でも示されます。色はデスクトップのスイッチと、ウィンドウ上部のタイトルバーに表示されます。

  ウィンドウが別のラベルのワークスペースに移動しても、このウィンドウは元のラベルを維持します。

- ゾーン – すべてのゾーンには固有のラベルがあります。ゾーンで所有されるファイルとディレクトリは、ゾーンのラベルになります。詳細は、getzonepath(1) のマニュアルページを参照してください。

◆ ◆ ◆ 第 2 章

Trusted Extensions 管理ツール

この章では、Solaris Trusted Extensions で利用可能なツール、ツールの場所、およびツールが操作するデータベースを説明します。

Trusted Extensions の管理ツール

Trusted Extensions が設定されたシステムの管理には、Solaris OS と同じ多数のツールを使用します。Trusted Extensions には、セキュリティーが強化されたツールも用意されています。管理ツールは、役割ワークスペースで役割だけが使用できます。

役割ワークスペース内で、信頼できるコマンド、アクション、アプリケーション、およびスクリプトにアクセスできます。次の表に、これらの管理ツールをまとめます。

表 2–1 Trusted Extensions 管理ツール

ツール	説明	詳細
`/usr/sbin/txzonemgr`	ゾーンの作成、インストール、初期化、および起動を行うためのメニューベースのウィザードを提供します。このスクリプトは、ゾーンを管理するTrusted CDE アクションに替わるものです。 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 `zenity` コマンドを使用します。	『Solaris Trusted Extensions 構成ガイド』の「ラベル付きゾーンの作成」を参照してください。 `zenity`(1) のマニュアルページも参照してください。
Trusted CDE のアプリケーションマネージャーフォルダにある、Trusted_Extensions フォルダのアクション	`/etc/system` などの Solaris 管理コンソールで管理されないローカルファイルを編集します。「ゾーンをインストール」などの一部のアクションは、スクリプトを実行します。	37 ページの「Trusted CDE アクション」および58 ページの「Trusted Extensions の CDE 管理アクションを起動する」を参照してください。
Trusted CDE のデバイス割り当てマネージャー Solaris Trusted Extensions (JDS) のデバイスマネージャー	デバイスのラベル範囲を管理し、デバイスの割り当てと割り当て解除を行います。	39 ページの「「デバイス割り当てマネージャー (Device Allocation Manager)」」および249 ページの「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。
Solaris 管理コンソール	ユーザー、役割、権利、ホスト、ゾーン、およびネットワークを構成します。このツールはローカルファイルまたは LDAP データベースを更新できます。 また、このツールでは旧バージョンの `dtappsession` アプリケーションも起動できます。	基本機能については、『System Administration Guide: Basic Administration』の第 2 章「Working With the Solaris Management Console (Tasks)」を参照してください。Trusted Extensions に固有の機能については、40 ページの「Solaris 管理コンソールツール」を参照してください。
`smuser` や `smtnzonecfg` などの Solaris 管理コンソールコマンド	Solaris 管理コンソールのコマンド行インタフェースです。	リストについては、表 2–4 を参照してください。
ラベルビルダー	ユーザーツールです。プログラムでラベルの選択が必要とされる場合に表示されます。	例については、96 ページの「Solaris 管理コンソールでユーザーのラベル範囲を修正する」を参照してください。
Trusted Extensions コマンド	Solaris 管理コンソールツールや CDE アクションでは処理できないタスクを実行します。	管理コマンドのリストについては、表 2–5 を参照してください。

txzonemgr スクリプト

Solaris 10 5/08 リリースから、txzonemgr スクリプトを使用してラベル付きゾーンが設定されるようになりました。この zenity(1) スクリプトでは、「Labeled Zone Manager」というタイトルのダイアログボックスが表示されます。この GUI の動的に決定されるメニューには、ラベル付きゾーンの現在の設定状態に対して有効な選択肢だけが表示されます。たとえば、ゾーンがすでにラベル付きであれば、「Label」メニュー項目は表示されません。

Trusted CDE アクション

次の表に、Trusted Extensions の役割が実行できる CDE アクションを示します。これらの Trusted CDE アクションは、Trusted_Extensions フォルダにあります。この Trusted_Extensions フォルダは、CDE デスクトップ上のアプリケーションマネージャーフォルダから使用できます。

表 2–2 Trusted CDE の管理アクション、用途、および関連する権利プロファイル

アクション名	用途	デフォルトの権利プロファイル
「割り当て可能なデバイスの追加」	デバイスデータベースにエントリを追加してデバイスを作成します。add_allocatable(1M) のマニュアルページを参照してください。	Device Security
「管理エディタ」	指定したファイルを編集します。59 ページの「Trusted Extensions の管理ファイルを編集する」を参照してください。	Object Access Management
「監査クラス」	audit_class ファイルを編集します。audit_class(4) のマニュアルページを参照してください。	Audit Control
「監査制御」	audit_control ファイルを編集します。audit_control(4) のマニュアルページを参照してください。	Audit Control
「監査イベント」	audit_event ファイルを編集します。audit_event(4) のマニュアルページを参照してください。	Audit Control
「監査の開始」	audit_startup.sh スクリプトを編集します。audit_startup(1M) のマニュアルページを参照してください。	Audit Control
「エンコーディングの検査」	指定したエンコーディングファイルで chk_encodings コマンドを実行します。chk_encodings(1M) のマニュアルページを参照してください。	Object Label Management
「TN ファイルの検査」	tnrhdb、 tnrhtp、および tnzonecfg データベースで tnchkdb コマンドを実行します。tnchkdb(1M) のマニュアルページを参照してください。	Network Management

表 2–2 Trusted CDE の管理アクション、用途、および関連する権利プロファイル (続き)

アクション名	用途	デフォルトの権利プロファイル
「選択構成の確認」	/usr/dt/config/sel_config ファイルを編集します。sel_config(4) のマニュアルページを参照してください。	Object Label Management
「LDAP クライアントを作成」	大域ゾーンを既存の LDAP ディレクトリサービスのクライアントにします。	Information Security
「エンコーディングの編集」アクション	指定した label_encodings ファイルを編集し、chk_encodings コマンドを実行します。chk_encodings(1M) のマニュアルページを参照してください。	Object Label Management
「ネーム・サービス・スイッチ」	nsswitch.conf ファイルを編集します。nsswitch.conf(4) のマニュアルページを参照してください。	Network Management
「DNS サーバの設定」	resolv.conf ファイルを編集します。resolv.conf(4) のマニュアルページを参照してください。	Network Management
「本日のメッセージの設定」	/etc/motd ファイルを編集します。ログイン時に、このファイルの内容が「最後のログイン」ダイアログボックスに表示されます。	Network Management
「デフォルトの経路の設定」	デフォルトの静的経路を指定します。	Network Management
「ファイルシステムの共有」	dfstab ファイルを編集します。share コマンドは実行しません。dfstab(4) のマニュアルページを参照してください。	File System Management

次のアクションは、初期設定チームがゾーンの作成中に使用します。これらのアクションの一部は、保守やトラブルシューティングの目的で使用することができます。

表 2–3 Trusted CDE のインストールアクション、用途、および関連する権利プロファイル

アクション名	用途	デフォルトの権利プロファイル
「ゾーンのクローンを作成」	既存のゾーンの ZFS スナップショットからラベル付きゾーンを作成します。	Zone Management
「ゾーンをコピー」	既存のゾーンからラベル付きゾーンを作成します。	Zone Management
「ゾーンを構成」	ラベルをゾーン名に関連付けます。	Zone Management
「LDAP 用ゾーンを初期化」	LDAP クライアントとして起動するようにゾーンを初期化します。	Zone Management

表 2–3 Trusted CDE のインストールアクション、用途、および関連する権利プロファイル *(続き)*

アクション名	用途	デフォルトの権利プロファイル
「ゾーンをインストール」	ラベル付きゾーンが必要とするシステムファイルをインストールします。	Zone Management
「ゾーンを再起動」	既に起動されているゾーンを再起動します。	Zone Management
「論理インターフェースを共有」	大域ゾーンの 1 つのインタフェースとラベル付きゾーンの独立したインタフェースを、共有するように設定します。	Network Management
「物理インタフェースを共有」	大域ゾーンとラベル付きゾーンで共有される 1 つのインタフェースを設定します。	Network Management
「ゾーンをシャットダウン」	インストールされたゾーンをシャットダウンします。	Zone Management
「ゾーンを起動」	インストールされたゾーンを起動し、このゾーンのサービスを開始します。	Zone Management
「ゾーン端末コンソール」	インストールされたゾーンのプロセスを表示するためにコンソールを開きます。	Zone Management

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

「デバイス」は、コンピュータに接続された物理的な周辺装置、または「疑似デバイス」と呼ばれるソフトウェアでシミュレートされたデバイスのいずれかです。デバイスはシステムにデータをインポートおよびエクスポートする手段を提供するため、データが適切に保護されるように制御する必要があります。Trusted Extensions は、デバイス割り当てとデバイスのラベル範囲を使用して、デバイスを通過するデータを制御します。

ラベル範囲を持つデバイスの例として、フレームバッファー、テープドライブ、フロッピーディスクドライブ、CD-ROM ドライブ、プリンタ、USB デバイスなどがあります。

ユーザーはデバイス割り当てマネージャーを使用して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はデバイスをマウントし、クリーンスクリプトを実行してデバイスを準備し、割り当てを実行します。終了すると、ユーザーはデバイス割り当てマネージャーを使用してデバイスを割り当て解除します。別のクリーンスクリプトが実行され、デバイスのマウント解除と割り当て解除が実行されます。

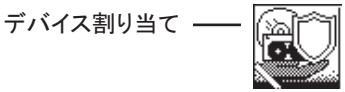


図 2–1　Trusted CDE のデバイス割り当てマネージャーアイコン

デバイス割り当てマネージャーの「デバイス管理」ツールを使用してデバイスを管理できます。一般ユーザーは「デバイス管理」ツールにアクセスできません。

注 – Solaris Trusted Extensions (JDS) では、この GUI はデバイスマネージャーという名前になり、「デバイス管理」ボタンは管理という名前になります。

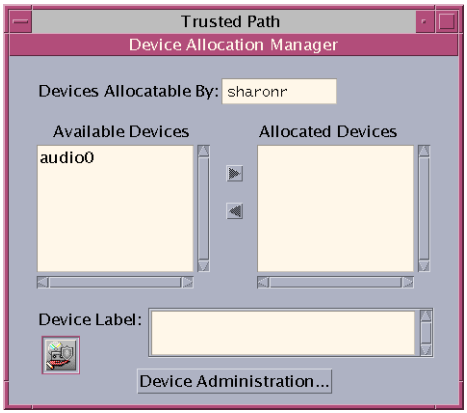


図 2–2　デバイス割り当てマネージャー GUI

Trusted Extensions でのデバイス保護については、第 17 章「Trusted Extensions でのデバイス管理 (手順)」を参照してください。

Solaris 管理コンソールツール

Solaris 管理コンソールから、GUI ベースの管理ツールのツールボックスにアクセスできます。これらのツールを使用して、さまざまな構成データベースの項目を編集できます。Trusted Extensions では、Solaris 管理コンソールはユーザー、役割、およびトラステッドネットワークデータベースの管理インタフェースになります。

Trusted Extensions は Solaris 管理コンソールを拡張します。

- Trusted Extensions は、&SMC の Users ツールセットを変更します。ツールセットの概要については、『System Administration Guide: Basic Administration』の第 2 章「Working With the Solaris Management Console (Tasks)」を参照してください。
- Trusted Extensions は、「コンピュータとネットワーク」ツールセットに「セキュリティーテンプレート」ツールと「トラステッドネットワークゾーン」ツールを追加します。

Solaris 管理コンソールツールはスコープとセキュリティーポリシーに従って「ツールボックス」にまとめられます。Trusted Extensions を管理するために、Trusted Extensions には `Policy=TSOL` のツールボックスが用意されています。ツールには、有効範囲、つまりネームサービスに従ってアクセスできます。利用可能な有効範囲は、ローカルホストと LDAP です。

次の図に Solaris 管理コンソールを示します。`Scope=Files` の Trusted Extensions ツールボックスがロードされ、Users ツールセットが開かれています。

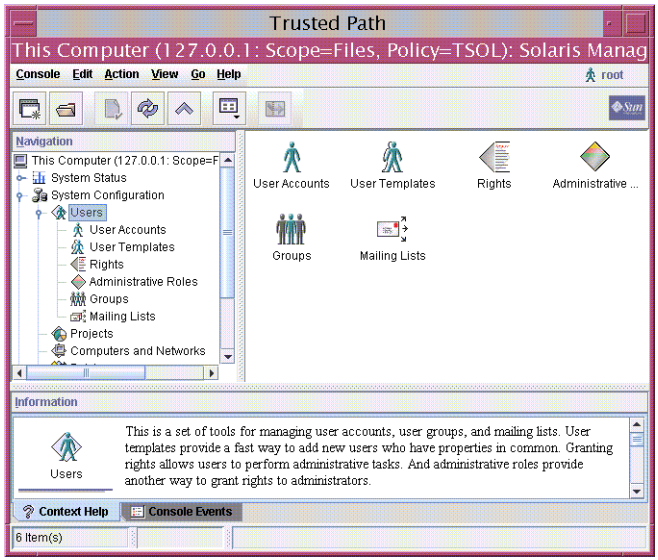


図 2–3　Solaris 管理コンソールの一般的な Trusted Extensions ツールボックス

Solaris 管理コンソールの Trusted Extensions ツール

Trusted Extensions は、次の 3 つのツールに構成可能なセキュリティー属性を追加します。

- 「ユーザーアカウント」ツール – ユーザーのラベルの変更、ユーザーに対するラベル表示の変更、およびアカウントの使用の制御のための管理インタフェースです。
- 「管理役割」ツール – 役割のラベル範囲とアイドル時の画面ロックの動作を変更するための管理インタフェースです。
- 「権利」ツール – 権利プロファイルに割り当てることができる CDE アクションが含まれます。これらのアクションに、セキュリティー属性を割り当てることができます。

Trusted Extensions は、「コンピュータとネットワーク」ツールセットに次の 2 つのツールを追加します。

- 「セキュリティーテンプレート」ツール – ホストとネットワークのラベルを管理するための管理インタフェースです。このツールは `tnrhtp` および `tnrhdb` データベースを修正し、構文の正確さを強制します。また、これらの変更を使用してカーネルを更新します。
- 「トラステッドネットワークゾーン」ツール – ゾーンのラベルを管理するための管理インタフェースです。このツールは `tnzonecfg` データベースを修正し、構文の正確さを強制します。また、これらの変更を使用してカーネルを更新します。

図 2–4 では、「ファイル」ツールボックスの「コンピュータとネットワーク」ツールセットが強調表示されています。Trusted Extensions ツールはツールセットの下に表示されます。

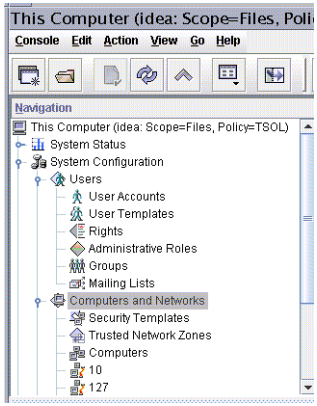


図 2–4　Solaris 管理コンソールの「コンピュータとネットワーク」ツールセット

「セキュリティーテンプレート」ツール

「セキュリティーテンプレート」は、ホストのグループに割り当てることができる一連のセキュリティー属性について説明します。「セキュリティーテンプレート」ツールを使用すると、特定の組み合わせのセキュリティー属性をホストのグループに簡単に割り当てることができます。これらの属性は、データをパッケージ、転送、および解釈する方法を制御します。1 つのテンプレートに割り当てられたホストは、いずれもセキュリティー設定が同じです。

ホストは「コンピュータ」ツールで定義されます。ホストのセキュリティー属性は「セキュリティーテンプレート」ツールで割り当てます。「テンプレートの変更」ダイアログボックスには、次の 2 つのタブがあります。

- 「一般」タブ – テンプレートを設定します。テンプレートの名前、ホストの種類、デフォルトのラベル、解釈のドメイン (DOI)、認可範囲、および不連続の機密ラベルのセットを設定します。
- 「テンプレートに割り当てるホスト」タブ – このテンプレートに割り当てたネットワーク上のすべてのホストが表示されます。

トラステッドネットワークとセキュリティーテンプレートについては、第 12 章「トラステッドネットワーク (概要)」を参照してください。

「トラステッドネットワークゾーン」ツール

「トラステッドネットワークゾーン」ツールは、システムのゾーンを識別します。最初は、大域ゾーンが表示されています。ゾーンとそのラベルを追加すると、区画にゾーン名が表示されます。ゾーンの作成は、一般的にシステムの構成中に行います。ラベルの割り当て、マルチレベルポートの構成、およびラベルポリシーは、このツールで構成します。詳細は、第 10 章「Trusted Extensions でのゾーンの管理 (手順)」を参照してください。

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

一般に、Solaris 管理コンソール クライアントはシステムを遠隔で管理します。ネームサービスとして LDAP を使用しているネットワークでは、Solaris 管理コンソール クライアントは LDAP サーバー上で動作する Solaris 管理コンソール サーバーに接続します。この構成を示したのが次の図です。

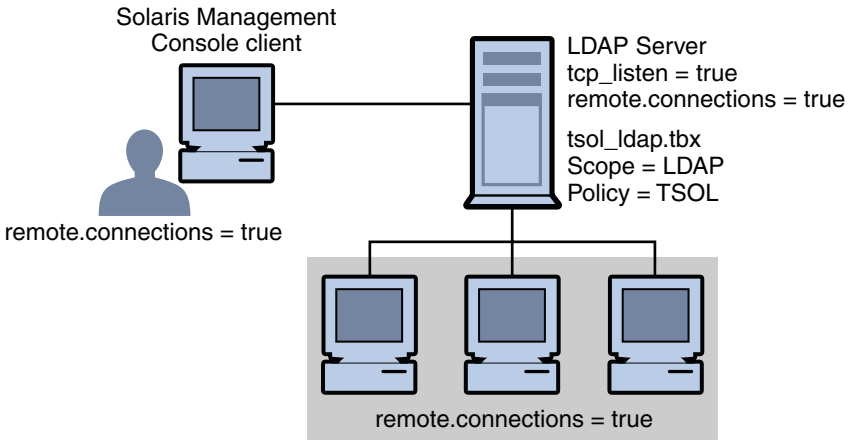


図 2–5　LDAP サーバーを使用してネットワークを管理する Solaris 管理コンソール クライアント

図 2–6 は、LDAP サーバーが構成されていないネットワークを示します。管理者は、Solaris 管理コンソール サーバーを使用して各遠隔システムを設定しました。

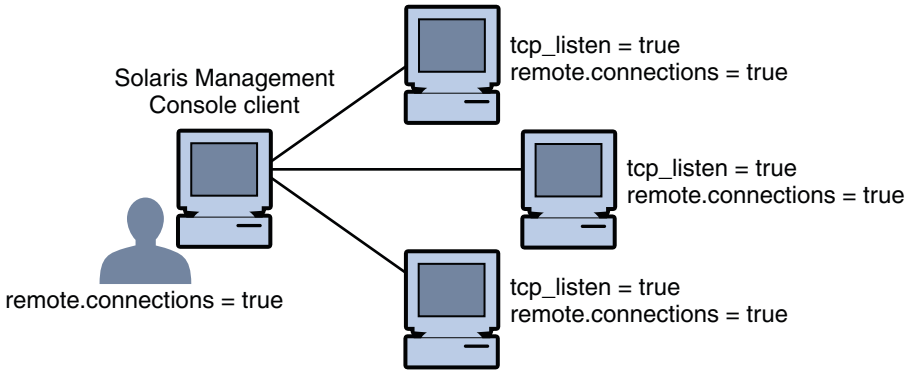


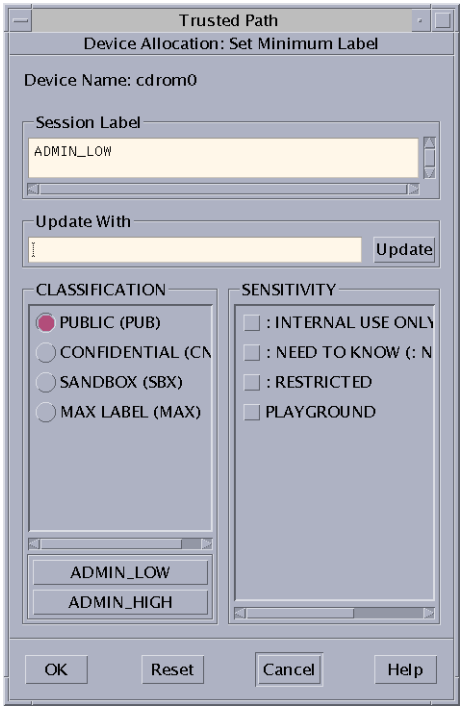
図 2–6 ネットワーク上の個々の遠隔システムを管理する Solaris 管理コンソール クライアント

Solaris 管理コンソールのマニュアル

Solaris 管理コンソールの主要なマニュアルは、オンラインヘルプで用意されています。現在選択している機能にコンテキストヘルプが関連付けられ、情報区画に表示されます。拡張ヘルプトピックは、「ヘルプ」メニューから、またはコンテキストヘルプのリンクをクリックして使用できます。詳細については、『System Administration Guide: Basic Administration』の第 2 章「Working With the Solaris Management Console (Tasks)」を参照してください。また、『System Administration Guide: Basic Administration』の「Using the Solaris Management Tools With RBAC (Task Map)」も参照してください。

Trusted Extensions のラベルビルダー

ラベルビルダー GUI では、プログラムでラベルの割り当てが必要とされるときに有効なラベルまた認可上限を選択します。たとえば、ラベルビルダーはログイン時に表示されます (『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)。ラベルビルダーは、ワークスペースのラベルの変更時、または Solaris 管理コンソールのユーザー、ゾーン、またはネットワークインタフェースにラベルを割り当てるときにも表示されます。新しいデバイスにラベル範囲を割り当てるときには、次のラベルビルダーが表示されます。



ラベルビルダーでは、「Classification」列の コンポーネント名 `label_encodings` ファイルの `CLASSIFICATIONS` セクションに対応します。「Sensitivity」列のコンポーネント名は`label_encodings` ファイルの `WORDS` セクションに対応します。

Trusted Extensions のコマンド行ツール

Trusted Extensions に固有なコマンドは、『Solaris Trusted Extensions リファレンスマニュアル』で説明しています。Trusted Extensions で Solaris のコマンドが修正されている場合、修正されたコマンドは『Solaris リファレンスマニュアル』で説明されています。`man` コマンドでは、すべてのコマンドのマニュアルページを表示できます。

次の表に、Trusted Extensions に固有なコマンドを示します。コマンドはマニュアルページの形式で示しています。

表 2–4 Trusted Extensions のユーザーコマンドおよび管理コマンド

マニュアルページ	Trusted Extensions による修正	詳細
add_allocatable(1M)	デバイスをデバイス割り当てデータベースに追加することで、デバイスを割り当て可能にします。デフォルトでは、リムーバブルデバイスを割り当て可能です。	251 ページの「Trusted Extensions でデバイスを構成する」
atohexlabel(1M)	ラベルを 16 進形式に変換します。	75 ページの「ラベルの 16 進値を求める」
chk_encodings(1M)	label_encodings ファイルの整合性を確認します。	『Solaris Trusted Extensions ラベルの管理』の「label_encodings ファイルをデバッグする」
dtappsession(1)	アプリケーションマネージャーを使用して、遠隔 Trusted CDE セッションを開きます。	第 8 章「Trusted Extensions での遠隔管理 (手順)」
getlabel(1)	選択したファイルまたはディレクトリのラベルを表示します。	135 ページの「マウントされたファイルのラベルを表示する」
getzonepath(1)	指定したゾーンのフルパス名を表示します。	『Solaris Trusted Extensions 開発ガイド』の「機密ラベルの取得」
hextoalabel(1M)	16 進形式のラベルを人が読める形式に変換します。	76 ページの「可読のラベルを 16 進形式から取得する」
plabel(1)	現在のプロセスのラベルを表示します。	マニュアルページを参照してください。
remove_allocatable(1M)	デバイス割り当てデータベースからエントリを削除して、デバイスの割り当てを防ぎます。	251 ページの「Trusted Extensions でデバイスを構成する」
setlabel(1)	選択した項目にラベルを付け直します。solaris.label.file.downgrade 承認または solaris.label.file.upgrade 承認が必要です。これらの承認は、Object Label Management 権利プロファイルにあります。	同等の GUI の手順については、『Solaris Trusted Extensions ユーザーズガイド』の「Trusted CDE でラベル間でファイルを移動する」を参照してください。
smtnrhdb(1M)	tnrhdb データベースのエントリを、ローカルまたはネームサービスデータベースで管理します。	Solaris 管理コンソールを使用する同等の手順については、184 ページの「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。
smtnrhtp(1M)	tnrhtp データベースのエントリを、ローカルまたはネームサービスデータベースで管理します。	マニュアルページを参照してください。

表 2–4 Trusted Extensions のユーザーコマンドおよび管理コマンド (続き)

マニュアルページ	Trusted Extensions による修正	詳細
smtnzonecfg(1M)	ローカル tnzonecfg データベースのエントリを管理します。	Solaris 管理コンソールを使用する同等の手順については、144 ページの「ゾーンにマルチレベルポートを作成する」を参照してください。
tnchkdb(1M)	tnrhdb データベースと tnrhtp データベースの整合性を確認します。	201 ページの「トラステッドネットワークデータベースの構文をチェックする」
tnctl(1M)	カーネルのネットワーク情報をキャッシュします。	203 ページの「カーネルキャッシュとトラステッドネットワークデータベースを同期する」
tnd(1M)	トラステッドネットワークデーモンを実行します。	203 ページの「カーネルキャッシュとトラステッドネットワークデータベースを同期する」
tninfo(1M)	カーネルレベルのネットワーク情報と統計を表示します。	202 ページの「トラステッドネットワークデータベース情報とカーネルキャッシュを比較する」
updatehome(1M)	現在のラベルの .copy_files と .link_files を更新します。	91 ページの「Trusted Extensions のユーザーの起動ファイルを構成する」

次の表に、Trusted Extensions で修正または拡張された Solaris コマンドを示します。コマンドはマニュアルページの形式で示しています。

表 2–5 Trusted Extensions で修正されたユーザーコマンドと管理コマンド

マニュアルページ	コマンドの用途	詳細
allocate(1)	割り当てたデバイスをクリーンアップするオプション、およびデバイスを特定のゾーンに割り当てるオプションを追加します。Trusted Extensions では、一般ユーザーはこのコマンドを使用しません。	『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」
deallocate(1)	デバイスをクリーンアップするオプション、および特定のゾーンからデバイスの割り当てを解除するオプションを追加します。Trusted Extensions では、一般ユーザーはこのコマンドを使用しません。	『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」

表 2–5 Trusted Extensions で修正されたユーザーコマンドと管理コマンド (続き)

マニュアルページ	コマンドの用途	詳細
list_devices(1)	承認やラベルなどの、デバイス属性を表示する -a オプションを追加します。割り当てられたデバイスタイプのデフォルト属性を表示する -d オプションを追加します。ラベル付きゾーンに割り当て可能なデバイスを表示する -z オプションを追加します。	マニュアルページを参照してください。
tar(1)	ラベル付きのファイルとディレクトリをアーカイブおよび抽出するための -T オプションを追加します。	155 ページの「Trusted Extensions でファイルをバックアップする」 and 155 ページの「Trusted Extensions でファイルを復元する」
auditconfig(1M)	windata_down および windata_up 監査ポリシーオプションを追加します。	『System Administration Guide: Security Services』の「How to Configure Audit Policy」
auditreduce(1M)	ラベルごとに監査レコードを選択するための -l オプションを追加します。	『System Administration Guide: Security Services』の「How to Select Audit Events From the Audit Trail」
automount(1M)	ゾーン名と上位ラベルからのゾーンの表示に対応するよう、auto_home マップの名前と内容を変更します。	152 ページの「Trusted Extensions のオートマウンタに対する変更」
ifconfig(1M)	インタフェースをシステムのすべてのゾーンで利用できるようにする all-zones オプションを追加します。	206 ページの「ホストのインタフェースが稼働していることを確認する」
netstat(1M)	ソケットと経路指定テーブルエントリの拡張されたセキュリティー属性を表示する -R オプションを追加します。	207 ページの「Trusted Extensions ネットワークをデバッグする」
route(1M)	-secattr オプションを追加します。このオプションは、送信経路のセキュリティー属性 cipso、doi、max_sl、および min_sl を表示します。	199 ページの「セキュリティー属性を使用して経路を構成する」

Trusted Extensions での遠隔管理

ssh コマンド、dtappsession プログラム、または Solaris 管理コンソールを使用すると、Trusted Extensions が設定されたシステムを遠隔で管理できます。サイトのセキュリティーポリシーで許可されている場合は、Trusted Extensions 以外のホストからログインできるように Trusted Extensions ホストを構成できます。ただし、この構成では安全性が低下します。詳細は、第 8 章「Trusted Extensions での遠隔管理 (手順)」を参照してください。

◆ ◆ ◆ 第 3 章

Trusted Extensions 管理者としての作業の開始 (手順)

この章では、Solaris Trusted Extensions が設定されたシステムの管理について概説します。

Trusted Extensions の新機能

Solaris 10 10/08 – このリリースでは、Trusted Extensions は次の機能を提供します。

- Trusted Extensions の共有 IP スタックを使用すると、デフォルトの経路のラベル付きゾーンを、互いに分離するか、または大域ゾーンから分離することができます。
- ループバックインタフェースの `lo0` は、`all-zones` インタフェースです。
- 役割によって責務分離を実施できます。システム管理者役割は、ユーザーの作成を行いますが、パスワードの割り当ては行えません。セキュリティー管理者役割は、パスワードの割り当てを行いますが、ユーザーの作成は行えません。詳細は、『Solaris Trusted Extensions 構成ガイド』の「責務分離を実施する権利プロファイルを作成する」を参照してください。
- このマニュアルの付録 B 「Trusted Extensions マニュアルページのリスト」には、Trusted Extensions のマニュアルページのリストが掲載されています。

Solaris 10 5/08 – このリリースでは、Trusted Extensions は次の機能を提供します。

- サービス管理機能 (SMF) では、Trusted Extensions を `svc:/system/labeld` サービスとして管理します。`labeld` サービスはデフォルトでは無効になっています。このサービスが有効になっているときは、引き続きシステムを設定および再起動して、Trusted Extensions のセキュリティーポリシーを適用する必要があります。
- システムが使用する CIPSO DOI (解釈のドメイン) の番号を設定できます。

  - DOI については、170 ページの「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。
  - デフォルトとは異なる DOI を指定する場合は、『Solaris Trusted Extensions 構成ガイド』の「解釈ドメインの構成」を参照してください。
- Trusted Extensions では、NFS バージョン 4 (NFSv4) だけでなく、NFS バージョン 3 (NFSv3) でマウントされたファイルシステムの CIPSO ラベルも認識します。そのため、NFSv3 ファイルシステムをラベル付きファイルシステムとして Trusted Extensions システムにマウントできます。NFSv3 のマルチレベルマウントの配下のプロトコルとして udp を使用する場合は、143 ページの「udp で NFSv3 のマルチレベルポートを構成する」を参照してください。
- ネームサービスキャッシュデーモン `nscd` を各ラベル付きゾーンでそれぞれのゾーンのラベルで実行されるように設定できます。

Trusted Extensions を管理する際のセキュリティー要件

Trusted Extensions では、通常、役割を使用してシステムを管理します。一般的に、スーパーユーザーは使用しません。役割は Solaris OS の場合と同様に作成され、ほとんどのタスクは役割によって実行されます。Trusted Extensions では、管理タスクの実行に `root` ユーザーを使用しません。

Trusted Extensions サイトでは、次の役割が一般的に使用されます。

- `root` 役割 – 初期設定チームによって作成されます。
- セキュリティー管理者役割 – 初期構成中または初期構成後に、初期設定チームによって作成されます
- システム管理者役割 – セキュリティー管理者役割によって作成されます

Solaris OS と同様に、主管理者、オペレータなどの役割を作成することもできます。`root` 役割を除き、作成する役割はネームサービスで管理できます。

Solaris OS 同様に、役割を割り当てられたユーザーだけが、その役割になることができます。Solaris Trusted Extensions (CDE) では、トラステッドパスメニューと呼ばれるデスクトップメニューから役割を引き受けることができます。 Solaris Trusted Extensions (JDS) では、ユーザー名がトラステッドストライプに表示されたときに役割を引き受けることができます。ユーザー名をクリックすると、役割の選択肢が表示されます。

Trusted Extensions での役割の作成

Trusted Extensions を管理するには、システムとセキュリティーの機能を分離する役割を作成します。初期設定チームは、構成中にセキュリティー管理者役割を作成しています。詳細は、『Solaris Trusted Extensions 構成ガイド』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。

Trusted Extensions で役割を作成する処理は、Solaris OS と同じです。第 2 章「Trusted Extensions 管理ツール」の説明のとおり、Solaris 管理コンソール は Trusted Extensions の役割を管理するためのグラフィカルユーザーインタフェースです。

- 役割の作成の概要については、『System Administration Guide: Security Services』の第 10 章「Role-Based Access Control (Reference)」と『System Administration Guide: Security Services』の「Using RBAC (Task Map)」を参照してください。
- スーパーユーザーと同等の役割を作成する場合は、『System Administration Guide: Basic Administration』の「Creating the Primary Administrator Role」を参照してください。Trusted Extensions を使用するサイトでは、主管理者役割はセキュリティーポリシーに違反する場合があります。これらのサイトでは、`root` を役割にして、セキュリティー管理者役割を作成します。
- `root` 役割の作成については、『System Administration Guide: Security Services』の「How to Make root User Into a Role」を参照してください。
- Solaris 管理コンソールを使用して役割を作成する方法については、『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。

Trusted Extensions での役割の引き受け

Solaris OS と異なり、Trusted Extensions には、トラステッドパスメニューに「*Rolename* の役割になる」メニュー項目があります。役割のパスワードを確認したあと、トラステッドパス属性を持つ役割のワークスペースが有効になります。役割のワークスペースは管理ワークスペースです。これらのワークスペースは大域ゾーンにあります。

Trusted Extensions 管理者としての作業の開始 (作業マップ)

Trusted Extensions の管理タスクを行う前に、次の手順に習熟するようにしてください。

作業	説明	参照先
ログインします。	安全にログインします。	『Solaris Trusted Extensions ユーザーズガイド』の「Trusted Extensions へのログイン」

作業	説明	参照先
デスクトップで共通のユーザータスクを実行します。	次のタスクが含まれます。 ■ ワークスペースの構成 ■ 異なるラベルでのワークスペースの使用 ■ Trusted Extensions マニュアルページへのアクセス ■ Trusted Extensions オンラインヘルプへのアクセス	『Solaris Trusted Extensions ユーザーズガイド』の「ラベル付きシステムでの作業」
トラステッドパスを必要とするタスクを実行します。	次のタスクが含まれます。 ■ デバイスの割り当て ■ パスワードの変更 ■ ワークスペースのラベルの変更	『Solaris Trusted Extensions ユーザーズガイド』の「トラステッドアクションの実行」
便利な役割を作成します。	サイトを管理するための役割を作成します。LDAP での役割の作成は一度だけのタスクです。 セキュリティー管理者役割は有効な役割です。	52 ページの「Trusted Extensions での役割の作成」 『Solaris Trusted Extensions 構成ガイド』の「Trusted Extensions でセキュリティー管理者役割を作成する」
(省略可能) root を役割にします。	root による匿名ログインを禁止します。このタスクはシステムごとに 1 度だけ実行します。	『System Administration Guide: Security Services』の「How to Make root User Into a Role」
役割になります。	役割の大域ゾーンに入ります。すべての管理タスクは大域ゾーンで実行されます。	55 ページの「Trusted Extensions の大域ゾーンに入る」
役割ワークスペースを終了し、一般ユーザーになります。	大域ゾーンを終了します。	56 ページの「Trusted Extensions の大域ゾーンを終了する」
ユーザー、役割、権利、ゾーン、およびネットワークをローカルで管理します。	Solaris 管理コンソールを使用して、分散システムを管理します。	57 ページの「Solaris 管理コンソールでローカルシステムを管理する」
Trusted CDE アクションを使用して、システムを管理します。	Trusted_Extensions フォルダの管理アクションを使用します。	58 ページの「Trusted Extensions の CDE 管理アクションを起動する」
管理ファイルを編集します。	トラステッドエディタでファイルを編集します。	59 ページの「Trusted Extensions の管理ファイルを編集する」
Trusted CDE でのデバイス割り当てを管理します。	デバイス割り当てマネージャー – 「デバイス管理」の GUI を使用します。	250 ページの「Trusted Extensions でのデバイスの管理 (作業マップ)」

▼ Trusted Extensions の大域ゾーンに入る

役割を引き受けることで、Trusted Extensions の大域ゾーンに入ります。システム全体の管理は、大域ゾーンからのみ実行することができます。大域ゾーンに入ることができるのは、スーパーユーザーと役割だけです。

役割になったあと、役割はユーザーのラベルでワークスペースを作成し、ラベル付きゾーンで管理ファイルを編集できます。

トラブルシューティングの場合は、フェイルセーフセッションを開始して大域ゾーンに入ることもできます。詳細については、95 ページの「Trusted Extensions でフェイルセーフセッションにログインする」を参照してください。

始める前に　1 つまたは複数の役割を作成しているか、大域ゾーンにスーパーユーザーとして入ることを計画します。52 ページの「Trusted Extensions での役割の作成」を参照してください。

1 トラステッド機構を使用します。

- **Solaris Trusted Extensions (JDS)** では、トラステッドストライプに表示されているユーザー名をクリックし、役割を選択します。

  役割が割り当てられている場合は、役割名がリストに表示されます。

  Trusted Extensions のデスクトップ機能の場所と意味については、『Solaris Trusted Extensions ユーザーズガイド』の第 4 章「Trusted Extensions の構成要素 (リファレンス)」を参照してください。

- **Solaris Trusted Extensions (CDE)** で、トラステッドパスメニューを開きます。

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

  b. トラステッドパスメニューの「*rolename* の役割になる」を選択します。

2 プロンプトが表示されたら、役割のパスワードを入力します。

Trusted CDE では、新しい役割のワークスペースが作成され、ワークスペーススイッチボタンが役割のデスクトップの色に変わり、各ウィンドウ上部のタイトルバーに「トラステッドパス」と表示されます。Trusted JDS では、現在のワークスペースが役割のワークスペースに変わります。

Trusted CDE では、マウスを使用して一般ユーザーのワークスペースを選択することで、役割のワークスペースを終了します。最後の役割のワークスペースを削除して、役割を終了することもできます。Trusted JDS では、トラステッドストライプ上の役割名をクリックし、メニューから別の役割またはユーザーを選択できます。このアクションにより、現在のワークスペースが新しい役割またはユーザーのプロセスに変わります。

▼ Trusted Extensions の大域ゾーンを終了する

役割を終了するためのメニューの場所は、Trusted JDS とTrusted CDE とでは異なります。

始める前に ここは大域ゾーンです。

- どちらのデスクトップでも、ワークスペーススイッチ領域でユーザーのワークスペースをクリックできます。

  また、次のいずれかの操作を実行して、役割のワークスペースを終了し、その結果、大域ゾーンを終了することもできます。

  - **Trusted JDS** では、トラステッドストライプに表示されている役割名をクリックします。

    役割名をクリックすると、ユーザー名と、引き受けることのできる役割のリストが表示されます。ユーザー名を選択すると、そのワークスペースで作成する以降のすべてのウィンドウが選択した名前で作成されます。現在のデスクトップで以前作成したウィンドウは、その役割の名前とラベルで引き続き表示されます。

    別の役割名を選択した場合は、別の役割で大域ゾーンに残ります。

  - **Trusted CDE** では、役割のワークスペースを削除します。

    ワークスペースボタンでマウスボタン 3 をクリックし、「削除」を選択します。最後に使用したワークスペースに戻ります。

▼ Solaris 管理コンソールでローカルシステムを管理する

システムで最初に Solaris 管理コンソールを起動する場合は、ツールの登録とさまざまなディレクトリの作成のために、待ち時間が発生します。この待ち時間は、一般的にシステムの構成中に発生します。手順については、『Solaris Trusted Extensions 構成ガイド』の「Trusted Extensions で Solaris 管理コンソールサーバーを初期化する」を参照してください。

遠隔システムを管理する場合は、110 ページの「Trusted Extensions の遠隔管理 (作業マップ)」を参照してください。

始める前に　役割になっている必要があります。詳細は、55 ページの「Trusted Extensions の大域ゾーンに入る」を参照してください。

1. **Solaris 管理コンソールを起動します。**

   Solaris Trusted Extensions (JDS) で、コマンド行を使用します。Trusted CDE では、次の 3 つの方法があります。

   - 端末ウィンドウで `smc` コマンドを使用します。

     ```
     $ /usr/sbin/smc &
     ```

   - フロントパネルの「ツール」プルアップメニューで、**Solaris 管理コンソール**のアイコンをクリックします。

   - **Trusted_Extensions** フォルダで、**Solaris 管理コンソール**のアイコンをダブルクリックします。

2. 「コンソール」の「ツールボックスを開く」を選択します。

3. リストから、適切な有効範囲の **Trusted Extensions** ツールボックスを選択します。

   Trusted Extensions ツールボックスには、名前の一部に `Policy=TSOL` が含まれています。Files の有効範囲は、現在のシステムのローカルファイルを更新します。LDAP の有効範囲は、Sun Java™ System Directory Server の LDAP ディレクトリを更新します。ツールボックスの名前は次のようになります。

   このコンピュータ (*remote-system*: `Scope=Files, Policy=TSOL`)
   このコンピュータ (*ldap-server*: `Scope=LDAP, Policy=TSOL`)

4. **目的の Solaris 管理コンソールツールに移動します。**

   パスワードプロンプトが表示されます。

   Trusted Extensions で修正されているツールについては、「システムの構成」をクリックします。

5 パスワードを入力します。

Solaris 管理コンソールツールのその他の情報については、オンラインヘルプを参照してください。Trusted Extensions で修正されたツールについては、40 ページの「Solaris 管理コンソールツール」を参照してください。

6 **GUI** を閉じるには、「コンソール」メニューの「終了」を選択します。

▼ Trusted Extensions の CDE 管理アクションを起動する

1 役割になります。

詳細は、55 ページの「Trusted Extensions の大域ゾーンに入る」を参照してください。

2 **Trusted CDE** で、アプリケーションマネージャーを開きます。

a. 背景でマウスボタン **3** をクリックし、「ワークスペース」メニューを開きます。

b. 「アプリケーション」をクリックし、「アプリケーション・マネージャ」メニュー項目をクリックします。

アプリケーションマネージャーに Trusted_Extensions フォルダが表示されます。

3 **Trusted_Extensions** フォルダを開きます。

4 該当するアイコンをダブルクリックします。
管理アクションのリストについては、37 ページの「Trusted CDE アクション」を参照してください。

▼ Trusted Extensions の管理ファイルを編集する

管理ファイルは、監査を伴うトラステッドエディタで編集します。このエディタは、ユーザーがシェルコマンドを実行したり、元のファイルの名前と異なるファイル名で保存したりすることも防止します。

1 役割になります。
詳細は、55 ページの「Trusted Extensions の大域ゾーンに入る」を参照してください。

2 トラステッドエディタを開きます。

- **Solaris Trusted Extensions (CDE)** で、次の操作を行います。

  a. エディタを開くには、背景でマウスボタン **3** をクリックし、「ワークスペース」メニューを開きます。

  b. 「アプリケーション」をクリックし、「アプリケーション・マネージャ」メニュー項目をクリックします。
  アプリケーションマネージャーに Trusted_Extensions フォルダが表示されます。

  c. **Trusted_Extensions** フォルダを開きます。

  d. 「管理エディタ」アクションをダブルクリックします。
  ファイル名を入力するように要求されます。形式については、手順 3 と手順 4 を参照してください。

- **Solaris Trusted Extensions (JDS)** で、次の操作を行います。

  - (省略可能) `gedit` をトラステッドエディタとして使用するには、`EDITOR` 変数を変更します。
  詳細は、72 ページの「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。

  - コマンド行を使用して、トラステッドエディタを開きます。
  `# /usr/dt/bin/trusted_edit` *filename*
  filename 引数を入力してください。

3 新しいファイルを作成するには、新しいファイルのフルパス名を入力します。
ファイルを保存する場合、エディタは一時ファイルを作成します。

4 既存のファイルを編集するには、既存のファイルのフルパス名を入力します。

注 – エディタに「Save As」オプションがある場合、そのオプションは使用しないでください。ファイルを保存するには、エディタの「Save」オプションを使用してください。

---

5 ファイルを指定のパス名で保存するには、エディタを閉じます。

◆ ◆ ◆ 第 4 章

Trusted Extensions システムのセキュリティー要件 (概要)

この章では、Solaris Trusted Extensions が設定されたシステムの、構成可能なセキュリティー機能について説明します。

Solaris の構成可能なセキュリティー機能

Trusted Extensions には、Solaris OS と同じセキュリティー機能に加え、いくつかの機能が追加されています。たとえば、Solaris OS には `eeprom` 保護、パスワードの要件、強力なパスワードアルゴリズム、ユーザーのロックアウトによるシステムの保護、キーボードによるシャットダウンからの保護が用意されています。

これらのセキュリティーのデフォルトを修正するために行う実際の手順は、Trusted Extensions と Solaris OS で異なっています。Trusted Extensions では、一般的に役割を引き受けることによってシステムを管理します。ローカル設定は、トラステッドエディタを使用して修正します。ユーザー、役割、およびホストのネットワークに影響を与える変更は、Solaris 管理コンソールで行います。

セキュリティー機能を構成するための Trusted Extensions インタフェース

このマニュアルでは、Trusted Extensions でセキュリティー設定を変更するために特定のインタフェースが必要とされるときに、そのインタフェースが Solaris OS ではオプションである場合の手順について説明します。Trusted Extensions でトラステッドエディタを使用してローカルファイルを編集する必要がある場合については、このマニュアルでは説明していません。たとえば、102 ページの「ユーザーのアカウント

ロックを禁止する」の手順では、アカウントがロックされるのを防ぐために、Solaris 管理コンソールを使用してユーザーのアカウントを更新する方法を説明しています。ただし、システム全体のパスワードロックのポリシーを設定する手順は説明していません。Trusted Extensions ではトラステッドエディタを使用してシステムファイルを修正することを除き、Solaris の指示に従います。

Trusted Extensions による Solaris セキュリティー機構の拡張

次の Solaris のセキュリティー機構は、Solaris OS の場合と同様に、Trusted Extensions で拡張可能です。

- 監査イベントと監査クラス – 監査イベントと監査クラスの追加については、『System Administration Guide: Security Services』の第 30 章「Managing Solaris Auditing (Tasks)」で説明しています。
- 権利プロファイル – 権利プロファイルの追加については、『System Administration Guide: Security Services』のパート III「Roles, Rights Profiles, and Privileges」を参照してください。
- 役割 – 役割の追加については、『System Administration Guide: Security Services』のパート III「Roles, Rights Profiles, and Privileges」を参照してください。
- 承認– 新しい承認の追加例については、260 ページの「Trusted Extensions でのデバイス承認のカスタマイズ (作業マップ)」を参照してください。

Solaris OS と同様に、特権を拡張することはできません。

Trusted Extensions のセキュリティー機能

Trusted Extensions には、次に示す固有のセキュリティー機能が用意されています。

- ラベル – サブジェクトとオブジェクトにはラベルが付けられます。プロセスにラベルが付けられます。ゾーンとネットワークにラベルが付けられます。
- デバイス割り当てマネージャー – デフォルトでは、デバイスは割り当て要件により保護されます。このデバイス割り当てマネージャーの GUI は、管理者と一般ユーザー用のインタフェースです。
- 「パスワードを変更」メニュー項目– トラステッドパスメニューにより、ユーザーパスワードと、自分がなった役割のパスワードを変更できます。

セキュリティー要件の実施

システムのセキュリティーを低下させないため、管理者は、パスワード、ファイル、および監査データを保護する必要があります。ユーザーは、各自の役目を果たせるようにトレーニングを受ける必要があります。評価された構成の要件に矛盾しないように、この節のガイドラインに従ってください。

ユーザーとセキュリティーの要件

各サイトのセキュリティー管理者は、ユーザーがセキュリティー手順のトレーニングを受けたか確認します。セキュリティー管理者は、新しい従業員に次の規則を伝え、既存の従業員に対してもこれらの規則への注意を定期的に喚起する必要があります。

- 他人に教えないでください。

  パスワードを他人に知られると、権限のない人物が自分と同じ情報にアクセスできることになります。
- 自分のパスワードを書き留めたり、電子メールのメッセージに入力しないでください。
- 推測しにくいパスワードを選択してください。
- パスワードを電子メールで他人に送信しないでください。
- 画面をロックせずに、またはログオフすることなく、コンピュータから離れないでください。
- ユーザーに指示を出すときに管理者は電子メールを信頼していないことに留意してください。管理者からの指示が電子メールで届いた場合は、最初に必ず管理者に確認してください。

  電子メールの送信者情報は偽造されている可能性があることに注意してください。
- 作成したファイルとディレクトリのアクセス権は各自に責任があるため、自分で作成したファイルやディレクトリのアクセス権が適切に設定されていることを確認してください。権限のないユーザーに対して、ファイルの読み取り、ファイルの変更、ディレクトリの内容の表示、またはディレクトリへの追加を許可しないでください。

管理者のサイトでは、ほかにも提案を追加できます。

電子メールの使用

電子メールを使用してユーザーに指示を伝えるのは安全な方法ではありません。

管理者を装って送信された電子メールの指示は信用しないように、ユーザーに通知してください。これにより、偽の電子メールメッセージによって、ユーザーがパスワードを特定の値に変更したり、パスワードを公表したりする可能性を避けることができます。結果的に、攻撃者が入手したパスワードでシステムにログインし被害を与えることを防止できます。

パスワードの強化

システム管理者役割は、新しいアカウントを作成するときに一意のユーザー名とユーザー ID を指定する必要があります。管理者は新しいアカウントの名前と ID を選択するときに、ユーザー名とユーザー名に関連付ける ID のどちらもネットワーク全体で重複がなく、以前に使用されていないことを確認する必要があります。

セキュリティー管理者役割は、各アカウントの初期パスワードを指定し、これを新しいアカウントのユーザーに伝える責任があります。パスワードを管理するときに次の情報を考慮してください。

- セキュリティー管理者役割になることができるユーザーのアカウントは、アカウントがロックされないように構成してください。これにより、少なくとも 1 つのアカウントは常にログイン可能で、ほかのアカウントがすべてロックされた場合でも、セキュリティー管理者役割になってこれらのアカウントを再度開くことができるようにします。
- 新しいアカウントのユーザーにパスワードを伝えるときには、他人に知られないような方法を使用してください。
- アカウントのパスワードを知るべきではない第三者に知られた疑いがある場合は、パスワードを変更してください。
- そのシステムが存続している間は、一度使用したユーザー名やユーザー ID は再利用しないでください。

  ユーザー名やユーザー ID を再利用しないことで、次のような混乱を避けることができます。

  - 監査記録を分析するときに、だれがどのアクションを実行したかがわからなくなる。
  - アーカイブしたファイルを復元するときに、どのユーザーがどのファイルを所有しているかわからなくなる。

情報の保護

管理者は、セキュリティーが重要なファイルについて、任意アクセス制御 (DAC) と必須アクセス制御 (MAC) の保護を正しく設定して保守する責任があります。重要なファイルには、次のようなファイルが含まれます。

- `shadow` ファイル – 暗号化されたパスワードが含まれます。`shadow(4)` のマニュアルページを参照してください。
- `prof_attr` データベース – 権利プロファイルの定義が含まれます。`prof_attr(4)` のマニュアルページを参照してください。
- `exec_attr` データベース – 権利プロファイルの一部であるコマンドとアクションが含まれます。`exec_attr(4)` のマニュアルページを参照してください。
- `user_attr` **file** – ローカルユーザーに割り当てられている権利プロファイル、特権、および承認が含まれます。`user_attr(4)` のマニュアルページを参照してください。
- **Audit trail** – 監査サービスによって収集された監査記録が含まれます。`audit.log(4)` のマニュアルページを参照してください。

注意 – LDAP エントリの保護機構は、Trusted Extensions ソフトウェアで実施されるアクセス制御ポリシーの影響を受けないため、デフォルトの LDAP エントリを拡張したり、LDAP のアクセス規則を変更してはいけません。

パスワードの保護

ローカルファイルでは、パスワードは DAC によって表示から保護され、DAC と MAC の両方によって修正から保護されます。ローカルアカウントのパスワードは `/etc/shadow` ファイルに保持されます。このファイルを読み取ることができるのはスーパーユーザーだけです。詳細は、`shadow(4)` のマニュアルページを参照してください。

グループ管理

システム管理者役割は、ローカルシステムとネットワークで、すべてのグループに一意のグループ ID (GID) が設定されていることを確認する必要があります。

ローカルグループをシステムから削除する場合、システム管理者役割は次のことを確認する必要があります。

- 削除するグループの GID を持つオブジェクトはすべて、削除するか、別のグループに割り当てる必要があります。
- 削除対象のグループを一次グループとして所有するユーザーはすべて、別の一次グループに再割り当てされる必要があります。

ユーザーの削除について

アカウントをシステムから削除する場合、システム管理者役割とセキュリティー管理者役割は、次の操作を実行する必要があります。

- 各ゾーンのアカウントのホームディレクトリを削除します。
- 削除するアカウントに属するプロセスまたはジョブをすべて削除します。
  - そのアカウントが所有するオブジェクトをすべて削除するか、または所有権を別のユーザーに割り当てます。
  - ユーザーの代わりに、予定されている `at` または `batch` ジョブをすべて削除します。詳細は、`at(1)` および `crontab(1)` のマニュアルページを参照してください。
- 絶対にユーザー (アカウント) 名またはユーザー ID を再利用しないでください。

データのセキュリティーレベルを変更する際の規則

デフォルトでは、一般ユーザーはファイルと選択範囲の両方に対して、カット&ペースト、コピー&ペースト、およびドラッグ&ドロップ操作を実行できます。ソースとターゲットは、同じラベルである必要があります。

ファイルのラベルや、ファイルに含まれる情報のラベルを変更するには、承認が必要です。ユーザーがデータのセキュリティーレベルを変更することが承認されている場合は、選択マネージャーアプリケーションを介して転送が行われます。`/usr/dt/config/sel_config` ファイルは、ファイルのラベルを再設定するアクションや、別のラベルへの情報のカットおよびコピーを制御します。`/usr/dt/bin/sel_mgr` アプリケーションは、ウィンドウ間のドラッグ&ドロップ操作を制御します。次の表が示すように、選択範囲の再ラベル付けはファイルの再ラベル付けよりも多くの制限が加わります。

次の表に、ファイルの再ラベル付け規則の概要を示します。この規則は、カット&ペースト、コピー&ペースト、およびドラッグ&ドロップを対象としています。

表 4–1 新しいラベルにファイルを移動する条件

トランザクションの説明	ラベルの関係	所有者の関係	必要な承認
ファイルマネージャー間でのファイルのコピー&ペースト、カット&ペースト、またはドラッグ&ドロップ	同一ラベル	同一 UID	なし
	ダウングレード	同一 UID	`solaris.label.file.downgrade`
	アップグレード	同一 UID	`solaris.label.file.upgrade`
	ダウングレード	異なる UID	`solaris.label.file.downgrade`
	アップグレード	異なる UID	`solaris.label.file.upgrade`

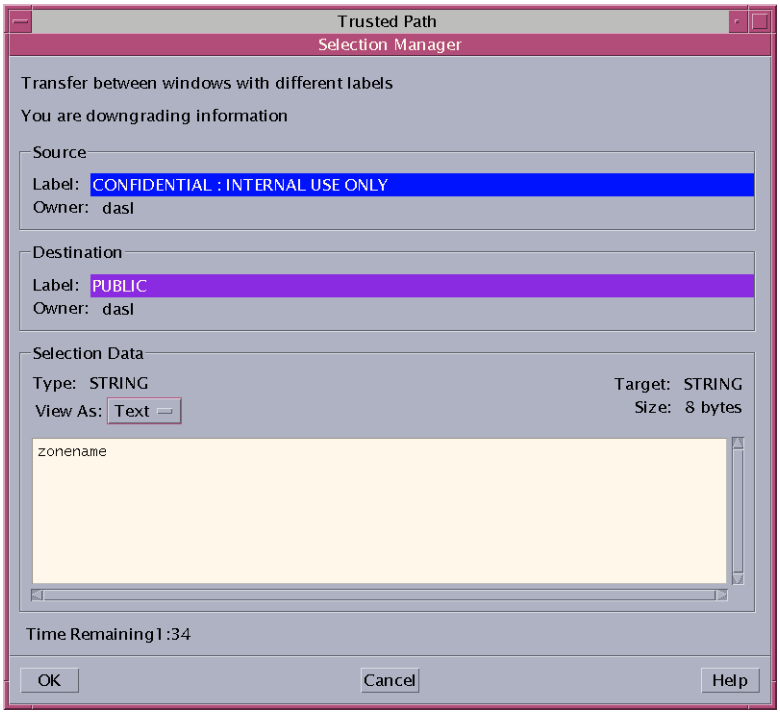
ウィンドウ内やファイル内の選択範囲には、異なる規則が適用されます。「選択範囲」のドラッグ&ドロップでは、常にラベルと所有者が同じである必要があります。ウィンドウ間のドラッグ&ドロップは、`sel_config` ファイルではなく、`sel_mgr` アプリケーションを介して行われます。

選択範囲のラベルを変更するための規則を、次の表に示します。

表 4–2 新しいラベルに選択範囲を移動する条件

トランザクションの説明	ラベルの関係	所有者の関係	必要な承認
ウィンドウ間での選択範囲のコピー&ペースト、またはカット&ペースト	同一ラベル	同一 UID	なし
	ダウングレード	同一 UID	`solaris.label.win.downgrade`
	アップグレード	同一 UID	`solaris.label.win.upgrade`
	ダウングレード	異なる UID	`solaris.label.win.downgrade`
	アップグレード	異なる UID	`solaris.label.win.upgrade`
ウィンドウ間での選択範囲のドラッグ&ドロップ	同一ラベル	同一 UID	適用なし

Trusted Extensions により、ラベル変更を伝達するための選択確認ダイアログボックスが表示されます。承認されたユーザーがファイルまたは選択範囲のラベルを変更しようとすると、このダイアログボックスが表示されます。ユーザーは 120 秒以内に操作を確定します。このウィンドウを使用せずにデータのセキュリティーレベルを変更するには、ラベル変更の承認に加えて、`solaris.label.win.noview` 承認が必要です。次の図はウィンドウでの選択範囲 `zonename` を示しています。



デフォルトでは、データを別のラベルに転送するごとに選択範囲確認のダイアログボックスが表示されます。1 つの選択範囲に複数の転送を決定する必要がある場合は、自動応答メカニズムにより複数の転送に 1 度で応答できます。詳細は、`sel_config(4)` のマニュアルページと次の節を参照してください。

sel_config ファイル

`sel_config` ファイルは、操作によってラベルがアップグレードまたはダウングレードされる場合の、選択範囲確認ダイアログボックスの動作を決定するために確認されます。

この `sel_config` ファイルでは、次の内容を定義します。

- 自動応答する選択範囲の種類のリスト
- 特定の種類の操作を自動的に確認するかどうか
- 選択範囲確認のダイアログボックスを表示するかどうか

セキュリティー管理者役割は、Trusted CDE で Trusted_Extensions フォルダの「選択範囲確認の設定」アクションを使用して、デフォルトを変更できます。新しい設定は、次回のログイン時に有効になります。Solaris Trusted Extensions (JDS) でファイルを修正している場合は、CDE アクションを使用しないでください。`sel_config`

ファイルを /etc/dt/config ディレクトリにコピーします。ほかの CDE 構成ファイルをカスタマイズする場合と同じように、作成したコピーをカスタマイズします。

Solaris Trusted Extensions (CDE) のカスタマイズ

Solaris Trusted Extensions (CDE) では、ユーザーは、フロントパネルにアクションを追加したり、ワークスペースメニューをカスタマイズしたりできます。Trusted Extensions ソフトウェアは、ユーザーによる CDE へのプログラムとコマンドの追加を制限しています。

フロントパネルのカスタマイズ

アプリケーションマネージャーの既存のアクションは、修正を行うアカウントのプロファイルにそのアクションがあれば、だれでもフロントパネルにドラッグ&ドロップすることができます。/usr/dt/ または /etc/dt/ ディレクトリにあるアクションはフロントパネルに追加できます。ただし、$HOME/.dt/appconfig ディレクトリにあるアプリケーションは追加できません。ユーザーは「アクション作成」アクションを使用できますが、システム全体で使用するアクションが保存されているディレクトリに書き込みを行うことはできません。したがって、一般ユーザーは使用可能なアクションを作成できません。

Trusted Extensions では、アクションの検索パスが変更されています。個人のホームディレクトリにあるアクションは、最初ではなく最後に処理されます。したがって、既存のアクションをカスタマイズすることはできません。

セキュリティー管理者役割には「管理エディタ」アクションが割り当てられているので、/usr/dt/appconfig/types/C/dtwm.fp ファイルやフロントパネルサブパネル用のほかの構成ファイルに必要な修正を行うことができます。

ワークスペースメニューのカスタマイズ

ワークスペースメニューは、ワークスペースの背景をマウスボタン 3 でクリックしたときに表示されるメニューです。一般ユーザーは、メニューをカスタマイズし、メニューに項目を追加することができます。

複数ラベルでの作業がユーザーに許可されている場合は、次の条件が適用されます。

- ユーザーは大域ゾーンにホームディレクトリを所有している必要があります。

  カスタマイズを保存するには、大域ゾーンのプロセスが正しいラベルでユーザーのホームディレクトリに書き込める必要があります。大域ゾーンプロセスで書き込み可能なユーザーのホームディレクトリへのゾーンパスは、次のようなパスになります。

  /zone/*zone-name*/home/*username*

- ユーザーは一般ユーザーのワークスペースで、「メニューをカスタマイズ」と「ワークスペースメニューに項目を追加」のオプションを使用する必要があります。ユーザーは各ラベルごとに異なるカスタマイズを作成できます。
- ユーザーが役割になるときに、ワークスペースメニューへの変更は維持されます。
- ワークスペースメニューに対する変更は、ユーザーの現在のラベルのホームディレクトリに保存されます。カスタマイズされるメニューファイルは `.dt/wsmenu` です。
- ユーザーの権利プロファイルでは、必要なアクションをユーザーが実行できるようにします。

  ワークスペースメニューに追加するアクションは、ユーザーの権利プロファイルのいずれかで処理する必要があります。そうしなければ、アクションの呼び出しに失敗し、エラーメッセージが表示されます。

  たとえば、アクションまたはアクションが呼び出すコマンドがアカウントの権利プロファイルのいずれにもない場合でも、「実行」アクションを設定したユーザーはだれでも、任意の実行可能ファイルのアイコンをダブルクリックして実行することができます。デフォルトでは、役割に「実行」アクションは割り当てられていません。したがって、「実行」アクションを必要とするメニュー項目は、役割によって実行された場合に失敗します。

◆ ◆ ◆ 第 5 章

Trusted Extensions でのセキュリティー要件の管理 (手順)

この章では、Solaris Trusted Extensions が設定されたシステムで実行されることの多いタスクについて説明します。

Trusted Extensions の一般的なタスク (作業マップ)

次の作業マップでは、Trusted Extensions の管理者の作業環境を設定する手順について説明します。

作業	説明	参照先
トラステッドエディタとしてのエディタプログラムを変更します。	管理ファイル用のエディタを指定します。	72 ページの「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」
root ユーザーのパスワードを変更します。	root ユーザーまたは root 役割に新しいパスワードを指定します。	73 ページの「root ユーザーのパスワードを変更する」
役割のパスワードを変更します。	現在の役割に新しいパスワードを指定します。	例 5–2
セキュアアテンションキーの組み合わせを使用します。	マウスまたはキーボードを制御します。また、マウスまたはキーボードが信頼できるかもテストします。	74 ページの「デスクトップの現在のフォーカスへの制御を取り戻す」
ラベルの 16 進値を決定します。	テキストラベルの内部形式を表示します。	75 ページの「ラベルの 16 進値を求める」
ラベルのテキスト表現を確認します。	16 進ラベルのテキスト表現を表示します。	76 ページの「可読のラベルを 16 進形式から取得する」
システムファイルを編集します。	Solaris または Trusted Extensions のシステムファイルを安全に編集します。	77 ページの「システムファイルでセキュリティーデフォルトを変更する」

作業	説明	参照先
デバイスを割り当てます。	周辺機器を使用して、システムに情報を追加したりシステムから情報を削除したりします。	『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」
ホストを遠隔で管理します。	Solaris または Trusted Extensions ホストを遠隔ホストから管理します。	第 8 章「Trusted Extensions での遠隔管理 (手順)」

▼ 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

トラステッドエディタは、環境変数 `$EDITOR` の値をエディタとして使用します。

始める前に　大域ゾーンで、役割になっている必要があります。

1. `$EDITOR` 変数の値を確認します。

   ```
   # echo $EDITOR
   ```

   次のエディタを使用できます。`$EDITOR` 変数は設定されていない場合もあります。

   - `/usr/dt/bin/dtpad` – CDE で用意されているエディタです。
   - `/usr/bin/gedit` – Java Desktop System, Release *number* で用意されているエディタです。Solaris Trusted Extensions (JDS) はそのデスクトップのトラステッドバージョンです。
   - `/usr/bin/vi` – ビジュアルエディタです。

2. `$EDITOR` 変数の値を設定します。

   - 値を固定的に設定するには、役割のシェル初期設定ファイルで値を修正します。
     たとえば、役割のホームディレクトリで、Korn シェルについては `.kshrc` ファイルを、C シェルについては `.cshrc` ファイルを修正します。

   - 現在のシェル用に値を設定するには、端末ウィンドウで値を設定します。
     たとえば、Korn シェルでは次のコマンドを使用します。

     ```
     # setenv EDITOR=pathname-of-editor
     # export $EDITOR
     ```

     C シェルでは次のコマンドを使用します。

     ```
     # setenv EDITOR=pathname-of-editor
     ```

Bourne シェルでは次のコマンドを使用します。

```
# EDITOR=pathname-of-editor
# export EDITOR
```

例 5–1 トラステッドエディタ用のエディタの指定

セキュリティー管理者役割が、システムファイルの編集に vi を使用するとします。この役割になっているユーザーが、役割のホームディレクトリにある .kshrc 初期設定ファイルを修正します。

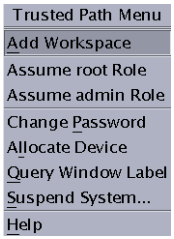
```
$ cd /home/secadmin
$ vi .kshrc

## Interactive shell
set -o vi
...
export EDITOR=vi
```

次にどのユーザーがセキュリティー管理者役割になっても、 vi がトラステッドエディタとなります。

▼ root ユーザーのパスワードを変更する

セキュリティー管理者役割は、Solaris 管理コンソールを使っていつでも任意のアカウントのパスワードを変更することが承認されています。ただし、Solaris 管理コンソールではシステムアカウントのパスワードは変更できません。「システムアカウント」とは、UID が 100 未満のアカウントです。root は、UID が 0 なのでシステムアカウントです。

1. スーパーユーザーになります。
   サイトでスーパーユーザーを root 役割にしている場合は、root 役割になります。
2. トラステッドパスメニューから「パスワード変更 **(Change Password)**」を選択します。



3 パスワードを変更し、変更を確定します。

例 5–2 役割のパスワードの変更

LDAP で定義されている役割になることのできるユーザーならだれでも、トラステッドパスメニューを使用して、その役割のパスワードを変更できます。こうすると、その役割になろうとするすべてのユーザーに対して LDAP でパスワードが変更されます。

Solaris OS と同様に、主管理者役割は Solaris 管理コンソールを使用して役割のパスワードを変更できます。Trusted Extensions では、セキュリティー管理者役割は Solaris 管理コンソールを使用して別の役割のパスワードを変更できます。

▼ デスクトップの現在のフォーカスへの制御を取り戻す

「セキュアアテンション」キーの組み合わせは、信頼できないアプリケーションによるポインタグラブやキーボードグラブを解除するために使用できます。また、このキーの組み合わせは、ポインタまたはキーボードが信頼できるアプリケーションによってグラブされているかどうかを確認するためにも使用できます。複数のトラステッドストライプを表示するようにスプーフィングされているマルチヘッドシステムでは、このキーの組み合わせにより、ポインタは承認されているトラステッドストライプに移動します。

1 **Sun 製キーボードの制御を取り戻すには、次のキーの組み合わせを使用します。**

キーを同時に押して、現在のデスクトップのフォーカスへの制御を取り戻します。Sun 製キーボードでは、ダイヤモンドマークの付いたキーが Meta キーです。

```
<Meta> <Stop>
```

ポインタなどのグラブが信頼できない場合は、このポインタはストライプに移動します。信頼できるポインタはトラステッドストライプには移動しません。

2 **Sun 製以外のキーボードでは、次のキーの組み合わせを使用してください。**

```
<Alt> <Break>
```

キーを同時に押して、ラップトップコンピュータ上で現在のデスクトップのフォーカスへの制御を取り戻します。

例 5–3 パスワードのプロンプトが信頼できるかどうかテストする

Sun 製キーボードを使用している x86 システム上で、ユーザーがパスワードの入力を求められたとします。カーソルはグラブされた状態になり、パスワード入力ダイアログボックスの中にあります。プロンプトが信頼できることを確認するために、ユーザーは <Meta> <Stop> キーを同時に押します。ポインタがダイアログボックスの中に残っているときに、ユーザーはパスワードプロンプトが信頼できることを認識します。

ポインタがトラステッドストライプに移動していた場合は、ユーザーはパスワードプロンプトが信頼できないことがわかるので、管理者に連絡します。

例 5–4 ポインタを強制的にトラステッドストライプに移動させる

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

▼ ラベルの 16 進値を求める

この手順では、ラベルの内部 16 進形式について説明します。この形式は、公共ディレクトリでの格納に安全です。詳細は、`atohexlabel(1M)` のマニュアルページを参照してください。

始める前に 大域ゾーンでセキュリティー管理者役割になります。詳細は、55 ページの「Trusted Extensions の大域ゾーンに入る」を参照してください。

- ラベルの 16 進値を求めるには、次のいずれかの操作を行います。
  - 機密ラベルの 16 進値を求めるには、ラベルをコマンドに渡します。

    ```
    $ atohexlabel "CONFIDENTIAL : NEED TO KNOW"
    0x0004-08-68
    ```

  - 認可上限の 16 進値を求めるには、`-c` オプションを使用します。

    ```
    $ atohexlabel -c "CONFIDENTIAL NEED TO KNOW"
    0x0004-08-68
    ```

注 – 可読式の機密ラベルと認可上限ラベルは label_encodings ファイルの中のルールに従って形成されます。各ラベルタイプでは、このファイルの別々のセクションにあるルールを使用します。機密ラベルと認可上限ラベルの両方が根本的に同じレベルの機密性を表している場合は、両方のラベルはまったく同じ 16 進形式になります。ただし、両ラベルの可読形式は異なることがあります。可読形式のラベルを入力として受け入れるシステムインタフェースは、1 つのタイプのラベルを想定しています。ラベルタイプの文字列が異なっている場合、これらの文字列は相互に利用することはできません。

デフォルトの label_encodings ファイルでは、認可上限ラベルと同等のテキストにコロン (:) は含まれません 。

例 5–5 atohexlabel コマンドの使用法

有効なラベルを 16 進形式で渡すと、コマンドは次のように引数を返します。

```
$ atohexlabel 0x0004-08-68
0x0004-08-68
```

管理ラベルを渡すと、コマンドは次のように引数を返します。

```
$ atohexlabel admin_high
ADMIN_HIGH
atohexlabel admin_low
ADMIN_LOW
```

注意事項 atohexlabel parsing error found in <string> at position 0 というエラーメッセージは、atohexlabel に渡した <string> 引数が有効なラベルまたは認可上限でないことを意味しています。入力を確認し、インストールした label_encodings ファイルにラベルが存在していることを確認します。

▼ 可読のラベルを 16 進形式から取得する

この手順では、内部データベースに格納されているラベルを確認する方法について説明します。詳細は、hextoalabel(1M) のマニュアルページを参照してください。

始める前に 大域ゾーンでセキュリティー管理者役割になります。

- ラベルの内部表現に相当するテキストを取得するには、次のいずれかの操作を行います。
  - 機密ラベルに相当するテキストを取得するには、ラベルの 16 進形式を渡します。

    ```
    $ hextoalabel 0x0004-08-68
    CONFIDENTIAL : NEED TO KNOW
    ```

  - 認可上限に相当するテキストを求めるには、-c オプションを使用します。

    ```
    $ hextoalabel -c 0x0004-08-68
    CONFIDENTIAL NEED TO KNOW
    ```

▼ システムファイルでセキュリティーデフォルトを変更する

Trusted Extensions では、セキュリティー管理者がシステムのデフォルトのセキュリティー設定を変更したり、それにアクセスしたりします。

セキュリティー設定は、/etc/security ディレクトリと /etc/default ディレクトリにあるファイルに記述されています。Solaris システムでは、スーパーユーザーがこれらのファイルを編集することができます。Solaris のセキュリティー情報については、『System Administration Guide: Security Services』の第 3 章「Controlling Access to Systems (Tasks)」を参照してください。

注意 – システムのセキュリティーデフォルトを変更するのは、サイトのセキュリティーポリシーで許可されている場合のみにしてください。

始める前に　大域ゾーンでセキュリティー管理者役割になります。

- トラステッドエディタを使用して、システムファイルを編集します。
  詳細は、59 ページの「Trusted Extensions の管理ファイルを編集する」を参照してください。

ファイル	作業	参照先
/etc/default/login	パスワード試行の許容回数を減らします。	『System Administration Guide: Security Services』の「How to Monitor All Failed Login Attempts」にある例を参照してください。 passwd(1) のマニュアルページ

ファイル	作業	参照先
/etc/default/kbd	キーボードでの停止を無効にします。	『System Administration Guide: Security Services』の「How to Disable a System's Abort Sequence」 注 – 管理者がデバッグの目的で使用するホストでは、KEYBOARD_ABORT のデフォルト設定によって kadb カーネルデバッガへのアクセスが許可されています。デバッガの詳細は、kadb(1M) のマニュアルページを参照してください。
/etc/security/policy.conf	ユーザーパスワードに対してより強力なアルゴリズムを要求します。 このホストのすべてのユーザーから基本的な特権を削除します。 このホストのユーザーを Basic Solaris User の承認に制限します。	policy.conf(4) のマニュアルページ
/etc/default/passwd	ユーザーに頻繁なパスワード変更を要求します。 ユーザーに最大限に異なるパスワードの設定を要求します。 より長いユーザーパスワードを要求します。 辞書で見つからないようなパスワードを要求します。	passwd(1) のマニュアルページ

◆ ◆ ◆ 第 6 章

Trusted Extensions でのユーザー、権利、および役割 (概要)

この章では、一般ユーザーを作成する前に必要な決定事項と、ユーザーアカウントを管理する際の背景情報について説明します。この章は、初期設定チームが役割を設定し、最小限のユーザーアカウントを設定していることを前提としています。これらのユーザーは、Solaris Trusted Extensions を構成および管理するために使用する役割になることができます。詳細は、『Solaris Trusted Extensions 構成ガイド』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 のユーザーセキュリティー機能

Trusted Extensions ソフトウェアは、ユーザー、役割、または権利プロファイルに次のセキュリティー機能を追加します。

- ユーザーには、システムを使用できるラベル範囲が設定されます。
- 役割には、管理タスクを実行するために使用できるラベル範囲が設定されます。
- Trusted Extensions 権利プロファイルには、CDE 管理アクションを含めることができます。コマンドと同様に、アクションにセキュリティー属性を設定できます。
- Trusted Extensions 権利プロファイルのコマンドとアクションは、ラベル属性を持ちます。コマンドまたはアクションは、ラベル範囲内または特定のラベルで実行される必要があります。
- Trusted Extensions ソフトウェアは、Solaris OS で定義された特権と承認のセットに特権と承認を追加します。

ユーザーに関する管理者のタスク

システム管理者役割は、ユーザーアカウントを作成します。セキュリティー管理者役割は、アカウントのセキュリティー面を設定します。

LDAP ネームサービス用に Sun Java™ System Directory Server を使用している場合は、初期設定チームが `tsol_ldap.tbx` ツールボックスを設定していることを確認してください。手順については、『Solaris Trusted Extensions 構成ガイド』の「LDAP のための Solaris 管理コンソールの設定 (作業マップ)」を参照してください。

ユーザーと役割の設定については、次を参照してください。

- 『System Administration Guide: Basic Administration』の「How to Create the First Role (Primary Administrator)」
- 『System Administration Guide: Basic Administration』の「Setting Up User Accounts (Task Map)」
- 『System Administration Guide: Security Services』のパート III「Roles, Rights Profiles, and Privileges」

ユーザーに関するシステム管理者のタスク

Trusted Extensions では、システム管理者役割がシステムにアクセスできるユーザーを決定します。システム管理者は、次のタスクを行います。

- ユーザーの追加と削除
- 役割の追加と削除
- ユーザーと役割の設定の修正 (セキュリティー属性を除く)

ユーザーに関するセキュリティー管理者のタスク

Trusted Extensions では、セキュリティー管理者役割がユーザーまたは役割のすべてのセキュリティー属性を設定します。セキュリティー管理者は、次のタスクを行います。

- ユーザー、役割、または権利プロファイルのセキュリティー属性の割り当てと修正
- 権利プロファイルの作成と修正
- ユーザーまたは役割への権利プロファイルの割り当て
- ユーザー、役割、または権利プロファイルへの特権の割り当て
- ユーザー、役割、または権利プロファイルへの承認の割り当て
- ユーザー、役割、または権利プロファイルからの特権の削除
- ユーザー、役割、または権利プロファイルからの承認の削除

一般的には、セキュリティー管理者役割が権利プロファイルを作成します。ただし、セキュリティー管理者役割では付与できない機能がプロファイルに必要な場合は、スーパーユーザーまたは主管理者役割がプロファイルを作成できます。

権利プロファイルを作成する前に、セキュリティー管理者は新しいプロファイルにあるコマンドまたはアクションの実行に、特権または承認が必要かどうかを分析する必要があります。各コマンドのマニュアルページに、コマンドで必要な特権と承認が記載されています。特権や承認が必要なアクションの例については、`exec_attr` データベースを参照してください。

Trusted Extensions でユーザーを作成する前に必要な決定事項

次の決定事項は、ユーザーが Trusted Extensions で実行可能な操作とその使いやすさに影響します。一部の決定事項は、Solaris OS のインストール時に行なった内容と同じです。Trusted Extensions に固有の決定事項は、サイトのセキュリティーや使いやすさに影響する場合があります。

- `policy.conf` ファイルでユーザーのデフォルトセキュリティー属性を変更するかどうかを決定する。`label_encodings` ファイル中のユーザーデフォルトは、初期設定チームによって設定されています。デフォルトの説明については、82 ページの「Trusted Extensions のデフォルトのユーザーセキュリティー属性」を参照してください。
- 各ユーザーの最小ラベルのホームディレクトリから上位レベルのホームディレクトリにコピーまたはリンクする、起動ファイルを決定する。手順については、91 ページの「Trusted Extensions のユーザーの起動ファイルを構成する」を参照してください。
- ユーザーがマイクロフォン、CD-ROM ドライブ、JAZ ドライブなどの周辺機器にアクセスできるかどうかを決定する。

  ユーザーにアクセスを許可する場合は、サイトセキュリティーを満たすために追加の承認が必要かどうかを決定します。デバイスに関する承認のデフォルトリストについては、264 ページの「デバイス承認を割り当てる」を参照してください。より詳しいデバイス承認のセットについては、260 ページの「Trusted Extensions でのデバイス承認のカスタマイズ (作業マップ)」を参照してください。

Trusted Extensions のデフォルトのユーザーセキュリティー属性

label_encodings ファイルと policy.conf ファイルの設定により、ユーザーアカウントのデフォルトのセキュリティー属性が決まります。ユーザーに対して明示的に設定した値は、これらのシステム値よりも優先されます。これらのファイルで設定した値の一部は、役割のアカウントにも適用されます。明示的に設定できるセキュリティー属性については、83 ページの「Trusted Extensions の構成可能なユーザー属性」を参照してください。

label_encodings ファイルのデフォルト

label_encodings ファイルは、ユーザーの最小ラベル、認可上限、およびデフォルトのラベル表示を定義します。ファイルの詳細は、label_encodings(4) のマニュアルページを参照してください。サイトの label_encodings ファイルは、初期設定チームによってインストールされています。初期設定チームが行う決定は、『Solaris Trusted Extensions 構成ガイド』の「ラベルストラテジの作成」と、『Solaris Trusted Extensions ラベルの管理』の例に基づいています。

セキュリティー管理者が Solaris 管理コンソールで個々のユーザーに明示的に設定するラベルの値は、label_encodings ファイルから派生しています。明示的に設定した値は、label_encodings ファイルの値よりも優先されます。

Trusted Extensions の policy.conf ファイルのデフォルト

Solaris の /etc/security/policy.conf ファイルには、システムのデフォルトセキュリティー設定が含まれています。Trusted Extensions はこのファイルに 2 つのキーワードを追加します。システム全体の値を変更する場合は、これらのキーワードと値の組をファイルに追加できます。これらのキーワードはTrusted CDE で実施されます。

表 6–1 policy.conf ファイル内の Trusted Extensions セキュリティーのデフォルト

キーワード	デフォルト値	取り得る値	注釈
IDLECMD	LOCK	LOCK | LOGOUT	役割には適用されません。
IDLETIME	30	0 ～ 120 分	役割には適用されません。

policy.conf ファイルで定義される承認と権利プロファイルは、個々のアカウントに割り当てられる承認とプロファイルに追加されます。その他のフィールドについては、個々のユーザーの値がシステムの値に優先します。

『Solaris Trusted Extensions 構成ガイド』の「Trusted Extensions でのユーザーセキュリティーの計画」に、policy.conf のキーワードの表があります。policy.conf(4) のマニュアルページも参照してください。

Trusted Extensions の構成可能なユーザー属性

Solaris 管理コンソール 2.1 は、ユーザーアカウントを作成および修正するためのツールです。複数のラベルでログインできるユーザーに対して、管理者は各ユーザーの最小ラベルのホームディレクトリに .copy_files と .link_files ファイルを設定する場合があります。

Solaris 管理コンソールのユーザーアカウントツールは、Solaris OS の場合と同様に機能します。ただし、次の 2 点が異なります。

- Trusted Extensions は、ユーザーアカウントに属性を追加します。
- Trusted Extensions では、ホームディレクトリサーバーアクセスに管理上の注意が必要です。
  - ホームディレクトリサーバーエントリを、Solaris システムの場合と同様に作成します。
  - 次に、管理者とユーザーがホームディレクトリをユーザーの各ラベルでマウントする追加手順を実行します。

『System Administration Guide: Basic Administration』の「How to Add a User With the Solaris Management Console's Users Tool」で説明したように、ウィザードを使用してユーザーアカウントを簡単に作成できます。ウィザードを使用したあと、ユーザーのデフォルトの Trusted Extensions 属性を修正できます。

.copy_files と .link_files ファイルについては、86 ページの「.copy_files ファイルと .link_files ファイル」を参照してください。

ユーザーに割り当てる必要のあるセキュリティー属性

セキュリティー管理者役割は、次の表のように、新しいユーザーのためにいくつかセキュリティー属性を指定する必要があります。デフォルト値を含むファイルについては、82 ページの「Trusted Extensions のデフォルトのユーザーセキュリティー属性」を参照してください。

表 6–2 ユーザーの作成後に割り当てられるセキュリティー属性

ユーザー属性	デフォルト値の設定場所	操作の要/不要	効果
パスワード	なし	必要	ユーザーにパスワードが設定されます
役割	なし	任意	ユーザーは役割を引き受けることができます
承認	policy.conf ファイル	任意	ユーザーに追加承認が割り当てられます
権利プロファイル	policy.conf ファイル	任意	ユーザーに追加の権利プロファイルが割り当てられます
ラベル	label_encodings ファイル	任意	ユーザーに異なるデフォルトラベルまたは認可範囲が与えられます
特権	policy.conf ファイル	任意	ユーザーに特権の異なるセットが与えられます
アカウントの使用	policy.conf ファイル	任意	アイドル時に、ユーザーにコンピュータの異なる設定が与えられます
監査	audit_control ファイル	任意	ユーザーはシステム監査設定と異なる監査を受けます

Trusted Extensions でのユーザーへのセキュリティー属性の割り当て

ユーザーアカウントが作成されると、セキュリティー管理者役割は Solaris 管理コンソールを使用して、ユーザーにセキュリティー属性を割り当てます。正しいデフォルトを設定した場合、次の手順としては、デフォルトに対する例外を必要とするユーザーのみにセキュリティー属性を割り当てることです。

セキュリティー属性をユーザーに割り当てる場合、セキュリティー管理者は次の事項について考慮する必要があります。

パスワードの割り当て
: ユーザーアカウントが作成されたら、セキュリティー管理者役割はユーザーアカウントにパスワードを割り当てます。最初の割り当てのあと、ユーザーはパスワードを変更できます。

  Solaris OS の場合と同様に、ユーザーに定期的なパスワードの変更を強制することができます。パスワードの有効期限オプションは、パスワードを推測または盗むことができる侵入者がシステムにアクセスできる期間を制限します。変更が可能になるまでの最低期間を設定すると、新しいパスワードに変更したユーザーがすぐに古いパスワードに戻すのを防ぐこともできます。詳細は、passwd(1) のマニュアルページを参照してください。

注 – 役割になれるユーザーのパスワードは、パスワードの有効期限の制約を受けないようにします。

役割の割り当て
1 人のユーザーに 1 つの役割を割り当てる必要はありません。サイトのセキュリティーポリシーに矛盾しなければ、1 人のユーザーに複数の役割を割り当てることができます。

承認の割り当て
Solaris OS と同様、承認をユーザーに直接割り当てると、これらの承認は既存の承認に追加されます。Trusted Extensions では、承認を権利プロファイルに追加し、プロファイルをユーザーに割り当てます。

権利プロファイルの割り当て
Solaris OS と同様に、 プロファイルの順序は重要です。プロファイルの機構は、アカウントのプロファイルセットにある最初のコマンドまたはアクションのインスタンスを使用します。

プロファイルの整列順を利用することができます。既存のプロファイルの定義と異なるセキュリティー属性でコマンドを実行する場合は、コマンドに目的の属性を割り当てた新しいプロファイルを作成します。続いて、既存のプロファイルの前に新しいプロファイルを挿入します。

注 – 管理アクションまたは管理コマンドを含む権利プロファイルは、一般ユーザーに割り当てないでください。一般ユーザーは大域ゾーンに入れないため、プロファイルが機能しません。

特権デフォルトの変更
多くのサイトにとって、デフォルトの特権セットでは厳格さが足りません。システム上のすべての一般ユーザーに対して特権セットを制限するには、`policy.conf` ファイルの設定を変更します。個々のユーザーの特権セットを変更するには、Solaris 管理コンソール を使用します。例については、100 ページの「ユーザーの特権セットを制限する」を参照してください。

ラベルのデフォルトの変更
ユーザーのラベルのデフォルトを変更すると、`label_encodings` ファイルのユーザーデフォルトの例外が作成されます。

監査デフォルトの変更
Solaris OS の場合と同様、ユーザーに監査クラスを割り当てると、システムの`/etc/security/audit_control` ファイルに割り当てられている監査クラスの例外が作成されます。監査の詳細は、第 18 章「Trusted Extensions での監査 (概要)」を参照してください。

.copy_files ファイルと .link_files ファイル

Trusted Extensions では、ファイルはスケルトンディレクトリからアカウントの最小ラベルを含むゾーンにのみ、自動的にコピーされます。上位ラベルのゾーンで起動ファイルを使用できるようにするには、ユーザーまたは管理者が .copy_files ファイルと .link_files ファイルを作成する必要があります。

Trusted Extensions の .copy_files ファイルと .link_files ファイルは、起動ファイルをアカウントの各ラベルのホームディレクトリに自動的にコピーまたはリンクします。ユーザーが新しいラベルでワークスペースを作成するごとに、updatehome コマンドはアカウントの最小ラベルで .copy_files ファイルと .link_files ファイルの内容を読み取ります。続いてコマンドは、リストに指定されたファイルを上位ラベルのワークスペースにコピーまたはリンクします。

.copy_files ファイルは、ユーザーが別のラベルで少しだけ異なる起動ファイルを使用する場合に有効です。たとえば、ユーザーが別のラベルで異なるメールエイリアスを使用する場合は、コピーが適しています。.link-files ファイルは、起動ファイルを、そのファイルが呼び出されたすべてのラベルでまったく同じにする必要がある場合に便利です。たとえば、すべてのラベル付き印刷ジョブを 1 台のプリンタで処理する場合は、リンクが適しています。サンプルファイルについては、91 ページの「Trusted Extensions のユーザーの起動ファイルを構成する」を参照してください。

次のリストに、ユーザーに上位ラベルへのコピーまたはリンクを許可する起動ファイルの例を示します。

- .acrorc
- .aliases
- .cshrc
- .dtprofile
- .emacs
- .login
- .mailrc
- .mime_types
- .newsrc
- .profile
- .signature
- .soffice
- .Xdefaults
- .Xdefaults-*hostname*

◆ ◆ ◆ 第 7 章

Trusted Extensions でのユーザー権利、役割の管理 (手順)

この章では、ユーザー、ユーザーアカウント、権利プロファイルを構成および管理する Solaris Trusted Extensions の手順について説明します。

セキュリティーのためのユーザー環境のカスタマイズ (作業マップ)

すべてのユーザー用にシステムをカスタマイズする、または個々のユーザーアカウントをカスタマイズするときに実行できる一般的なタスクは、次の作業マップのとおりです。

作業	説明	参照先
ラベル属性の変更	最小ラベルやデフォルトのラベル表示など、ユーザーアカウントのラベル属性を変更します。	88 ページの「デフォルトのユーザーラベル属性を修正する」

作業	説明	参照先
システムのすべてのユーザーに対して Trusted Extensions ポリシーを変更します。	policy.conf ファイルを変更します。	89 ページの「policy.conf のデフォルトを修正する」
	設定した時間のあとにスクリーンセーバーを起動します。 設定した一定時間システムがアイドルになったあとにユーザーをログアウトします。	例 7–1
	システムの一般ユーザーすべてから不要な特権を削除します。	例 7–2
	シングルラベルシステムでラベルを非表示にします。	例 7–3
	公共キオスクでのプリントアウトからラベルを削除します。	例 7–4
ユーザーの初期設定ファイルを構成します。	.cshrc、.copy_files、.soffice など、すべてのユーザーの起動ファイルを構成します。	91 ページの「Trusted Extensions のユーザーの起動ファイルを構成する」
ファイルのラベル再設定のタイムアウトを延長します。	一部のアプリケーションで承認ユーザーがファイルのラベルを再設定できるように構成します。	94 ページの「情報にラベルを再設定するときのタイムアウトを延長する」
フェイルセーフセッションへログインします。	ユーザーの初期設定ファイルの障害を修正します。	95 ページの「Trusted Extensions でフェイルセーフセッションにログインする」

▼ デフォルトのユーザーラベル属性を修正する

最初のシステムの構成中に、デフォルトのユーザーラベル属性を変更することができます。変更はすべての Trusted Extensions ホストにコピーする必要があります。

始める前に　大域ゾーンでセキュリティー管理者役割になります。詳細は、55 ページの「Trusted Extensions の大域ゾーンに入る」を参照してください。

1. /etc/security/tsol/label_encodings ファイルで、デフォルトのユーザー属性設定を確認します。
   デフォルトについては 82 ページの「label_encodings ファイルのデフォルト」を参照してください。

2. label_encodings ファイルで、ユーザー属性設定を修正します。
   トラステッドエディタを使用します。詳細は、59 ページの「Trusted Extensions の管理ファイルを編集する」を参照してください。Trusted CDE では、「ラベルエン

コーディングの編集」アクションも使用できます。詳細は、58 ページの「Trusted Extensions の CDE 管理アクションを起動する」を参照してください。

label_encodings ファイルは、すべてのホストで同一である必要があります。

3 ファイルのコピーを各 **Trusted Extensions** ホストに配布します。

▼ policy.conf のデフォルトを修正する

Trusted Extensions で policy.conf のデフォルトを変更する方法は、Solaris OS でセキュリティー関連のシステムファイルを変更する方法に類似しています。Trusted Extensions では、トラステッドエディタを使用してシステムファイルを修正します。

始める前に 大域ゾーンでセキュリティー管理者役割になります。詳細は、55 ページの「Trusted Extensions の大域ゾーンに入る」を参照してください。

1 /etc/security/policy.conf ファイルで、デフォルト設定を確認します。
Trusted Extensions のキーワードについては、表 6–1 を参照してください。

2 設定を修正します。
トラステッドエディタを使用して、システムファイルを編集します。詳細は、59 ページの「Trusted Extensions の管理ファイルを編集する」を参照してください。

例 7–1 システムのアイドル設定の変更

この例では、セキュリティー管理者が、アイドル状態のシステムがログイン画面に戻るように設定します。デフォルトでは、アイドル状態のシステムはロックされます。そこで、セキュリティー管理者役割は次のようにして、IDLECMD キーワード = 値のペアを /etc/security/policy.conf ファイルに追加します。

```
IDLECMD=LOGOUT
```

また管理者は、システムがアイドル状態になってからログアウトするまでの時間を短くします。そこで、セキュリティー管理者役割は次のようにして、IDLETIME キーワード = 値のペアを policy.conf ファイルに追加します。

```
IDLETIME=10
```

これで、システムが 10 分間アイドル状態になったあとでユーザーがログアウトされるようになります。

例 7–2 各ユーザーの基本的な特権セットの修正

この例では、Sun Ray™ インストールのセキュリティー管理者が、一般ユーザーにほかの Sun Ray ユーザーのプロセスを表示できないようにします。そこで、Trusted Extensions によって構成されている各システムで、管理者は基本的な特権セットから proc_info を削除します。/etc/policy.conf ファイルの PRIV_DEFAULT 設定を、次のように修正します。

```
PRIV_DEFAULT=basic,!proc_info
```

例 7–3 システムでのラベルの非表示

この例では、セキュリティー管理者がシステムの policy.conf ファイルでデフォルト設定を変更して、ラベルを非表示にします。このシステムでは、ラベルを表示できるよう特別に構成されているユーザーを除くすべてのユーザーにラベルが見えなくなります。この設定は、シングルラベルシステムに、または不特定多数の人が利用できるシステムに適しています。

```
# /etc/security/policy.conf
...
LABELVIEW=hidesl
```

この設定を上書きするようユーザーを構成する方法については、102 ページの「ユーザーに対してラベルを非表示にする」を参照してください。

例 7–4 システムのすべてのユーザーに対する印刷関連の承認の割り当て

この例では、セキュリティー管理者が、コンピュータの /etc/security/policy.conf ファイルで次のように入力して、公共キオスクコンピュータからラベルのない印刷をできるようにしています。次の起動以降、このキオスクのあらゆるユーザーによる印刷ジョブは、ページラベルなしで実行されます。

```
AUTHS_GRANTED= solaris.print.unlabeled
```

管理者は次に、バナーページとトレーラページを削除して、紙を節約することにします。管理者はまず、印刷マネージャーの「バナーを常に印刷」チェックボックスがチェックされていないことを確認します。次に、policy.conf エントリを次のように修正し、再起動します。これで、すべての印刷ジョブはラベルなしになり、バナーページもトレーラページもなくなります。

```
AUTHS_GRANTED= solaris.print.unlabeled,solaris.print.nobanner
```

▼ Trusted Extensions のユーザーの起動ファイルを構成する

ユーザーは、.copy_files ファイルと .link_files ファイルを、最小の機密ラベルに対応するラベルのホームディレクトリに配置することができます。また、ユーザーの最小ラベルで既存の .copy_files および .link_files ファイルを修正することもできます。この手順は、管理者役割がサイトの設定を自動化するためのものです。

始める前に　大域ゾーンで、システム管理者役割になっている必要があります。詳細は、55 ページの「Trusted Extensions の大域ゾーンに入る」を参照してください。

1. **2 つの Trusted Extensions 起動ファイルを作成します。**

   起動ファイルのリストに、.copy_files および .link_files を追加します。

   ```
   # cd /etc/skel
   # touch .copy_files .link_files
   ```

2. **.copy_files ファイルをカスタマイズします。**

   a. トラステッドエディタを起動します。

      詳細は、59 ページの「Trusted Extensions の管理ファイルを編集する」を参照してください。

   b. .copy_files ファイルへのフルパス名を入力します。

      ```
      /etc/skel/.copy_files
      ```

   c. .copy_files に、すべてのラベルでユーザーのホームディレクトリにコピーするファイルを、1 行に 1 ファイルずつ入力します。

      86 ページの「.copy_files ファイルと .link_files ファイル」を参照してください。サンプルファイルについては、例 7–5 を参照してください。

3. **.link_files ファイルをカスタマイズします。**

   a. トラステッドエディタで、.link_files ファイルへのフルパス名を入力します。

      ```
      /etc/skel/.link_files
      ```

   b. .link_files に、すべてのラベルでユーザーのホームディレクトリにリンクするファイルを、1 行に 1 ファイルずつ入力します。

4. **ユーザーのほかの起動ファイルをカスタマイズします。**

- 起動ファイルに含める内容については、『System Administration Guide: Basic Administration』の「Customizing a User's Work Environment」を参照してください。
- 詳細は、『System Administration Guide: Basic Administration』の「How to Customize User Initialization Files」を参照してください。
- 例については、例 7–5 を参照してください。

5 (省略可能) デフォルトのシェルがプロファイルシェルであるユーザーに、`skelP` サブディレクトリを作成します。

`P` はプロファイルシェルを表します。

6 カスタマイズした起動ファイルを、適切なスケルトンディレクトリにコピーします。

7 ユーザーを作成するときには、適切な `skel`*X* パス名を使用します。

X はシェル名の先頭の文字を表します。たとえば、Bourne シェルの場合は `B`、Korn シェルの場合は `K`、C シェルの場合は `C`、プロファイルシェルの場合は `P` です。

例 7–5 ユーザーの起動ファイルのカスタマイズ

この例では、セキュリティー管理者が各ユーザーのホームディレクトリのファイルを構成します。ファイルは、ユーザーのログイン前に配置されています。ファイルは、ユーザーの最小ラベルにあります。このサイトでは、ユーザーのデフォルトのシェルは C シェルです。

セキュリティー管理者は、トラステッドエディタで次の内容を含む `.copy_files` および `.link_files` ファイルを作成します。

```
## .copy_files for regular users
## Copy these files to my home directory in every zone
.mailrc
.mozilla
.soffice
:wq

## .link_files for regular users with C shells
## Link these files to my home directory in every zone
.cshrc
.login
.Xdefaults
.Xdefaults-hostname
:wq

## .link_files for regular users with Korn shells
# Link these files to my home directory in every zone
```

```
.ksh
.profile
.Xdefaults
.Xdefaults-hostname
:wq
```

シェルの初期設定ファイルで、管理者はユーザーの印刷ジョブがラベル付きプリンタで実行されることを確認します。

```
## .cshrc file
setenv PRINTER conf-printer1
setenv LPDEST  conf-printer1

## .ksh file
export PRINTER conf-printer1
export LPDEST  conf-printer1
```

管理者は、.Xdefaults- *home-directory-server* ファイルを修正して、dtterm コマンドによる新しい端末の .profile ファイルの読み取りを強制しました。

```
## Xdefaults-HDserver
Dtterm*LoginShell: true
```

カスタマイズしたファイルが、適切なスケルトンディレクトリにコピーされます。

```
$ cp .copy_files .link_files .cshrc .login .profile \
.mailrc .Xdefaults .Xdefaults-home-directory-server \
/etc/skelC
$ cp .copy_files .link_files .ksh .profile \
.mailrc .Xdefaults .Xdefaults-home-directory-server \
/etc/skelK
```

注意事項　最小のラベルで .copy_files ファイルを作成する場合、上位のゾーンにログインして updatehome コマンドを実行します。コマンドがアクセスエラーで失敗したら、次のようにしてください。

- 上位レベルのゾーンから下位レベルのディレクトリを表示できるかどうかを確認します。

  ```
  higher-level zone# ls /zone/lower-level-zone/home/username
  ACCESS ERROR: there are no files under that directory
  ```

- そのディレクトリを表示できない場合、上位レベルのゾーンで自動マウントサービスを再起動します。

  ```
  higher-level zone# svcadm restart autofs
  ```

ホームディレクトリの NFS マウントを使用しないかぎり、上位ゾーンのオートマウンタは /zone/*lower-level-zone*/export/home/*username* から /zone/*lower-level-zone*/home/*username* にループバックマウントするはずです。

▼ 情報にラベルを再設定するときのタイムアウトを延長する

Trusted Extensions では、選択マネージャーがラベル間の情報の転送を仲介します。選択マネージャーは、ドラッグ＆ドロップ操作やカット＆ペースト操作のときに表示されます。一部のアプリケーションでは、選択マネージャーが介入する時間を考慮して、適切なタイムアウトを設定する必要があります。時間は 2 分で十分です。

注意 – ラベルなしのシステムでは、デフォルトのタイムアウト値を変更しないでください。デフォルト値よりも長いタイムアウト値に変更すると、処理はエラーとなります。

始める前に　大域ゾーンで、システム管理者役割になっている必要があります。詳細は、55 ページの「Trusted Extensions の大域ゾーンに入る」を参照してください。

1. **StarSuite™ アプリケーションの場合は、次の手順を実行します。**

   a. ファイル *office-install-directory*/VCL.xcu にナビゲートします。

   office-install-directory は StarSuite のインストールディレクトリで、たとえば次のようになります。

   office-top-dir/share/registry/data/org/staroffice

   b. SelectionTimeout プロパティーの値を **120** に変更します。

   トラステッドエディタを使用します。詳細は、59 ページの「Trusted Extensions の管理ファイルを編集する」を参照してください。

   デフォルト値は 3 秒です。値を 120 に設定すると、タイムアウトは 2 分になります。

2. **GNOME ToolKit (GTK) ライブラリを利用するアプリケーションのユーザーの場合は、選択タイムアウトのプロパティー値を 2 分に変更します。**

注 – 別な方法として、各ユーザーに選択タイムアウトのプロパティー値を変更させることもできます。

大部分の Sun Java™ Desktop System アプリケーションは、GTK ライブラリを利用します。Mozilla、Firefox、Thunderbird などの Web ブラウザも GTK ライブラリを利用しています。

デフォルトでは、選択のタイムアウト値は 300、つまり 5 秒です。値を 7200 に設定すると、タイムアウトは 2 分になります。

a. **GTK 起動ファイルを作成します。**

   ファイル名は `.gtkrc-mine` とします。 `.gtkrc-mine` ファイルは、最小ラベルのユーザーのホームディレクトリに所属します。

b. **このファイルに、選択のタイムアウト値を追加します。**

```
## $HOME/.gtkrc-mine file
*gtk-selection-timeout: 7200
```

   Solaris OS の場合と同じように、`gnome-settings-daemon` が起動時にこのファイルを読み取ります。

3 **(省略可能) `.gtkrc-mine` ファイルを、各ユーザーの `.link_files` ファイルのリストに追加します。**

詳細については、91 ページの「Trusted Extensions のユーザーの起動ファイルを構成する」を参照してください。

▼ Trusted Extensions でフェイルセーフセッションにログインする

Trusted Extensions では、復旧ログインは保護されています。一般ユーザーがシェル初期設定ファイルをカスタマイズしており、現在ログインできない場合は、フェイルセーフログインを使用してユーザーのファイルを修正することができます。

始める前に `root` のパスワードを知っている必要があります。

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

2 **プロンプトに従って、ユーザーがユーザー名とパスワードを入力します。**

3 **`root` のパスワードを求めるプロンプトで、`root` のパスワードを入力します。**

これで、ユーザーの初期設定ファイルをデバッグできるようになります。

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)

Trusted Extensions では、Solaris 管理コンソールを使用してユーザー、承認、権利、および役割を管理する必要があります。ユーザーとそのセキュリティー属性を管理するには、セキュリティー管理者役割である必要があります。

作業	説明	参照先
ユーザーのラベル範囲を変更します。	ユーザーが作業できるラベルを修正します。この変更により、`label_encodings` ファイルで許可される範囲を制限または拡張できます。	96 ページの「Solaris 管理コンソールでユーザーのラベル範囲を修正する」
使いやすい承認のための権利プロファイルを作成します。	一般ユーザーに役立つ承認はいくつか存在します。これらの承認の資格を持つユーザーのプロファイルを作成します。	98 ページの「便利な承認のための権利プロファイルを作成する」
ユーザーのデフォルト特権セットを修正します。	ユーザーのデフォルトの特権セットから特権を削除します。	100 ページの「ユーザーの特権セットを制限する」
特定ユーザーのアカウントロックを回避します。	役割になることができるユーザーに対しては、アカウントロックをオフにする必要があります。	102 ページの「ユーザーのアカウントロックを禁止する」
ユーザーの画面でラベルを非表示にします。	シングルラベルシステムでは、ユーザーにラベルを表示しないようにできます。	102 ページの「ユーザーに対してラベルを非表示にする」
ユーザーがデータに再ラベル付けできるようにします。	ユーザーによる情報のダウングレードまたはアップグレードを許可します。	103 ページの「ユーザーによるデータのセキュリティーレベルの変更を有効にする」
システムからユーザーを削除します。	ユーザーおよびユーザーのプロセスを完全に削除します。	104 ページの「Trusted Extensions システムからユーザーアカウントを削除する」
ほかのタスクを処理します。	Solaris 管理コンソールを使用して、Trusted Extensions に固有ではないタスクを処理します。	105 ページの「Solaris 管理コンソールでほかのタスクを処理する (作業マップ)」

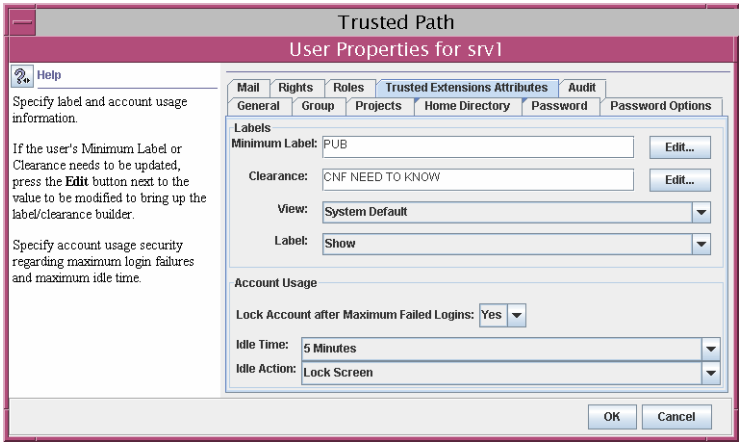
▼ Solaris 管理コンソールでユーザーのラベル範囲を修正する

ユーザーのラベル範囲を拡張して、ユーザーに管理用アプリケーションへの読み取りアクセスを許可したい場合があります。たとえば、大域ゾーンにログインできるユーザーは、Solaris 管理コンソールを実行できます。ユーザーは内容を表示できますが、内容の変更はできません。

また、ユーザーのラベル範囲を制限したい場合もあります。たとえば、ゲストユーザーを 1 つのラベルに制限することができます。

始める前に　大域ゾーンでセキュリティー管理者役割になります。

1. **Solaris 管理コンソールで Trusted Extensions ツールボックスを開きます。**
   適切な有効範囲のツールボックスを使用します。詳細は、『Solaris Trusted Extensions 構成ガイド』の「Trusted Extensions で Solaris 管理コンソールサーバーを初期化する」を参照してください。
2. 「システムの構成」で、「ユーザーアカウント」にナビゲートします。
   パスワードプロンプトが表示されます。
3. 役割のパスワードを入力します。
4. ユーザーアカウントから個々のユーザーを選択します。
5. 「**Trusted Extensions** の属性」タブをクリックします。



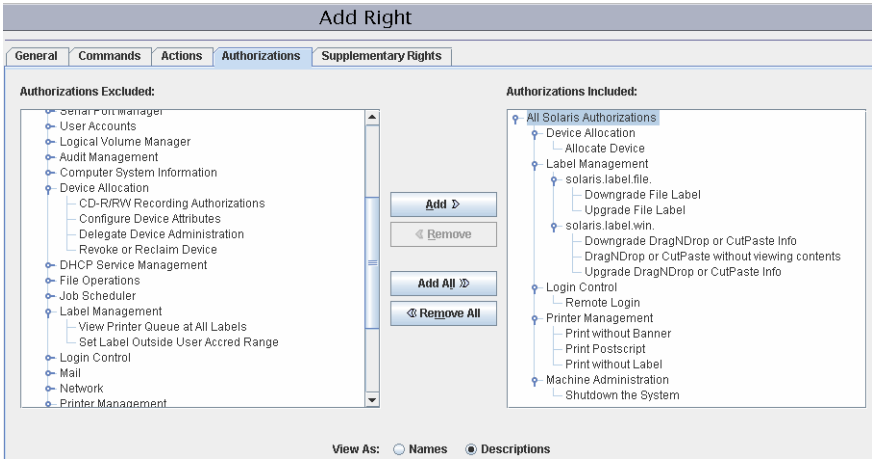
   - ユーザーのラベル範囲を拡張するには、より高位の認可上限を選択します。
     最小ラベルを低くすることもできます。
   - ラベル範囲を 1 つのラベルに制限するには、認可上限を最小ラベルと等しくします。
6. 「了解」をクリックして変更を保存します。

▼ 便利な承認のための権利プロファイルを作成する

サイトのセキュリティーポリシーで許可される場合、承認の必要なタスクを実行できるユーザーに対する承認を含む権利プロファイルを作成することができます。特定システムのすべてのユーザーが承認されるようにするには、89 ページの「policy.conf のデフォルトを修正する」を参照してください。

始める前に　大域ゾーンでセキュリティー管理者役割になります。

1. **Solaris 管理コンソールで Trusted Extensions ツールボックスを開きます。**
   適切な有効範囲のツールボックスを使用します。詳細は、『Solaris Trusted Extensions 構成ガイド』の「Trusted Extensions で Solaris 管理コンソールサーバーを初期化する」を参照してください。
2. 「システムの構成」で、「権利」にナビゲートします。
   パスワードプロンプトが表示されます。
3. 役割のパスワードを入力します。
4. 権利プロファイルを追加するには、「アクション」 –> 「権利を追加」をクリックします。
5. 次の 1 つ以上の承認を含む権利プロファイルを作成します。
   詳細な手順については、『System Administration Guide: Security Services』の「How to Create or Change a Rights Profile」を参照してください。
   次の図では、ユーザーにとって便利な承認が「含まれる承認」ウィンドウに表示されています。



- 「デバイスの割り当て」– マイクロフォンなどの周辺機器の割り当てをユーザーに承認します。

  デフォルトでは、Solaris のユーザーは CD-ROM に対して読み取りと書き込みが可能です。一方、Trusted Extensions で CD-ROM ドライブにアクセスできるのは、デバイスを割り当てることができるユーザーだけです。使用するドライブを割り当てるには、承認が必要です。したがって、Trusted Extensions で CD-ROM に対する読み取りと書き込みを行うには、ユーザーは「デバイスの割り当て」承認が必要です。
- 「Downgrade DragNDrop or CutPaste Info」– 下位レベルファイルからの情報の選択と、上位レベルファイルへの情報の配置をユーザーに承認します。
- 「Downgrade File Label」– ファイルのセキュリティーレベル引き下げをユーザーに承認します。
- 「内容を表示せずに DragNDrop またはCutPaste を行う」– 移動する情報を表示せずに情報を移動することをユーザーに承認します。
- 「Postscript を印刷」– PostScript™ ファイルの印刷をユーザーに承認します。
- 「バナーなしで印刷」- バナーページなしのハードコピーの印刷をユーザーに承認します。
- 「ラベルなしで印刷」– ラベルを表示しないハードコピーの印刷をユーザーに承認します。
- 「リモートログイン」– 遠隔ログインをユーザーに承認します。
- 「システムの停止」– システムの停止とゾーンの停止をユーザーに承認します。
- 「Upgrade DragNDrop or CutPaste Info」– 低レベルファイルからの情報の選択と、高レベルファイルへの情報の配置をユーザーに承認します。
- 「Upgrade File Label」– ファイルのセキュリティーレベル引き上げをユーザーに承認します。

6 ユーザーまたは役割に権利プロファイルを割り当てます。

詳細は、オンラインヘルプを参照してください。詳細な手順については、『System Administration Guide: Security Services』の「How to Change the RBAC Properties of a User」を参照してください。

例 7–6 役割への印刷関連の承認の割り当て

次の例では、セキュリティー管理者が、本文ページのラベルなしでジョブを印刷することを、役割に許可します。

Solaris 管理コンソールで、セキュリティー管理者は管理者役割にナビゲートします。特定の役割に含まれている権利プロファイルを確認してから、印刷関連の承認が役割の権利プロファイルの 1 つに含まれていることを確認します。

▼ ユーザーの特権セットを制限する

サイトのセキュリティーのために、ユーザーに割り当てられた特権をデフォルトより少なくしなければならないことがあります。たとえば、Sun Ray システム上で Trusted Extensions を使用するサイトで、ユーザーが Sun Ray サーバー上のほかのユーザーのプロセスを表示できないようにすることができます。

始める前に 大域ゾーンでセキュリティー管理者役割になります。

1 **Solaris 管理コンソールで Trusted Extensions ツールボックスを開きます。**

適切な有効範囲のツールボックスを使用します。詳細は、『Solaris Trusted Extensions 構成ガイド』の「Trusted Extensions で Solaris 管理コンソールサーバーを初期化する」を参照してください。

2 「システムの構成」で、「ユーザーアカウント」にナビゲートします。

パスワードプロンプトが表示されます。

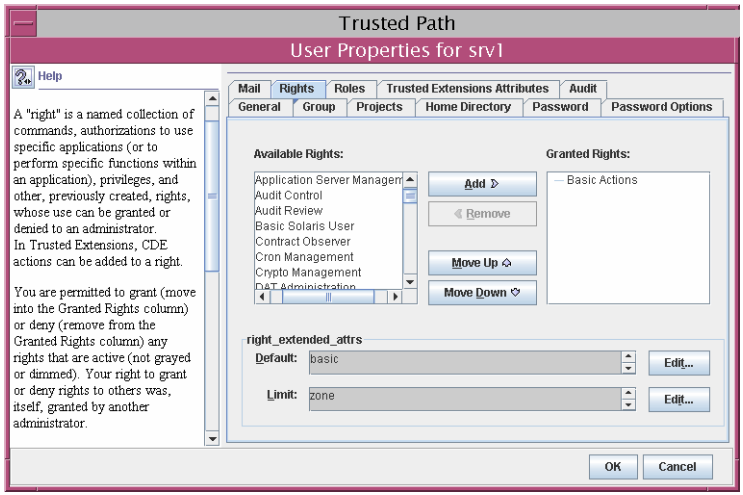
3 役割のパスワードを入力します。

4 ユーザーのアイコンをダブルクリックします。

5 `basic` セットにある 1 つ以上の特権を削除します。

a. ユーザーのアイコンをダブルクリックします。

b. 「権利」タブをクリックします。

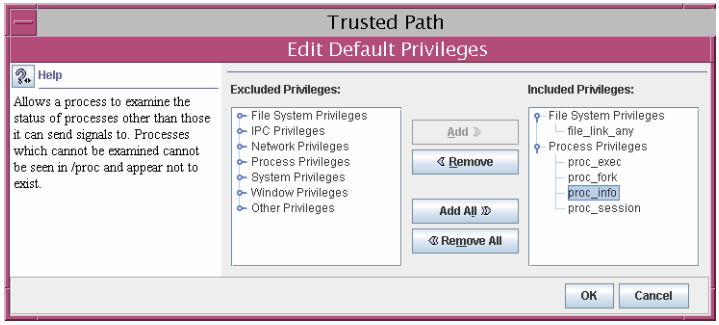


c. `right_extended_attr` フィールドの `basic` セットの右にある「編集」ボタンをクリックします。

d. `proc_session` または `file_link_any` を削除します。

`proc_session` 特権を削除することにより、ユーザーは現在のセッション外のプロセスを検査できなくなります。`file_link_any` 特権を削除することにより、ユーザーは所有していないファイルへのハードリンクを作成できなくなります。

注意 – `proc_fork` 特権または `proc_exec` 特権は削除しないでください。これらの特権がないと、ユーザーはシステムを使用することができません。



6 「了解」をクリックして変更を保存します。

▼ ユーザーのアカウントロックを禁止する

Trusted Extensions では、Solaris 管理コンソールのユーザーセキュリティー機能を拡張してアカウントロックが追加されています。役割になれるユーザーに対してアカウントロックをオフにする必要があります。

始める前に　大域ゾーンでセキュリティー管理者役割になります。

1. **Solaris 管理コンソールを起動します。**
   適切な有効範囲のツールボックスを使用します。詳細は、『Solaris Trusted Extensions 構成ガイド』の「Trusted Extensions で Solaris 管理コンソールサーバーを初期化する」を参照してください。
2. 「システムの構成」で、「ユーザーアカウント」にナビゲートします。
   パスワードプロンプトが表示されます。
3. 役割のパスワードを入力します。
4. ユーザーのアイコンをダブルクリックします。
5. 「**Trusted Extensions** の属性」タブをクリックします。
6. 「アカウントの利用」セクションで、「ログイン失敗の最大回数に達したあとでアカウントをロックする」 の隣にあるプルダウンメニューから 「いいえ」 を選択します。
7. 「了解」をクリックして変更を保存します。

▼ ユーザーに対してラベルを非表示にする

ラベルを非表示にすることは、ユーザーがシングルラベルのみで作業できるサイトで役に立ちます。一般ユーザーにラベルを表示したくない場合や、必須アクセス制御によってユーザーアクセスが制限されていることを認識させたくない場合があります。こうすると、一般ユーザーは、Solaris システムの Java Desktop System, Release *number* または CDE デスクトップに類似したデスクトップで作業することができます。

始める前に　大域ゾーンでセキュリティー管理者役割になります。

1. **Solaris** 管理コンソールで **Trusted Extensions** ツールボックスを開きます。
   適切な有効範囲のツールボックスを使用します。詳細は、『Solaris Trusted Extensions 構成ガイド』の「Trusted Extensions で Solaris 管理コンソールサーバーを初期化する」を参照してください。
2. 「システムの構成」で、「ユーザーアカウント」にナビゲートします。
   パスワードプロンプトが表示されます。
3. 役割のパスワードを入力します。
4. ユーザーのアイコンをダブルクリックします。
5. 「**Trusted Extensions** の属性」タブをクリックします。
6. 「ラベル：」選択リストから「非表示」を選択します。
   この設定によって、システムの `policy.conf` ファイルの `LABELVIEW` の値が上書きされます。詳細については、82 ページの「Trusted Extensions のデフォルトのユーザーセキュリティー属性」を参照してください。
7. 「了解」をクリックして変更を保存します。

▼ ユーザーによるデータのセキュリティーレベルの変更を有効にする

一般ユーザーまたは役割には、ファイルおよびディレクトリのセキュリティーレベルまたはラベルを変更する承認を与えることができます。この承認に加えて、ユーザーまたは役割を、複数のラベルで作業するように構成する必要があります。ラベル付きゾーンは、再ラベル付けを許可するように構成する必要があります。手順については、141 ページの「ラベル付きゾーンからファイルに再ラベル付けできるようにする」を参照してください。

注意 – データのセキュリティーレベルの変更は特権操作です。このタスクは、信頼できるユーザーのみを対象とします。

始める前に　大域ゾーンでセキュリティー管理者役割になります。

1. **98** ページの「便利な承認のための権利プロファイルを作成する」の手順に従って、権利プロファイルを作成します。

次の承認によって、ユーザーがファイルに再ラベル付けできるようになります。

- 「Downgrade File Label」
- 「Upgrade File Label」

次の承認によって、ユーザーがファイル内の情報に再ラベル付けできるようになります。

- 「Downgrade DragNDrop or CutPaste Info」
- 「DragNDrop or CutPaste Info Without Viewing」
- 「Upgrade DragNDrop or CutPaste Info」

2 **Solaris** 管理コンソールを使用して、適切なユーザーおよび役割にプロファイルを割り当てます。

詳細は、オンラインヘルプを参照してください。詳細な手順については、『System Administration Guide: Security Services』の「How to Change the RBAC Properties of a User」を参照してください。

▼ Trusted Extensions システムからユーザーアカウントを削除する

ユーザーをシステムから削除する場合、管理者は、ユーザーのホームディレクトリと、そのユーザーが所有するオブジェクトも、確実に削除する必要があります。ユーザーの所有するオブジェクトを削除する代わりに、管理者はそのオブジェクトの所有権を有効なユーザーに変更することができます。

管理者は、削除されたユーザーに関連付けられているバッチジョブも、すべて確実に削除する必要があります。削除されたユーザーに属するオブジェクトまたはプロセスがシステムに残っていないことを確認してください。

始める前に　システム管理者役割である必要があります。

1 各ラベルでユーザーのホームディレクトリをアーカイブします。

2 各ラベルでユーザーのメールファイルをアーカイブします。

3 **Solaris** 管理コンソールで、ユーザーアカウントを削除します。

a. **Solaris** 管理コンソールで **Trusted Extensions** ツールボックスを開きます。

適切な有効範囲のツールボックスを使用します。詳細は、『Solaris Trusted Extensions 構成ガイド』の「Trusted Extensions で Solaris 管理コンソールサーバーを初期化する」を参照してください。

b. 「システムの構成」で、「ユーザーアカウント」にナビゲートします。
パスワードプロンプトが表示されます。

c. 役割のパスワードを入力します。

d. 削除するユーザーアカウントを選択して、「削除」ボタンをクリックします。
ユーザーのホームディレクトリとメールファイルを削除するプロンプトが表示されます。プロンプトを受け入れると、ユーザーのホームディレクトリとメールファイルが大域ゾーンでのみ削除されます。

4 各ラベル付きゾーンで、ユーザーのディレクトリとメールファイルを手動で削除します。

注 – すべてのラベルで、`/tmp` ディレクトリのファイルなど、ユーザーの一時ファイルを検索して削除します。

Solaris 管理コンソールでほかのタスクを処理する (作業マップ)

Solaris の手順に従って、Solaris 管理コンソールでタスクを処理します。スーパーユーザーになるか、大域ゾーンで役割になる必要があります。

作業	参照先
Solaris 管理コンソールを使用して管理タスクを実行します。	『System Administration Guide: Basic Administration』の第 2 章「Working With the Solaris Management Console (Tasks)」
ユーザーを作成します。	『System Administration Guide: Basic Administration』の「Using the Solaris Management Tools With RBAC (Task Map)」
役割を作成します。	『System Administration Guide: Security Services』の「How to Create and Assign a Role by Using the GUI」
役割を修正します。	『System Administration Guide: Security Services』の「How to Change the Properties of a Role」
権利プロファイルを作成または修正します。	『System Administration Guide: Security Services』の「How to Create or Change a Rights Profile」

作業	参照先
ユーザーのほかのセキュリティー属性を変更します。	『System Administration Guide: Security Services』の「How to Change the RBAC Properties of a User」
役割のアクションを監査します。	『System Administration Guide: Security Services』の「How to Audit Roles」
`smprofile list -D` *name-service-type*`:/`*server-name*`/` *domain-name* を使用して権利プロファイルをリスト	『System Administration Guide: Security Services』の第 9 章「Using Role-Based Access Control (Tasks)」または`smprofile`(1M) のマニュアルページ

◆ ◆ ◆ 第 8 章

Trusted Extensions での遠隔管理 (手順)

この章では、Trusted Extensions の管理ツールを使用して遠隔システムを管理する方法について説明します。

Trusted Extensions でのセキュリティー保護された遠隔管理

デフォルトでは、Trusted Extensions では遠隔管理が許可されていません。Trusted Extensions が設定されたシステムを、信頼できない遠隔システムで管理できるとしたら、遠隔管理によって重大なセキュリティーリスクが発生します。そのため、システムは遠隔で管理されているオプションなしで最初にインストールされます。

ネットワークが構成されるまで、すべての遠隔ホストには `admin_low` のセキュリティーテンプレートが割り当てられます。したがって、どの接続でも CIPSO プロトコルは使用されず、受け付けられません。この初期状態の間、システムは複数のメカニズムによって遠隔攻撃から保護されています。このメカニズムには、`netservices` 設定、デフォルトログインポリシー、PAM ポリシーなどがあります。

- `netservices` サービス管理機能 (SMF) プロファイルが `limited` に設定されている場合、遠隔サービスは Secure Shell だけが有効になっています。しかし、ログインポリシーおよび PAM ポリシーのため、`ssh` サービスを使用して遠隔ログインすることはできません。
- `/etc/default/login` ファイルの `CONSOLE` のデフォルトポリシーによって `root` による遠隔ログインが禁止されているため、`root` アカウントを使用して遠隔ログインすることはできません。

- 遠隔ログインは、PAM の 2 つの設定の影響も受けます。

  pam_roles モジュールは、アカウントタイプ role からのローカルログインを常に拒否します。デフォルトでは、このモジュールは遠隔ログインも拒否します。ただし、システムの pam.conf エントリで allow_remote を指定すれば、遠隔ログインを受け付けるようにシステムを構成することができます。

  また、pam_tsol_account モジュールは、CIPSO プロトコルを使用しない限り、大域ゾーンへの遠隔ログインを拒否します。このポリシーの目的は、ほかの Trusted Extensions システムを使用して遠隔管理を実行できるようにすることです。

遠隔ログイン機能を有効にするには、両方のシステムでその接続先を CIPSO セキュリティーテンプレートに割り当てる必要があります。この方法が現実的でない場合は、pam.conf ファイルで allow_unlabeled オプションを指定して、ネットワークプロトコルポリシーを引き下げることができます。これらのポリシーのいずれかを引き下げた場合、任意のマシンが大域ゾーンにアクセスできないようにデフォルトのネットワークテンプレートを変更する必要があります。admin_low テンプレートは慎重に使用し、tnrhdb データベースを修正して、ワイルドカードアドレス 0.0.0.0 が ADMIN_LOW ラベルのデフォルトにならないようにしてください。詳細は、110 ページの「Trusted Extensions の遠隔管理 (作業マップ)」および195 ページの「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。

Trusted Extensions での遠隔システムの管理方式

通常、管理者はrlogin および ssh コマンドを使用して、コマンド行から遠隔システムを管理します。Solaris 管理コンソールも使用できます。Trusted CDE では、dtappsession プログラムで遠隔から Trusted CDE アクションを起動できます。Solaris 10 5/09 リリースから、仮想ネットワークコンピュータ (virtual networking computer、VNC) を使用してマルチレベルデスクトップを遠隔表示できるようになります。

Trusted Extensions では、次の遠隔管理方式が可能です。

- root ユーザーは、端末から遠隔ホストにログインすることができます。111 ページの「Trusted Extensions でコマンド行から遠隔でログインする」を参照してください。この方式は、Solaris システムの場合と同じように機能します。この方式はセキュリティー保護されません。
- 役割は、役割ワークスペースで端末から遠隔ホストにログインすることができます。111 ページの「Trusted Extensions でコマンド行から遠隔でログインする」を参照してください。
- 管理者は、遠隔システム上で実行中の Solaris 管理コンソールサーバーを起動することができます。113 ページの「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。

- Trusted_Extensions フォルダのアクションは、 `dtappsession` コマンドを使用して遠隔で起動することができます。112 ページの「dtappsession で Trusted Extensions を遠隔管理する」を参照してください。
- ユーザーは、VNC クライアントプログラムを使用して Trusted Extensions システム上の Xvnc サーバーに接続して、遠隔のマルチレベルデスクトップにログインできます。117 ページの「Xvnc を使用して Trusted Extensions システムに遠隔アクセスする」を参照してください。

Trusted Extensions での役割による遠隔ログイン

Solaris OS の場合と同じように、遠隔ログインを許可するには、各ホスト上の `/etc/default/login` ファイルの設定を変更する必要があります。また、場合によっては `pam.conf` ファイルを変更する必要もあります。Trusted Extensions では、セキュリティー管理者が変更を行います。手順については、『Solaris Trusted Extensions 構成ガイド』の「Trusted Extensions での root による遠隔ログインを有効にする」および『Solaris Trusted Extensions 構成ガイド』の「Trusted Extensions での役割による遠隔ログインを有効にする」を参照してください。

Trusted Extensions と Solaris のどちらのホストでも、遠隔ログインには承認が必要な場合と不要な場合があります。承認が必要なログインの条件とタイプについては、110 ページの「Trusted Extensions での遠隔ログイン管理」で説明しています。デフォルトで、役割には「リモートログイン」承認が与えられています。

ラベルなしホストからの役割ベースの遠隔管理

Trusted Extensions で、ユーザーはトラステッドパスメニューから役割になります。その結果、役割がトラステッドワークスペースで機能するようになります。デフォルトでは、トラステッドパス以外から役割になることはできません。サイトポリシーで許可される場合、セキュリティー管理者はこのデフォルトポリシーを変更できます。これで、Solaris 管理コンソール 2.1 クライアントソフトウェアを実行しているラベルなしホストの管理者は、トラステッドホストを管理できるようになります。

- デフォルトポリシーを変更するには、『Solaris Trusted Extensions 構成ガイド』の「Trusted Extensions での役割による遠隔ログインを有効にする」を参照してください。
- システムの遠隔管理については、111 ページの「Trusted Extensions でコマンド行から遠隔でログインする」を参照してください。

このポリシー変更は、遠隔のラベルなしシステム上のユーザーが Trusted Extensions ホストにユーザーアカウントを持っている場合にのみ適用されます。Trusted Extensions のユーザーは、管理者役割になれる必要があります。管理者役割は、Solaris 管理コンソールを使用して遠隔システムを管理できます。

注意 – Trusted Extensions 以外のホストからの遠隔管理が有効な場合、管理環境は Trusted Extensions の管理ワークスペースより安全性が低くなります。パスワードやほかのセキュリティーデータを入力するときは注意してください。予防策として、信頼できないアプリケーションはすべて、Solaris 管理コンソールを起動する前に停止してください。

Trusted Extensions での遠隔ログイン管理

2 つの Trusted Extensions ホスト間の遠隔ログインは、現在のログインセッションの延長とみなされます。

`rlogin` コマンドがパスワードを要求しない場合、承認は必要ありません。遠隔ホスト上のユーザーのホームディレクトリにある `/etc/hosts.equiv` または `.rhosts` ファイルに、遠隔ログインを試行しているユーザー名またはホストがリストされている場合、パスワードは必要ありません。詳細は、`rhosts(4)` および `rlogin(1)` のマニュアルページを参照してください。

ほかのすべての遠隔ログインの場合、`ftp` コマンドを使用したログインの場合も含めて、「リモートログイン」承認が必要です。

「リモートログイン」承認を含む権利プロファイルの作成については、96 ページの「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)」を参照してください。

Trusted Extensions の遠隔管理 (作業マップ)

次の作業マップでは、遠隔の Trusted Extensions システムを管理するためのタスクについて説明します。

作業	説明	参照先
`root` が Trusted Extensions システムに遠隔でログインできるようにします。	`root` ユーザーがラベル付きシステムから遠隔で作業できるようにします。	『Solaris Trusted Extensions 構成ガイド』の「Trusted Extensions での root による遠隔ログインを有効にする」
役割が Trusted Extensions システムに遠隔でログインできるようにします。	役割がラベル付きシステムから遠隔で作業できるようにします。	『Solaris Trusted Extensions 構成ガイド』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 システムへの遠隔ログインを有効にします。	任意のユーザーや役割がラベルなしシステムから遠隔で作業できるようにします。	『Solaris Trusted Extensions 構成ガイド』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」

作業	説明	参照先
Trusted Extensions システムに遠隔でログインします。	役割として Trusted Extensions システムにログインします。	111 ページの「Trusted Extensions でコマンド行から遠隔でログインする」
システムを遠隔で管理します。	`dtappsession` コマンドを使用して、Trusted_Extensions アクションで遠隔システムを管理します。	112 ページの「`dtappsession` で Trusted Extensions を遠隔管理する」
	Trusted Extensions システムから、Solaris 管理コンソールを使用して遠隔ホストを管理します。	113 ページの「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」
	ラベルなしシステムから、Solaris 管理コンソールを使用して遠隔の Trusted Extensions ホストを管理します。	115 ページの「ラベルなしシステムから Solaris 管理コンソールを使ってシステムを遠隔管理する」
遠隔システムを管理および使用する	任意のクライアントから、遠隔の 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。	117 ページの「Xvnc を使用して Trusted Extensions システムに遠隔アクセスする」
特定ユーザーが大域ゾーンにログインできるようにします。	Solaris 管理コンソールのユーザーツールやネットワークツールを使用して、特定ユーザーが大域ゾーンにアクセスできるようにします。	116 ページの「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」

▼ Trusted Extensions でコマンド行から遠隔でログインする

注 – `telnet` コマンドは基本および役割のアイデンティティーを `pam_roles` モジュールに渡すことができないため、このコマンドを使用して遠隔の役割になることはできません。

始める前に　ユーザーと役割は、ローカルシステムと遠隔システムで同一に定義されている必要があります。

役割は、「リモートログイン」承認を持っている必要があります。デフォルトでは、この承認は Remote Administration 、 Maintenance、および Repair 権利プロファイルにあります。

セキュリティー管理者は、遠隔で管理できるすべてのシステム上で『Solaris Trusted Extensions 構成ガイド』の「Trusted Extensions での役割による遠隔ログインを有効にする」の手順を完了しておきます。システムをラベルなしシステムから管理できる

場合は、『Solaris Trusted Extensions 構成ガイド』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」の手順も完了しておいてください。

- 役割を引き受けることができるユーザーのワークスペースから、遠隔ホストにログインします。

  rlogin コマンド、ssh コマンド、または ftp コマンドを使用します。

  - rlogin -l または ssh コマンドを使用してログインする場合は、役割の権利プロファイルにあるすべてのコマンドを使用できます。
  - ftp コマンドを使用する場合は、ftp(1) のマニュアルページで使用可能なコマンドを参照してください。

▼ dtappsession で Trusted Extensions を遠隔管理する

dtappsession プログラムを使用すると、管理者は CDE を実行している遠隔システムを管理することができます。

dtappsession は、遠隔システムにモニターがないときに役立ちます。たとえば、大規模サーバーでドメインを管理するとき、dtappsession がしばしば使用されます。詳細は、dtappsession(1) のマニュアルページを参照してください。

始める前に　ラベル付きシステムでは、大域ゾーンの管理役割である必要があります。ラベルなしシステムでは、遠隔システムで定義されている役割である必要があります。役割のプロファイルシェルから、遠隔ログインを実行します。

1. (省略可能) 遠隔セッション専用のワークスペースを作成します。

   遠隔の CDE アプリケーションとローカルアプリケーションとの混同を避けるために、この手順専用の管理役割ワークスペースを作成します。詳細は、『Solaris Trusted Extensions ユーザーズガイド』の「特定のラベルのワークスペースを追加する」を参照してください。

2. 遠隔ホストにログインします。

   rlogin コマンドまたは ssh コマンドを使用することができます。

   ```
   $ ssh remote-host
   ```

3. 遠隔の管理を開始します。

   端末ウィンドウで、dtappsession コマンドに続いてローカルホストの名前を入力します。

   ```
   $ /usr/dt/bin/dtappsession local-host
   ```

   遠隔ホスト上で実行されているアプリケーションマネージャーが、ローカルホスト上で表示されます。「終了」ダイアログボックスも表示されます。

4 遠隔ホストを管理します。

Trusted CDE から遠隔セッションを起動した場合、Trusted_Extensions フォルダのアクションを使用することができます。

5 終了したら、「終了」ボタンをクリックします。

注意 – アプリケーションマネージャーを閉じてもログインセッションは終了しないため、これはお勧めできません。

6 端末ウィンドウで、遠隔のログインセッションを終了します。

`hostname` コマンドを使用して、ローカルホスト上にいることを確認します。

```
$ exit
$ hostname
local-host
```

▼ 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

Solaris 管理コンソールは、ユーザー、権利、役割、およびネットワークを管理するための遠隔管理インタフェースを提供します。コンソールを使用する役割になります。この手順では、コンソールをローカルシステムで実行し、遠隔システムをサーバーとして指定します。

始める前に 次の手順を完了しておきます。

- 両方のシステムでの手順 – 『Solaris Trusted Extensions 構成ガイド』の「Trusted Extensions で Solaris 管理コンソールサーバーを初期化する」
- 遠隔システムでの手順 – 『Solaris Trusted Extensions 構成ガイド』の「Trusted Extensions での役割による遠隔ログインを有効にする」および『Solaris Trusted Extensions 構成ガイド』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 サーバーである遠隔システムでの手順 – 『Solaris Trusted Extensions 構成ガイド』の「LDAP のための Solaris 管理コンソールの設定 (作業マップ)」

1. ローカルシステムで、遠隔システム上で同一に定義されているユーザーとしてログインします。

2. システムの管理に使用する役割になります。

3. その役割で、**Solaris** 管理コンソールを起動します。
   詳細は、『Solaris Trusted Extensions 構成ガイド』の「Trusted Extensions で Solaris 管理コンソールサーバーを初期化する」を参照してください。

   a. 「サーバー」ダイアログボックスで、遠隔サーバーの名前を入力します。

      - **LDAP** をネームサービスとして使用している場合、**LDAP** サーバーの名前を入力します。
        次に、次のスコープのいずれかを選択します。

        - ネームサービスのデータベースを管理するには、`Scope=LDAP` ツールボックスを選択します。
          このコンピュータ (*ldap-server*: `Scope=LDAP, Policy=TSOL`)

        - **LDAP** サーバーのローカルファイルを管理するには、`Scope=Files` ツールボックスを選択します。
          このコンピュータ (*ldap-server*: `Scope=Files, Policy=TSOL`)

      - **LDAP** をネームサービスとして使用していない場合、管理する遠隔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`)

4. 「システムの構成」でツールを選択します。
   「ユーザー」などのツールを選択すると、ダイアログボックスに Solaris 管理コンソールのサーバー名、ユーザー名、役割名、および役割のパスワードを入力する場所が表示されます。それらのエントリが正しいことを確認します。

5. ローカルシステムと遠隔システムで同一に定義されている役割で、**Solaris** 管理コンソールサーバーにログインします。
   役割のパスワードを入力し、役割として「ログイン」を押します。これで、Solaris 管理コンソールを使ってシステムを管理できます。

注 – Solaris 管理コンソールを使って `dtappsession` を実行することもできますが、`dtappsession` のもっとも簡単な使用方法については、112 ページの「`dtappsession` で Trusted Extensions を遠隔管理する」に説明されています。

▼ ラベルなしシステムから Solaris 管理コンソールを使ってシステムを遠隔管理する

この手順では、Solaris 管理コンソールのクライアントとサーバーを遠隔システムで実行し、ローカルシステムでコンソールを表示します。

始める前に　Trusted Extensions システムによってラベル ADMIN_LOW がローカルシステムに割り当てられている必要があります。

注 – Trusted Solaris システムなど、CIPSO プロトコルを実行していないシステムは、Trusted Extensions システムの観点からラベルなしシステムとみなされます。

遠隔システムの Solaris 管理コンソールサーバーは、遠隔接続を受け入れるように構成する必要があります。手順については、『Solaris Trusted Extensions 構成ガイド』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」を参照してください。

どちらのシステムにも、Solaris 管理コンソールを使用できる同じ役割が割り当てられている同じユーザーが必要です。ユーザーは通常のユーザーのラベル範囲で構いませんが、役割の範囲は ADMIN_LOW ～ ADMIN_HIGH である必要があります。

大域ゾーンで、管理者役割になっている必要があります。

1. ローカルの X サーバーを有効にして遠隔の Solaris 管理コンソールを表示します。

```
# xhost + TX-SMC-Server
# echo $DISPLAY
:n.n
```

2. ローカルシステムで、Solaris 管理コンソールの役割を引き受けることができるユーザーになります。

```
# su - same-username-on-both-systems
```

3. そのユーザーで、遠隔サーバーに役割としてログインします。

```
$ rlogin -l same-rolename-on-both-systems TX-SMC-Server
```

4. Solaris 管理コンソールが使用する環境変数に正しい値が設定されていることを確認します。

   a. DISPLAY 変数の値を設定します。

```
$ DISPLAY=local:n.n
$ export DISPLAY=local:n.n
```

b. LOGNAME 変数の値をユーザー名に設定します。

```
$ LOGNAME=same-username-on-both-systems
$ export LOGNAME=same-username-on-both-systems
```

c. USER 変数の値を役割名に設定します。

```
$ USER=same-rolename-on-both-systems
$ export USER=same-rolename-on-both-systems
```

5 その役割で、コマンド行から **Solaris** 管理コンソールを起動します。

```
$ /usr/sbin/smc &
```

6 「システムの構成」でツールを選択します。

「ユーザー」などのツールを選択すると、ダイアログボックスに Solaris 管理コンソールのサーバー名、ユーザー名、役割名、および役割のパスワードを入力する場所が表示されます。それらのエントリが正しいことを確認します。

7 その役割として、サーバーにログインします。

役割のパスワードを入力し、役割として「ログイン」を押します。これで、Solaris 管理コンソールを使ってシステムを管理できます。

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.
```

▼ 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

役割がない状態で遠隔ログインできるようにするには、ユーザーのデフォルトのラベル範囲とゾーンのデフォルト動作を変更します。この手順は、ラベル付きシステムを遠隔で使用しているテスターに対して実行する場合があります。セキュリティーのため、テスターのシステムはほかのユーザーと無関係のラベルで実行されている必要があります。

始める前に　このユーザーが大域ゾーンにログインする正当な理由が必要です。

大域ゾーンでセキュリティー管理者役割になります。

1 特定のユーザーが大域ゾーンにログインできるようにするためには、そのユーザーに管理ラベルの範囲を割り当てます。

Solaris 管理コンソールを使用して、ADMIN_HIGH の認可上限と、ADMIN_LOW の最小ラベルを各ユーザーに割り当てます。詳細は、96 ページの「Solaris 管理コンソールでユーザーのラベル範囲を修正する」を参照してください。

ユーザーのラベル付きゾーンもログインを許可する必要があります。

2 ラベル付きゾーンから大域ゾーンに遠隔ログインできるようにするには、次のようにします。

a. 遠隔ログイン用マルチレベルポートを大域ゾーンに追加します。

Solaris 管理コンソールを使用します。TCP プロトコル上のポート 513 で遠隔ログインが可能です。例については、144 ページの「ゾーンにマルチレベルポートを作成する」を参照してください。

b. tnzonecfg の変更をカーネルに読み込みます。

```
# tnctl -fz /etc/security/tsol/tnzonecfg
```

c. 遠隔ログインサービスを再起動します。

```
# svcadm restart svc:/network/login:rlogin
```

▼ Xvnc を使用して Trusted Extensions システムに遠隔アクセスする

仮想ネットワークコンピューティング (Virtual Network Computing、VNC) テクノロジは、クライアントを遠隔サーバーに接続し、クライアントのウィンドウに遠隔サーバーのデスクトップを表示します。Xvnc は UNIX バージョンの VNC であり、標準 X サーバーをベースにしています。Trusted Extensions では、どのプラットフォーム上のクライアントでも、Trusted Extensions ソフトウェアが実行されている Xvnc に接続して、Xvnc サーバーにログインし、マルチレベルデスクトップ上で表示して作業できます。

始める前に Xvnc サーバーとして使用するシステムに Trusted Extensions ソフトウェアをインストールして設定しておきます。また、ラベル付きゾーンを作成してブートしておきます。Xvnc サーバーはホスト名または IP アドレスによって VNC クライアントを認識します。

Xvnc サーバーとして使用するシステムの大域ゾーンのスーパーユーザーになります。

1 **Xvnc サーバーを構成します。**

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

注意 – Solaris 10 10/08 または Solaris 10 5/08 リリースを実行している場合、サーバーを構成する前にシステムにパッチを適用してください。SPARC システムでは、パッチ 125719 の最新バージョンをインストールします。x86 システムでは、パッチ 125720 の最新バージョンをインストールします。

a. X サーバーの構成ディレクトリを作成します。

```
# mkdir -p /etc/dt/config
```

b. /usr/dt/config/Xservers ファイルを /etc/dt/config ディレクトリにコピーします。

```
# cp /usr/dt/config/Xservers /etc/dt/config/Xservers
```

c. /etc/dt/config/Xservers ファイルを編集して、**X サーバーや Xorg ではなく Xvnc プログラムを起動します。**

次の例では、パスワードなしでサーバーにログインするようにエントリが構成されています。デスクトップに正常にログインするには、ローカル UID は console ではなく none にします。

例では表示の便宜上、エントリが分割されています。実際には、エントリは 1 行で入力してください。

```
#   :0  Local local_uid@console root /usr/X11/bin/Xserver :0 -nobanner
  :0  Local local_uid@none root /usr/X11/bin/Xvnc :0 -nobanner
  -AlwaysShared -SecurityTypes None -geometry 1024x768x24 -depth 24
```

注 – 構成の安全性を高めるには、-SecurityTypes VncAuth パラメータを使用してパスワードを要求します。パスワードの要件については、Xvnc(1) のマニュアルページで説明しています。

d. サーバーを再起動するか、Xvnc サーバーを起動します。

```
# reboot
```

再起動後、Xvnc プログラムが実行されていることを確認します。

```
# ps -ef | grep Xvnc
  root  2145  932  0  Jan 18 ?  6:15 /usr/X11/bin/Xvnc :0 -nobanner
  -AlwaysShared -SecurityTypes None -geometry 1024
```

2 **Trusted Extensions の Xvnc サーバーの VNC クライアントすべてに対して、VNC クライアントソフトウェアをインストールします。**

クライアントシステムでは、ソフトウェアを選択できます。次の例では、Sun の VNC ソフトウェアを使用します。

```
# cd SUNW-pkg-directory
# pkgadd -d . SUNWvncviewer
```

3 **VNC クライアントの端末ウィンドウで、サーバーに接続します。**

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

4 **表示されるウィンドウで、名前とパスワードを入力します。**

ログイン手順に進みます。残りの手順については、『Solaris Trusted Extensions ユーザーズガイド』の「Trusted Extensions へのログイン」を参照してください。

スーパーユーザーとしてサーバーにログインした場合は、サーバーをすぐに管理できます。一般ユーザーとしてサーバーにログインした場合は、システムを管理する役割になってください。

◆ ◆ ◆ 第 9 章

Trusted Extensions と LDAP (概要)

この章では、Solaris Trusted Extensions が設定されたシステムでの Sun Java™ System Directory Server (ディレクトリサーバー) の使用法について説明します。

Trusted Extensions でのネームサービスの使用法

複数の Trusted Extensions システムを使用するセキュリティードメイン内で ユーザー、ホスト、ネットワーク属性の一貫性を達成するために、ほとんどの構成情報の配布にはネームサービスを使用します。LDAP はネームサービスの一例です。どのネームサービスを使用するかは、`nsswitch.conf` ファイルによって決定されます。LDAP は、Trusted Extensions で推奨されるネームサービスです。

Directory Server は、Trusted Extensions および Solaris クライアントに LDAP ネームサービスを提供することができます。サーバーには Trusted Extensions ネットワークデータベースが含まれている必要があり、Trusted Extensions クライアントはマルチレベルポートでサーバーに接続する必要があります。セキュリティー管理者は、Trusted Extensions を構成する際にマルチレベルポートを指定します。

Trusted Extensions は、LDAP サーバーに 2 つのトラステッドネットワークデータベース、 tnrhdb および tnrhtp を追加します。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」ツールを使用して管理されます。Scope=LDAP, Policy=TSOL のツールボックスは構成の変更をディレクトリサーバーに格納します。

- Solaris OS での LDAP ネームサービスの使用法については、『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)』を参照してください。
- Trusted Extensions クライアントに対するディレクトリサーバーの設定については、『Solaris Trusted Extensions 構成ガイド』を参照してください。Trusted Extensions システムは、Trusted Extensions が設定された LDAP プロキシサーバーを使用して、Solaris LDAP サーバーのクライアントになることができます。

注 – Trusted Extensions が設定されたシステムは、NIS または NIS+ マスターのクライアントになることはできません。

ネットワーク接続されていない Trusted Extensions システム

サイトでネームサービスを使用していない場合は、ユーザー、ホスト、ネットワークの構成情報がすべてのホストで同じであることを、管理者が確認する必要があります。1 つのホストで行なった変更は、すべてのホストで行う必要があります。

ネットワーク接続されていない Trusted Extensions システムでは、構成情報は /etc、/etc/security、および /etc/security/tsol ディレクトリに格納されます。Trusted_Extensions フォルダ内のアクションによって、一部の構成情報を変更できます。Solaris 管理コンソールの「セキュリティーテンプレート」ツールを使用すると、ネットワークデータベースのパラメータを修正することができます。ユーザー、役割、権利は、「ユーザーアカウント」、「管理役割」、および「権利」の各ツールで修正します。このコンピュータ Scope=Files, Policy=TSOL のツールボックスにローカルの構成変更が格納されています。

Trusted Extensions LDAP データベース

Trusted Extensions では、ディレクトリサーバーのスキーマを拡張して、tnrhdb データベースおよび tnrhtp データベースに対応しています。Trusted Extensions では、ipTnetNumber および ipTnetTemplateName の 2 つの属性と、ipTnetHost および ipTnetTemplate の 2 つのオブジェクトクラスが新しく定義されています。

属性の定義は次のとおりです。

```
ipTnetNumber
   ( 1.3.6.1.1.1.1.34 NAME 'ipTnetNumber'
     DESC 'Trusted network host or subnet address'
     EQUALITY caseExactIA5Match
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
     SINGLE-VALUE )

ipTnetTemplateName
   ( 1.3.6.1.1.1.1.35 NAME 'ipTnetTemplateName'
     DESC 'Trusted network template name'
     EQUALITY caseExactIA5Match
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
     SINGLE-VALUE )
```

オブジェクトクラスの定義は次のとおりです。

```
ipTnetTemplate
   ( 1.3.6.1.1.1.2.18 NAME 'ipTnetTemplate' SUP top STRUCTURAL
     DESC 'Object class for Trusted network host templates'
     MUST ( ipTnetTemplateName )
     MAY ( SolarisAttrKeyValue ) )

ipTnetHost
   ( 1.3.6.1.1.1.2.19 NAME 'ipTnetHost' SUP top AUXILIARY
     DESC 'Object class for Trusted network host/subnet address
           to template mapping'
     MUST ( ipTnetNumber $ ipTnetTemplateName ) )
```

LDAP での `cipso` テンプレート定義は、次のようなものです。

```
ou=ipTnet,dc=example,dc=example1,dc=exampleco,dc=com
 objectClass=top
 objectClass=organizationalUnit
 ou=ipTnet

 ipTnetTemplateName=cipso,ou=ipTnet,dc=example,dc=example1,dc=exampleco,dc=com
 objectClass=top
 objectClass=ipTnetTemplate
 ipTnetTemplateName=cipso
 SolarisAttrKeyValue=host_type=cipso;doi=1;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH;

 ipTnetNumber=0.0.0.0,ou=ipTnet,dc=example,dc=example1,dc=exampleco,dc=com
 objectClass=top
 objectClass=ipTnetTemplate
 objectClass=ipTnetHost
 ipTnetNumber=0.0.0.0
 ipTnetTemplateName=internal
```

Trusted Extensions での LDAP ネームサービスの使用法

Trusted Extensions では、LDAP ネームサービスは Solaris OS の場合と同じように管理されます。次に、役立つコマンドの例と、詳細情報の参照先を示します。

- 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。
- クライアントとサーバーの LDAP 接続においてラベルの影響を受ける問題のトラブルシューティングについては、210 ページの「LDAP サーバーへのクライアント接続をデバッグする」を参照してください。
- クライアントとサーバーの LDAP 接続におけるその他の問題のトラブルシューティングについては、『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 クライアントから LDAP エントリを表示するには、次のように入力します。

```
$ ldaplist -l
$ ldap_cachemgr -g
```

- LDAP サーバーから LDAP エントリを表示するには、次のように入力します。

```
$ ldap_cachemgr -g
$ idsconfig -v
```

- LDAP が管理するホストを一覧表示するには、次のように入力します。

```
$ ldaplist -l hosts      Long listing
$ ldaplist hosts         One-line listing
```

- LDAP 上のディレクトリ情報ツリー (DIT) 内の情報を一覧表示するには、次のように入力します。

```
$ ldaplist -l services | more
dn: cn=apocd+ipServiceProtocol=udp,ou=Services,dc=exampleco,dc=com
  objectClass: ipService
  objectClass: top
  cn: apocd
  ipServicePort: 38900
  ipServiceProtocol: udp

...
$ ldaplist services name
dn=cn=name+ipServiceProtocol=udp,ou=Services,dc=exampleco,dc=com
```

- クライアント上の LDAP サービスのステータスを表示するには、次のように入力します。

```
# svcs -xv network/ldap/client
svc:/network/ldap/client:default (LDAP client)
 State: online since date
   See: man -M /usr/share/man -s 1M ldap_cachemgr
   See: /var/svc/log/network-ldap-client:default.log
Impact: None.
```

- LDAP クライアントを起動および停止するには、次のように入力します。

```
# svcadm enable network/ldap/client

# svcadm disable network/ldap/client
```

- バージョン 5.2 の Sun Java System Directory Server ソフトウェアで LDAP サーバーを起動および停止するには、次のように入力します。

```
# installation-directory/slap-LDAP-server-hostname/start-slapd
# installation-directory/slap-LDAP-server-hostname/stop-slapd
```

- バージョン 6 の Sun Java System Directory Server ソフトウェアで LDAP サーバーを起動および停止するには、次のように入力します。

```
# dsadm start /export/home/ds/instances/your-instance
# dsadm stop /export/home/ds/instances/your-instance
```

- バージョン 6 の Sun Java System Directory Server ソフトウェアで LDAP プロキシサーバーを起動および停止するには、次のように入力します。

```
# dpadm start /export/home/ds/instances/your-instance
# dpadm stop /export/home/ds/instances/your-instance
```

◆ ◆ ◆ 第 10 章

Trusted Extensions でのゾーンの管理 (手順)

この章では、Solaris Trusted Extensions が設定されたシステムで非大域ゾーンがどのように動作するかについて説明します。Trusted Extensions のゾーンに特有の手順についても記載します。

Trusted Extensions のゾーン

適切に構成された Trusted Extensions システムは、オペレーティングシステムのインスタンスである大域ゾーンと、1 つ以上のラベル付きの非大域ゾーンで構成されます。構成中に Trusted Extensions は各ゾーンに一意のラベルを添付し、それによってラベル付きゾーンが作成されます。ラベルは、`label_encodings` ファイルから取得されます。管理者はすべてのラベルにゾーンを作成できますが、必須ではありません。システム上で、ラベル付きゾーンの数より多くのラベルを持つことができます。ラベルの数より多くのラベル付きゾーンを持つことはできません。

Trusted Extensions システムで、ゾーンのファイルシステムは通常、ループバックファイルシステム (lofs) としてマウントされます。ラベル付きゾーンの書き込み可能なファイルおよびディレクトリには、ゾーンと同じラベルが付いています。デフォルトでは、ユーザーは自身の現在のラベルより下位のラベルのゾーンにあるファイルを表示できます。この構成によって、ユーザーは現在のワークスペースのラベルより下位のラベルのホームディレクトリを表示することができます。ユーザーは下位のラベルのファイルを表示できますが、それらを変更することはできません。ユーザーは、ファイルと同じラベルのプロセスからしかファイルを変更できません。

Trusted Extensions では、大域ゾーンが管理ゾーンです。ラベル付きゾーンは一般ユーザー用です。ユーザーは、自身の認可範囲内にあるラベルのゾーンで作業することができます。

各ゾーンには、関連付けられた IP アドレスとセキュリティー属性があります。ゾーンは、マルチレベルポート (MLP) を使用して構成できます。また、ゾーンには `ping` などの ICMP (Internet Control Message Protocol) ブロードキャストのポリシーで構成することができます。

ラベル付きゾーンのディレクトリの共有とラベル付きゾーンのディレクトリの遠隔マウントについては、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。

Trusted Extensions のゾーンは、Solaris ゾーン製品の上に構築されます。詳細は、『System Administration Guide: Solaris Containers-Resource Management and Solaris Zones』のパート II「Zones」を参照してください。具体的には、パッチとパッケージのインストールの問題が Trusted Extensions に影響します。詳細は、『System Administration Guide: Solaris Containers-Resource Management and Solaris Zones』の第 24 章「About Packages and Patches on a Solaris System With Zones Installed (Overview)」と『System Administration Guide: Solaris Containers-Resource Management and Solaris Zones』の第 29 章「Troubleshooting Miscellaneous Solaris Zones Problems」を参照してください。

Trusted Extensions のゾーンと IP アドレス

初期設定チームは、大域ゾーンとラベル付きゾーンに IP アドレスを割り当てています。3 タイプの構成については、『Solaris Trusted Extensions 構成ガイド』の「ラベル付きゾーンの作成」に説明されています。

- システムに、大域ゾーンとすべてのラベル付きゾーン用の 1 つの IP アドレスを設定します。

  この構成は、DHCP ソフトウェアを使用して IP アドレスを取得するシステムで役に立ちます。ログインする予定のユーザーがいない場合は、LDAP サーバーをこのように構成します。
- システムに、大域ゾーン用の 1 つの IP アドレスと、大域ゾーンを含めたすべてのゾーンで共有される 1 つの IP アドレスを設定します。任意のゾーンが、一意のアドレスと共有アドレスの組み合わせを持つことができます。

  この構成は、一般ユーザーがログインするシステムで役に立ちます。プリンタや NFS サーバーにも使用できます。この構成では IP アドレスが節約されます。
- システムに、大域ゾーン用の 1 つの IP アドレスを設定し、ラベル付きの各ゾーンが一意の IP アドレスを持ちます。

この構成は、シングルレベルシステムの個々の物理ネットワークにアクセスするときに役に立ちます。通常、各ゾーンはほかのラベル付きゾーンとは異なる物理ネットワーク上の IP アドレスを持ちます。この構成は単一の IP インスタンスによって実装されるため、大域ゾーンで物理インタフェースを制御し、経路テーブルなどの大域リソースを管理します。

非大域ゾーン用の排他的 IP インスタンスの導入に伴って、Solaris OS では 4 番目の構成タイプを使用できるようになりました。Solaris 10 8/07 リリース以降、非大域ゾーンにそれぞれの IP インスタンスを割り当てて、非大域ゾーンでそれぞれの物理インタフェースを管理できるようになりました。この構成では、各ゾーンは別個のシステムであるかのように動作します。詳細は、『System Administration Guide: Solaris Containers-Resource Management and Solaris Zones』の「Zone Network Interfaces」を参照してください。

ただし、このような構成では、各ラベル付きゾーンは別個のシングルラベル付きシステムのように動作します。Trusted Extensions のマルチレベルネットワーク機能は、共有 IP スタックの機能に依存しています。Trusted Extensions の管理手順は、ネットワーク接続が大域ゾーンによって完全に制御されることを前提としています。したがって、初期設定チームが排他的 IP インスタンスでラベル付きゾーンをインストールした場合は、サイト固有のマニュアルを用意するか参照する必要があります。

ゾーンとマルチレベルポート

デフォルトでは、ゾーンはほかのゾーンとの間でパケットを送受信できません。マルチレベルポート (MLP) を使用すると、ポート上の特定のサービスがラベルの範囲内の、またはラベルセットからの要求を受け取ることができます。これらの特権サービスは、要求のラベルで返信できます。たとえば、すべてのラベルで待機できるが、その返信はラベルによって制限されるような特権 Web ブラウザポートを作成することができます。デフォルトでは、ラベル付きゾーンは MLP を持ちません。

MLP で受け取れるパケットを制約するラベル範囲またはラベルセットは、ゾーンの IP アドレスに基づきます。`tnrhdb` データベースで、IP アドレスに遠隔ホストテンプレートが割り当てられます。遠隔ホストテンプレートのラベル範囲またはラベルセットによって、MLP が受け取れるパケットが制約されます。

- 異なる IP アドレス構成での MLP の制約は次のとおりです。
- 大域ゾーンが IP アドレスを持ち、各ラベル付きゾーンが一意の IP アドレスを持つシステムでは、特定のサービス用の MLP を各ゾーンに追加することができます。たとえば、TCP ポート 22 上の `ssh` サービスが大域ゾーンと各ラベル付きゾーンで MLP であるようにシステムを構成できます。
- 通常の構成では、大域ゾーンには 1 つの IP アドレスが割り当てられ、ラベル付きゾーンは 2 番目の IP アドレスを大域ゾーンと共有します。MLP を共有インタフェースに追加すると、サービスパケットは MLP が定義されているラベル付きゾーンに経路指定されます。パケットは、ラベル付きゾーンの遠隔ホストテンプ

レートがパケットのラベルを含んでいる場合にだけ受け取られます。範囲が ADMIN_LOW から ADMIN_HIGH の場合、すべてのパケットが受け取られます。範囲がこれより狭い場合、範囲内にないパケットは破棄されます。

最大で 1 つのゾーンが、特定のポートを共有インタフェースでの MLP として定義することができます。前述のシナリオでは、ssh ポートが非大域ゾーンの共有 MLP として構成され、それ以外のゾーンは共有アドレスで ssh 接続を受け取ることができません。ただし、大域ゾーンはゾーン固有のアドレスで接続を受け取るプライベート MLP として ssh ポートを定義できます。

- 大域ゾーンとラベル付きゾーンが IP アドレスを共有するシステムでは、ssh サービス用の MLP を 1 つのゾーンに追加することができます。ssh 用の MLP を大域ゾーンに追加した場合、ラベル付きゾーンは ssh サービス用の MLP を追加できません。同様に、ssh サービス用の MLP をラベル付きゾーンに追加した場合、ssh MLP を使用して大域ゾーンを構成することはできません。

ラベル付きゾーンに MLP を追加する例については、例 13–16 を参照してください。

Trusted Extensions のゾーンと ICMP

ネットワークはブロードキャストメッセージを送信し、ネットワーク上のシステムに ICMP パケットを送信します。マルチレベルシステムでは、これらの送信が各ラベルでシステムの容量を超えることがあります。ラベル付きゾーンのデフォルトのネットワークポリシーでは、一致するラベルでだけ ICMP パケットが受け取られるようにする必要があります。

大域ゾーンプロセスとラベル付きゾーン

Trusted Extensions では、大域ゾーンのプロセスを含むすべてのプロセスに MAC ポリシーが適用されます。大域ゾーンのプロセスは ADMIN_HIGH ラベルで実行されます。大域ゾーンのファイルが共有される場合、ADMIN_LOW ラベルで共有されます。MAC では上位のラベルの付いたプロセスが下位のオブジェクトを変更できないため、通常、大域ゾーンは NFS マウントシステムに書き込むことができません。

ただし、限定的ではあるものの、ラベル付きゾーンのアクションでは、大域ゾーンのプロセスにそのゾーンのファイルの変更を要求することがあります。

大域ゾーンのプロセスが読み取り/書き込み権を持つ遠隔ファイルシステムをマウントできるようにするには、遠隔ファイルシステムのラベルと一致するラベルを持ったゾーンのゾーンパスの下にマウントする必要があります。ただし、そのゾーンのルートパスの下にマウントしてはいけません。

- マウントする側のシステムには、遠隔ファイルシステムと同じラベルのゾーンが必要です。

- システムは同じラベルの付いたゾーンのゾーンパスの下に遠隔ファイルシステムをマウントする必要があります。

  システムは遠隔ファイルシステムを同じラベルの付いたゾーンの「ゾーンルートパス」の下にマウントしてはいけません。

PUBLIC というラベルで public という名前のゾーンを考えてみましょう。「ゾーンパス」は /zone/public/ です。このゾーンパスの下にあるディレクトリはすべて、次のように、PUBLIC ラベルになります。

```
/zone/public/dev
/zone/public/etc
/zone/public/home/username
/zone/public/root
/zone/public/usr
```

ゾーンパスの下のディレクトリの中では、/zone/public/root の下にあるファイルのみ public ゾーンから表示できます。ほかの PUBLIC ラベルのディレクトリとファイルはすべて、大域ゾーンからのみアクセスできます。/zone/public/root は「ゾーンルートパス」です。

ゾーンルートパスは、public ゾーン管理者には / として表示されます。同様に、public ゾーン管理者は、ゾーンパスのユーザーのホームディレクトリである、/zone/public/home/*username* ディレクトリにはアクセスできません。そのディレクトリは、大域ゾーンからのみ表示できます。Public ゾーンはそのディレクトリをゾーンルートパスに /home/ *username* としてマウントします。そのマウントは、大域ゾーンには /zone/public/root/home/ *username* として表示されます。

Public ゾーン管理者は /home/ *username* を変更できます。ユーザーのホームディレクトリのファイルを変更する必要がある場合、大域ゾーンプロセスはそのパスを使用しません。大域ゾーンは、ゾーンパスのユーザーのホームディレクトリ /zone/public/home/*username* を使用します。

- ゾーンパス /zone/*zonename*/ の下にあり、ゾーンルートパス /zone/*zonename* /root ディレクトリの下にないファイルおよびディレクトリは、ADMIN_HIGH ラベルで実行される大域ゾーンプロセスで変更できます。
- ラベル付きゾーン管理者は、ゾーンルートパス /zone/public/root の下にあるファイルおよびディレクトリを変更できます。

たとえば、ユーザーがデバイスを public ゾーンに割り当てる場合、ADMIN_HIGH ラベルで実行される大域ゾーンプロセスでは、ゾーンパス /zone/public/dev の dev ディレクトリが変更されます。同様に、ユーザーがデスクトップ構成を保存する場合、デスクトップ構成ファイルは /zone/public/home/*username* の大域ゾーンプロセスによって変更されます。最後に、ラベル付きゾーンのファイルを共有する場合、大域ゾーン管理者は構成ファイル dfstab をゾーンパス /zone/public/etc/dfs/dfstab に作成します。ラベル付きゾーン管理者はそのファイルにアクセスできません。また、ラベル付きゾーンのファイルも共有できませ

ん。ラベル付きディレクトリを共有する場合は、156 ページの「ラベル付きゾーンのディレクトリを共有する」を参照してください。

Trusted Extensions でのゾーン管理ユーティリティー

一部のゾーン管理タスクは、コマンド行から実行できます。しかし、ゾーン管理のもっとも簡単な方法は、Trusted Extensions に用意されている GUI を使用することです。

- ゾーンのセキュリティー属性の構成は、Solaris 管理コンソールの「トラステッドネットワークゾーン」ツールを使用して実行します。このツールについては、43 ページの「「トラステッドネットワークゾーン」ツール」を参照してください。ゾーンの構成および作成の例については、『Solaris Trusted Extensions 構成ガイド』の第 4 章「Trusted Extensions の構成 (手順)」と144 ページの「ゾーンにマルチレベルポートを作成する」を参照してください。
- シェルスクリプト `/usr/sbin/txzonemgr` では、ゾーンの作成、インストール、初期化、起動を行うメニューベースのウィザードが提供されます。Solaris Trusted Extensions (JDS) からゾーンを管理している場合、Trusted CDE アクションではなく `txzonemgr` スクリプトを使用します。`txzonemgr` は `zenity` コマンドを使用します。詳細は、`zenity`(1) のマニュアルページを参照してください。
- Trusted CDE では、ゾーンの構成と作成は Trusted_Extensions フォルダのアクションを使用して実行できます。アクションについては、37 ページの「Trusted CDE アクション」を参照してください。アクションを使用する手順については、58 ページの「Trusted Extensions の CDE 管理アクションを起動する」を参照してください。

ゾーンの管理 (作業マップ)

次の作業マップでは、Trusted Extensions に固有のゾーン管理タスクについて説明します。このマップでは、Solaris システムの場合と同様に、Trusted Extensions で実行される一般的な手順も説明しています。

作業	説明	参照先
すべてのゾーンの表示	任意のラベルで、現在のゾーンのほうが優位であるゾーンを表示します。	134 ページの「作成済みまたは実行中のゾーンを表示する」
マウントされたディレクトリの表示	任意のラベルで、現在のラベルのほうが優位であるディレクトリを表示します。	135 ページの「マウントされたファイルのラベルを表示する」

作業	説明	参照先
一般ユーザーが /etc ファイルを表示できるようにする	ラベル付きゾーンでデフォルトでは表示されない大域ゾーンから、ディレクトリまたはファイルをループバックマウントします。	137 ページの「通常はラベル付きゾーンから表示されないファイルをループバックマウントする」
一般ユーザーが上位レベルのラベルから下位レベルのホームディレクトリを表示できないようにします。	デフォルトでは、上位レベルのゾーンから下位レベルのディレクトリを表示できます。下位ゾーンの 1 つのマウントを無効にすると、下位ゾーンのマウントはすべて無効になります。	138 ページの「下位ファイルのマウントを無効にする」
ファイルのラベルを変更できるようにゾーンを構成します。	ラベル付きゾーンには制限付きの特権があります。デフォルトでは、ラベル付きゾーンには、承認ユーザーがファイルに再ラベル付けする特権がありません。ゾーン構成を修正して特権を追加します。	141 ページの「ラベル付きゾーンからファイルに再ラベル付けできるようにする」
ラベル付きゾーンとの間でファイルまたはディレクトリを移動します。	ラベルを変更して、ファイルまたはディレクトリのセキュリティーレベルを変更します。	『Solaris Trusted Extensions ユーザーズガイド』の「Trusted CDE でラベル間でファイルを移動する」
ZFS データセットをラベル付きゾーンに接続して共有します。	ZFS データセットを読み取り/書き込み権でラベル付きゾーンにマウントし、そのデータセットを読み取り専用で上位のゾーンと共有します。	139 ページの「ラベル付きゾーンの ZFS データセットを共有する」.
新しいゾーンを構成します。	このシステムでゾーンのラベル付けに現在使用されていないラベルに、ゾーンを作成します。	『Solaris Trusted Extensions 構成ガイド』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。 次に、初期設定チームがほかのゾーンを作成した手順に従います。手順については、『Solaris Trusted Extensions 構成ガイド』の「ラベル付きゾーンの作成」を参照してください。
アプリケーション用のマルチレベルポートを作成します。	マルチレベルポートは、ラベル付きゾーンへのマルチレベルフィードを必要とするプログラムに役立ちます。	143 ページの「udp で NFSv3 のマルチレベルポートを構成する」 144 ページの「ゾーンにマルチレベルポートを作成する」
NFS マウントとアクセスの問題をトラブルシューティングします。	マウントと、場合によってはゾーンに関する一般的なアクセス上の問題をデバッグします。	163 ページの「Trusted Extensions でマウントの失敗をトラブルシューティングする」

作業	説明	参照先
ラベル付きゾーンを削除します。	ラベル付きゾーンをシステムから完全に削除します。	『System Administration Guide: Solaris Containers-Resource Management and Solaris Zones』の「How to Remove a Non-Global Zone」

▼ 作成済みまたは実行中のゾーンを表示する

この手順では、現在のゾーンと、現在のゾーンのほうが優位であるすべてのゾーンのラベルを表示するシェルスクリプトを作成します。

始める前に　大域ゾーンで、システム管理者役割になっている必要があります。

1. トラステッドエディタを使用して、getzonelabels スクリプトを作成します。

   詳細は、59 ページの「Trusted Extensions の管理ファイルを編集する」を参照してください。

   /usr/local/scripts/getzonelabels など、スクリプトへのパス名を入力します。

2. 次の内容を入力して、ファイルを保存します。

```
#!/bin/sh
#
echo "NAME\t\tSTATUS\t\tLABEL"
echo "====\t\t======\t\t====="
myzone=‘zonename‘
for i in ‘/usr/sbin/zoneadm list -p‘ ; do
        zone=‘echo $i | cut -d ":" -f2‘
        status=‘echo $i | cut -d ":" -f3‘
        path=‘echo $i | cut -d ":" -f4‘
        if [ $zone != global ]; then
                if [ $myzone = global ]; then
                        path=$path/root/tmp
                else
                        path=$path/export/home
                fi
        fi
        label=‘/usr/bin/getlabel -s $path |cut -d ":" -f2-9‘
        if [ ‘echo $zone|wc -m‘ -lt 8 ]; then
                echo "$zone\t\t$status\t$label"
        else
                echo "$zone\t$status\t$label"
        fi
done
```

3 大域ゾーンでスクリプトをテストします。

```
# getzonelabels
NAME            STATUS          LABEL
====            ======          =====
global          running         ADMIN_HIGH
needtoknow      running         CONFIDENTIAL : NEED TO KNOW
restricted      ready           CONFIDENTIAL : RESTRICTED
internal        running         CONFIDENTIAL : INTERNAL
public          running         PUBLIC
```

大域ゾーンからこのスクリプトを実行すると、作成済みまたは実行中のすべてのゾーンのラベルが表示されます。デフォルトの `label_encodings` ファイルから作成されたゾーンの大域ゾーン出力は、次のとおりです。

例 **10–1** 作成済みまたは実行中のゾーンすべてのラベルの表示

次の例では、`internal` ゾーンでユーザーが `getzonelabels` スクリプトを実行します。

```
# getzonelabels
NAME            STATUS          LABEL
====            ======          =====
internal        running         CONFIDENTIAL : INTERNAL
public          running         PUBLIC
```

▼ マウントされたファイルのラベルを表示する

この手順では、現在のゾーンでマウントされたファイルシステムを表示するシェルスクリプトを作成します。大域ゾーンからこのスクリプトを実行すると、各ゾーンでマウントされたすべてのファイルシステムのラベルが表示されます。

始める前に 大域ゾーンで、システム管理者役割になっている必要があります。

1 トラステッドエディタを使用して、`getmounts` スクリプトを作成します。

詳細は、59 ページの「Trusted Extensions の管理ファイルを編集する」を参照してください。

`/usr/local/scripts/getmounts` など、スクリプトへのパス名を入力します。

2 次の内容を追加して、ファイルを保存します。

```
#!/bin/sh
#
for i in `/usr/sbin/mount -p | cut -d " " -f3` ; do
        /usr/bin/getlabel $i
done
```

3 大域ゾーンでスクリプトをテストします。

```
# /usr/local/scripts/getmounts
/:      ADMIN_LOW
/dev:   ADMIN_LOW
/kernel:        ADMIN_LOW
/lib:   ADMIN_LOW
/opt:   ADMIN_LOW
/platform:      ADMIN_LOW
/sbin:  ADMIN_LOW
/usr:   ADMIN_LOW
/var/tsol/doors:        ADMIN_LOW
/zone/needtoknow/export/home:   CONFIDENTIAL : NEED TO KNOW
/zone/internal/export/home:     CONFIDENTIAL : INTERNAL USE ONLY
/zone/restricted/export/home:   CONFIDENTIAL : RESTRICTED
/proc:  ADMIN_LOW
/system/contract:       ADMIN_LOW
/etc/svc/volatile:      ADMIN_LOW
/etc/mnttab:    ADMIN_LOW
/dev/fd:        ADMIN_LOW
/tmp:           ADMIN_LOW
/var/run:       ADMIN_LOW
/zone/public/export/home:  PUBLIC
/root:          ADMIN_LOW
```

例 10–2 restricted ゾーンでのファイルシステムのラベルの表示

一般ユーザーがラベル付きゾーンから getmounts スクリプトを実行すると、そのゾーンでマウントされたすべてのファイルシステムのラベルが表示されます。デフォルトの label_encodings ファイル内の各ラベルに対してゾーンが作成されたシステムでは、restricted ゾーンの出力は次のとおりです。

```
# /usr/local/scripts/getmounts
/:      CONFIDENTIAL : RESTRICTED
/dev:   CONFIDENTIAL : RESTRICTED
/kernel:        ADMIN_LOW
/lib:   ADMIN_LOW
/opt:   ADMIN_LOW
/platform:      ADMIN_LOW
/sbin:  ADMIN_LOW
/usr:   ADMIN_LOW
/var/tsol/doors:        ADMIN_LOW
/zone/needtoknow/export/home:   CONFIDENTIAL : NEED TO KNOW
/zone/internal/export/home:     CONFIDENTIAL : INTERNAL USE ONLY
/proc:  CONFIDENTIAL : RESTRICTED
/system/contract:       CONFIDENTIAL : RESTRICTED
/etc/svc/volatile:      CONFIDENTIAL : RESTRICTED
/etc/mnttab:    CONFIDENTIAL : RESTRICTED
```

```
/dev/fd:        CONFIDENTIAL : RESTRICTED
/tmp:   CONFIDENTIAL : RESTRICTED
/var/run:       CONFIDENTIAL : RESTRICTED
/zone/public/export/home:       PUBLIC
/home/gfaden:   CONFIDENTIAL : RESTRICTED
```

▼ 通常はラベル付きゾーンから表示されないファイルをループバックマウントする

この手順では、指定されたラベル付きゾーンのユーザーが、デフォルトでは大域ゾーンからエクスポートされないファイルを表示できるようにします。

始める前に　大域ゾーンで、システム管理者役割になっている必要があります。

1 構成を変更するゾーンを停止します。

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

2 ファイルまたはディレクトリをループバックマウントします。

たとえば、一般ユーザーが /etc ディレクトリにあるファイルを表示できるようにします。

```
# zonecfg -z zone-name
 add filesystem
 set special=/etc/filename
 set directory=/etc/filename
 set type=lofs
 add options [ro,nodevices,nosetuid]
 end
 exit
```

注 – 特定のファイルはループバックマウントしても影響しないようにシステムで使用されません。たとえば、ラベル付きゾーンの /etc/dfs/dfstab ファイルは Trusted Extensions ソフトウェアでは検査されません。詳細は、149 ページの「ラベル付きゾーンのファイルの共有」を参照してください。

---

3 ゾーンを起動します。

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

例 10–3　/etc/passwd ファイルのループバックマウント

この例でセキュリティー管理者は、テスターおよびプログラマのローカルパスワードが設定されていることをそのテスターやプログラマ自身が確認できるように

します。sandbox ゾーンが停止されたあと、passwd ファイルをループバックマウントするように構成されます。次に、ゾーンが再起動されます。

```
# zoneadm -z sandbox halt
# zonecfg -z sandbox
 add filesystem
    set special=/etc/passwd
    set directory=/etc/passwd
    set type=lofs
    add options [ro,nodevices,nosetuid]
 end
 exit
# zoneadm -z sandbox boot
```

▼ 下位ファイルのマウントを無効にする

デフォルトでは、ユーザーは下位レベルのファイルを表示できます。特定ゾーンから下位レベルのすべてのファイルを表示することを禁止するには、net_mac_aware 特権を削除します。net_mac_aware 特権については、privileges(5) のマニュアルページを参照してください。

始める前に　大域ゾーンで、システム管理者役割になっている必要があります。

1. 構成を変更するゾーンを停止します。

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

2. 下位レベルのファイルの表示を禁止するようにゾーンを構成します。

   ゾーンから net_mac_aware 特権を削除します。

   ```
   # zonecfg -z zone-name
    set limitpriv=default,!net_mac_aware
    exit
   ```

3. ゾーンを再起動します。

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

例 10–4 ユーザーによる下位ファイルの表示を禁止する

この例でセキュリティー管理者は、このシステム上のユーザーが混乱しないように構成しようとします。そのため、ユーザーは自身が作業中のラベルでしかファイルを表示できなくなります。セキュリティー管理者は、下位レベルのすべてのファイルの表示を禁止します。このシステムで、ユーザーは PUBLIC ラベルで作業しない限り、共通で利用可能なファイルを表示することができません。また、ユーザーはゾーンのラベルでファイルを NFS マウントできるだけです。

```
# zoneadm -z restricted halt
# zonecfg -z restricted
 set limitpriv=default,!net_mac_aware
 exit
# zoneadm -z restricted boot

# zoneadm -z needtoknow halt
# zonecfg -z needtoknow
 set limitpriv=default,!net_mac_aware
 exit
# zoneadm -z needtoknow boot

# zoneadm -z internal halt
# zonecfg -z internal
 set limitpriv=default,!net_mac_aware
 exit
# zoneadm -z internal boot
```

PUBLIC は最小のラベルなので、セキュリティー管理者は PUBLIC ゾーンに対するコマンドは実行しません。

▼ ラベル付きゾーンの ZFS データセットを共有する

この手順では、ZFS データセットを読み取り/書き込み権でラベル付きゾーンにマウントします。すべてのコマンドが大域ゾーンで実行されるため、大域ゾーン管理者がラベル付きゾーンへの ZFS データセットの追加を制御します。

データセットを共有するには、最低でもラベル付きゾーンが ready 状態である必要があります。ラベル付きゾーンが running 状態であっても構いません。

始める前に　データセットを持つゾーンを構成するには、最初にそのゾーンを停止します。

1. **ZFS データセットを作成します。**

   `# zfs create` *datasetdir/subdir*

   データセットの名前には、zone/data などのディレクトリを含めることができます。

2. **大域ゾーンで、ラベル付きゾーンを停止します。**

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

3. **データセットのマウントポイントを設定します。**

   `# zfs set mountpoint=legacy` *datasetdir/subdir*

   ZFS mountpoint プロパティーで、マウントポイントがラベル付きゾーンに対応付けられたときのマウントポイントのラベルを設定します。

4 ラベル付きゾーンにデータセットをファイルシステムとして追加します。

```
# zonecfg -z labeled-zone-name
# zonecfg:labeled-zone-name> add fs
# zonecfg:labeled-zone-name:dataset> set dir=/subdir
# zonecfg:labeled-zone-name:dataset> set special=datasetdir/subdir
# zonecfg:labeled-zone-name:dataset> set type=zfs
# zonecfg:labeled-zone-name:dataset> end
# zonecfg:labeled-zone-name> exit
```

データセットをファイルシステムとして追加することにより、dfstab ファイルが解釈される前に、データセットがゾーンの /data にマウントされます。この手順により、ゾーンが起動する前にデータセットがマウントされないようになります。具体的に言うと、ゾーンが起動し、データセットがマウントされてから、dfstab ファイルが解釈されます。

5 データセットを共有します。

データセットファイルシステムのエントリを /zone/*labeled-zone-name*/etc/dfs/dfstab ファイルに追加します。このエントリには、*/subdir* パス名も使用されます。

```
share  -F nfs  -d "dataset-comment"  /subdir
```

6 ラベル付きゾーンを起動します。

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

ゾーンが起動すると、データセットが、*labeled-zone-name* ゾーンのラベルを持つ *labeled-zone-name* ゾーンの読み取り/書き込みマウントポイントとして自動的にマウントされます。

例 10–5 ラベル付きゾーンの ZFS データセットを共有してマウントする

この例では、管理者は ZFS データセットを needtoknow ゾーンに追加し、そのデータセットを共有します。データセット zone/data は現在、/mnt マウントポイントに割り当てられています。restricted ゾーンのユーザーはそのデータセットを表示できます。

最初に、管理者はゾーンを停止します。

```
# zoneadm -z needtoknow halt
```

データセットは現在別のマウントポイントに割り当てられているため、管理者は以前の割り当てを削除してから、新しいマウントポイントを設定します。

```
# zfs set zoned=off zone/data
# zfs set mountpoint=legacy zone/data
```

次に、zonecfg 対話型インタフェースで、管理者はデータセットを needtoknow ゾーンに明示的に追加します。

```
# zonecfg -z needtoknow
# zonecfg:needtoknow> add fs
# zonecfg:needtoknow:dataset> set dir=/data
# zonecfg:needtoknow:dataset> set special=zone/data
# zonecfg:needtoknow:dataset> set type=zfs
# zonecfg:needtoknow:dataset> end
# zonecfg:needtoknow> exit
```

さらに、管理者はそのデータセットを共有するように /zone/needtoknow/etc/dfs/dfstab ファイルを変更してから、needtoknow ゾーンを起動します。

```
## Global zone dfstab file for needtoknow zone
share  -F nfs  -d "App Data on ZFS"  /data
```

```
# zoneadm -z needtoknow boot
```

これで、データセットはアクセス可能になります。

restricted ゾーンのユーザーは、needtoknow ゾーンを独占しており、/data ディレクトリに変更することでマウントされたデータセットを表示できます。ユーザーは、大域ゾーンを基準にして、マウントされたデータセットへのフルパスを使用します。この例では、machine1 はラベル付きゾーンを含むシステムのホスト名です。管理者は、このホスト名を共有していない IP アドレスに割り当てています。

```
# cd /net/machine1/zone/needtoknow/root/data
```

注意事項　上位ラベルからデータセットにアクセスしようとして、エラー not found または No such file or directory が返された場合、管理者は svcadm restart autofs コマンドを実行して、オートマウンタサービスを再起動する必要があります。

▼ ラベル付きゾーンからファイルに再ラベル付けできるようにする

ユーザーがファイルに再ラベル付けできるようにする場合、この手順が前提条件となります。

始める前に　大域ゾーンでセキュリティー管理者役割になります。

1 構成を変更するゾーンを停止します。

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

2 再ラベル付けできるようにゾーンを構成します。

ゾーンに適切な特権を追加します。ウィンドウ特権により、ユーザーはドラッグ&ドロップ操作と、カット&ペースト操作を使うことができます。

- ダウングレードを可能にするには、ゾーンに `file_downgrade_sl` 特権を追加します。

```
# zonecfg -z zone-name
 set limitpriv=default,win_dac_read,win_mac_read,win_dac_write,
 win_mac_write,win_selection,file_downgrade_sl
 exit
```

- アップグレードを可能にするには、ゾーンに `sys_trans_label` および `file_upgrade_sl` 特権を追加します。

```
# zonecfg -z zone-name
 set limitpriv=default,win_dac_read,win_mac_read,win_dac_write,
 win_mac_write,win_selection,sys_trans_label,file_upgrade_sl
 exit
```

- アップグレードとダウングレードの両方を可能にするには、ゾーンに **3** つの特権をすべて追加します。

```
# zonecfg -z zone-name
 set limitpriv=default,win_dac_read,win_mac_read,win_dac_write,
 win_mac_write,win_selection,sys_trans_label,file_downgrade_sl,
 file_upgrade_sl
 exit
```

3 ゾーンを再起動します。

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

再ラベル付けを許可するユーザーおよびプロセスの要件については、`setflabel`(3TSOL) のマニュアルページを参照してください。ユーザーによるファイルの再ラベル付けを承認する方法については、103 ページの「ユーザーによるデータのセキュリティーレベルの変更を有効にする」を参照してください。

例 10–6 `internal` ゾーンからのアップグレードを可能にする

この例でセキュリティー管理者は、このシステム上の承認ユーザーがファイルをアップグレードできるようにします。ユーザーによる情報のアップグレードを可能にすることで、管理者はさらに高いセキュリティーレベルでユーザーが情報を保護できるようにします。大域ゾーンで、管理者は次のゾーン管理コマンドを実行します。

```
# zoneadm -z internal halt
# zonecfg -z internal
 set limitpriv=default,sys_trans_label,file_upgrade_sl
```

```
 exit
# zoneadm -z internal boot
```

これで、承認ユーザーは internal 情報を internal ゾーンから restricted にアップグレードできます。

例 10–7 restricted ゾーンからのダウングレードを可能にする

この例でセキュリティー管理者は、このシステム上の承認ユーザーがファイルをダウングレードできるようにします。管理者がゾーンにウィンドウ特権を追加しないため、承認ユーザーはファイルマネージャーを使用してファイルに再ラベル付けはできません。ファイルを再ラベル付けする場合、ユーザーは setlabel コマンドを使用します。

ユーザーによる情報のダウングレードを可能にすることにより、管理者はセキュリティーの下位のユーザーがファイルにアクセスできるようにします。大域ゾーンで、管理者は次のゾーン管理コマンドを実行します。

```
# zoneadm -z restricted halt
# zonecfg -z restricted
 set limitpriv=default,file_downgrade_sl
 exit
# zoneadm -z restricted boot
```

これで、承認ユーザーは setlabel コマンドを使用して、restricted 情報を restricted ゾーンから internal または public にダウングレードできます。

▼ udp で NFSv3 のマルチレベルポートを構成する

この手順は、udp で NFSv3 の下位読み取りマウントを有効にする場合に使用されます。MLP の追加には Solaris 管理コンソールを使用します。

始める前に　大域ゾーンでセキュリティー管理者役割になります。

1. **Solaris 管理コンソールを起動します。**
   詳細は、57 ページの「Solaris 管理コンソールでローカルシステムを管理する」を参照してください。
2. 「ファイル」ツールボックスを選択します。
   ツールボックスのタイトルには、Scope=Files, Policy=TSOL が含まれています。
3. ゾーンと MLP を構成します。
   a. 「トラステッドネットワークゾーン」ツールにナビゲートします。

b. 大域ゾーンをダブルクリックします。

c. **UDP** プロトコルのマルチレベルポートを追加します。

i. 「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。

ii. ポート番号として **2049** と入力し、「了解」をクリックします。

d. 「了解」をクリックして設定を保存します。

4 **Solaris** 管理コンソールを閉じます。

5 カーネルを更新します。

```
# tnctl -fz /etc/security/tsol/tnzonecfg
```

▼ ゾーンにマルチレベルポートを作成する

この手順は、ラベル付きゾーンで実行されるアプリケーションがマルチレベルポート (MLP) とゾーンとの通信を必要としている場合に使用されます。この手順では、Web プロキシがゾーンと通信します。MLP の追加には Solaris 管理コンソールを使用します。

始める前に 大域ゾーンでセキュリティー管理者役割になります。ラベル付きゾーンが存在する必要があります。詳細は、『Solaris Trusted Extensions 構成ガイド』の「ラベル付きゾーンの作成」を参照してください。

1 **Solaris** 管理コンソールを起動します。
詳細は、57 ページの「Solaris 管理コンソールでローカルシステムを管理する」を参照してください。

2 「ファイル」ツールボックスを選択します。
ツールボックスのタイトルには、`Scope=Files, Policy=TSOL` が含まれています。

3 コンピュータのリストに、プロキシホストと **Web** サービスホストを追加します。

a. 「システム構成」で「コンピュータとネットワーク」ツールにナビゲートします。

b. 「コンピュータ」ツールで「アクション」メニューをクリックし、「コンピュータの追加」を選択します。

c. プロキシホストのホスト名と **IP** アドレスを追加します。

d. 変更を保存します。

e. **Web** サービスホストのホスト名と **IP** アドレスを追加します。

f. 変更を保存します。

4 ゾーンと **MLP** を構成します。

a. 「トラステッドネットワークゾーン」ツールにナビゲートします。

b. ラベル付きゾーンを選択します。

c. 「ローカル **IP** アドレスの **MLP** 構成」セクションで、適切なポートとプロトコルフィールドを指定します。

d. 変更を保存します。

5 次の手順に従って、ゾーンのテンプレートをカスタマイズします。

a. 「セキュリティーテンプレート」ツールにナビゲートします。
「アクション」メニューをクリックし、「テンプレートの追加」を選択します。

b. テンプレート名には、ホスト名を使用します。

c. 「ホストタイプ」に「**CIPSO**」を指定します。

d. 「最小ラベル」および「最大ラベル」にはゾーンのラベルを使用します。

e. 「機密ラベルセット」にゾーンラベルを割り当てます。

f. 「明示的に割り当てられたホスト」タブを選択します。

g. 「エントリの追加」セクションで、ゾーンに関連付ける **IP** アドレスを追加します。

h. 変更を保存します。

6 **Solaris** 管理コンソールを閉じます。

7 ゾーンを起動します。

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

8 大域ゾーンで、新しいアドレスの経路を追加します。

たとえば、ゾーンに共有 IP アドレスがある場合は、次のようにします。

```
# route add proxy labeled-zones-IP-address
# route add webservice labeled-zones-IP-address
```

◆ ◆ ◆ 第 11 章

Trusted Extensions でのファイルの管理とマウント (手順)

この章では、Trusted Extensions が設定されたシステムで LOFS マウントおよび NFS マウントがどのように動作するかについて説明します。この章では、ファイルのバックアップと復元方法についても説明します。

Trusted Extensions でのファイルの共有とマウント

Trusted Extensions ソフトウェアでは、Solaris OS と同じファイルシステムとファイルシステム管理コマンドがサポートされています。Trusted Extensions は、非大域ゾーンがファイルを共有するための機能を追加します。さらに、Trusted Extensions は各非大域ゾーンに一意のラベルを追加します。そのゾーンに属するファイルとディレクトリはすべて、そのゾーンのラベルにマウントされます。ほかのゾーンまたは NFS サーバーに属する共有ファイルシステムは、所有者のラベルにマウントされます。Trusted Extensions では、ラベル付けするための必須アクセス制御 (MAC) ポリシーに違反する可能性のあるマウントは禁止されています。たとえば、ゾーンのラベルはマウントされるファイルシステムのラベルより優位でなければならず、読み取り/書き込み権によってマウントできるのはラベルが同等のファイルシステムだけです。

Trusted Extensions の NFS マウント

Trusted Extensions の NFS マウントは Solaris マウントと類似しています。その相違点は、Trusted Extensions にラベル付きゾーンをマウントする場合のゾーンルートパス名の使用と MAC ポリシーの実施によって生じます。

Trusted Extensions の NFS 共有は、大域ゾーンの Solaris 共有と類似しています。ただし、マルチレベルシステムでのラベル付きゾーンからのファイルの共有は Trusted Extensions に特有のものです。

- 大域ゾーンでの共有とマウント – Trusted Extensions システムの大域ゾーンでのファイルの共有とマウントは、Solaris OS での手順とほぼ同じです。ファイルのマウントについては、オートマウンタ、`vfstab` ファイル、`mount` コマンドを使用できます。ファイルの共有については、`dfstab` ファイルが使用されます。
- ラベル付きゾーンでのマウント – Trusted Extensions のラベル付きゾーンでのファイルのマウントは、Solaris OS の非大域ゾーンでのファイルのマウントとほぼ同じです。ファイルのマウントについては、オートマウンタ、`vfstab` ファイル、`mount` コマンドを使用できます。Trusted Extensions では、各ラベル付きゾーンに対して、一意の `automount_home_`*label* 構成ファイルが存在します。
- ラベル付きゾーンでの共有 – ラベル付きゾーンのファイルは、ゾーンのラベルにあるが、大域ゾーンにのみ表示される `dfstab`ファイルを使用することによって、ゾーンのラベルで共有することができます。したがって、ファイルを共有するためにラベル付きゾーンを構成することは、大域ゾーンの大域ゾーン管理者によって実行されます。この構成ファイルは、そのラベル付きゾーンからは表示できません。詳細は、130 ページの「大域ゾーンプロセスとラベル付きゾーン」を参照してください。

どのファイルをマウントできるかには、ラベルが影響します。ファイルは特定のラベルで共有されてマウントされます。Trusted Extensions クライアントが NFS マウントされたファイルに書き込みできるためには、そのファイルが読み取り/書き込み権付きでマウントされ、かつクライアントと同じラベルにある必要があります。2 つの Trusted Extensions ホスト間でファイルをマウントする場合は、サーバーとクライアントに、互換性のある `cipso` というタイプの遠隔ホストテンプレートがなければなりません。Trusted Extensions ホストとラベルなしホストの間でファイルをマウントする場合は、`tnrhdb` ファイルでラベルなしホストに指定されたシングルラベルにあるファイルをマウントすることができます。LOFS でマウントされたファイルは、表示できますが修正することはできません。NFS マウントについては、150 ページの「Trusted Extensions で NFS マウントされたディレクトリへのアクセス」を参照してください。

どのディレクトリおよびファイルを表示できるかにも、ラベルが影響します。デフォルトでは、下位レベルのオブジェクトはユーザーの環境で利用できます。したがって、デフォルト構成の場合、一般ユーザーはそのユーザーの現在のレベルより下位レベルのゾーンにあるファイルを表示することができます。たとえ

ば、ユーザーは上位レベルのラベルから下位レベルのホームディレクトリを表示することができます。詳細は、151 ページの「Trusted Extensions でのホームディレクトリの作成」を参照してください。

サイトのセキュリティーによって下位レベルのオブジェクトの表示が禁止されている場合、管理者はユーザーに対して下位レベルのディレクトリを非表示にすることができます。詳細は、138 ページの「下位ファイルのマウントを無効にする」を参照してください。

Trusted Extensions のマウントポリシーが MAC より優先されることはありません。下位ラベルで表示されるマウント済みファイルは、上位ラベルのプロセスで変更できません。この MAC ポリシーは大域ゾーンでも有効です。大域ゾーン `ADMIN_HIGH` プロセスは、`PUBLIC` ファイルまたは `ADMIN_LOW` ファイルなど、下位ラベルの NFS マウントされたファイルを変更することはできません。MAC ポリシーはデフォルト構成を強制し、一般ユーザーからは不可視です。一般ユーザーは、MAC アクセスできない限りオブジェクトを表示できません。

ラベル付きゾーンのファイルの共有

Solaris OS では、非大域ゾーンはそのゾーンのディレクトリを共有できません。ただし、Trusted Extensions では、ラベル付きゾーンはディレクトリを共有できます。ラベル付きゾーンのどのディレクトリを共有できるかを指定する処理は、ゾーンの `root` パス外にあるディレクトリを使用して、大域ゾーンで実行されます。詳細は、130 ページの「大域ゾーンプロセスとラベル付きゾーン」を参照してください。

`/zone/`*labeled-zone*`/` ディレクトリ
: ゾーンパスとも呼ばれます。大域ゾーンからラベル付きゾーンへのパスです。*labeled-zone* の下にあるすべてのディレクトリには、ゾーンと同じラベルが付けられます。

`/zone/`*labeled-zone*`/root/` *directories*
: ゾーンルートパスとも呼ばれます。大域ゾーンから見た場合は、ラベル付きゾーンの `root` パスです。ラベル付きゾーンから見た場合、これはゾーンのルートで、`/` ディレクトリです。ゾーンを管理する場合、このパスは大域ゾーンでは使用されません。

ラベル付きゾーンのディレクトリを共有する場合、大域ゾーン管理者は、ゾーンパスの `/etc` ディレクトリの `dfstab` ファイルを作成および変更します。

`/zone/`*labeled-zone*`/etc/dfs/dfstab`

この `/etc` ディレクトリは、ラベル付きゾーンから表示されません。このディレクトリは、ゾーンで表示される `/etc` ディレクトリとは異なります。

```
Global zone view: /zone/labeled-zone/root/etc
Labeled zone view of the same directory: /etc
```

このパスの dfstab ファイルでは、ラベル付きディレクトリを共有させることができません。

ラベル付きゾーンの状態が ready または running である場合、/zone/*labeled-zone*/etc/dfs/dfstab ファイルに記載されているファイルはゾーンのラベルで共有されます。手順については、156 ページの「ラベル付きゾーンのディレクトリを共有する」を参照してください。

Trusted Extensions で NFS マウントされたディレクトリへのアクセス

デフォルトでは、NFS マウントされたファイルシステムは、エクスポートされたファイルシステムのラベルで表示可能です。ファイルシステムが読み取り/書き込み権付きでエクスポートされた場合、そのラベルのユーザーはファイルに書き込むことができます。ユーザーの現在のセッションよりも下位のラベルにある NFS マウントは、ユーザーに表示されますが、書き込みはできません。ファイルシステムが読み取り/書き込み権付きで共有されている場合でも、マウントする側のシステムはマウントのラベルでだけそのファイルシステムに書き込むことができます。

NFS マウントされた下位レベルのディレクトリを上位ゾーンのユーザーに表示可能にするには、NFS サーバー上の大域ゾーンの管理者が親ディレクトリをエクスポートする必要があります。親ディレクトリは、そのラベルでエクスポートされます。クライアント側では、各ゾーンに net_mac_aware 特権が必要です。デフォルトでは、ラベル付きゾーンは limitpriv セットに net_mac_aware 特権を含みます。

- サーバー構成 – NFS サーバーでは、dfstab ファイルで親ディレクトリをエクスポートします。親ディレクトリがラベル付きゾーンにある場合、親ディレクトリのラベル付きゾーンで dfstab ファイルを変更する必要があります。ラベル付きゾーンの dfstab ファイルは、大域ゾーンからのみ表示できます。手順については、156 ページの「ラベル付きゾーンのディレクトリを共有する」を参照してください。
- クライアント構成 – 初期ゾーン構成中に使用されるゾーン構成ファイルで、net_mac_aware 特権を指定する必要があります。そのため、下位ホームディレクトリの表示をすべて許可されているユーザーは、最小ゾーンを除く各ゾーンで net_mac_aware 特権を持っている必要があります。例については、158 ページの「ラベル付きゾーンでファイルを NFS マウントする」を参照してください。

例 11–1　下位ホームディレクトリへのアクセスの許可

ホームディレクトリサーバーで、管理者はすべてのラベル付きゾーンで /zone/*labeled-zone*/etc/dfs/dfstab ファイルを作成および変更します。dfstab ファイルは、読み取り/書き込み権付きで /export/home ディレクトリをエクスポートします。したがって、ディレクトリが同じラベルでマウントされると、ホームディレクトリは書き込み可能になります。PUBLIC の /export/home ディレクトリをエクスポートする場合、管理者はホームディレクトリサーバー上に PUBLIC ラベルのワークスペースを作成し、大域ゾーンから /zone/public/etc/dfs/dfstab ファイルを変更します。

クライアントで、大域ゾーンの管理者は、最小ラベルを除く各ラベル付きゾーンに net_mac_aware 特権があることを確認します。この特権によってマウントが許可されます。この特権は、ゾーン構成の際に zonecfg コマンドを使用して指定することができます。下位レベルのホームディレクトリは、表示だけが可能です。ディレクトリ内のファイルは変更できないよう、MAC により保護されています。

Trusted Extensions でのホームディレクトリの作成

Trusted Extensions で、ホームディレクトリは特別な存在です。ユーザーが使用できる各ゾーンに、必ずホームディレクトリが作成されている必要があります。また、ホームディレクトリのマウントポイントは、ユーザーのシステム上のゾーンに作成する必要があります。NFS マウントされたホームディレクトリが正常に動作するためには、通常のディレクトリ位置 /export/home を使用します。Trusted Extensions では、オートマウンタは、各ゾーンつまり各ラベルのホームディレクトリを処理できるように修正されています。詳細は、152 ページの「Trusted Extensions のオートマウンタに対する変更」を参照してください。

ホームディレクトリは、ユーザーの作成時に作成されます。Trusted Extensions では、Solaris 管理コンソール (コンソール) を使用してユーザーを作成するため、ホームディレクトリはコンソールによって作成されます。ただし、ホームディレクトリサーバーの大域ゾーンにあるホームディレクトリは、コンソールによって作成されます。このサーバー上では、ディレクトリは LOFS によりマウントされます。ホームディレクトリは、LOFS マウントとして指定されている場合、オートマウンタによって自動的に作成されます。

注 – コンソールを使用してユーザーを削除すると、大域ゾーンにあるユーザーのホームディレクトリのみが削除されます。ラベル付きゾーンにあるユーザーのホームディレクトリは削除されません。ラベル付きゾーンにあるホームディレクトリのアーカイブと削除についてはユーザー自身が行う必要があります。手順については、104 ページの「Trusted Extensions システムからユーザーアカウントを削除する」を参照してください。

ただし、遠隔 NFS サーバー上のホームディレクトリはオートマウンタで自動的に作成できません。ユーザーがまず NFS サーバーにログインするか、管理者の操作が必要になります。ユーザーのホームディレクトリの作成については、『Solaris Trusted Extensions 構成ガイド』の「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」を参照してください。

Trusted Extensions のオートマウンタに対する変更

Trusted Extensions では、ラベルごとに別個のホームディレクトリマウントが必要です。`automount` コマンドは、これらのラベル付き自動マウントを処理できるように修正されています。各ゾーンでは、オートマウンタ `autofs` が `auto_home_`*zone-name* ファイルをマウントします。たとえば、`auto_home_global` ファイルの大域ゾーンに対するエントリは次のようになります。

```
+auto_home_global
*       -fstype=lofs    :/export/home/&
```

下位レベルのゾーンのマウントを許可するゾーンが起動すると、次のようになります。下位レベルのゾーンのホームディレクトリは、`/zone/<`*zone-name*`>/export/home` 以下に読み取り専用でマウントされます。`auto_home_<`*zone-name*`>` マップにより、`/zone` パスが、`/zone/<` *zone-name*`>/home/<`*username*`>` への `lofs` 再マウントのソースディレクトリとして指定されます。

たとえば、上位レベルのゾーンから生成された `auto_home_`*zone-at-higher-label* マップにおける `auto_home_public` エントリは、次のようになります。

```
+auto_home_public
*       -fstype=lofs    :/zone/public/export/home/&
```

公共ゾーンで対応するエントリは次のとおりです。

```
auto_home_public
*       -fstype=lofs    :/export/home/&
```

ホームディレクトリが参照され、その名前が `auto_home_<`*zone-name*`>` マップのどのエントリにも一致しない場合、マップはこのループバックマウント指定との照合を試行します。次の 2 つの条件が満たされた場合に、ホームディレクトリが作成されます。

1. マップが、一致するループバックマウント指定を検出する
2. ホームディレクトリ名が、*zone-name* にまだホームディレクトリを持たない有効なユーザーに一致する

オートマウンタに対する変更については、automount(1M) のマニュアルページを参照してください。

Trusted Extensions ソフトウェアと NFS のプロトコルバージョン

Solaris 10 11/06 および Solaris 10 8/07 リリースでは、Trusted Extensions は NFS バージョン 4 (NFSv4) の複数ラベルのみを認識します。Solaris 10 5/08 リリース以降、Trusted Extensions ソフトウェアは NFS バージョン 3 (NFSv3) および NFSv4 のラベルを認識します。次のマウントオプションのセットのいずれかを使用できます。

```
vers=4 proto=tcp
vers=3 proto=tcp
vers=3 proto=udp
```

Trusted Extensions には、tcp プロトコルでのマウントに対する制限はありません。NFSv3 および NFSv4 では、tcp プロトコルを同じラベルでのマウントおよび下位読み取りマウントに使用できます。下位読み取りマウントには、マルチレベルポート (MLP) が必要です。

NFSv3 の場合、Trusted Extensions は Solaris OS のように動作します。udp プロトコルは NFSv3 のデフォルトですが、udp は初期マウント操作にしか使用されません。それ以降の NFS 操作では、システムは tcp を使用します。したがって、下位読み取りマウントは、デフォルトの構成の NFSv3 に対して機能します。

まれに初期およびそれ以降の NFS 操作に udp プロトコルを使用するように NFSv3 マウントを制限した場合は、udp プロトコルを使用する NFS 操作に対して MLP を 作成する必要があります。手順については、143 ページの「udp で NFSv3 のマルチレベルポートを構成する」を参照してください。

Trusted Extensions が設定されたホストは、それ自体のファイルシステムをラベルなしホストと共有することもできます。ラベルなしホストにエクスポートされるファイルまたはディレクトリは、そのラベルが、トラステッドネットワークデータベースエントリで遠隔ホストに関連付けられているラベルと同等の場合に、書き込み可能です。ラベルなしホストにエクスポートされるファイルまたはディレクトリは、そのラベルよりも優位のラベルが遠隔ホストに関連付けられている場合にのみ、読み取り可能です。

Trusted Solaris ソフトウェアのリリースを実行しているシステムとの通信は、シングルラベルでのみ可能です。Trusted Extensions システムと Trusted Solaris システムは、ラベルなしホストタイプのテンプレートをほかのシステムに割り当てる必要が

あります。ラベルなしホストタイプには、同じシングルラベルを指定する必要があります。Trusted Solaris サーバーのラベルなし NFS クライアントとして、クライアントのラベルは ADMIN_LOW にはできません。

使用される NFS のプロトコルは、ローカルファイルシステムのタイプに依存しません。その代わり、プロトコルは共有コンピュータのオペレーティングシステムのタイプに依存します。mount コマンドに指定される、または遠隔ファイルシステムの場合に vfstab ファイルで指定される、ファイルシステムのタイプは常に NFS です。

ラベル付きファイルのバックアップ、共有、マウント (作業マップ)

次の作業マップでは、ラベル付きファイルシステムからデータをバックアップおよび復元する場合と、ラベル付けされているディレクトリおよびファイルを共有およびマウントする場合に使用される、一般的なタスクについて説明します。

作業	説明	参照先
ファイルをバックアップします。	バックアップすることによってデータを保護します。	155 ページの「Trusted Extensions でファイルをバックアップする」
データを復元します。	バックアップからデータを復元します。	155 ページの「Trusted Extensions でファイルを復元する」
ラベル付きゾーンのディレクトリの内容を共有します。	ラベル付きディレクトリの内容をユーザー間で共有できるようにします。	156 ページの「ラベル付きゾーンのディレクトリを共有する」
ラベル付きゾーンで共有されたディレクトリの内容をマウントします。	ディレクトリの内容を読み取り/書き込みにのために同じラベルのゾーンにマウントできるようにします。上位レベルのゾーンが共有ディレクトリをマウントする場合、ディレクトリは読み取り専用でマウントされます。	158 ページの「ラベル付きゾーンでファイルを NFS マウントする」
ホームディレクトリのマウントポイントを作成します。	各ラベルで全ユーザー用のマウントポイントを作成します。これによって、ユーザーは NFS ホームディレクトリサーバーではないシステム上のホームディレクトリにアクセスできるようになります。	『Solaris Trusted Extensions 構成ガイド』の「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」
上位のラベルで作業中のユーザーに対して下位レベルの情報を非表示にします。	上位レベルのウィンドウから下位レベルの情報を表示できないようにします。	138 ページの「下位ファイルのマウントを無効にする」

作業	説明	参照先
ファイルシステムのマウントに関する問題をトラブルシューティングします。	ファイルシステムのマウントに関する問題を解決します。	163 ページの「Trusted Extensions でマウントの失敗をトラブルシューティングする」

▼ Trusted Extensions でファイルをバックアップする

1. オペレータ役割になります。
   この役割には、Media Backup 権利プロファイルが含まれます。
2. 次のいずれかのバックアップ方法を使用します。
   - 大規模なバックアップの場合は、`/usr/lib/fs/ufs/ufsdump`
   - 小規模バックアップの場合は、`/usr/sbin/tar cT`
   - これらのいずれかのコマンドを呼び出すスクリプト

     たとえば、Budtool バックアップアプリケーションでは `ufsdump` コマンドを呼び出します。`ufsdump(1M)` のマニュアルページを参照してください。`tar` コマンドの `T` オプションについては、`tar(1)` のマニュアルページを参照してください。

▼ Trusted Extensions でファイルを復元する

1. システム管理者役割になります。
   この役割には、Media Restore 権利プロファイルが含まれます。
2. 次のいずれかの方法を使用します。
   - 大規模な復元の場合は、`/usr/lib/fs/ufs/ufsrestore`
   - 小規模な復元の場合は、`/usr/sbin/tar xT`
   - これらのいずれかのコマンドを呼び出すスクリプト

   `tar` コマンドの `T` オプションについては、`tar(1)` のマニュアルページを参照してください。

注意 – ラベルが維持されるのはこれらのコマンドのみです。

▼ ラベル付きゾーンのディレクトリを共有する

Solaris OS の場合と同様に、Solaris 管理コンソールの「マウントと共有」ツールを使用すると、大域ゾーンのファイルを共有およびマウントできます。ラベル付きゾーンで作成しているディレクトリをマウントまたは共有する場合、このツールは使用できません。ゾーンのラベルで `dfstab` ファイルを作成し、ゾーンを再起動してラベル付きディレクトリを共有します。

注意 – 共有ファイルシステムに、占有的な名前は使用しないでください。共有ファイルシステムの名前は、どのユーザーにも表示されます。

始める前に ファイルサーバー上の大域ゾーンで、スーパーユーザーまたはシステム管理者役割である必要があります。

1. 共有しようとしているディレクトリのラベルで、ワークスペースを作成します。

   詳細は、『Solaris Trusted Extensions ユーザーズガイド』の「特定のラベルのワークスペースを追加する」を参照してください。

2. そのゾーンのラベルで `dfstab` ファイルを作成します。

   ディレクトリを共有するゾーンごとに、次の手順を繰り返します。

   a. そのゾーンに `/etc/dfs` ディレクトリを作成します。

      ```
      # mkdir -p /zone/zone-name/etc/dfs
      ```

   b. トラステッドエディタを開きます。

      詳細は、59 ページの「Trusted Extensions の管理ファイルを編集する」を参照してください。

   c. エディタに `dfstab` ファイルのフルパス名を入力します。

      ```
      # /zone/zone-name/etc/dfs/dfstab
      ```

   d. エントリを追加して、そのゾーンのディレクトリを共有します。

      エントリは、ゾーンルートパスの観点からディレクトリを説明します。たとえば、次のエントリでは、外側のゾーンのラベルでアプリケーションのファイルを共有します。

      ```
      share -F nfs -o ro /viewdir/viewfiles
      ```

3 各ゾーンについて、ゾーンを起動してディレクトリを共有します。

大域ゾーンで、ゾーンごとに次のいずれかのコマンドを実行します。各ゾーンは、これらのどの方法でもディレクトリを共有することができます。実際の共有は、各ゾーンが ready または running 状態になったときに実行されます。

- ゾーンが実行中の状態ではなく、ゾーンのラベルでユーザーがサーバーにログインしないようにする場合は、ゾーンの状態を ready に設定します。

  ```
  # zoneadm -z zone-name ready
  ```

- ゾーンが実行中の状態ではなく、ゾーンのラベルでユーザーがサーバーにログインすることを許可する場合は、ゾーンを起動します。

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

- ゾーンがすでに実行中の場合は、ゾーンを再起動します。

  ```
  # zoneadm -z zone-name reboot
  ```

4 システムから共有されているディレクトリを表示します。

```
# showmount -e
```

5 エクスポートされたファイルをクライアントがマウントできるようにする方法は、158 ページの「ラベル付きゾーンでファイルを NFS マウントする」を参照してください。

例 11–2 PUBLIC ラベルで /export/share ディレクトリを共有する

PUBLIC ラベルで実行されるアプリケーションの場合、システム管理者はユーザーが public ゾーンの /export/share ディレクトリにある文書を読めるようにします。public という名前のゾーンは、PUBLIC ラベルで実行されます。

最初に、管理者は public ワークスペースを作成し、dfstab ファイルを編集します。

```
# mkdir -p /zone/public/etc/dfs
# /usr/dt/bin/trusted_edit /zone/public/etc/dfs/dfstab
```

このファイルに、管理者は次のエントリを追加します。

```
## Sharing PUBLIC user manuals
share -F nfs -o ro /export/appdocs
```

管理者は public ワークスペースから出て、トラステッドパスワークスペースに戻ります。ユーザーはこのシステムへのログインが許可されていないため、管理者はゾーンを実行可能状態にしてファイルを共有します。

```
# zoneadm -z public ready
```

ディレクトリがユーザーのシステムにマウントされると、ユーザーは共有ディレクトリにアクセスできます。

▼ ラベル付きゾーンでファイルを NFS マウントする

Trusted Extensions では、ラベル付きゾーンによってゾーン内のファイルのマウントが管理されます。

ラベルなし、およびラベル付きホストのファイルは、Trusted Extensions のラベル付きホストにマウントすることができます。

- シングルラベルホストからファイルを読み書き可能な状態でマウントするには、リモートホストの割り当てラベルはファイルがマウントされているゾーンと同じである必要があります。
- 上位ゾーンによってマウントされるファイルは読み取り専用です。
- Trusted Extensions では、`auto_home` 構成ファイルはゾーンごとにカスタマイズされます。ファイルにはゾーン名ごとに名前が付けられます。たとえば、大域ゾーンおよび公共ゾーンのあるシステムには、`auto_home_global` と `auto_home_public` の 2 つの `auto_home` ファイルがあります。

Trusted Extensions では、Solaris OS と同じマウントインタフェースが使用されます。

- ブート時にファイルをマウントするには、ラベル付きゾーンで `/etc/vfstab` ファイルを使用します。
- ファイルを動的にマウントするには、ラベル付きゾーンで `mount` コマンドを使用します。
- ホームディレクトリを自動マウントするには、`auto_home_` *zone-name* ファイルを使用します。
- ほかのディレクトリを自動マウントするには、標準の自動マウントマップを使用します。自動マウントマップが LDAP にある場合、LDAP コマンドを使用して管理します。

始める前に クライアントシステム上で、マウントしようとするファイルのラベルのゾーンにいる必要があります。オートマウンタを使用しない限り、スーパーユーザーまたはシステム管理者役割のいずれかである必要があります。下位レベルのサーバーからマウントする場合、ゾーンを `net_mac_aware` 特権で構成してください。

- ラベル付きゾーンでファイルを NFS マウントするには、次の手順に従います。

  ほとんどの手順には、特定ラベルでのワークスペースを作成する方法が含まれています。ワークスペースの作成方法は、『Solaris Trusted Extensions ユーザーズガイド』の「特定のラベルのワークスペースを追加する」を参照してください。

  - ファイルを動的にマウントします。

    ラベル付きゾーンで、mount コマンドを使用します。ファイルを動的にマウントする例については、例 11–3 を参照してください。

  - ゾーンの起動時にファイルをマウントします。

    ラベル付きゾーンで、マウントを vfstab ファイルに追加します。

    ラベル付きゾーンの起動時にファイルをマウントする例については、例 11–4 および例 11–5 を参照してください。

  - LDAP で管理されるシステムに対してホームディレクトリをマウントします。

    a. すべてのラベルで、auto_home_ *zone-name* ファイルにユーザー指定を追加します。

    b. 次に、これらのファイルを使用して、LDAP サーバー上で auto_home_ *zone-name* データベースを生成します。

    例については、例 11–6 を参照してください。

  - ファイルで管理されるシステムに対してホームディレクトリをマウントします。

    a. /export/home/auto_home_*lowest-labeled-zone-name* ファイルを作成し、生成します。

    b. 新しく生成されたファイルをポイントするように、/etc/auto_home_*lowest-labeled-zone-name* ファイルを編集します。

    c. 手順 a で作成したファイルをポイントするように、すべての上位ゾーンで /etc/auto_home_*lowest-labeled-zone-name* ファイルを変更します。

    例については、例 11–7 を参照してください。

例 11–3 mount コマンドを使用してラベル付きゾーンでファイルをマウントする

この例では、システム管理者が public ゾーンから遠隔ファイルシステムをマウントします。Public ゾーンはマルチレベルサーバー上にあります。

システム管理者役割になったあと、管理者は PUBLIC ラベルでワークスペースを作成します。そのワークスペースで、管理者は mount コマンドを実行します。

```
# zonename
public
# mount -F nfs remote-sys:/zone/public/root/opt/docs  /opt/docs
```

PUBLIC ラベルのシングルラベルファイルサーバーには、マウント対象の文書も含まれています。

```
# mount -F nfs public-sys:/publicdocs  /opt/publicdocs
```

remote-sys ファイルサーバーの public ゾーンが ready または running 状態である場合、remote-sys ファイルはこのシステムに正しくマウントされます。public-sys ファイルサーバーが動作している場合、ファイルは正しくマウントされます。

例 11–4 vfstab ファイルを修正してラベル付きゾーンにファイルを読み書き可能な状態でマウントする

この例では、 public ゾーンの起動時に、システム管理者がローカルシステムの public ゾーンに PUBLIC ラベルで 2 つの遠隔ファイルシステムをマウントします。1 つのファイルシステムマウントはマルチレベルシステムからで、もう 1 つのファイルシステムマウントはシングルラベルシステムからです。

システム管理者役割になったあと、管理者は PUBLIC ラベルでワークスペースを作成します。作成したワークスペースで、管理者はそのゾーンの vfstab ファイルを修正します。

```
## Writable books directories at PUBLIC
remote-sys:/zone/public/root/opt/docs  - /opt/docs  nfs  no  yes  rw
public-sys:/publicdocs    - /opt/publicdocs  nfs no yes rw
```

マルチレベルシステムのラベル付き遠隔ゾーンのファイルにアクセスする場合、vfstab エントリが遠隔システムの public ゾーンのゾーンルートパス /zone/public/root をマウント対象のディレクトリへのディレクトリパス名として使用します。シングルラベルシステムへのパスは、Solaris システム上で使用されるパスと同じです。

PUBLIC ラベルの端末ウィンドウで、管理者はファイルをマウントします。

```
# mountall
```

例 11–5 vfstab ファイルを修正してラベル付きゾーンで下位レベルファイルをマウントする

この例では、システム管理者は public ゾーンの遠隔ファイルシステムをローカルシステムの internal ゾーンにマウントします。システム管理者役割になったあと、管理者は INTERNAL ラベルでワークスペースを作成し、次に、そのゾーンで vfstab ファイルを修正します。

```
## Readable books directory at PUBLIC
## ro entry indicates that PUBLIC docs can never be mounted rw in internal zone
remote-sys:/zone/public/root/opt/docs  - /opt/docs  nfs  no  yes  ro
```

ラベル付きの遠隔ゾーンのファイルにアクセスする場合、vfstab エントリが遠隔システムの public ゾーンのゾーンルートパス /zone/public/root をマウント対象のディレクトリへのディレクトリパス名として使用します。

Internal ゾーンのユーザーからは、/opt/docs でファイルにアクセスできます。

INTERNAL ラベルの端末ウィンドウで、管理者はファイルをマウントします。

```
# mountall
```

例 11–6 LDAP を使用して管理されているネットワークでラベル付きホームディレクトリをマウントする

この例で、システム管理者は新規ユーザー ikuk がすべてのラベルで自身のホームディレクトリにアクセスできるようにします。このサイトはホームディレクトリサーバーを 2 つ使用し、LDAP を使用して管理されます。2 つめのサーバーには、ユーザー jdoe および pkai のホームディレクトリが含まれます。新規ユーザーはこのリストに追加されます。

最初に、システム管理者役割になったあと、管理者は大域ゾーンの /etc ディレクトリにある auto_home_*zone-name* ファイルを修正して、2 つめのホームディレクトリサーバー上の新規ユーザーを取り込みます。

```
## auto_home_global file
jdoe   homedir2-server:/export/home/jdoe
pkai   homedir2-server:/export/home/pkai
ikuk   homedir2-server:/export/home/ikuk
*      homedir-server:/export/home/&

## auto_home_internal file
## Mount the home directory from the internal zone of the NFS server
jdoe   homedir2-server:/export/home/jdoe
pkai   homedir2-server:/export/home/pkai
ikuk   homedir2-server:/export/home/ikuk
*      homedir-server:/export/home/&
```

```
## auto_home_public
## Mount the home directory from the public zone of the NFS server
jdoe   homedir2-server:/export/home/jdoe
pkai   homedir2-server:/export/home/pkai
ikuk   homedir2-server:/export/home/ikuk
*      homedir-server:/export/home/&
```

次に、ユーザーがすべてのラベルでログインできるようにするために、管理者はすべてのラベルで auto_home_*zone-name* ファイルに対してこれらの編集を繰り返します。

最後に、このシステム上のすべての auto_home_*zone-name* ファイルを修正したあと、管理者はこれらのファイルを使用して、LDAP データベースにエントリを追加します。

Solaris OS と同様に、 /etc/auto_home_*zone-name* ファイルの +auto_home_public エントリは、オートマウンタに LDAP エントリを使用するよう指示します。ネットワーク上のほかのシステムにある auto_home_ *zone-name* ファイルは、LDAP データベースから更新されます。

例 11–7 ファイルを使用して管理されるシステムで下位レベルのホームディレクトリをマウントする

この例では、システム管理者はユーザーがすべてのラベルで自身のホームディレクトリにアクセスできるようにします。サイトのラベルは PUBLIC、INTERNAL および NEEDTOKNOW です。このサイトはホームディレクトリサーバーを 2 つ使用し、ファイルを使用して管理されます。2 つめのサーバーには、ユーザー jdoe および pkai のホームディレクトリが含まれます。

このタスクを遂行するために、システム管理者は public ゾーンで public ゾーン NFS ホームディレクトリを定義し、この構成を internal ゾーンと needtoknow ゾーンで共有します。

最初に、システム管理者役割になったあと、管理者は PUBLIC ラベルでワークスペースを作成します。このワークスペースで、管理者は新規ファイル /export/home/auto_home_public を作成します。このファイルには、ユーザー別のカスタマイズされた NFS 指定エントリがすべて含まれます。

```
## /export/home/auto_home_public file at PUBLIC label
jdoe   homedir2-server:/export/home/jdoe
pkai   homedir2-server:/export/home/pkai
*      homedir-server:/export/home/&
```

次に、管理者は、この新規ファイルを使用するように /etc/auto_home_public ファイルを修正します。

```
## /etc/auto_home_public file in the public zone
## Use /export/home/auto_home_public for the user entries
## +auto_home_public
+ /export/home/auto_home_public
```

このエントリにより、オートマウンタはローカルファイルの内容を使用するように指示されます。

最後に、管理者は internal ゾーンと needtoknow ゾーンにある /etc/auto_home_public ファイルを同様に修正します。管理者は internal ゾーンと needtoknow ゾーンに表示される public ゾーンへのパス名を使用します。

```
## /etc/auto_home_public file in the internal zone
## Use /zone/public/export/home/auto_home_public for PUBLIC user home dirs
## +auto_home_public
+ /zone/public/export/home/auto_home_public

## /etc/auto_home_public file in the needtoknow zone
## Use /zone/public/export/home/auto_home_public for PUBLIC user home dirs
## +auto_home_public
+ /zone/public/export/home/auto_home_public
```

管理者が新規ユーザー ikuk を追加すると、PUBLIC ラベルで /export/home/auto_home_public ファイルに新規ユーザーの追加が行われます。

```
## /export/home/auto_home_public file at PUBLIC label
jdoe   homedir2-server:/export/home/jdoe
pkai   homedir2-server:/export/home/pkai
ikuk   homedir2-server:/export/home/ikuk
*      homedir-server:/export/home/&
```

上位ゾーンは下位レベルを読み取り、下位の public ゾーンからユーザー別のホームディレクトリを入手します。

▼ Trusted Extensions でマウントの失敗をトラブルシューティングする

始める前に　マウントしようとするファイルのラベルでゾーン内にいる必要があります。スーパーユーザー、またはシステム管理者役割である必要があります。

1 **NFS サーバーのセキュリティー属性を確認します。**

適切な有効範囲で、Solaris 管理コンソールの「セキュリティーテンプレート」ツールを使用します。詳細は、『Solaris Trusted Extensions 構成ガイド』の「Trusted Extensions で Solaris 管理コンソールサーバーを初期化する」を参照してください。

a. **NFS サーバーの IP アドレスが、セキュリティーテンプレートの 1 つで割り当てられたホストであることを確認します。**

このアドレスは、直接割り当てられる場合も、ワイルドカードを使用して間接的に割り当てられる場合もあります。アドレスは、ラベル付きテンプレートのものでも、ラベルなしテンプレートのものでもかまいません。

b. **テンプレートが NFS サーバーに割り当てるラベルを確認します。**

そのラベルは、ファイルをマウントしようとしているラベルと一致している必要があります。

2 **現在のゾーンのラベルを確認します。**

ラベルがマウント済みファイルシステムのラベルよりも上位である場合、遠隔ファイルシステムが読み取り/書き込み権付きでエクスポートされたときでも、マウントに書き込みはできません。マウントのラベルでは、マウント済みファイルシステムにのみ書き込み可能です。

3 **古いバージョンの Trusted Solaris ソフトウェアを実行している NFS サーバーからファイルシステムをマウントするには、次のようにします。**

- **Trusted Solaris 1 NFS サーバーの場合は、**`mount` **コマンドで** `vers=2` **および** `proto=udp` **オプションを使用します。**
- **Trusted Solaris 2.5.1 NFS サーバーの場合は、**`mount` **コマンドで** `vers=2` **および** `proto=udp` **オプションを使用します。**
- **Trusted Solaris 8 NFS サーバーの場合は、**`mount` **コマンドで** `vers=3` **および** `proto=udp` **オプションを使用します。**

これらのサーバーからファイルシステムをマウントするには、サーバーにラベルなしテンプレートを割り当てる必要があります。

◆ ◆ ◆ 第 12 章

トラステッドネットワーク (概要)

この章では、Trusted Extensions のトラステッドネットワークの概念とメカニズムを説明します。

トラステッドネットワーク

Trusted Extensions は、ゾーン、ホスト、およびネットワークにセキュリティー属性を割り当てます。これらの属性により、ネットワークで次のセキュリティー機能が実施されます。

- ネットワーク通信で、データに適切なラベルが付けられます。
- 必須アクセス制御 (MAC) の規則が、ローカルネットワークを通してデータを送受信するとき、およびファイルシステムをマウントするときに実施されます。
- データが遠隔地のネットワークに経路指定されるときに、MAC の規則が実施されます。
- データがゾーンに経路指定されるときに、MAC 規則が実施されます。

Trusted Extensions では、ネットワークパケットは MAC によって保護されます。MAC に関する決定には、ラベルが使用されます。データには、機密度を表すラベルが明示的または暗黙的に付けられます。ラベルには、ID フィールド、格付け (「レベル」) フィールド、およびコンパートメント (「カテゴリ」) フィールドがあります。データは、認可検査に合格する必要があります。この検査は、ラベルが適格な形式であるかどうか、およびラベルが受信側ホストの認可範囲内にあるかどうかを確認します。受信側ホストの認可範囲内にある適格な形式のパケットは、アクセスが許可されます。

信頼されたシステム間で交換される IP パケットには、ラベルが付けられます。Trusted Extensions は Commercial IP Security Option (CIPSO) ラベルをサポートします。パケットの CIPSO ラベルは、IP パケットの分類、分離、および経路指定を行います。経路指定の決定では、データの機密ラベルが宛先のラベルと比較されます。

一般的にトラステッドネットワークでは、ラベルは送信側ホストによって生成され、受信側ホストによって処理されます。ただし、信頼されたルーターは、トラステッドネットワークでパケットを転送するときにラベルを追加したり取り除くことができます。機密ラベルは、転送の前に CIPSO ラベルにマップされます。CIPSO ラベルは IP パケットに埋め込まれます。通常、パケットの送信側と受信側は、同じラベルで操作を行います。

トラステッドネットワークソフトウェアは、サブジェクト (プロセス) とオブジェクト (データ) が別のホストに配置されている場合でも、Trusted Extensions のセキュリティーポリシーが実施されるようにします。Trusted Extensions ネットワークは、分散型アプリケーション全体で MAC を保存します。

Trusted Extensions のデータパケット

Trusted Extensions のデータパケットには、CIPSO ラベルオプションが含まれます。データパケットは、IPv4 または IPv6 ネットワークで送信できます。

標準の IPv4 形式では、オプションを指定した IPv4 ヘッダーのあとに TCP か UDP または SCTP ヘッダーが続き、そのあとに実際のデータが続きます。Trusted Extensions の IPv4 パケットは、セキュリティー属性として IP ヘッダーに CIPSO オプションを使用します。

IPv4 ヘッダーと CIPSO オプション	TCP、UDP、または SCTP　　データ

標準の IPv6 形式では、拡張した IPv6 ヘッダーのあとに TCP か UDP または SCTP ヘッダーが続き、そのあとに実際のデータが続きます。Trusted Extensions の IPv6 パケットでは、ヘッダー拡張にマルチレベルのセキュリティーオプションが含まれます。

IPv6 拡張ヘッダー	TCP、UDP、または SCTP　　データ

トラステッドネットワークの通信

Trusted Extensions は、トラステッドネットワークでラベル付きホストとラベルなしホストをサポートします。LDAP は、完全にサポートされるネームサービスです。さまざまなコマンドと GUI でネットワークを管理できます。

Trusted Extensions ソフトウェアを実行しているシステムは、Trusted Extensions ホストと次のタイプのシステムとのネットワーク通信をサポートします。

- Trusted Extensions を実行している、ほかのシステム
- セキュリティー属性を認識しないが、TCP/IP をサポートするオペレーティングシステムを実行しているシステム (Solaris システム、ほかの UNIX® システム、Microsoft Windows、Macintosh OS システムなどを実行しているシステム)
- CIPSO ラベルを認識するほかのトラステッドオペレーティングシステムを実行しているシステム

Solaris OS の場合と同様に、Trusted Extensions ネットワークの通信とサービスは、ネームサービスによって管理できます。Trusted Extensions は、Solaris のネットワークインタフェースに次のインタフェースを追加します。

- Trusted Extensions は、`tnzonecfg`、`tnrhdb`、および `tnrhtp` の 3 つのネットワーク構成データベースを追加します。詳しくは、168 ページの「Trusted Extensions のネットワーク構成データベース」を参照してください。
- Trusted Extensions のネームサービスのスイッチファイル `nsswitch.conf` には、`tnrhtp` および `tnrhdb` データベースのエントリが含まれます。これらのエントリは、各サイトの構成に応じて修正できます。

  Trusted Extensions は LDAP ネームサービスを使用して、ホスト、ネットワーク、およびユーザーを定義する構成ファイルを集中的に管理します。LDAP ネームサービスに関する、トラステッドネットワークデータベースの `nsswitch.conf` のデフォルトエントリを次に示します。

  ```
  # Trusted Extensions
  tnrhtp: files ldap
  tnrhdb: files ldap
  ```

  Sun Java System Directory Server の LDAP ネームサービスは、Trusted Extensions で完全にサポートされる唯一のネームサービスです。Trusted Extensions が設定されたシステムでの LDAP の使用方法については、第 9 章「Trusted Extensions と LDAP (概要)」を参照してください。
- Trusted Extensions は、Solaris 管理コンソールにツールを追加します。コンソールを使用して、ゾーン、ホスト、およびネットワークを集中的に管理します。ネットワークツールについては、40 ページの「Solaris 管理コンソールツール」を参照してください。

  『Solaris Trusted Extensions 構成ガイド』では、ネットワークを構成するときにゾーンとホストを定義する方法について説明しています。詳細は、第 13 章「Trusted Extensions でのネットワークの管理 (手順)」を参照してください。

- Trusted Extensions は、トラステッドネットワークを管理するためのコマンドを追加します。また、Trusted Extensions は Solaris ネットワークコマンドにオプションを追加します。コマンドの説明については、169 ページの「Trusted Extensions のネットワークコマンド」を参照してください。

Trusted Extensions のネットワーク構成データベース

Trusted Extensions は、カーネルに 3 つのネットワーク構成データベースをロードします。これらのデータベースは、データがホスト間で転送されるときの認可検査に使用されます。

- `tnzonecfg` – このローカルデータベースは、セキュリティーに関連するゾーン属性を格納します。各ゾーンの属性は、ゾーンラベルと、シングルレベルおよびマルチレベルポートへのゾーンのアクセスを指定します。 `ping` などの制御メッセージへの応答は、別の属性が処理します。ゾーンのラベルは、`label_encodings` ファイルで定義します。詳細は、`label_encodings(4)` と `smtnzonecfg(1M)` のマニュアルページを参照してください。マルチレベルポートについては、129 ページの「ゾーンとマルチレベルポート」を参照してください。
- `tnrhtp` – このデータベースは、ホストとゲートウェイのセキュリティー属性を表すテンプレートを格納します。`tnrhtp` は、ローカルデータベースにすることも、LDAP サーバーに保存することもできます。ホストとゲートウェイはトラフィックを送信するときに、宛先ホストと次のホップのゲートウェイの属性を使用して MAC を実施します。トラフィックを受信する場合、ホストとゲートウェイは送信側の属性を使用します。セキュリティー属性については、170 ページの「トラステッドネットワークのセキュリティー属性」を参照してください。詳細は、`smtnrhtp(1M)` のマニュアルページを参照してください。
- `tnrhdb` – このデータベースは、通信が許可されたすべてのホストに対応する IP アドレスとネットワーク接頭辞 (代替機構) を保持します。`tnrhdb` は、ローカルデータベースにすることも、LDAP サーバーに保存することもできます。各ホストまたはネットワーク接頭辞には、`tnrhtp` データベースからセキュリティーテンプレートが割り当てられます。テンプレートの属性は、割り当てられたホストの属性を定義します。詳細は、`smtnrhdb(1M)` のマニュアルページを参照してください。

Trusted Extensions では、Solaris 管理コンソールはこれらのデータベースを処理できるように拡張されています。詳しくは、40 ページの「Solaris 管理コンソールツール」を参照してください。

Trusted Extensions のネットワークコマンド

Trusted Extensions は、トラステッドネットワークを管理するために、次のコマンドを追加します。

- `tnchkdb` – このコマンドは、トラステッドネットワークデータベースの正しさを確認するために使用します。`tnchkdb` コマンドは、セキュリティーテンプレート (`tnrhtp`)、セキュリティーテンプレートの割り当て (`tnrhdb`)、またはゾーンの構成 (`tnzonecfg`) を変更するごとに使用されます。Solaris 管理コンソールツールは、データベースが修正されたときに、このコマンドを自動的に実行します。詳しくは、`tnchkdb(1M)` のマニュアルページを参照してください。
- `tnctl` – このコマンドは、カーネルのトラステッドネットワーク情報を更新するために使用できます。また、`tnctl` はシステムサービスです。`svcadm restart /network/tnctl` コマンドによる再起動は、ローカルシステムのトラステッドネットワークデータベースからカーネルキャッシュを更新します。Solaris 管理コンソールツールは、データベースがファイルの有効範囲で修正されたときに、このコマンドを自動的に実行します。詳しくは、`tnctl(1M)` のマニュアルページを参照してください。
- `tnd` – このデーモンは、LDAP ディレクトリから `tnrhdb` および `tnrhtp` 情報を取得します。`tnd` は、`svcadm start /network/tnd` のように、ブート時にサービスとして起動されます。このコマンドは、デバッグやポーリング間隔の変更にも使用できます。詳しくは、`tnd(1M)` のマニュアルページを参照してください。
- `tninfo` – このコマンドは、トラステッドネットワークカーネルキャッシュの現在の状態を詳細に表示します。出力は、ホスト名、ゾーン、およびセキュリティーテンプレートを使用してフィルタ処理できます。詳しくは、`tninfo(1M)` のマニュアルページを参照してください。

Trusted Extensions は、次の Solaris ネットワークコマンドにオプションを追加します。

- `ifconfig` – このコマンドの `all-zones` インタフェースフラグは、特定のインタフェースをシステムのすべてのゾーンで利用できるようにします。データを配信する適切なゾーンは、データに関連付けられたラベルによって決定されます。詳しくは、`ifconfig(1M)` のマニュアルページを参照してください。
- `netstat` – `-R` オプションは、マルチレベルソケットのセキュリティー属性や経路指定テーブルエントリなどの Trusted Extensions 固有の情報を表示するために、Solaris の `netstat` の使用法を拡張します。拡張されたセキュリティー属性には、接続先のラベルや、ソケットがゾーンに固有か複数ゾーンで利用できるかの区別などがあります。詳しくは、`netstat(1M)` のマニュアルページを参照してください。
- `route` – `-secattr` オプションは Solaris の `route` を拡張し、経路のセキュリティー属性を表示します。オプションの値は、次の形式で指定します。

  `min_sl=`*label*`,max_sl=`*label*`,doi=`*integer*`,cipso`

cipso キーワードは省略可能で、デフォルトで設定されます。詳しくは、route(1M) のマニュアルページを参照してください。

- snoop – Solaris OS と同様、このコマンドに -v オプションを指定すると、IP ヘッダーを詳細に表示できます。Trusted Extensions では、ヘッダーにラベル情報が含まれます。

トラステッドネットワークのセキュリティー属性

Trusted Extensions のネットワーク管理は、セキュリティーテンプレートに基づきます。セキュリティーテンプレートは、共通のプロトコルおよび同じセキュリティー属性を持つ一連のホストを記述します。

セキュリティー属性はテンプレートにより、システム (ホストとルーターの両方) に管理の目的で割り当てられます。セキュリティー管理者はテンプレートを管理し、これらをシステムに割り当てます。システムにテンプレートが割り当てられていない場合、このシステムとの通信は許可されません。

すべてのテンプレートには名前が付けられ、次の情報が含まれます。

- 「ラベルなし」または「CIPSO」のいずれかの「ホストタイプ」。ネットワーク通信に使用されるプロトコルは、テンプレートのホストタイプによって決定されます。

  ホストタイプは、CIPSO オプションを使用するかどうかを決定し、MAC に影響します。172 ページの「セキュリティーテンプレートのホストタイプとテンプレート名」を参照してください。
- 各ホストタイプに適用される一連のセキュリティー属性。

ホストタイプとセキュリティー属性の詳細は、170 ページの「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。

Trusted Extensions のネットワークセキュリティー属性

Trusted Extensions には、セキュリティーテンプレートのデフォルトのセットがインストールされています。ホストにテンプレートを割り当てると、テンプレートのセキュリティー値がホストに適用されます。Trusted Extensions では、ネットワーク上のラベルなしホストとラベル付きホストの両方に、テンプレートによってセキュリティー属性が割り当てられます。セキュリティーテンプレートが割り当てられていないホストとは通信できません。テンプレートは、ローカルに保存したり、Sun Java System Directory Server の LDAP ネームサービスに保存することができます。

テンプレートはホストに直接または間接的に割り当てることができます。直接割り当てでは、テンプレートを特定の IP アドレスに割り当てます。間接割り当てでは、ホストを含むネットワークアドレスにテンプレートを割り当てます。セキュリ

ティーテンプレートがないホストは、Trusted Extensions が設定されたホストと通信できません。直接割り当てと間接割り当てについては、174 ページの「トラステッドネットワーク代替機構」を参照してください。

テンプレートは、Solaris 管理コンソールの「セキュリティーテンプレート」ツールを使用して修正または作成することができます。「セキュリティーテンプレート」ツールは、テンプレートの必要なフィールドへの入力を実施します。どのフィールドが必要かは、ホストタイプに基づきます。

各ホストタイプには、必須および任意のセキュリティー属性の独自セットがあります。セキュリティーテンプレートで、次のセキュリティー属性を指定します。

- ホストタイプ – パケットに CIPSO セキュリティーラベルを付けるか、ラベルを付けないかを定義します。
- デフォルトラベル – ラベルなしホストの信頼レベルを定義します。ラベルなしホストから送信されたパケットは、受信側の Trusted Extensions ホストまたはゲートウェイにより、このラベルで読み取られます。

  「デフォルトラベル」属性は、ラベルなしホストタイプに固有です。詳細は、`smtnrhtp(1M)` のマニュアルページと、次の節を参照してください。
- **DOI** – 解釈のドメインを識別するゼロ以外の正の整数です。DOI は、ネットワーク通信またはネットワークエンティティーに適用するラベルエンコーディングのセットを識別するために使用されます。DOI が異なるラベル同士は、その他の設定が同じでも無関係です。ラベルなしホストでは、DOI はデフォルトラベルに適用されます。Trusted Extensions では、デフォルト値は 1 です。
- 最小ラベル – ラベル認可範囲の下限を定義します。ホストおよび次のホップのゲートウェイは、テンプレートで指定された最小ラベルより下位レベルのパケットを受信しません。
- 最大ラベル – ラベル認可範囲の上限を定義します。ホストおよび次のホップのゲートウェイは、テンプレートで指定された最大ラベルを超えるパケットを受信しません。
- セキュリティーラベルセット – 省略可能です。セキュリティーテンプレート用のセキュリティーラベルの不連続なセットを指定します。セキュリティーラベルセットが指定されたテンプレートに割り当てられたホストは、最大ラベルと最小ラベルで決定される認可範囲に加え、ラベルセット内のいずれかのラベルに一致するパケットも送受信できます。指定できる最大のラベル数は 4 です。

セキュリティーテンプレートのホストタイプとテンプレート名

Trusted Extensions は、トラステッドネットワークデータベースで 2 種類のホストタイプをサポートし、2 つのデフォルトテンプレートを提供します。

- **CIPSO** ホストタイプ – トラステッドオペレーティングシステムを実行するホストに使用します。Trusted Extensions は、このホストタイプに対して `cipso` という名前のテンプレートを提供します。

  Common IP Security Option (CIPSO) プロトコルは、IP オプションフィールドで渡すセキュリティーラベルを指定するために使用されます。CIPSO ラベルは、データのラベルから自動的に派生します。CIPSO セキュリティーラベルの受け渡しには、タグタイプ 1 が使用されます。続いてこのラベルは、IP レベルでセキュリティー検査を行い、ネットワークパケットのデータにラベルを付けるために使用されます。
- ラベルなしホストタイプ - 標準ネットワークプロトコルを使用し、CIPSO オプションをサポートしないホストに使用します。Trusted Extensions は、このホストタイプに対して `admin_low` という名前のテンプレートを提供します。

  このホストタイプは、Solaris OS またはほかのラベルなしオペレーティングシステムを実行するホストに割り当てられます。このホストタイプは、ラベルなしホストとの通信に適用するデフォルトラベルとデフォルト認可上限を提供します。また、ラベル範囲または一連の不連続ラベルを指定して、ラベルなしゲートウェイへの転送用パケットの送信を許可できます。

注意 – `admin_low` テンプレートは、ラベルなしテンプレートをサイト固有のラベルで構築する例を提供します。Trusted Extensions のインストールには `admin_low` テンプレートが必要ですが、通常のシステム操作に対してセキュリティー設定が適切でない場合があります。システム保守やサポート上の理由により、提供されているテンプレートは変更を加えずそのまま保持してください。

セキュリティーテンプレートのデフォルトラベル

ラベルなしホストタイプのテンプレートでは、デフォルトラベルが指定されます。このラベルは、Solaris システムなど、ラベルを認識しないオペレーティングシステムを実行しているホストとの通信を制御するために使用します。割り当てられるデフォルトラベルは、ホストとそのユーザーに適切な信頼レベルを反映します。

ラベルなしホストとの通信は原則的にデフォルトラベルのみに限定されるため、これらのホストは「シングルラベルのホスト」とも呼ばれます。

セキュリティーテンプレートの解釈のドメイン

同じ DOI (解釈のドメイン) を使用する組織は、ラベル情報やその他のセキュリティー属性を同じ方法で解釈します。Trusted Extensions がラベルの比較を行う場合、DOI が同じであるかどうかが確認されます。

Trusted Extensions システムでは、1 つの DOI 値に対してラベルポリシーを適用します。Trusted Extensions システムのすべてのゾーンは、同じ DOI で動作する必要があります。Trusted Extensions システムでは、異なる DOI を使用するシステムから受信されるパケットに対する例外処理を用意していません。

サイトでデフォルト値と異なる DOI 値を使用する場合は、その値を `/etc/system` ファイルに追加し、各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。初期手順については、『Solaris Trusted Extensions 構成ガイド』の「解釈ドメインの構成」を参照してください。各セキュリティーテンプレートで DOI を設定する場合は、例 13–1 を参照してください。

セキュリティーテンプレートのラベル範囲

「最小ラベル」および「最大ラベル」属性は、ラベル付きホストおよびラベルなしホストのラベル範囲を決定するために使用されます。これらの属性は、次の処理に使用されます。

- 遠隔 CIPSO ホストと通信するときに使用できるラベル範囲を設定する

  パケットを宛先ホストに送信するには、パケットのラベルが、宛先ホストのセキュリティーテンプレートでホストに割り当てられたラベル範囲内にある必要があります。
- CIPSO ゲートウェイまたはラベルなしゲートウェイを通して転送されるパケットのラベル範囲を設定する

  ラベルなしホストタイプのラベル範囲はテンプレートで指定できます。ラベル範囲を使用すると、ホストは、指定のラベル範囲内にあるパケットであれば、ホストのラベルにあるものではなくても転送できます。

セキュリティーテンプレートのセキュリティーラベルセット

セキュリティーラベルセットは、遠隔ホストでパケットを受信、転送、または送信できる不連続なラベルを、最大で 4 つ定義します。この属性は省略可能です。デフォルトでは、セキュリティーラベルセットは定義されていません。

トラステッドネットワーク代替機構

tnrhdb データベースは、セキュリティーテンプレートを特定のホストに直接または間接的に割り当てることができます。直接割り当てでは、テンプレートをホストの IP アドレスに割り当てます。間接割り当ては、代替機構で処理されます。トラステッドネットワークソフトウェアは、ホストの IP アドレスをテンプレートに割り当てる固有のエントリを最初に検索します。ホストに固有のエントリが見つからない場合、ソフトウェアは「最長接頭辞一致」で検索します。ホストの IP アドレスが、接頭辞を固定長にした IP アドレスの「最長接頭辞一致」を満たす場合は、ホストをセキュリティーテンプレートに間接的に割り当てることができます。

IPv4 では、サブネットを利用して間接割り当てが可能です。4、3、2、または 1 個の後続ゼロ (0) オクテットを使用して間接割り当てを行う場合、ソフトウェアは接頭辞の長さをそれぞれ 0、8、16、または 24 に計算します。表 12–1 のエントリ 3 – 6 は、この代替機構を示します。

スラッシュと固定ビット数を追加して、接頭辞の長さを設定することもできます。IPv4 ネットワークアドレスの接頭辞長は、1 - 32 です。IPv6 ネットワークアドレスの接頭辞長は、1 - 128 です。

次の表に、代替アドレスとホストアドレスの例を示します。代替アドレスセットに含まれるアドレスが直接割り当てられる場合、そのアドレスに対して代替機構は使用されません。

表 12–1 tnrhdb ホストアドレスと代替機構のエントリ

IP バージョン	tnrhdb エントリ	含まれるアドレス
IPv4	192.168.118.57:cipso	192.168.118.57
	192.168.118.57/32:cipso	/32 は、接頭辞長が 32 ビットであることを示します。
	192.168.118.128/26:cipso	192.168.118.0 潤ォ 192.168.118.63
	192.168.118.0:cipso 192.168.118.0/24:cipso	192.168.118. ネットワーク上のすべてのアドレス。
	192.168.0.0/24:cipso	192.168.0. ネットワーク上のすべてのアドレス。
	192.168.0.0:cipso 192.168.0.0/16:cipso	192.168. ネットワーク上のすべてのアドレス。
	192.0.0.0:cipso 192.0.0.0/8:cipso	192. ネットワーク上のすべてのアドレス。
	192.168.0.0/32:cipso	ネットワークアドレス 192.168.0.0。ワイルドカードアドレスではありません。
	192.168.118.0/32:cipso	ネットワークアドレス 192.168.118.0。ワイルドカードアドレスではありません。
	192.0.0.0/32:cipso	ネットワークアドレス 192.0.0.0。ワイルドカードアドレスではありません。
	0.0.0.0/32:cipso	ホストアドレス 0.0.0.0。ワイルドカードアドレスではありません。
	0.0.0.0:cipso	全ネットワーク上の全アドレス。
IPv6	2001\:DB8\:22\:5000\:\:21f7:cipso	2001:DB8:22:5000::21f7
	2001\:DB8\:22\:5000\:\:0/52:cipso	2001:DB8:22:5000::0 潤ォ 2001:DB8:22:5fff:ffff:ffff:ffff:ffff
	0\:\:0/0:cipso	全ネットワーク上の全アドレス。

アドレス 0.0.0.0/32 は、アドレス 0.0.0.0 に一致することに注意してください。tnrhdb エントリ 0.0.0.0/32:admin_low は、リテラルアドレス 0.0.0.0 が発信元 IP アドレスとして使用されているシステムで便利です。たとえば、DHCP クライアントは、DHCP サーバーがクライアントに IP アドレスを割り当てるまでは、DHCP サーバーに 0.0.0.0 として接続します。

DHCP クライアントにサービスを提供する Sun Ray サーバー上で tnrhdb エントリを作成する方法については、例 13–13 を参照してください。0.0.0.0:admin_low はデフォルトのワイルドカードエントリであるため、このデフォルトを削除または変更する前に、195 ページの「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」の留意事項を参照してください。

IPv4 および IPv6 アドレスの接頭辞長については、『System Administration Guide: IP Services』の「Designing Your CIDR IPv4 Addressing Scheme」と『System Administration Guide: IP Services』の「IPv6 Addressing Overview」を参照してください。

Trusted Extensions の経路指定の概要

Trusted Extensions では、異なるネットワーク上にあるホスト間の送信経路は、伝送の各ステップでセキュリティーを維持する必要があります。Trusted Extensions は、Solaris OS の経路制御プロトコルに拡張セキュリティー属性を追加します。Solaris OS と異なり、この Trusted Extensions のリリースは動的な経路指定をサポートしません。静的な経路指定の詳細は、route(1M) のマニュアルページの -p オプションを参照してください。

ゲートウェイとルーターはパケットを経路指定します。この説明では、「ゲートウェイ」と「ルーター」の 2 つの用語を同じ意味で使用しています。

同じサブネット上のホスト間の通信では、ルーターが必要ないため、認可検査は終端のみで実行されます。ラベル範囲検査は発信元で実行されます。受信側ホストが Trusted Extensions ソフトウェアを実行している場合は、宛先でもラベル範囲検査が実行されます。

発信元ホストと宛先ホストが別のサブネット上にある場合、パケットは発信元ホストからゲートウェイに送信されます。経路を選択するときに、宛先のラベル範囲と 1 ホップ目のゲートウェイのラベル範囲が発信元で検査されます。ゲートウェイは、宛先ホストが接続されたネットワークにパケットを転送します。宛先に届くまでに、パケットが複数のゲートウェイを通過する場合もあります。

経路指定に関する背景

Trusted Extensions ゲートウェイでは、特定の場合にラベル範囲検査が実行されます。Trusted Extensions システムが 2 つのラベルなしホスト間でパケットを経路指定している場合、発信元ホストのデフォルトラベルと宛先ホストのデフォルトラベルが比較されます。ラベルなしホストがデフォルトラベルを共有している場合は、パケットが経路指定されます。

各ゲートウェイは、すべての宛先への経路をリストで維持します。標準の Solaris の経路指定では、最適となる経路が選択されます。Trusted Extensions は、経路の選択に適用されるセキュリティー要件を検査するための追加ソフトウェアを提供します。セキュリティー要件を満たさない Solaris の選択はスキップされます。

Trusted Extensions の経路指定テーブルエントリ

Trusted Extensions の経路指定テーブルのエントリには、セキュリティー属性を組み込むことができます。セキュリティー属性には、`cipso` キーワードを含めることができます。セキュリティー属性には、最大ラベル、最小ラベル、および DOI を含める必要があります。

セキュリティー属性を指定しないエントリには、ゲートウェイのセキュリティーテンプレートの属性が使用されます。

Trusted Extensions の認可検査

Trusted Extensions ソフトウェアは、セキュリティーの見地から、送信経路の適切さを判定します。ソフトウェアは「認可検査」と呼ばれる一連のテストを、発信元ホスト、宛先ホスト、および中間ゲートウェイで実行します。

注 – 次の説明では、ラベル範囲の認可検査はセキュリティーラベルセットの検査も意味します。

認可検査では、ラベル範囲と CIPSO ラベル情報が確認されます。経路のセキュリティー属性は、経路指定テーブルのエントリから取得されるか、エントリにセキュリティー属性がない場合はゲートウェイのセキュリティーテンプレートから取得されます。

通信の着信時には、Trusted Extensions ソフトウェアは可能であればパケット自体からラベルを取得します。パケットからのラベルの取得は、ラベルをサポートするシステムからメッセージが送信されている場合にのみ可能です。パケットからラベルを取得できない場合は、トラステッドネットワークデータベースファイルからデフォルトラベルがメッセージに割り当てられます。これらのラベルは認可検査時にも使用されます。Trusted Extensions は、発信メッセージ、転送メッセージ、および着信メッセージに対して複数の検査を実施します。

発信元の認可検査

送信側プロセスまたは送信側ゾーンで、次の認可検査が実行されます。

- すべての宛先について、データのラベルが、送信経路の次のホップ (最初のホップ) のラベル範囲内にある必要があります。また、ラベルは 1 ホップ目のゲートウェイのセキュリティー属性に含まれる必要があります。
- すべての宛先について、発信パケットの DOI が宛先ホストの DOI に一致している必要があります。DOI は、1 ホップ目のゲートウェイを含め、経路に沿ったすべてのホップの DOI にも一致する必要があります。

- 宛先ホストがラベルなしホストの場合、次のいずれかの条件を満たす必要があります。
  - 送信側ホストのラベルが、宛先ホストのデフォルトラベルに一致する必要がある。
  - 送信側ホストにラベル間通信を行う権限が与えられ、送信側のラベルが宛先のデフォルトラベルよりも優位である。
  - 送信側ホストにラベル間通信を行う権限が与えられ、送信側のラベルが `ADMIN_LOW` である。つまり、送信側が大域ゾーンから送信を行っている。

注 – 最初のホップ検査は、メッセージが任意のネットワーク上のホストからゲートウェイを経由して別のネットワーク上のホストに送信されているときに行われます。

ゲートウェイの認可検査

Trusted Extensions ゲートウェイシステムでは、次のホップのゲートウェイに対して認可検査が実行されます。

- 着信パケットにラベルがない場合、パケットは `tnrhdb` エントリから発信元ホストのデフォルトラベルを継承します。それ以外の場合、パケットは指定された CIPSO ラベルを受け取ります。
- パケット転送の検査は、発信元の認可と同様に処理されます。
  - すべての宛先について、データのラベルは次のホップのラベル範囲内にある必要があります。また、ラベルは次のホップのホストのセキュリティー属性に含まれる必要があります。
  - すべての宛先について、発信パケットの DOI が宛先ホストの DOI に一致している必要があります。DOI は、次のホップのホストの DOI にも一致する必要があります。
  - ラベルなしパケットのラベルは、宛先ホストのデフォルトラベルに一致する必要があります。
  - CIPSO パケットのラベルは、宛先ホストのラベル範囲内にある必要があります。

宛先の認可検査

Trusted Extensions ホストがデータを受信するときに、ソフトウェアは次の検査を実行します。

- 着信パケットにラベルがない場合、パケットは `tnrhdb` エントリから発信元ホストのデフォルトラベルを継承します。それ以外の場合、パケットは指定された CIPSO ラベルを受け取ります。
- パケットのラベルと DOI は、宛先ゾーンまたは宛先プロセスのラベルおよび DOI と一致する必要があります。プロセスがマルチレベルポートで待機している場合は例外です。プロセスにラベル間通信が許可され、プロセスが大域ゾーンで実行されているか、パケットのラベルよりも優位なラベルを持つ場合、待機中のプロセスはパケットを受信できます。

Trusted Extensions での経路指定の管理

Trusted Extensions は、ネットワーク間通信の経路指定を、複数の方法でサポートしています。セキュリティー管理者役割は、サイトのセキュリティーポリシーで要求されるセキュリティーレベルを実施できる経路を設定できます。

たとえば、サイトではローカルネットワークの外部の通信をシングルラベルに制限できます。このラベルは、公開情報に適用します。`UNCLASSIFIED` や `PUBLIC` などのラベルで公開情報を表すことができます。制限を実施するために、これらのサイトはシングルラベルテンプレートを外部ネットワークに接続されたネットワークインタフェースに割り当てます。TCP/IP と経路指定の詳細は、次のマニュアルを参照してください。

- 『System Administration Guide: IP Services』の「Planning for Routers on Your Network」
- 『System Administration Guide: IP Services』の「Configuring Systems on the Local Network」
- 『System Administration Guide: IP Services』の「Major TCP/IP Administrative Tasks (Task Map)」
- 『Solaris のシステム管理 (IP サービス)』の「DHCP サービスを使用するためのネットワークの準備 (作業マップ)」

Trusted Extensions でのルーターの選択

Trusted Extensions ホストは、信頼度のもっとも高いルーターとして動作します。ほかの種類のルーターは、Trusted Extensions のセキュリティー属性を認識するとは限りません。管理アクションを行わないと、MAC セキュリティー保護を提供しないルーターを経由してパケットが送信される可能性があります。

- CIPSO ルーターは、パケットの IP オプションセクションに正しい種類の情報が見つからなかった場合、パケットを破棄します。たとえば、CIPSO ルーターは、必要な CIPSO オプションが IP オプションに見つからない場合、または IP オプションの DOI が宛先の認可と一致しない場合に、パケットを破棄します。
- Trusted Extensions ソフトウェアを実行していないほかの種類のルーターを構成して、CIPSO オプションを含むパケットを通過させたり破棄させたりできます。Trusted Extensions などが提供する CIPSO を認識するゲートウェイのみが、CIPSO IP オプションの内容を使用して、MAC を実施することができます。

トラステッド経路指定をサポートするために、Trusted Extensions セキュリティー属性を含むように Solaris 10 経路指定テーブルが拡張されます。属性については、177 ページの「Trusted Extensions の経路指定テーブルエントリ」を参照してください。Trusted Extensions では、経路指定テーブルのエントリを管理者が手動で作成する、静的経路指定がサポートされます。詳しくは、`route(1M)` のマニュアルページの `-p` オプションを参照してください。

経路指定ソフトウェアは、経路指定テーブルで宛先ホストへの送信経路を探します。ホストが明示的に定義されていない場合、経路指定ソフトウェアは、ホストが配置されているサブネットワークのエントリを探します。ホストと、ホストが配置されているネットワークのどちらも定義されていない場合、デフォルトゲートウェイが定義されていれば、ホストはデフォルトゲートウェイにパケットを送信します。複数のデフォルトゲートウェイを定義可能で、それぞれが同等に扱われます。

このリリースの Trusted Extensions では、セキュリティー管理者は経路を手動で設定し、条件が変更されたときに手動で経路指定テーブルを変更します。たとえば、多くのサイトは外部との通信を単一のゲートウェイで行なっています。この場合、ネットワーク上の各ホストで、単一のゲートウェイを「デフォルト」として静的に定義することができます。動的な経路指定のサポートは、Trusted Extensions の今後のリリースで利用できるようになる可能性があります。

Trusted Extensions のゲートウェイ

Trusted Extensions の経路指定の例は次のとおりです。図と表では、ホスト 1 とホスト 2 の間で可能な 3 つの送信経路を示しています。

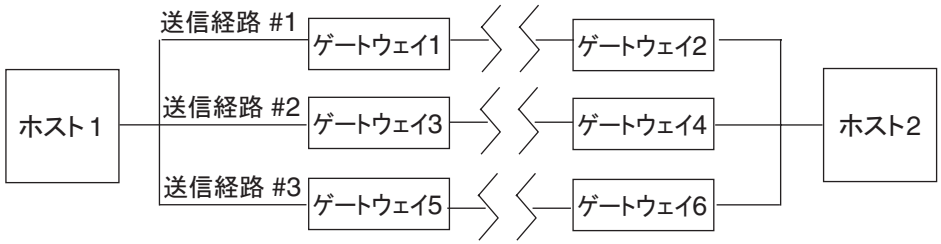


図 12–1　一般的な Trusted Extensions 経路と経路指定テーブルのエントリ

経路	最初のホップのゲートウェイ	最小ラベル	最大ラベル	DOI
#1	ゲートウェイ 1	CONFIDENTIAL	SECRET	1
#2	ゲートウェイ 3	ADMIN_LOW	ADMIN_HIGH	1
#3	ゲートウェイ 5			

- 送信経路 #1 は、CONFIDENTIAL から SECRET のラベル範囲のパケットを伝送できます。
- 送信経路 #2 は、ADMIN_LOW から ADMIN_HIGH の範囲のパケットを伝送できます。
- 送信経路 #3 には、経路指定情報が指定されていません。したがって、セキュリティー属性は tnrhtp データベースにあるゲートウェイ 5 のテンプレートから取得されます。

Trusted Extensions の経路指定コマンド

ラベルやソケットの拡張されたセキュリティー属性を表示するために、Trusted Extensions では次の Solaris のネットワークコマンドが修正されています。

- netstat -rR コマンドは、経路指定テーブルのエントリにあるセキュリティー属性を表示します。
- netstat -aR コマンドは、ソケットのセキュリティー属性を表示します。
- route -p コマンドに add または delete オプションを指定すると、経路指定テーブルエントリが変更されます。

詳しくは、netstat(1M) と route(1M) のマニュアルページを参照してください。

例については、199 ページの「セキュリティー属性を使用して経路を構成する」を参照してください。

◆ ◆ ◆ 第 13 章

Trusted Extensions でのネットワークの管理 (手順)

この章では、Solaris Trusted Extensions ネットワークを保護するための実装の詳細と手順について説明します。

- 183 ページの「トラステッドネットワークの管理 (作業マップ)」
- 184 ページの「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)」
- 199 ページの「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)」
- 206 ページの「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)」

トラステッドネットワークの管理 (作業マップ)

一般的なトラステッドネットワーキング手順の作業マップは、次の表のとおりです。

作業	説明	参照先
ネットワークデータベースを構成します。	遠隔ホストテンプレートを作成し、ホストをテンプレートに割り当てます。	184 ページの「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)」
経路指定の構成と、ネットワークデータベースおよびカーネルのネットワーク情報をチェックします。	ラベル付きまたはラベルなしゲートウェイ経由で、ラベル付きパケットを宛先に到達させる、静的送信経路を構成します。 ネットワークの状態も表示します。	199 ページの「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)」
ネットワークの問題をトラブルシューティングします。	ラベル付きパケットに関連したネットワークの問題を診断するときの手順です。	206 ページの「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)」

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)

Trusted Extensions ソフトウェアには、tnrhtp および tnrhdb データベースが含まれています。これらのデータベースが、システムに接続する遠隔ホストにラベルを提供します。Solaris 管理コンソールには、これらのデータベースの管理に使用する GUI が用意されています。

作業	説明	参照先
カスタマイズしたセキュリティーテンプレートがサイトに必要かどうかを判断します。	サイトのセキュリティー要件に照らし合わせて、既存のテンプレートを評価します。	185 ページの「サイト固有のセキュリティーテンプレートが必要かどうかを判断する」
Solaris 管理コンソールの「セキュリティーテンプレート」ツールへのアクセス	トラステッドネットワークデータベースを修正するツールにアクセスします。	186 ページの「トラステッドネットワーキングのツールを開く」
セキュリティーテンプレートを修正します。	トラステッドネットワークデータベースを修正して、トラステッドネットワークのセキュリティー属性の定義を修正します。	187 ページの「遠隔ホストテンプレートを構築する」
	DOI を 1 以外の値に変更します。	例 13–1
	ほかのホストとの間の通信をシングルラベルに制限するラベル付きホスト用のセキュリティーテンプレートを作成します。	例 13–2
	シングルラベルゲートウェイとして動作するラベルなしホスト用のセキュリティーテンプレートを作成します。	例 13–3
	ラベル範囲が制限されているホスト用のセキュリティーテンプレートを作成します。	例 13–4
	ラベル範囲内で個別一連のラベルを指定するホスト用のセキュリティーテンプレートを作成します。	例 13–5
	ラベルなしのシステムとネットワーク用のセキュリティーテンプレートを作成します。	例 13–6
	2 つの開発者システム用のセキュリティーテンプレートを作成します。	例 13–7

作業	説明	参照先
既知のネットワークへホストを追加します。	システムとネットワークをトラステッドネットワークに追加します。	192 ページの「システムの既知のネットワークにホストを追加する」
ワイルドカードエントリによる遠隔ホストアクセスを提供します。	各ホストを同じセキュリティーテンプレートに間接的に割り当てることによって、IP アドレスの一定範囲内にあるホストがシステムと通信することを許可します。	例 13–8 例 13–9 例 13–10
tnrhdb ファイルで admin_low ワイルドカードエントリを変更します。	ワイルドカードエントリを、起動時に接続するホストの特定アドレスに置き換えることによって、セキュリティーを引き上げます。	195 ページの「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」
	ワイルドカードエントリを、デフォルトとしてラベル付きホストのネットワークで置き換えることによって、セキュリティーを引き上げます。	例 13–11
ホストアドレス 0.0.0.0 のエントリを作成します。	遠隔クライアントからの初期接続を受け入れるように Sun Ray サーバーを構成します。	例 13–13
セキュリティーテンプレートを割り当てます。	テンプレートに IP アドレス、または連続する IP アドレスのリストを関連付けます。	193 ページの「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」

▼ サイト固有のセキュリティーテンプレートが必要かどうかを判断する

始める前に　大域ゾーンでセキュリティー管理者役割になります。

1 **Trusted Extensions のテンプレートを十分に理解します。**

ローカルホストにある tnrhtp ファイルをお読みください。ファイル内のコメントが役に立ちます。セキュリティー属性値は、Solaris 管理コンソールの「セキュリティーテンプレート」ツールでも確認できます。

- デフォルトのテンプレートは、どのインストールにも一致します。各テンプレートのラベル範囲は、ADMIN_LOW から ADMIN_HIGH までです。
- cipso テンプレートでは、DOI が 1 である CIPSO ホストタイプが定義されます。テンプレートのラベル範囲は、ADMIN_LOW から ADMIN_HIGH までです。
- admin_low テンプレートでは、DOI が 1 であるラベルなしホストが定義されます。テンプレートのデフォルトラベルは ADMIN_LOW です。テンプレートのラベル範囲は、ADMIN_LOW から ADMIN_HIGH までです。デフォルト構成では、アドレス

`0.0.0.0` がこのテンプレートに割り当てられます。したがって、CIPSO 以外のすべてのホストは、`ADMIN_LOW` のセキュリティーラベルで動作するホストとして扱われます。

2 デフォルトのテンプレートを確保しておきます。

サポートの目的上、デフォルトのテンプレートは削除したり修正したりしないでください。これらのデフォルトのテンプレートが割り当てられているホストは変更できます。例については、195 ページの「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。

3 次のいずれかの操作が必要な場合は、新しいテンプレートを作成します。

- ホスト、またはホストのグループのラベル範囲を制限します。
- シングルラベルホストを作成します。
- 複数の個別のラベルを認識するホストを作成します。
- 1 以外の DOI を使用します。
- `ADMIN_LOW` でないラベルなしホストにデフォルトのラベルを要求します。

詳細は、187 ページの「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。

▼ トラステッドネットワーキングのツールを開く

始める前に ネットワークセキュリティーを修正できる役割で、大域ゾーンにいる必要があります。たとえば、Information Security または Network Security の権利プロファイルを割り当てられた役割は、セキュリティー設定を修正することができます。セキュリティー管理者役割には、これらのプロファイルが含まれています。

LDAP ツールボックスを使用する場合は、『Solaris Trusted Extensions 構成ガイド』の「LDAP のための Solaris 管理コンソールの設定 (作業マップ)」を完了しておいてください。

1 **Solaris 管理コンソールを起動します。**

詳細は、『Solaris Trusted Extensions 構成ガイド』の「Trusted Extensions で Solaris 管理コンソールサーバーを初期化する」を参照してください。

2 適切なツールを使用します。

- テンプレートを修正するには、「セキュリティーテンプレート」ツールを使用します。

  現在定義されているすべてのテンプレートが右側の区画に表示されます。テンプレートを選択または作成すると、左側の区画でオンラインヘルプを使用できます。
- テンプレートにホストを割り当てるには、「セキュリティーテンプレート」ツールを使用します。

- テンプレートに割り当て可能なホストを作成するには、「コンピュータとネットワーク」ツールを使用します。
- ゾーンにラベルを割り当てるには、「トラステッドネットワークゾーン」ツールを使用します。Trusted Extensions のゾーンについては、第 10 章「Trusted Extensions でのゾーンの管理 (手順)」を参照してください。

▼ 遠隔ホストテンプレートを構築する

始める前に　ネットワークセキュリティーを修正できる役割で、大域ゾーンにいる必要があります。たとえば、Information Security または Network Security の権利プロファイルを割り当てられた役割は、セキュリティー設定を修正することができます。セキュリティー管理者役割には、これらのプロファイルが含まれています。

1. **Solaris 管理コンソールで、「セキュリティーテンプレート」ツールを開きます。**
   詳細な手順については、186 ページの「トラステッドネットワーキングのツールを開く」を参照してください。

2. **「コンピュータとネットワーク」の下の「セキュリティーテンプレート」をダブルクリックします。**
   既存のテンプレートは、「表示」区画に表示されます。これらのテンプレートには、このシステムが接続できるホストのセキュリティー属性が記述されています。このようなホストには、Trusted Extensions を実行している CIPSO ホストや、ラベルなしホストがあります。

3. **`cipso` テンプレートを調べます。**
   このテンプレートがすでに割り当てられているホストとネットワークを表示します。

4. **`admin_low` テンプレートを調べます。**
   このテンプレートがすでに割り当てられているホストとネットワークを表示します。

5. **テンプレートを作成します。**
   用意されているテンプレートで、このシステムと通信できるホストに関する記述が不十分な場合、「アクション」メニューから「テンプレートの追加」を選択します。

   詳細はオンラインヘルプを参照してください。ホストをテンプレートに割り当てる前に、サイトで必要なテンプレートをすべて作成します。

6 (省略可能) デフォルトのテンプレートでない既存のテンプレートを修正します。

テンプレートをダブルクリックします。詳細はオンラインヘルプを参照してください。割り当てられているホストまたはネットワークを変更することができます。

例 13–1 異なる DOI 値を持つセキュリティーテンプレートの作成

この例では、セキュリティー管理者のネットワークに、1 以外の値を持つ DOI が含まれています。最初にシステムを構成したチームは、『Solaris Trusted Extensions 構成ガイド』の「解釈ドメインの構成」を完了しています。

最初に、セキュリティー管理者が /etc/system ファイルに含まれる DOI の値を確認します。

```
# grep doi /etc/system
set default_doi = 4
```

次に、「セキュリティーテンプレート」ツールで、管理者がテンプレートを作成するたびに、doi の値が 4 に設定されます。例 13–2 で説明されているシングルラベルシステムの場合、セキュリティー管理者は次のテンプレートを作成します。

```
template: CIPSO_PUBLIC
host_type: CIPSO
doi: 4
min_sl: PUBLIC
max_sl: PUBLIC
```

例 13–2 シングルラベルを持つセキュリティーテンプレートの作成

この例では、セキュリティー管理者が、シングルラベル PUBLIC でのみパケットを通過させることのできるゲートウェイを作成します。管理者は、Solaris 管理コンソールの「セキュリティーテンプレート」ツールを使用して、テンプレートを作成し、ゲートウェイホストをテンプレートに割り当てます。

最初に、ゲートウェイホストと IP アドレスが、「コンピュータとネットワーク」ツールに追加されます。

```
gateway-1
192.168.131.75
```

次に、テンプレートが「セキュリティーテンプレート」ツールで作成されます。 テンプレート内の値は次のとおりです。

```
template: CIPSO_PUBLIC
host_type: CIPSO
doi: 1
min_sl: PUBLIC
max_sl: PUBLIC
```

ツールで、PUBLIC の 16 進値 0X0002-08-08 が提供されます。

最後に、gateway-1 のホストは、その名前と IP アドレスでテンプレートに割り当てられます。

```
gateway-1
192.168.131.75
```

ローカルホストで、tnrhtp エントリが次のようになります。

```
cipso_public:host_type=cipso;doi=1;min_sl=0X0002-08-08;max_sl=0X0002-08-08;
```

ローカルホストで、tnrhdb エントリが次のようになります。

```
# gateway-1
192.168.131.75:cipso_public
```

例 13–3 ラベルなしルーター用のセキュリティーテンプレートの作成

IP ルーターは、明示的にラベルをサポートしていない場合でも、CIPSO ラベルの付いたメッセージを転送することができます。このようなラベルなしルーターには、ルーターへの接続 (多くの場合ルーター管理のため) を処理するレベルを定義するデフォルトラベルが必要です。この例では、セキュリティー管理者が、任意のラベルでトラフィックを転送できるルーターを作成しますが、ルーターとの直接の通信はデフォルトラベル PUBLIC で処理されます。

Solaris 管理コンソールで、管理者がテンプレートを作成し、ゲートウェイホストをテンプレートに割り当てます。

最初に、ルーターとその IP アドレスが、「コンピュータとネットワーク」ツールに追加されます。

```
router-1
192.168.131.82
```

次に、テンプレートが「セキュリティーテンプレート」ツールで作成されます。テンプレート内の値は次のとおりです。

```
Template Name: UNL_PUBLIC
Host Type: UNLABELED
DOI: 1
Default Label: PUBLIC
Minimum Label: ADMIN_LOW
Maximum Label: ADMIN_HIGH
```

ツールで、ラベルの 16 進値が提供されます。

最後に、router-1 のルーターは、その名前と IP アドレスでテンプレートに割り当てられます。

```
router-1
192.168.131.82
```

例 13–4 制限されたラベル範囲を持つセキュリティーテンプレートの作成

この例では、セキュリティー管理者が、パケットを狭いラベル範囲に制限するゲートウェイを作成します。Solaris 管理コンソールで、管理者がテンプレートを作成し、ゲートウェイホストをテンプレートに割り当てます。

最初に、ホストとその IP アドレスが、「コンピュータとネットワーク」ツールに追加されます。

```
gateway-ir
192.168.131.78
```

次に、テンプレートが「セキュリティーテンプレート」ツールで作成されます。テンプレート内の値は次のとおりです。

```
Template Name: CIPSO_IUO_RSTRCT
Host Type: CIPSO
DOI: 1
Minimum Label: CONFIDENTIAL : INTERNAL USE ONLY
Maximum Label: CONFIDENTIAL : RESTRICTED
```

ツールで、ラベルの 16 進値が提供されます。

最後に、`gateway-ir` のゲートウェイは、その名前と IP アドレスでテンプレートに割り当てられます。

```
gateway-ir
192.168.131.78
```

例 13–5 セキュリティーラベルセットを持つセキュリティーテンプレートの作成

この例では、セキュリティー管理者が、2 つのラベルのみを認識するセキュリティーテンプレートを作成します。Solaris 管理コンソールで、管理者がテンプレートを作成し、ゲートウェイホストをテンプレートに割り当てます。

最初に、このテンプレートを使用する各ホストと IP アドレスが、「コンピュータとネットワーク」ツールに追加されます。

```
host-slset1
192.168.132.21

host-slset2
```

```
192.168.132.22

host-slset3
192.168.132.23

host-slset4
192.168.132.24
```

次に、テンプレートが「セキュリティーテンプレート」ツールで作成されます。テンプレート内の値は次のとおりです。

```
Template Name: CIPSO_PUB_RSTRCT
Host Type: CIPSO
DOI: 1
Minimum Label: PUBLIC
Maximum Label: CONFIDENTIAL : RESTRICTED
SL Set: PUBLIC, CONFIDENTIAL : RESTRICTED
```

ツールで、ラベルの 16 進値が提供されます。

最後に、IP アドレスの範囲をテンプレートに割り当てるには、「ワイルドカード」ボタンと接頭辞を使用します。

```
192.168.132.0/17
```

例 13–6 ラベル PUBLIC でのラベルなしテンプレートの作成

この例では、セキュリティー管理者が、Solaris システムのサブネットワークにトラステッドネットワークで PUBLIC ラベルを付けることができるようにします。テンプレートには次の値があります。

```
Template Name: public
Host Type: Unlabeled
Default Label: Public
Minimum Label: Public
Maximum Label: Public
DOI: 1

Wildcard Entry: 10.10.0.0
Prefix: 16
```

10.10.0.0 サブネットワーク上のすべてのシステムは、PUBLIC ラベルで処理されます。

例 13–7 開発者用のラベル付きテンプレートの作成

この例では、セキュリティー管理者が SANDBOX テンプレートを作成します。このテンプレートは、トラステッドソフトウェアの開発者が使うシステムに割り当てられます。このテンプレートを割り当てられた 2 つのシステムでは、ラベル付きプログラムを作成およびテストします。ただし、そのテストでほかのラベル付きシステムが影響を受けることはありません。SANDBOX ラベルはネットワーク上のほかのラベルから独立しているからです。

```
Template Name: cipso_sandbox
Host Type: CIPSO
Minimum Label: SANDBOX
Maximum Label: SANDBOX
DOI: 1

Hostname: DevMachine1
IP Address: 196.168.129.129

Hostname: DevMachine2
IP Address: 196.168.129.102
```

これらのシステムを使用する開発者は、SANDBOX ラベルで相互に通信できます。

▼ システムの既知のネットワークにホストを追加する

Solaris 管理コンソールの「コンピュータ」ツールは、Solaris OS の「コンピュータ」ツールと同じです。この手順は、利便性を考慮して記載されています。ホストが既知になったら、ホストをセキュリティーテンプレートに割り当てます。

始める前に ネットワークを管理できる管理者である必要があります。たとえば、Network Management または System Administrator の権利プロファイルを持つ役割が、ネットワークを管理できます。

1. **Solaris 管理コンソールで、「コンピュータ」ツールを開きます。**
   詳細は、186 ページの「トラステッドネットワーキングのツールを開く」を参照してください。
2. 「コンピュータ」ツールで、ネットワーク上のすべてのコンピュータを表示することを確定します。

3. このシステムが接続できるホストを追加します。
   静的ルーターや監査サーバーなど、このシステムが接続する可能性のあるホストをすべて追加する必要があります。

   a. 「アクション」メニューから「コンピュータの追加」を選択します。

   b. 名前と IP アドレスでホストを指定します。

   c. (省略可能) ホストに関する追加情報を入力します。

   d. 「適用」をクリックしてホストを追加します。

   e. 入力が完了したら、「了解」をクリックします。

4. このシステムが接続できるホストのグループを追加します。
   オンラインヘルプに従い、ネットワーク IP アドレスを使用して、ホストのグループを追加します。

▼ 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

始める前に　大域ゾーンでセキュリティー管理者役割になります。

テンプレートに割り当てるホストはすべて、「コンピュータとネットワーク」ツールに存在する必要があります。詳細は、192 ページの「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。

1. Solaris 管理コンソールで、「セキュリティーテンプレート」ツールを開きます。
   詳細は、186 ページの「トラステッドネットワーキングのツールを開く」を参照してください。

2. 適切なテンプレート名をダブルクリックします。

3. 「テンプレートに割り当てるホスト」タブをクリックします。

4. 1 つのホストにテンプレートを割り当てるには、次のようにします。

   a. 「ホスト名」フィールドにホストの名前を入力します。

   b. 「IP アドレス」フィールドにホストのアドレスを入力します。

   c. 「追加」ボタンをクリックします。

d. 「了解」をクリックして変更を保存します。

5 アドレスが連続しているホストのグループにテンプレートを割り当てるには、次のようにします。

a. 「ワイルドカード」をクリックします。

b. 「**IP** アドレス」フィールドに **IP** アドレスを入力します。

c. 「プレフィックス」フィールドに、連続するアドレスのグループを表す接頭辞を入力します。

d. 「追加」ボタンをクリックします。

e. 「了解」をクリックして変更を保存します。

例 **13–8** ワイルドカードエントリとして IPv4 ネットワークを追加

この例では、セキュリティー管理者が複数の IPv4 サブネットワークを、同じセキュリティーテンプレートに割り当てます。「テンプレートに割り当てるホスト」タブで、管理者は次のワイルドカードエントリを追加します。

```
IP Address: 192.168.113.0
IP address: 192.168.75.0
```

例 **13–9** ワイルドカードエントリとして IPv4 ホストのリストを追加

次の例では、セキュリティー管理者が、オクテット境界にない連続 IPv4 アドレスを、同じセキュリティーテンプレートに割り当てます。「テンプレートに割り当てるホスト」タブで、管理者は次のワイルドカードエントリを追加します。

```
IP Address: 192.168.113.100
Prefix Length: 25
```

このワイルドカードエントリは、`192.168.113.0` から `192.168.113.127` までのアドレス範囲をカバーします。このアドレスには、`192.168.113.100` が含まれます。

例 **13–10** ワイルドカードエントリとして IPv6 ホストのリストを追加

この例では、セキュリティー管理者が連続する IPv6 アドレスを、同じセキュリティーテンプレートに割り当てます。「テンプレートに割り当てるホスト」タブで、管理者は次のワイルドカードエントリを追加します。

```
IP Address: 2001:a08:3903:200::0
Prefix Length: 56
```

このワイルドカードエントリは、2001:a08:3903:200::0 から 2001:a08:3903:2ff:ffff:ffff:ffff:ffff までのアドレス範囲をカバーします。このアドレスには、2001:a08:3903:201:20e:cff:fe08:58c が含まれます。

▼ 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

この手順では、任意のラベルなしホストによる接続から、ラベル付きホストを保護します。Trusted Extensions をインストールする場合、このデフォルトのテンプレートでネットワーク上のすべてのホストが定義されます。この手順を使って、特定のラベルなしホストを列挙します。

各システム上のローカルの tnrhdb ファイルは、起動時のネットワーク接続に使用されます。デフォルトでは、CIPSO テンプレートで提供されない各ホストはadmin_low テンプレートで定義されます。このテンプレートは、ほかで定義されていない各システム (0.0.0.0) を、admin_low のデフォルトラベルでラベルなしシステムとして割り当てます。

注意 – デフォルトの admin_low テンプレートは、Trusted Extensions ネットワークでセキュリティー上のリスクになる場合があります。サイトのセキュリティーに強い保護が必要な場合、セキュリティー管理者はシステムのインストール後に 0.0.0.0 ワイルドカードエントリを削除することができます。このエントリは、起動時にシステムが接続する各ホストのエントリに置き換える必要があります。

たとえば、0.0.0.0 ワイルドカードエントリを削除したあとに、DNS サーバー、ホームディレクトリサーバー、監査サーバー、ブロードキャストおよびマルチキャストアドレス、およびルーターがローカルの tnrhdb ファイルになければなりません。

アプリケーションが最初にホストアドレス 0.0.0.0 のクライアントを認識する場合、tnrhdb データベースに 0.0.0.0/32:admin_low ホストエントリを追加してください。たとえば、潜在的な Sun Ray クライアントからの初期接続要求を受信するには、Sun Ray サーバーにこのエントリを含めます。すると、サーバーはクライアントを認識したとき、クライアントに IP アドレスを付与して、クライアントを CIPSO クライアントとして接続します。

始める前に　大域ゾーンでセキュリティー管理者役割になります。

起動時に接続されるすべてのホストは、「コンピュータとネットワーク」ツールに存在している必要があります。

1 **Solaris 管理コンソールのファイルの有効範囲で、「セキュリティーテンプレート」ツールを開きます。**

ファイルの有効範囲は、起動中にシステムを保護します。「セキュリティーテンプレート」ツールへのアクセスについては、186 ページの「トラステッドネットワーキングのツールを開く」を参照してください。

2 `admin_low` テンプレートに割り当てられているホストを修正します。

a. `admin_low` テンプレートをダブルクリックします。
追加される各ホストには、ラベル `ADMIN_LOW` で起動中に接続できます。

b. 「テンプレートに割り当てるホスト」タブをクリックします。
追加される各ホストには、ラベル `ADMIN_LOW` で起動中に接続できます。

c. 起動時に接続する必要のある各ラベルなしホストを追加します。
詳細は、193 ページの「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。

このホストが通信時に経由する必要のある、Trusted Extensions を実行していないオンリンクルーターをすべて追加します。

d. 起動時に接続する必要のあるホストの範囲を追加します。

e. `0.0.0.0` エントリを削除します。

3 `cipso` テンプレートに割り当てられているホストを修正します。

a. `cipso` テンプレートをダブルクリックします。
追加される各ホストには、起動時に接続できます。

b. 「テンプレートに割り当てるホスト」タブをクリックします。
追加される各ホストには、ラベル `ADMIN_LOW` で起動中に接続できます。

c. 起動時に接続する必要のある各ラベル付きホストを追加します。
詳細は、193 ページの「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 サーバーを追加します。
- このホストが通信時に経由する必要のある、 Trusted Extensions を実行してしていないオンリンクルーターをすべて追加します。
- すべてのネットワークインタフェースがテンプレートに割り当てられていることを確認します。
- ブロードキャストアドレスを追加します。

d. 起動時に接続する必要のあるホストの範囲を追加します。

4 ホスト割り当てによってシステムの起動が許可されていることを確認します。

例 13–11 0.0.0.0 tnrhdb エントリのラベルの変更

この例では、セキュリティー管理者が公共ゲートウェイシステムを作成します。管理者は、admin_low テンプレートから 0.0.0.0 エントリを削除し、そのエントリを public という名前のラベルなしテンプレートに割り当てます。システムは、その tnrhdb ファイルにリストされていないシステムを、public セキュリティーテンプレートのセキュリティー属性を持つラベルなしシステムとして認識するようになります。

公共ゲートウェイ用に特別に作成されたラベルなしテンプレートは、次のとおりです。

```
Template Name: public
Host Type: Unlabeled
Default Label: Public
Minimum Label: Public
Maximum Label: Public
DOI: 1
```

例 13–12 tnrhdb データベースで起動中に接続するコンピュータの列挙

次の例は、2 つのネットワークインタフェースを持つ LDAP クライアント用のエントリを持つローカルの tnrhdb データベースを示しています。クライアントは、ほかのネットワークおよびルーターと通信します。

```
127.0.0.1:cipso             Loopback address
192.168.112.111:cipso       Interface 1 of this host
192.168.113.111:cipso       Interface 2 of this host
10.6.6.2:cipso              LDAP server
192.168.113.6:cipso         Audit server
192.168.112.255:cipso       Subnet broadcast address
192.168.113.255:cipso       Subnet broadcast address
192.168.113.1:cipso         Router
192.168.117.0:cipso         Another Trusted Extensions network
192.168.112.12:public       Specific network router
192.168.113.12:public       Specific network router
224.0.0.2:public            Multicast address
255.255.255.255:admin_low       Broadcast address
```

例 13–13 ホストアドレス 0.0.0.0 を有効な tnrhdb エントリにする

この例では、セキュリティー管理者は、潜在的なクライアントからの初期接続要求を受け入れるように Sun Ray サーバーを構成します。サーバーは、プライベートトポロジおよび標準設定を使用します。

```
# utadm -a bge0
```

まず、管理者は Solaris 管理コンソールのドメイン名を決定します。

```
SMCserver # /usr/sadm/bin/dtsetup scopes
Getting list of managable scopes...
Scope 1 file:/machine1.ExampleCo.COM/machine1.ExampleCo.COM
```

次に、管理者は、Sun Ray サーバーの tnrhdb データベースにクライアントの初期接続用のエントリを追加します。管理者がテストしている段階なので、すべての不明なアドレスに対してデフォルトのワイルドカードアドレスを使用します。

```
SunRayServer # /usr/sadm/bin/smtnrhdb \
add -D file:/machine1.ExampleCo.COM/machine1.ExampleCo.COM \
-- -w 0.0.0.0 -p 32 -n admin_low
Authenticating as user: root

Please enter a string value for: password ::
... from machine1.ExampleCo.COM was successful.
```

このコマンドの実行後、tnhrdb データベースは次のようになります。smtnrhdb コマンドの結果は強調表示されています。

```
## tnrhdb database
## Sun Ray server address
       192.168.128.1:cipso
## Sun Ray client addresses on 192.168.128 network
       192.168.128.0/24:admin_low
## Initial address for new clients
       0.0.0.0/32:admin_low
## Default wildcard address
0.0.0.0:admin_low
     Other addresses to be contacted at boot
```

```
# tnchkdb -h /etc/security/tsol/tnrhdb
```

テストがこの段階まで成功したあと、管理者は、構成の安全性を高めるためにデフォルトのワイルドカードアドレスを削除し、tnrhdb データベースの構文をチェックしてから再度テストを実行します。最終的な tnhrdb データベースは次のようになります。

```
## tnrhdb database
## Sun Ray server address
       192.168.128.1:cipso
## Sun Ray client addresses on 192.168.128 network
       192.168.128.0/24:admin_low
## Initial address for new clients
       0.0.0.0/32:admin_low
## 0.0.0.0:admin_low - no other systems can enter network at admin_low
     Other addresses to be contacted at boot
```

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)

次の作業マップでは、ネットワークの構成と構成の確認を行うためのタスクについて説明します。

作業	説明	参照先
静的経路を構成します。	ホスト間の最適な経路を手動で記述します。	199 ページの「セキュリティー属性を使用して経路を構成する」
ローカルネットワークデータベースの正しさをチェックします。	`tnchkdb` コマンドを使用して、ローカルネットワークデータベースの構文の妥当性をチェックします。	201 ページの「トラステッドネットワークデータベースの構文をチェックする」
ネットワークデータベースエントリと、カーネルキャッシュ内のエントリを比較します。	`tninfo` コマンドを使用して、カーネルキャッシュが最新のデータベース情報で更新されたかどうかを判定します。	202 ページの「トラステッドネットワークデータベース情報とカーネルキャッシュを比較する」
カーネルキャッシュとネットワークデータベースの同期をとります。	`tnctl` コマンドを使用して、カーネルキャッシュを、実行中のシステム上の最新ネットワークデータベース情報で更新します。	203 ページの「カーネルキャッシュとトラステッドネットワークデータベースを同期する」

▼ セキュリティー属性を使用して経路を構成する

始める前に　大域ゾーンでセキュリティー管理者役割になります。

1. トラステッドネットワーク上でのパケットの経路指定に使用する宛先のホストとゲートウェイをすべて追加します。

   アドレスは、ローカルの `/etc/hosts` ファイル、または LDAP サーバー上の同等のファイルに追加されます。Solaris 管理コンソール の「コンピュータとネットワーク」ツールを使用します。ファイルの有効範囲は `/etc/hosts` ファイルを修正し

ます。LDAP の有効範囲は LDAP サーバー上のエントリを修正します。詳細は、192 ページの「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。

2 宛先の各ホスト、ネットワーク、ゲートウェイをセキュリティーテンプレートに割り当てます。

アドレスは、ローカルの /etc/security/tsol/tnrhdb ファイル、または LDAP サーバー上の同等のファイルに追加されます。Solaris 管理コンソール の「セキュリティーテンプレート」ツールを使用します。詳細は、193 ページの「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。

3 経路を設定します。

端末ウィンドウで、route add コマンドを使用して経路を指定します。

最初のエントリでデフォルトの経路が設定されます。このエントリは、ホストにもパケットの宛先にも特定の経路が定義されていない場合に使用するゲートウェイのアドレス、192.168.113.1 を指定します。

```
# route add default 192.168.113.1  -static
```

詳細は、route(1M) のマニュアルページを参照してください。

4 1 つ以上のネットワークエントリを設定します。

-secattr フラグを使用して、セキュリティー属性を指定します。

次のコマンドリストでは、2 行目がネットワークエントリを示しています。3 行目は、PUBLIC … CONFIDENTIAL : INTERNAL USE ONLY のラベル範囲を持つネットワークエントリを示しています。

```
# route add default 192.168.113.36
# route add -net 192.168.102.0 gateway-101
# route add -net 192.168.101.0 gateway-102 \
-secattr min_sl="PUBLIC",max_sl="CONFIDENTIAL : INTERNAL USE ONLY",doi=1
```

5 1 つ以上のホストエントリを設定します。

新しい 4 行目は、シングルラベルホスト gateway-pub のホストエントリを示しています。gateway-pub のラベル範囲は PUBLIC から PUBLIC までです。

```
# route add default 192.168.113.36
# route add -net 192.168.102.0 gateway-101
# route add -net 192.168.101.0 gateway-102 \
-secattr min_sl="PUBLIC",max_sl="CONFIDENTIAL : INTERNAL USE ONLY",doi=1
# route add -host 192.168.101.3 gateway-pub \
-secattr min_sl="PUBLIC",max_sl="PUBLIC",doi=1
```

例 13–14 CONFIDENTIAL : INTERNAL USE ONLY から CONFIDENTIAL : RESTRICTED までのラベル範囲を持つ経路の追加

次の route コマンドは、192.168.118.39 をゲートウェイとして 192.168.115.0 のホストを経路指定テーブルに追加します。ラベル範囲は CONFIDENTIAL : INTERNAL USE ONLY ... CONFIDENTIAL : RESTRICTED で、DOI は 1 です。

```
$ route add -net 192.168.115.0 192.168.118.39 \
-secattr min_sl="CONFIDENTIAL : INTERNAL USE ONLY",max_sl="CONFIDENTIAL : RESTRICTED",doi=1
```

追加したホストの結果は、netstat -rR コマンドを使用して表示されます。次の抜粋コードでは、ほかの送信経路は省略されて (...) で示されています。

```
$ netstat -rRn
...
192.168.115.0        192.168.118.39        UG       0      0
       min_sl=CNF : INTERNAL USE ONLY,max_sl=CNF : RESTRICTED,DOI=1,CIPSO
...
```

▼ トラステッドネットワークデータベースの構文をチェックする

tnchkdb コマンドでは、各ネットワークデータベースの構文が正確かどうかをチェックします。「セキュリティーテンプレート」ツールまたは「トラステッドネットワークゾーン」ツールを使用すると、Solaris 管理コンソールは自動的にこのコマンドを実行します。一般的に、このコマンドを実行すると、将来の使用に備えて構成しているデータベースファイルの構文をチェックできます。

始める前に ネットワーク設定をチェックできる役割で、大域ゾーンにいる必要があります。セキュリティー管理者役割とシステム管理者役割が、これらの設定をチェックできます。

- 端末ウィンドウで、tnchkdb コマンドを実行します。

```
$ tnchkdb [-h tnrhdb-path] [-t tnrhtp-path] [-z tnzonecfg-path]
checking /etc/security/tsol/tnrhtp ...
checking /etc/security/tsol/tnrhdb ...
checking /etc/security/tsol/tnzonecfg ...
```

例 13–15 評価ネットワークデータベースの構文テスト

この例では、セキュリティー管理者がネットワークデータベースファイルをテストします。最初は、管理者が誤ったオプションを使用します。チェックの結果は、tnrhdb ファイルの行に出力されます。

```
$ tnchkdb -h /opt/secfiles/trial.tnrhtp
checking /etc/security/tsol/tnrhtp ...
checking /opt/secfiles/trial.tnrhtp ...
line 12: Illegal name: min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH
line 14: Illegal name: min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH
checking /etc/security/tsol/tnzonecfg ...
```

セキュリティー管理者が `-t` オプションを使用してファイルをチェックすると、`tnrhtp` データベースの構文が正確であることが確認されます。

```
$ tnchkdb -t /opt/secfiles/trial.tnrhtp
checking /opt/secfiles/trial.tnrhtp ...
checking /etc/security/tsol/tnrhdb ...
checking /etc/security/tsol/tnzonecfg ...
```

▼ トラステッドネットワークデータベース情報とカーネルキャッシュを比較する

ネットワークデータベースには、カーネルにキャッシュされない情報が含まれている場合があります。この手順では、情報が同じことをチェックします。Solaris 管理コンソールを使用してネットワークを更新すると、カーネルキャッシュはネットワークデータベース情報を含み更新されます。`tninfo` コマンドはテスト時およびデバッグ時に役立ちます。

始める前に　ネットワーク設定をチェックできる役割で、大域ゾーンにいる必要があります。セキュリティー管理者役割とシステム管理者役割が、これらの設定をチェックできます。

- 端末ウィンドウで、`tninfo` コマンドを実行します。
  - `tninfo -h` *hostname* は、指定したホストの IP アドレスとテンプレートを表示します。
  - `tninfo -t` *templatename* は、次の情報を表示します。

    ```
    template: template-name
    host_type: either CIPSO or UNLABELED
    doi: 1
    min_sl: minimum-label
    hex: minimum-hex-label
    max_sl: maximum-label
    hex:maximum-hex-label
    ```

  - `tninfo -m` *zone-name* は、ゾーンのマルチレベルポート (MLP) 構成を表示します。

例 13–16 ホスト上のマルチレベルポートの表示

この例のシステムには、複数のラベル付きゾーンが設定されています。すべてのゾーンが、同じ IP アドレスを共有します。一部のゾーンは、ゾーン固有のアドレスでも構成されます。この構成では、Web ブラウザ用の TCP ポートであるポート 8080 が、Public ゾーンの共有インタフェース上の MLP です。管理者は、telnet、TCP ポート 23 も、Public ゾーンの MLP として設定します。これら 2 つの MLP は共有インタフェース上にあるので、大域ゾーンも含めたほかのゾーンは、ポート 8080 および 23 の共有インタフェース上ではパケットを受信できません。

さらに、ssh 用の TCP ポートであるポート 22 は、Public ゾーンのゾーンごとの MLP です。Public ゾーンの ssh サービスは、ゾーン固有のアドレスで、そのアドレスのラベル範囲にあるどのパケットも受信できます。

次のコマンドが Public ゾーンの MLP を示します。

```
$ tninfo -m public
private: 22/tcp
shared:  23/tcp;8080/tcp
```

次のコマンドが大域ゾーンの MLP を示します。大域ゾーンは Public ゾーンと同じアドレスを共有するため、ポート 23 および 8080 は大域ゾーンでは MLP になれません。

```
$ tninfo -m global
private: 111/tcp;111/udp;514/tcp;515/tcp;631/tcp;2049/tcp;
         6000-6003/tcp;38672/tcp;60770/tcp;
shared:  6000-6003/tcp
```

▼ カーネルキャッシュとトラステッドネットワークデータベースを同期する

カーネルがトラステッドネットワークデータベースの情報で更新されていない場合、カーネルキャッシュを更新する方法はいくつかあります。「セキュリティーテンプレート」ツールまたは「トラステッドネットワークゾーン」ツールを使用すると、Solaris 管理コンソールは自動的にこのコマンドを実行します。

始める前に 大域ゾーンでセキュリティー管理者役割になります。

- カーネルキャッシュをネットワークデータベースと同期するには、次のコマンドのいずれかを実行します。
  - tnctl サービスを再起動します。

注意 – この方法は、トラステッドネットワークデータベースの情報を LDAP サーバーから取得するシステムでは使用しないでください。LDAP サーバーから取得された情報がローカルデータベース情報で上書きされる可能性があります。

```
$ svcadm restart  svc:/network/tnctl
```

このコマンドでは、ローカルのトラステッドネットワークデータベースからカーネルにすべての情報を読み込みます。

- 最近追加したエントリのカーネルキャッシュを更新します。

  ```
  $ tnctl -h hostname
  ```

  このコマンドでは、選択したオプションからの情報だけをカーネルに読み込みます。各オプションについては、例 13–17 および tnctl(1M) のマニュアルページを参照してください。

- tnd ポーリング間隔を変更します。

  これによって、カーネルキャッシュは更新されません。ただし、ポーリング間隔を短くすることによって、カーネルキャッシュの更新頻度を高くすることはできます。詳細は、tnd(1M) のマニュアルページの例を参照してください。

- tnd をリフレッシュします。

  このサービス管理機能 (SMF) コマンドは、トラステッドネットワークデータベースの最新の変更とともにカーネルの即時更新をトリガーします。

  ```
  $ svcadm refresh svc:/network/tnd
  ```

- SMF を使用して tnd を再起動します。

  ```
  $ svcadm restart svc:/network/tnd
  ```

注意 – tnd を再起動する場合、tnd コマンドは実行しないでください。このコマンドにより、現在続行中の通信が中断される場合があります。

例 13–17 最新の tnrhdb エントリを使用してカーネルを更新する

この例では、管理者はローカル tnrhdb データベースに 3 つのアドレスを追加しました。まず、管理者は 0.0.0.0 ワイルドカードエントリを削除しました。

```
$ tnctl -d -h 0.0.0.0:admin_low
```

次に、管理者は、/etc/security/tsol/tnrhdb データベースにある最後の 3 つのエントリの書式を表示します。

```
$ tail /etc/security/tsol/tnrhdb
#\:\:0:admin_low
127.0.0.1:cipso
#\:\:1:cipso
192.168.103.5:admin_low
192.168.103.0:cipso
0.0.0.0/32:admin_low
```

さらに、管理者はカーネルキャッシュを更新します。

```
$ tnctl -h 192.168.103.5
tnctl -h 192.168.103.0
tnctl -h 0.0.0.0/32
```

最後に、管理者は、カーネルキャッシュが更新されていることを確認します。最初のエントリの出力は、次のようになります。

```
$ tninfo -h 192.168.103.5
IP Address: 192.168.103.5
Template: admin_low
```

例 13–18 カーネルでのネットワーク情報の更新

この例では、管理者が公共プリンタサーバーを使用してトラステッドネットワークを更新し、カーネル設定が正しいことをチェックします。

```
$ tnctl -h public-print-server
$ tninfo -h public-print-server
IP Address: 192.168.103.55
Template: PublicOnly
$ tninfo -t PublicOnly
================================
Remote Host Template Table Entries
--------------------------------
template: PublicOnly
host_type: CIPSO
doi: 1
min_sl: PUBLIC
hex: 0x0002-08-08
max_sl: PUBLIC
hex: 0x0002-08-08
```

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)

次の作業マップでは、ネットワークをデバッグするためのタスクについて説明します。

作業	説明	参照先
2 つのホストが通信できない原因を特定します。	1 台のシステムでインタフェースが稼働していることを確認します。	206 ページの「ホストのインタフェースが稼働していることを確認する」
	2 つのホストが相互に通信できないときにデバッグ用のツールを使用します。	207 ページの「Trusted Extensions ネットワークをデバッグする」
LDAP クライアントが LDAP サーバーに到達できない原因を特定します。	LDAP サーバーとクライアントの間の接続障害をトラブルシューティングします。	210 ページの「LDAP サーバーへのクライアント接続をデバッグする」

▼ ホストのインタフェースが稼働していることを確認する

システムが期待どおりにほかのシステムと通信しない場合は、この手順を使います。

始める前に　ネットワーク設定をチェックできる役割で、大域ゾーンにいる必要があります。セキュリティー管理者役割とシステム管理者役割が、これらの設定をチェックできます。

1 システムのネットワークインタフェースが稼働していることを確認します。

次の出力は、システムに `hme0` と `hme0:3` の 2 つのネットワークインタフェースがあることを示しています。どちらのインタフェースも稼働していません。

```
# ifconfig -a
...
hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 192.168.0.11 netmask ffffff00 broadcast 192.168.0.255
hme0:3 flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 192.168.0.12 netmask ffffff00 broadcast 192.168.0.255
```

2 インタフェースが稼動していない場合、インタフェースを起動させて、稼動していることを確認します。

次の出力は、両方のインタフェースが稼動していることを示します。

```
# ifconfig hme0 up
# ifconfig -a
...
hme0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,...
hme0:3 flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,..
```

▼ Trusted Extensions ネットワークをデバッグする

期待どおりに通信していない 2 つのホストをデバッグする場合、Trusted Extensions と Solaris のデバッグ用のツールを使用できます。たとえば、`snoop` や `netstat` など Solaris のネットワークデバッグコマンドを使用できます。詳細は、`snoop(1M)` および `netstat(1M)` のマニュアルページを参照してください。Trusted Extensions に固有のコマンドについては、表 2–4 を参照してください。

- ラベル付きゾーンを接続するときの問題については、132 ページの「ゾーンの管理 (作業マップ)」 を参照してください。
- NFS マウントのデバッグについては、163 ページの「Trusted Extensions でマウントの失敗をトラブルシューティングする」 を参照してください。
- LDAP 通信のデバッグについては、210 ページの「LDAP サーバーへのクライアント接続をデバッグする」 を参照してください。

始める前に ネットワーク設定をチェックできる役割で、大域ゾーンにいる必要があります。セキュリティー管理者役割またはシステム管理者役割が、これらの設定をチェックできます。

1 `tnd` デーモンをトラブルシューティングするには、ポーリング間隔を変更し、デバッグ情報を収集します。

詳細は、`tnd(1M)` のマニュアルページを参照してください。

2 通信できないホスト同士が同じネームサービスを使用していることを確認します。

a. 各ホストで、`nsswitch.conf` ファイルを確認します。

i. `nsswitch.conf` ファイルで、**Trusted Extensions** データベースの値を確認します。

たとえば、ネットワークの管理に LDAP を使用するサイトでは、エントリは次のようになります。

```
# Trusted Extensions
tnrhtp: files ldap
tnrhdb: files ldap
```

ii. 値が異なる場合、`nsswitch.conf` ファイルを修正します。
これらのエントリを修正する場合、システム管理者は「ネームサービススイッチ」アクションを使用します。詳細は、58 ページの「Trusted Extensions の CDE 管理アクションを起動する」を参照してください。このアクションでは、必要な DAC および MAC ファイルのアクセス権が維持されます。

b. **LDAP** ネームサービスが構成されていることを確認します。

```
$ ldaplist -l
```

c. 両方のホストが **LDAP** ネームサービスにあることを確認します。

```
$ ldaplist -l hosts | grep hostname
```

3 各ホストが正しく定義されていることを確認します。

a. **Solaris** 管理コンソールを使用して定義を確認します。

- 「セキュリティーテンプレート」ツールで、各ホストが他方のホストのセキュリティーテンプレートと互換性のあるセキュリティーテンプレートに割り当てられていることを確認します。
- ラベルなしシステムの場合、デフォルトのラベル割り当てが正しいことを確認します。
- 「トラステッドネットワークゾーン」ツールで、マルチレベルポート (MLP) が正しく構成されていることを確認します。

b. コマンド行を使用して、カーネルのネットワーク情報が最新であることを確認します。
各ホストのカーネルキャッシュでの割り当てが、ネットワーク上およびほかのホスト上の割り当てに一致することを確認します。

伝送のソース、宛先、ゲートウェイホストのセキュリティー情報を取得するには、`tninfo` コマンドを使用します。

- 任意のホストの **IP** アドレスと、割り当てられたセキュリティーテンプレートを表示します。

```
$ tninfo -h hostname
IP Address: IP-address
Template: template-name
```

- テンプレート定義を表示します。

```
$ tninfo -t template-name
template: template-name
host_type: one of CIPSO or UNLABELED
doi: 1
min_sl: minimum-label
```

```
hex: minimum-hex-label
max_sl: maximum-label
hex: maximum-hex-label
```

- ゾーンの MLP を表示します。

```
$ tninfo -m zone-name
private: ports-that-are-specific-to-this-zone-only
shared: ports-that-the-zone-shares-with-other-zones
```

4 正しくない情報があれば修正します。

- ネットワークセキュリティー情報を変更または確認するには、Solaris 管理コンソール ツールを使用します。詳細は、186 ページの「トラステッドネットワーキングのツールを開く」を参照してください。
- カーネルキャッシュを更新するには、情報が最新でないホストで `tnctl` サービスを再起動します。このプロセスが完了するにはしばらく時間がかかります。次に、`tnd` サービスをリフレッシュします。リフレッシュに失敗した場合は、`tnd` サービスの再起動を試みます。詳細は、203 ページの「カーネルキャッシュとトラステッドネットワークデータベースを同期する」を参照してください。

  再起動するとカーネルキャッシュが消去されます。起動時に、キャッシュにデータベース情報が生成されます。カーネルへの情報生成にローカルデータベースと LDAP データベースのどちらが使用されるかは、`nsswitch.conf` ファイルで決まります。

5 デバッグに役立つ伝送情報を収集します。

- 経路指定構成を確認します。

  `route` コマンドの `get` サブコマンドを使用します。

```
$ route get [ip] -secattr sl=label,doi=integer
```

  詳細は、`route(1M)` のマニュアルページを参照してください。

- パケットのラベル情報を表示します。

  `snoop -v` コマンドを使用します。

  `-v` オプションを使用すると、ラベル情報などパケットヘッダーの詳細が表示されます。このコマンドでは多くの情報が表示されるため、コマンドで調べられるパケットを制限したい場合があります。詳細は、`snoop(1M)` のマニュアルページを参照してください。

- 経路指定テーブルのエントリとソケットのセキュリティー属性を表示します。

  `netstat -a|-r` コマンドで、`-R` オプションを使用します。

-aR オプションを使用すると、ソケットの拡張セキュリティー属性が表示されます。-rR オプションを使用すると、経路指定テーブルのエントリが表示されます。詳細は、netstat(1M) のマニュアルページを参照してください。

▼ LDAP サーバーへのクライアント接続をデバッグする

LDAP サーバーでクライアントエントリの構成が誤っていると、クライアントがサーバーと通信できない場合があります。同様に、クライアント上のファイルの構成が誤っていると通信できない場合があります。クライアントサーバー間の通信問題をデバッグするときは、次のエントリとファイルを確認します。

始める前に　LDAP クライアント上の大域ゾーンで、セキュリティー管理者役割である必要があります。

1. **LDAP サーバーと LDAP サーバーへのゲートウェイの遠隔ホストテンプレートが正しいことを確認します。**

   ```
   # tninfo -h LDAP-server
   # route get LDAP-server
   # tninfo -h gateway-to-LDAP-server
   ```

   遠隔ホストテンプレートの割り当てが正しくない場合、Solaris 管理コンソールの「セキュリティーテンプレート」ツールを使用して、ホストを正しいテンプレートに割り当てます。

2. **/etc/hosts ファイルを確認し、修正します。**

   使用しているシステム、システム上のラベル付きゾーンのインタフェース、LDAP サーバーへのゲートウェイ、および LDAP サーバーがファイルに一覧表示されている必要があります。さらに多くのエントリがあるかもしれません。

   重複しているエントリを捜します。ほかのシステムのラベル付きゾーンであるエントリを削除します。たとえば、Lserver が LDAP サーバーの名前であり、LServer-zones がラベル付きゾーンの共有インタフェースである場合、/etc/hosts から LServer-zones を削除します。

3. **DNS を使用している場合、resolv.conf ファイルのエントリを確認し修正します。**

   ```
   # more resolv.conf
   search list of domains
   domain domain-name
   nameserver IP-address

   ...
   nameserver IP-address
   ```

4 nsswitch.conf ファイルの tnrhdb および tnrhtp エントリが正しいことを確認します。

5 サーバー上で、クライアントが正しく構成されていることを確認します。

```
# ldaplist -l tnrhdb client-IP-address
```

6 ラベル付きゾーンのインタフェースが **LDAP** サーバー上で正しく構成されていることを確認します。

```
# ldaplist -l tnrhdb client-zone-IP-address
```

7 現在実行中のすべてのゾーンから **LDAP** サーバーを ping できること確認します。

```
# ldapclient list
...
NS_LDAP_SERVERS= LDAP-server-address
# zlogin zone-name1 ping LDAP-server-address
LDAP-server-address is alive
# zlogin zone-name2 ping LDAP-server-address
LDAP-server-address is alive
...
```

8 **LDAP** を構成して再起動します。

a. 「**LDAP** クライアントを作成」アクションを実行します。

このアクションにより、大域ゾーンが LDAP サーバーのクライアントとして再構築されます。

b. 各ラベル付きゾーンで、ゾーンを **LDAP** サーバーのクライアントとして再構築します。

```
# zlogin zone-name1
# ldapclient init \
-a profileName=profileName \
-a domainName=domain \
-a proxyDN=proxyDN \
-a proxyPassword=password  LDAP-Server-IP-Address
# exit
# zlogin zone-name2 ...
```

c. すべてのゾーンを停止し、ファイルシステムをロックして再起動します。

Solaris ZFS を使用している場合は、再起動の前にゾーンを停止し、ファイルシステムをロックします。ZFS を使用していない場合は、ゾーンの停止とファイルシステムのロックを行わずに再起動することができます。

```
# zoneadm list
# zoneadm -z zone-name halt
# lockfs -fa
# reboot
```

◆ ◆ ◆ 第 14 章

Trusted Extensions でのマルチレベルメール (概要)

この章では、Solaris Trusted Extensions が設定されたシステムのセキュリティーとマルチレベルメーラーについて説明します。

マルチレベルメールサービス

Trusted Extensions では、任意のメールアプリケーションでマルチレベルメールを使用できます。一般ユーザーがメーラーを起動すると、アプリケーションはそのユーザーの現在のラベルで開かれます。ユーザーがマルチレベルシステムで作業している場合、メーラーの初期設定ファイルをリンクまたはコピーすることができます。詳細については、91 ページの「Trusted Extensions のユーザーの起動ファイルを構成する」を参照してください。

Trusted Extensions のメール機能

Trusted Extensions では、Solaris の操作方法、『Solaris のシステム管理 (上級編)』および『Solaris のシステム管理 (IP サービス)』に従って、システム管理者役割がメールサーバーを設定および管理します。また、Trusted Extensions メール機能をどのように構成する必要があるかもセキュリティー管理者が決定します。

次の説明は、Trusted Extensions に固有のメール管理です。

- .mailrc ファイルは、ユーザーの最小ラベルにあります。

  したがって、最小ラベルのディレクトリの .mailrc ファイルを上位レベルの各ディレクトリにコピーまたはリンクしない限り、複数のラベルで作業するユーザーには、上位レベルのラベルの .mailrc はありません。

  セキュリティー管理者役割または個々のユーザーは、.mailrc ファイルを .copy_files または .link_files に追加することができます。これらのファイルについては、updatehome(1M) のマニュアルページを参照してください。構成のヒントについては、86 ページの「.copy_files ファイルと .link_files ファイル」を参照してください。
- メールリーダーは、システムの各ラベルで実行できます。メールクライアントをサーバーに接続するには、一部の構成が必要です。

  たとえば、Mozilla メールをマルチレベルメール用に使用するためには、各ラベルで Mozilla メールクライアントを構成してメールサーバーを指定する必要があります。メールサーバーは各ラベルで同じでも異なっていてもかまいませんが、サーバーは指定する必要があります。
- メールエイリアスは、Solaris 管理コンソールの「メーリングリスト」ツールで管理されます。

  選択した Solaris 管理コンソールツールボックスの有効範囲に応じて、ローカルの /etc/aliases ファイルか Sun Java System Directory Server 上の LDAP エントリを更新できます。
- Trusted Extensions ソフトウェアで、メールの送信または転送の前に、ホストとユーザーのラベルがチェックされます。
  - このソフトウェアでは、メールがホストの認定範囲内にあることも確信します。チェックについては、このリストと第 13 章「Trusted Extensions でのネットワークの管理 (手順)」で説明されています。
  - メールがアカウントの認可上限と最小ラベルの間にあることがチェックされます。
  - ユーザーは、自身の認可範囲内で受信されるメールを読むことができます。セッション中、ユーザーは現在のラベルでのみメールを読むことができます。

    電子メールで一般ユーザーに連絡するには、管理者役割はユーザーが読み取れるラベルにあるワークスペースからメールを送信する必要があります。通常はユーザーのデフォルトラベルを選択することをお勧めします。

◆ ◆ ◆ 第 15 章

15 ラベル付き印刷の管理 (手順)

この章では、Solaris Trusted Extensions ソフトウェアを使用してラベル付き印刷を構成する方法について説明します。また、ラベルオプションなしで印刷ジョブを構成する方法も説明します。

ラベル、プリンタ、および印刷

Trusted Extensions ソフトウェアは、ラベルを使用してプリンタへのアクセスを制御します。ラベルは、プリンタへのアクセスと、待ち行列に入った印刷ジョブに関する情報へのアクセスの制御に使用されます。ソフトウェアは、印刷出力のラベル付けも行います。本文ページにラベルが付けられ、必須のバナーページとトレーラページにもラベルが付けられます。バナーページとトレーラページには、取り扱い指示を含めることもできます。

システム管理者は、基本的なプリンタ管理を担当します。セキュリティー管理者役割は、ラベル付き出力の処理方法とラベルも含めてプリンタのセキュリティーを管理します。管理者は Solaris の基本的なプリンタ管理手順に従ったあと、プリンタサーバーとプリンタにラベルを割り当てます。

Trusted Extensions ソフトウェアは、シングルレベルとマルチレベルの両方の印刷をサポートします。マルチレベル印刷は、大域ゾーンでのみ実装されます。大域ゾーンのプリンタサーバーを使用するには、ラベル付きのゾーンに大域ゾーンとは異なるホスト名が付けられている必要があります。ホスト名を区別する 1 つの方法は、ラベル付きゾーンに IP アドレスを割り当てることです。このアドレスは、大域ゾーンの IP アドレスとは別だからです。

Trusted Extensions でのプリンタと印刷ジョブ情報へのアクセス制限

Trusted Extensions ソフトウェアが設定されたシステムのユーザーと役割は、それぞれのセッションのラベルで印刷ジョブを作成します。印刷ジョブは、そのラベルを認識するプリンタでのみ実行できます。ラベルは、プリンタのラベル範囲内になければなりません。

ユーザーと役割は、セッションのラベルと同じラベルを持つ印刷ジョブを表示できます。大域ゾーンでは、役割はゾーンのラベルのほうが優位であるラベルを持つジョブを表示できます。

Trusted Extensions ソフトウェアが設定されたプリンタは、プリンタ出力でラベルを印刷します。ラベルなしのプリンタサーバーで管理されるプリンタは、プリンタ出力でラベルを印刷しません。そのようなプリンタのラベルは、ラベルなしサーバーと同じです。たとえば、Solaris のプリンタサーバーには、LDAP ネームサービスの `tnrhdb` データベースにある任意のラベルを割り当てることができます。こうすると、ユーザーは Solaris プリンタで、その任意のラベルでジョブを印刷できるようになります。Trusted Extensions のプリンタと同じく、これらの Solaris のプリンタも、プリンタサーバーに割り当てられたラベルで作業しているユーザーからの印刷ジョブだけを受け取ることができます。

ラベル付きプリンタ出力

Trusted Extensions は、本文ページ、バナーページ、およびトレーラページに、セキュリティー情報を印刷します。この情報は、`label_encodings` ファイルと `tsol_separator.ps` ファイルから取得されます。

セキュリティー管理者は、次の操作を実行して、ラベル設定のデフォルトを修正し、プリンタ出力に取り扱い指示を追加することができます。

- バナーページとトレーラページのテキストをローカライズまたはカスタマイズする
- 本文ページに、またはバナーページとトレーラページの各フィールドに印刷される代替ラベルを指定する
- テキストまたはラベルの変更、削除

セキュリティー管理者は、出力にラベルを印刷しないプリンタを使用するよう、ユーザーアカウントを構成することもできます。プリンタ出力でバナーやラベルを印刷しないよう選択できる承認を、ユーザーに与えることもできます。

ラベル付きの本文ページ

デフォルトでは、機密保護の格付けが、各本文ページの最上部と最下部に印刷されます。機密保護の格付けは、ジョブラベルの格付けと `minimum protect as classification` (最小の機密保護の格付け) を比較したときの優位な格付けです。`minimum protect as classification` は、`label_encodings` ファイルに定義されています。

たとえば、ユーザーが Internal Use Only セッションにログインした場合、そのユーザーの印刷ジョブはそのラベルにあります。`label_encodings` ファイルの `minimum protect as classification` が Public の場合、本文ページには Internal Use Only ラベルが印刷されます。

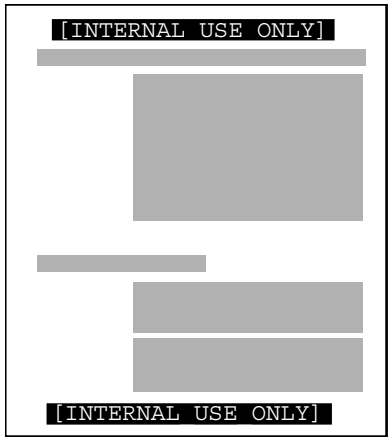


図 15–1 バナーページの最上部と最下部に印刷されたジョブのラベル

ラベル付きバナーページとトレーラページ

次の図は、デフォルトのバナーページとデフォルトのトレーラページの相違点を示したものです。引き出し線は、各セクションを示しています。トレーラページでは外側の線が異なります。

印刷ジョブで表示されるテキスト、ラベル、警告は構成可能です。テキストは、ローカライズしたほかの言語に置き換えることもできます。

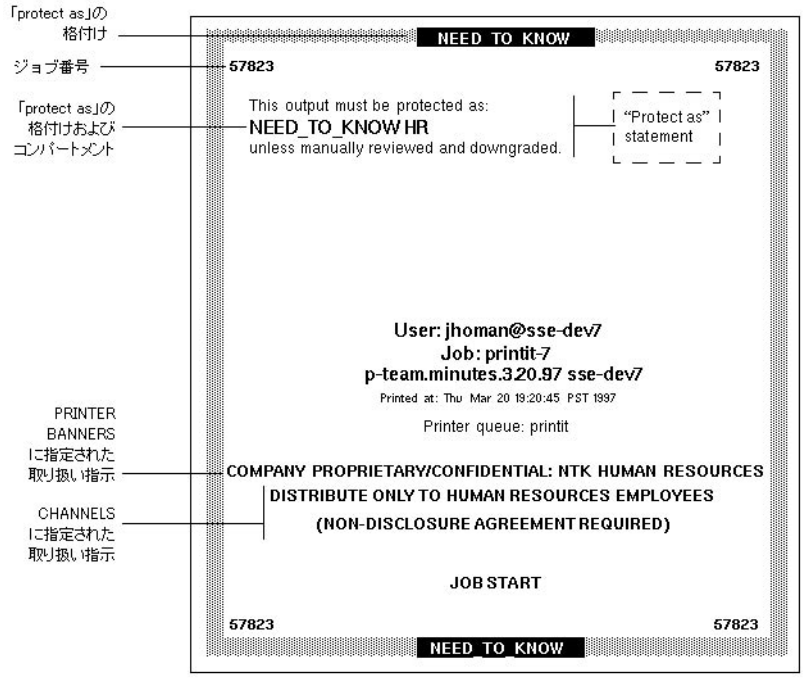


図 15–2 ラベル付き印刷ジョブの一般的なバナーページ

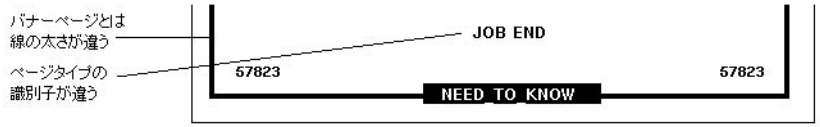


図 15–3 トレーラページでの違い

次の表に示した信頼できる印刷の諸要素は、`/usr/lib/lp/postscript/tsol_separator.ps` ファイルを編集することによってセキュリティー管理者が変更できます。

注 – 印刷される出力をローカライズまたは国際化する方法は、`tsol_separator.ps` ファイルのコメントを参照してください。

表 15–1 tsol_separator.ps ファイルで構成可能な値

出力	デフォルト値	定義の方法	変更の方法
PRINTER BANNERS	/Caveats Job_Caveats	/Caveats Job_Caveats	『Solaris Trusted Extensions ラベルの管理』の「プリンタバナーの指定」を参照してください。
CHANNELS	/Channels Job_Channels	/Channels Job_Channels	『Solaris Trusted Extensions ラベルの管理』の「チャネルの指定」を参照してください。
バナーページとトレーラページの最上部のラベル	/HeadLabel Job_Protect def	/PageLabel の説明を参照してください。	/PageLabel の変更と同じ。 『Solaris Trusted Extensions ラベルの管理』の「機密保護の格付けの指定」も参照してください。
本文ページの最上部と最下部のラベル	/PageLabel Job_Protect def	ジョブのラベルと、label_encodings ファイルのminimum protect as classification とを比較します。より優位な格付けを印刷します。 印刷ジョブのラベルにコンパートメントがある場合にコンパートメントを追加します。	/PageLabel 定義を変更してほかの値を指定します。 または、任意の文字列を入力します。 または、何も印刷しません。
機密保護の格付けの文のテキストとラベル	/Protect Job_Protect def /Protect_Text1 () def /Protect_Text2 () def	/PageLabel の説明を参照してください。 ラベルの上に表示されるテキスト。 ラベルの下に表示されるテキスト。	/PageLabel の変更と同じ。 Protect_Text1 と Protect_Text2 の () をテキスト文字列で置き換えます。

セキュリティー情報の PostScript 印刷

Trusted Extensions でのラベル付き印刷は、Solaris 印刷からの機能に依存します。Solaris OS では、プリンタモデルスクリプトがバナーページの作成を処理します。ラベル付けを実装するには、まずプリンタモデルスクリプトが印刷ジョブを PostScript™ ファイルに変換します。次に、PostScript ファイルを操作して本文ページにラベルを挿入し、バナーページとトレーラページを作成します。

Solaris プリンタモデルスクリプトは、PostScript をプリンタ固有の言語に変換することもできます。プリンタが PostScript 入力を受け付ける場合は、Solaris ソフトウェア

がジョブをプリンタに送信します。プリンタが PostScript 入力を受け付けない場合は、PostScript 形式がラスターイメージに変換されます。ラスターイメージは、次に適切なプリンタフォーマットに変換されます。

PostScript ソフトウェアはラベル情報の出力に使用されるため、デフォルトではユーザーは PostScript ファイルを印刷できません。この制限のため、知識のある PostScript プログラマでも、プリンタ出力のラベルを修正する PostScript ファイルを作成することができません。

セキュリティー管理者役割は、役割アカウントと信頼できるユーザーに `Print Postscript` 承認を割り当てることによって、この制限を無効にすることができます。この承認は、そのアカウントがプリンタ出力のラベルを偽造しないと信頼できる場合にのみ割り当てられます。また、ユーザーによる PostScript ファイルの印刷を許可することが、サイトのセキュリティーポリシーと矛盾しないことが必要です。

プリンタモデルスクリプト

プリンタモデルスクリプトを使うと、特定モデルのプリンタでバナーページとトレーラページを印刷できるようになります。Trusted Extensions には 4 つのスクリプトが用意されています。

- `tsol_standard` - パラレルポート接続されたプリンタなど、直接接続された PostScript プリンタ用
- `tsol_netstandard` - ネットワークアクセス可能な PostScript プリンタ用
- `tsol_standard_foomatic` - 直接接続された、PostScript 形式を印刷しないプリンタ用
- `tsol_netstandard_foomatic` - ネットワークアクセス可能な、PostScript 形式を印刷しないプリンタ用

`foomatic` スクリプトは、プリンタドライバ名が `Foomatic` で始まる場合に使用されます。Foomatic ドライバは、PostScript プリンタドライバ (PPD) です。デフォルトでは、「PPD を使用」はプリンタを追加するときに印刷マネージャーで指定されます。次に、PPD を使用してバナーページとトレーラページがプリンタの言語に変換されます。

追加の変換フィルタ

変換フィルタは、テキストファイルを PostScript 形式に変換します。フィルタのプログラムは、プリンタデーモンにより実行されるトラステッドプログラムです。インストールされているフィルタプログラムによって PostScript 形式に変換されるファイルは、正式なラベルとバナーページおよびトレーラページテキストであると信頼できます。

Solaris ソフトウェアには、サイトで必要な変換フィルタがほとんど用意されています。サイトのシステム管理者役割は、追加のフィルタをインストールすることがで

きます。これらのフィルタは、正式なラベルとバナーページおよびトレーラページを持つものと信頼できます。変換フィルタの追加については、『System Administration Guide: Solaris Printing』の第 7 章「Customizing Printing Services and Printers (Tasks)」を参照してください。

Trusted Solaris 8 の印刷と Trusted Extensions との相互運用性

互換性のある `label_encodings` ファイルを持ち、CIPSO テンプレートで相互を識別する Trusted Solaris 8 と Trusted Extensions のシステムは、相互を遠隔印刷に利用することができます。次の表では、印刷できるようにシステムを設定する方法について説明します。デフォルトでは、ユーザーはほかの OS の遠隔印刷サーバー上で印刷ジョブを一覧表示したり、取り消したりできません。任意で、ユーザーにそのような操作の承認を与えることができます。

元のシステム	プリンタサーバーシステム	動作	結果
Trusted Extensions	Trusted Solaris 8	印刷の構成 – Trusted Extensions の `tnrhdb` で、適切なラベル範囲を持つテンプレートを Trusted Solaris 8 のプリンタサーバーに割り当てます。ラベルは、CIPSO またはラベルなしのいずれかです。	Trusted Solaris 8 のプリンタは、プリンタのラベル範囲内で、Trusted Extensions システムからのジョブを印刷できます。
Trusted Extensions	Trusted Solaris 8	ユーザーの承認 – Trusted Extensions システムで、必要な承認を追加するプロファイルを作成します。そのプロファイルをユーザーに割り当てます。	Trusted Extensions ユーザーは、Trusted Solaris 8 のプリンタに送信する印刷ジョブを一覧表示したり、取り消したりできます。 ユーザーは、異なるラベルのジョブを表示したり削除したりできません。

元のシステム	プリンタサーバーシステム	動作	結果
Trusted Solaris 8	Trusted Extensions	印刷の構成 – Trusted Solaris 8 の `tnrhdb` で、適切なラベル範囲を持つテンプレートを Trusted Extensions のプリンタサーバーに割り当てます。ラベルは、CIPSO またはラベルなしのいずれかです。	Trusted Extensions のプリンタは、プリンタのラベル範囲内で、Trusted Solaris 8 システムからのジョブを印刷できます。
Trusted Solaris 8	Trusted Extensions	ユーザーの承認 – Trusted Solaris 8 システムで、必要な承認を追加するプロファイルを作成します。そのプロファイルをユーザーに割り当てます。	Trusted Solaris 8 ユーザーは、Trusted Extensions のプリンタに送信した印刷ジョブを一覧表示したり、取り消したりできます。 ユーザーは、異なるラベルのジョブを表示したり削除したりできません。

Trusted Extensions の印刷インタフェース (リファレンス)

Trusted Extensions セキュリティーポリシーに適合するように、次のユーザーコマンドが拡張されています。

- `cancel` – ジョブを取り消すには、呼び出し元が印刷ジョブのラベルと同等でなければなりません。デフォルトでは、一般ユーザーは自身のジョブしか取り消せません。
- `lp` – Trusted Extensions によって `-o nolabels` オプションが追加されます。ユーザーがラベルなしで印刷するには、承認が必要です。同様に、ユーザーが `-o nobanner` オプションを使用するにも、承認が必要です。
- `lpstat` – ジョブステータスを取得するには、呼び出し元が印刷ジョブのラベルと同等でなければなりません。デフォルトでは、一般ユーザーは自身の印刷ジョブしか表示できません。

Trusted Extensions のセキュリティーポリシーに適合するように、次の管理コマンドが拡張されています。Solaris OS の場合と同じように、これらのコマンドは Printer Management 権利プロファイルを含む役割でしか実行できません。

- `lpmove` – ジョブを移動するには、呼び出し元が印刷ジョブのラベルと同等でなければなりません。デフォルトでは、一般ユーザーは自身の印刷ジョブしか移動できません。
- `lpadmin` – 大域ゾーンでは、このコマンドがすべてのジョブに対して機能します。ラベル付きゾーンの場合、ジョブの表示には呼び出し元が印刷ジョブのラベルよりも優位でなければならず、ジョブの変更にはラベルと同等でなければなりません。

  Trusted Extensions が、`-m` オプションにプリンタモデルスクリプトを追加します。Trusted Extensions が `-o nolabels` オプションを追加します。
- `lpsched` – 大域ゾーンでは、このコマンドが常に成功します。Solaris OS の場合と同じように、印刷サービスの有効化、無効化、起動、または再起動には `svcadm` コマンドを使用します。ラベル付きゾーンの場合、印刷サービスを変更するには、呼び出し元が印刷サービスのラベルと同等でなければなりません。サービス管理機能については、`smf(5)`、`svcadm(1M)`、および `svcs(1)` のマニュアルページを参照してください。

Trusted Extensions が、`solaris.label.print` 承認を Printer Management 権利プロファイルに追加します。ラベルなしで本文ページを印刷するには、`solaris.print.unlabeled` 承認が必要です。

Trusted Extensions での印刷の管理 (作業マップ)

Trusted Extensions で印刷を構成する手順は、Solaris のプリンタ設定のあとに実行します。ラベル付き印刷を管理する主なタスクは、次の作業マップのとおりです。

作業	説明	参照先
ラベル付き出力のためにプリンタを構成します。	ユーザーが Trusted Extensions のプリンタに出力できるようにします。印刷ジョブはラベルでマークされます。	224 ページの「ラベル付き印刷の構成 (作業マップ)」
プリンタ出力から表示可能なラベルを削除します。	特定のラベルで Solaris のプリンタに出力できるようにします。印刷ジョブはラベルでマークされません。 または、Trusted Extensions プリンタでラベルを印刷しないようにします。	236 ページの「Trusted Extensions の印刷制限の引き下げ (作業マップ)」

ラベル付き印刷の構成 (作業マップ)

次の作業マップでは、ラベル付き印刷に関連する一般的な構成手順について説明します。

注 – プリンタクライアントは、Trusted Extensions のプリンタサーバーのラベル範囲内にあるジョブしか印刷できません。

作業	説明	参照先
印刷マネージャーを起動します。	GUI を使用して、ネットワークまたはローカルシステムに対するプリンタの識別を行います。システム管理者は、管理役割のワークスペースでこの GUI を起動します。	『System Administration Guide: Solaris Printing』の第 4 章「Setting Up Printers (Tasks)」
大域ゾーンから印刷を構成します。	大域ゾーンでマルチレベルプリンタサーバーを作成します。	224 ページの「マルチレベルプリンタサーバーとそのプリンタを構成する」
システムのネットワーク用に印刷を構成します。	大域ゾーンでマルチレベルプリンタサーバーを作成し、ラベル付きゾーンでこのプリンタを使用できるようにします。	226 ページの「Sun Ray クライアント用にネットワークプリンタを構成する方法」
ラベル付きシステムと同じサブネット内のラベルなしシステム用に印刷を構成します。	ラベルなしシステムでネットワークプリンタを使用できるようにします。	229 ページの「ラベル付きシステムでカスケード印刷を構成する方法」
ラベル付きゾーンから印刷を構成します。	ラベル付きゾーンに、シングルラベルのプリンタサーバーを作成します。	232 ページの「シングルラベル印刷用にゾーンを構成する」
マルチレベル印刷クライアントを構成します。	Trusted Extensions ホストをプリンタに接続します。	233 ページの「Trusted Extensions クライアントがプリンタにアクセスできるようにする」
プリンタのラベル範囲を制限します。	Trusted Extensions のプリンタを狭いラベル範囲に制限します。	235 ページの「プリンタに制限付きのラベル範囲を構成する」

▼ マルチレベルプリンタサーバーとそのプリンタを構成する

Trusted Extensions のプリンタサーバーで管理されるプリンタは、本文ページ、バナーページ、およびトレーラページにラベルを印刷します。このようなプリンタは、プリンタサーバーのラベル範囲内にあるジョブを印刷できます。プリンタサーバーにアクセスできる任意の Trusted Extensions ホストが、サーバーに接続されたプリンタを利用できます。

始める前に　Trusted Extensions ネットワーク用のプリンタサーバーを決定します。このプリンタサーバー上の大域ゾーンで、システム管理者役割である必要があります。

1. **Solaris 管理コンソールを起動します。**
   詳細は、57 ページの「Solaris 管理コンソールでローカルシステムを管理する」を参照してください。

2. 「ファイル」ツールボックスを選択します。
   ツールボックスのタイトルには、`Scope=Files, Policy=TSOL` が含まれています。

3. プリンタサーバーのポート **515/tcp** を使用して大域ゾーンを構成し、マルチレベル印刷を可能にします。
   ポートを大域ゾーンに追加して、プリンタサーバー用のマルチレベルポート (MLP) を作成します。

   a. 「トラステッドネットワークゾーン」ツールにナビゲートします。

   b. 「ゾーンの **IP** アドレスに対する多重レベルポート」で **515/tcp** を追加します。

   c. 「了解 **(OK)**」をクリックします。

4. 接続するプリンタの特性を定義します。

   a. 印刷マネージャーを起動します。

   b. 接続プリンタの製造業者とモデルを定義します。
      印刷マネージャーで、最初の 2 つのフィールドに値を入力すると、ドライバ名は印刷マネージャーで決定されます。

      ```
      Printer Make        manufacturer
      Printer Model       manufacturer-part-number
      Printer Driver      automatically filled in
      ```

5. プリンタサーバーに接続されている各プリンタにプリンタモデルスクリプトを割り当てます。
   モデルスクリプトが、指定したプリンタでバナーページとトレーラページをアクティブにします。

   スクリプトの選択については、220 ページの「プリンタモデルスクリプト」を参照してください。プリンタのドライバ名が `Foomatic` で始まる場合は、foomatic のモデルスクリプトを 1 つ指定します。次のコマンドを使用します。

   ```
   $ lpadmin -p printer -m model
   ```

   すべてのプリンタに対して、`ADMIN_LOW` から `ADMIN_HIGH` のデフォルトプリンタラベル範囲を使用する場合、ラベル設定はこれで完了です。

参照
- プリンタラベル範囲を制限する – 235 ページの「プリンタに制限付きのラベル範囲を構成する」
- ラベル付き出力を禁止する – 236 ページの「Trusted Extensions の印刷制限の引き下げ (作業マップ)」
- このゾーンをプリンタサーバーとして使用する – 233 ページの「Trusted Extensions クライアントがプリンタにアクセスできるようにする」
- プリンタ設定を完了する – 『System Administration Guide: Solaris Printing』の第 4 章「Setting Up Printers (Tasks)」

▼ Sun Ray クライアント用にネットワークプリンタを構成する方法

この手順では、単一の `all-zones` インタフェースを持つ Sun Ray サーバーに PostScript プリンタを構成します。このサーバーの Sun Ray クライアントのすべてのユーザーがこのプリンタを利用できます。初期構成は大域ゾーンで行われます。大域ゾーンが構成された後、各ラベル付きゾーンがこのプリンタを使用するように構成されます。

始める前に　Trusted CDE のマルチレベルセッションにログインしている必要があります。

1. 大域ゾーンでは、**Solaris** 印刷マネージャーを使用して、ネットワークプリンタに **IP** アドレスを割り当てます。
   手順については、『System Administration Guide: Solaris Printing』の第 4 章「Setting Up Printers (Tasks)」を参照してください。
2. **Solaris** 管理コンソールを起動します。
   - 手順については、『Solaris Trusted Extensions 構成ガイド』の「Trusted Extensions で Solaris 管理コンソールサーバーを初期化する」を参照してください。
   - `Scope=Files, Policy=TSOL` ツールボックスを選択し、ログインします。
3. `admin_low` テンプレートにプリンタを割り当てます。
   a. 「コンピュータとネットワーク」ツールで「セキュリティーテンプレート」をダブルクリックします。
   b. `admin_low` をダブルクリックします。
   c. 「テンプレートに割り当てるホスト」タブで、プリンタの **IP** アドレスを追加します。
      詳細は、左側の区画のオンラインヘルプを参照してください。

4 大域ゾーンの共有インタフェースにプリンタポートを追加します。

a. 「コンピュータとネットワーク」ツールで「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。

b. `global` をダブルクリックします。

c. 「共有 **IP** アドレスに対するマルチレベルポート」のリストに、ポート `515`、プロトコル `tcp` を追加します。

5 **Solaris** 管理コンソール割り当てがカーネル内にあることを確認します。

```
# tninfo -h printer-IP-address
   IP address= printer-IP-address
   Template = admin_low

# tninfo -m global
   private: 111/tcp;111/udp;513/tcp;515/tcp;631/tcp;2049/tcp;6000-6050/tcp;
7007/tcp;7010/tcp;7014/tcp;7015/tcp;32771/tcp;32776/ip
   shared: 515/tcp;6000-6050/tcp;7007/tcp;7010/tcp;7014/tcp;7015/tcp
```

注 – `6055` や `7007` などの追加のプライベートおよび共有マルチレベルポート (MLP) は、Sun Ray の要件に対応しています。

6 印刷サービスが大域ゾーンで有効になっていることを確認します。

```
# svcadm enable print/server
# svcadm enable rfc1179
```

7 システムが `netservices limited` を使用してインストールされている場合は、プリンタがネットワークにアクセスできるようにします。

`rfc1179` サービスは、`localhost` 以外のアドレスで待機する必要があります。LP サービスは名前付きパイプでのみ待機します。

```
# inetadm -m svc:/application/print/rfc1179:default bind_addr=''
# svcadm refresh rfc1179
```

注 – `netservices open` を実行している場合、前述のコマンドにより「`Error: "inetd" property group missing`」というエラーが生成されます。

8 すべてのユーザーが **PostScript** を印刷できるようにします。

トラステッドエディタで `/etc/default/print` ファイルを作成し、次の行を追加します。

```
PRINT_POSTSCRIPT=1
```

StarSuite や `gedit` などのアプリケーションでは、PostScript 出力が作成されます。

9 すべての **LP** フィルタを印刷サービスに追加します。

大域ゾーンで、次の C-Shell スクリプトを実行します。

```
csh
    cd /etc/lp/fd/
    foreach a (*.fd)
        lpfilter -f $a:r -F $a
    end
```

10 大域ゾーンにプリンタを追加します。

コマンド行を使用します。印刷マネージャーの GUI は大域ゾーンでは機能しません。

```
# lpadmin -p printer-name -v /dev/null -m tsol_netstandard \
-o protocol=tcp -o dest=printer-IP-address:9100 -T PS -I postscript
# accept printer-name
# enable printer-name
```

11 **(省略可能)** プリンタをデフォルトとして設定します。

コマンド行を使用します。印刷マネージャーの GUI は大域ゾーンでは機能しません。

```
# lpadmin -d printer-name
```

12 各ラベル付きゾーンでプリンタを構成します。

プリンタサーバーとして、大域ゾーンの `all-zones` IP アドレスを使用します。`all-zones` NIC が仮想ネットワークインタフェース (virtual network interface、vni) である場合は、`-s` オプションの引数として vni の IP アドレスを使用します。

a. ラベル付きゾーンのゾーンコンソールに **root** ユーザーとしてログインします。

```
# zlogin -C labeled-zonename
```

b. プリンタをゾーンに追加します。

```
# lpadmin -p printer-name -s global-zone-shared-IP-address
```

c. **(省略可能)** プリンタをデフォルトとして設定します。

```
# lpadmin -d printer-name
```

13 各ラベル付きゾーンで、プリンタをテストします。

- **root** ユーザーとして、`lp` コマンドとアプリケーションをテストします。

  ```
  # lp /etc/hosts
  ```

  StarSuite、ブラウザ、およびエディタを起動します。これらのアプリケーションから印刷します。カバーページ、トレーラページ、およびセキュリティーバナーが正しく印刷されることを確認します。

- ラベル付きゾーンに一般ユーザーとしてログインし、プリンタをテストします。root ユーザーとして実行したテストと同じテストを実行します。

例 15–1 ネットワークプリンタのプリンタステータスの確認

この例では、管理者は大域ゾーンとラベル付きゾーンからネットワークプリンタのステータスを確認します。

```
global # lpstat -t
    scheduler is running
    system default destination: math-printer
    system for _default: trusted1 (as printer math-printer)
    device for math-printer: /dev/null
    character set
    default accepting requests since Feb 28 00:00 2008
    lex accepting requests since Feb 28 00:00 2008
    printer math-printer is idle. enabled since Feb 28 00:00 2008. available.

Solaris1# lpstat -t
   scheduler is not running
   system default destination: math-printer
   system for _default: 192.168.4.17 (as printer math-printer)
   system for math-printer: 192.168.4.17
   default accepting requests since Feb 28 00:00 2008
   math-printer accepting requests since Feb 28 00:00 2008
   printer _default is idle. enabled since Feb 28 00:00 2008. available.
   printer math-printer is idle. enabled since Feb 28 00:00 2008. available.
```

▼ ラベル付きシステムでカスケード印刷を構成する方法

カスケード印刷では、Windows デスクトップセッションから Trusted Extensions のラベル付きゾーンインタフェースに印刷することができます。この際、物理インタフェースのゾーン IP アドレスは印刷スプーラとして動作します。物理インタフェースのゾーン IP アドレス上にあるマルチレベルポート (MLP) リスナーは、Trusted Extensions の印刷サブシステムに接続し、適切なラベルヘッダーとトレーラシートを付けてファイルを印刷します。

この手順により、ラベル付きシステムと同じサブネットにあるラベルなしシステムが、ラベル付きネットワークプリンタを使用できるようになります。`rfc1179` サービスはカスケード印刷を処理します。カスケード印刷を許可するすべてのラベル付きゾーンでこの手順を実行する必要があります。

始める前に 226 ページの「Sun Ray クライアント用にネットワークプリンタを構成する方法」の手順を完了しておきます。

1 ラベル付きゾーンのゾーンコンソールに **root** ユーザーとしてログインします。

```
# zlogin -C labeled-zonename
```

2 印刷/サーバーサービスで rfc1179 サービスの依存関係を削除します。

```
labeled-zone # cat <<EOF | svccfg
      select application/print/rfc1179
      delpg lpsched
      end
   EOF

labeled-zone # svcadm refresh application/print/rfc1179
```

3 rfc1179 サービスが有効になっていることを確認します。

```
labeled-zone # svcadm enable rfc1179
```

4 ラベル付きゾーンが netservices limited を使用してインストールされている場合は、プリンタがネットワークにアクセスできるようにします。

rfc1179 サービスは、localhost 以外のアドレスで待機する必要があります。LP サービスは名前付きパイプでのみ待機します。

```
# inetadm -m svc:/application/print/rfc1179:default bind_addr=''
# svcadm refresh rfc1179
```

注 – netservices open を実行している場合、前述のコマンドにより「Error: "inetd" property group missing」というメッセージが生成されます。

---

5 ラベル付きゾーンからカスケード印刷を構成します。

```
labeled-zone # lpset -n system -a spooling-type=cascade printer-name
```

このコマンドにより、ゾーンの /etc/printers.conf ファイルが更新されます。

6 このラベル付きゾーンと同じサブネットにある **Solaris** システムをテストします。

たとえば、Solaris1 システムをテストします。このシステムは、internal ゾーンと同じサブネットにあります。構成パラメータは次のようになります。

- math-printer の IP アドレスは 192.168.4.6 です。
- Solaris1 の IP アドレスは 192.168.4.12 です。
- internal ゾーンの IP アドレスは 192.168.4.17 です。

```
Solaris1# uname -a
SunOS Solaris1 Generic_120011-11 sun4u sparc SUNW,Sun-Blade-1000
Solaris1# lpadmin -p math-printer -s 192.168.4.17
Solaris1# lpadmin -d math-printer

Solaris1# lpstat -t
```

```
scheduler is not running
system default destination: math-printer
system for _default: 192.168.4.17 (as printer math-printer)
system for math-printer: 192.168.4.17
default accepting requests since Feb 28 00:00 2008
math-printer accepting requests since Feb 28 00:00 2008
printer _default is idle. enabled since Feb 28 00:00 2008. available.
printer math-printer is idle. enabled since Feb 28 00:00 2008. available.
```

- `lp` コマンドをテストします。

```
Solaris1# lp /etc/hosts
   request id is math-printer-1 (1 file)
```

- **StarSuite** などのアプリケーションやブラウザから印刷をテストします。

7 このラベル付きゾーンと同じサブネットにある **Windows 2003** サーバーをテストします。

a. Windows サーバーでプリンタを設定します。

「スタート」メニューの「設定」から、「プリンタと FAX」の GUI を使用します。

次のようにプリンタ構成を指定します。

- 「プリンタのインストール」
- 「このコンピュータに接続されているローカルプリンタ」
- 「新しいポートの作成」 – 「Standard TCP/IP Port」
- 「プリンタ名または IP アドレス」 – 192.168.4.17 (ラベル付きゾーンの IP アドレス)
- 「ポート名」 – デフォルトをそのまま使用
- 「ポート情報がさらに必要です」 – デフォルトをそのまま使用
  - 「デバイスの種類」 = 「カスタム」
  - 「設定」 – 「プロトコル」 = 「LPR」
  - 「LPR 設定」 – 「キュー名」 = math-printer (UNIX キュー名)
  - 「LPR バイトカウントを有効にする」

製造元、モデル、ドライバ、およびほかのプリンタパラメータを指定して、プリンタプロンプトを終了します。

8 アプリケーションからプリンタを選択して、プリンタをテストします。

たとえば、`internal` ゾーンと同じサブネットにある `winserver` システムをテストします。構成パラメータは次のようになります。

- `math-printer` の IP アドレスは 192.168.4.6 です。
- `winserver` の IP アドレスは 192.168.4.200 です。

- internal ゾーンの IP アドレスは 192.168.4.17 です。

```
winserver C:/> ipconfig
Windows IP Configuration
   Ethernet adapter TP-NIC:
      Connection-specific DNS Suffix  . :
      IP Address. . . . . . . . . . . . : 192.168.4.200
      Subnet Mask . . . . . . . . . . . : 255.255.255.0
      Default Gateway . . . . . . . . . : 192.168.4.17
```

▼ シングルラベル印刷用にゾーンを構成する

始める前に　ゾーンは、大域ゾーンと IP アドレスを共有しないようにします。大域ゾーンで、システム管理者役割になっている必要があります。

1. ワークスペースを追加します。

   詳細は、『Solaris Trusted Extensions ユーザーズガイド』の「特定のラベルのワークスペースを追加する」を参照してください。

2. 新しいワークスペースのラベルを、そのラベルのプリンタサーバーとなるゾーンのラベルに変更します。

   詳細は、『Solaris Trusted Extensions ユーザーズガイド』の「ワークスペースのラベルを変更する」を参照してください。

3. 接続するプリンタの特性を定義します。

   a. ゾーンのラベルで、印刷マネージャーを起動します。

      デフォルトでは、「PPD を使用」チェックボックスにチェックが付いています。システムで、プリンタの適切なドライバが検出されます。

   b. (省略可能) 異なるプリンタドライバを指定する場合は、次のようにします。

      i. 「PPD を使用」のチェックを外します。

      ii. 異なるドライバを使用するプリンタの製造業者とモデルを定義します。

      印刷マネージャーで、最初の 2 つのフィールドに値を入力すると、ドライバ名は印刷マネージャーで決定されます。

      ```
      Printer Make      manufacturer
      Printer Model     manufacturer-part-number
      Printer Driver    automatically filled in
      ```

4 ゾーンに接続されている各プリンタにプリンタモデルスクリプトを割り当てます。

モデルスクリプトが、指定したプリンタでバナーページとトレーラページをアクティブにします。

スクリプトの選択については、220 ページの「プリンタモデルスクリプト」を参照してください。プリンタのドライバ名が `Foomatic` で始まる場合は、foomatic のモデルスクリプトを 1 つ指定します。次のコマンドを使用します。

```
$ lpadmin -p printer -m model
```

接続されているプリンタは、そのゾーンのラベルでのみジョブを印刷できます。

参照
- ラベル付き出力を禁止する – 236 ページの「Trusted Extensions の印刷制限の引き下げ (作業マップ)」
- このゾーンをプリンタサーバーとして使用する – 233 ページの「Trusted Extensions クライアントがプリンタにアクセスできるようにする」
- プリンタ設定を完了する – 『System Administration Guide: Solaris Printing』の第 4 章「Setting Up Printers (Tasks)」

▼ Trusted Extensions クライアントがプリンタにアクセスできるようにする

初期設定では、プリンタサーバーが構成されているゾーンしかそのプリンタサーバーのプリンタに出力できません。ほかのゾーンおよびほかのシステムについては、システム管理者がそれらのプリンタへのアクセスを明示的に追加する必要があります。次のような場合が考えられます。

- 大域ゾーンについては、異なるシステムの大域ゾーンに接続されているプリンタへのアクセスを追加します。
- ラベル付きゾーンについては、そのシステムの大域ゾーンに接続されているプリンタへのアクセスを追加します。
- ラベル付きゾーンについては、同じラベルの遠隔ゾーンが構成されているプリンタへのアクセスを追加します。
- ラベル付きゾーンについては、異なるシステムの大域ゾーンに接続されているプリンタへのアクセスを追加します。

始める前に ラベル範囲またはシングルラベルでプリンタサーバーが構成されており、それに接続されたプリンタが構成されています。詳細は、次を参照してください。

- 224 ページの「マルチレベルプリンタサーバーとそのプリンタを構成する」
- 232 ページの「シングルラベル印刷用にゾーンを構成する」
- 237 ページの「ラベルなしのプリンタサーバーにラベルを割り当てる」

大域ゾーンでシステム管理者役割であるか、その役割になれる必要があります。

- システムがプリンタにアクセスできるようにする手順を完了します。

  `lpadmin` コマンドの代わりに印刷マネージャーを使用する場合は、例 15–2 を参照してください。

  - プリンタサーバーではないシステム上の大域ゾーンが、プリンタアクセスのためにほかのシステムの大域ゾーンを使用するように構成します。

    a. プリンタにアクセスできないシステムで、システム管理者役割になります。

    b. **Trusted Extensions** のプリンタサーバーに接続されているプリンタへのアクセスを追加します。

    ```
    $ lpadmin -s printer
    ```

  - ラベル付きゾーンが大域ゾーンを使ってプリンタにアクセスできるように構成します。

    a. 役割ワークスペースのラベルを、ラベル付きゾーンのラベルに変更します。

    詳細は、『Solaris Trusted Extensions ユーザーズガイド』の「ワークスペースのラベルを変更する」を参照してください。

    b. プリンタへのアクセスを追加します。

    ```
    $ lpadmin -s printer
    ```

  - ラベル付きのゾーンがほかのシステムのラベル付きゾーンを使ってプリンタにアクセスできるようにします。

    ゾーンのラベルは同一である必要があります。

    a. プリンタにアクセスできないシステムで、システム管理者役割になります。

    b. 役割ワークスペースのラベルを、ラベル付きゾーンのラベルに変更します。

    c. 遠隔のラベル付きゾーンのプリンタサーバーに接続されているプリンタへのアクセスを追加します。

    ```
    lpadmin -s printer
    ```

  - ラベル付きのゾーンが、ラベルなしプリンタサーバーを使ってプリンタにアクセスできるようにします。

    ゾーンのラベルは、プリンタサーバーのラベルと同一である必要があります。

    a. プリンタにアクセスできないシステムで、システム管理者役割になります。

b. 役割ワークスペースのラベルを、ラベル付きゾーンのラベルに変更します。
詳細は、『Solaris Trusted Extensions ユーザーズガイド』の「ワークスペースのラベルを変更する」を参照してください。

c. 任意のラベル付きのプリンタサーバーに接続されているプリンタへのアクセスを追加します。

```
$ lpadmin -s printer
```

例 15–2 印刷マネージャーを使用してプリンタへのアクセスを可能にする

lpadmin コマンドを使う代わりに、印刷マネージャーから「プリンタ」–>「プリンタへのアクセスを追加」を選択します。印刷マネージャーは、lpadmin -s *printer* コマンドと同じラベル、同じゾーンで起動してください。

▼ プリンタに制限付きのラベル範囲を構成する

プリンタのラベル範囲はデフォルトで ADMIN_LOW から ADMIN_HIGH までです。この手順では、Trusted Extensions のプリンタサーバーで制御されるプリンタのラベル範囲を狭めます。

始める前に 大域ゾーンでセキュリティー管理者役割になります。

1. デバイス割り当てマネージャーを起動します。
   - トラステッドパスメニューから「デバイスを割り当てる **(Allocate Device)**」オプションを選択します。
   - **Trusted CDE** では、フロントパネルの「ツール」サブパネルから「デバイス割り当てマネージャー」アクションを起動します。
2. 「デバイス管理」ボタンをクリックして、「デバイス割り当て」の「管理」ダイアログボックスを開きます。
3. 新しいプリンタの名前を入力します。
   システムにプリンタが接続されている場合は、プリンタの名前を検出します。
4. 「構成」ボタンをクリックして、「デバイス割り当て」の「構成」ダイアログボックスを開きます。

5 プリンタのラベル範囲を変更します。

a. 「最小ラベル」ボタンをクリックして、最小ラベルを変更します。
ラベルビルダーからラベルを選択します。ラベルビルダーの詳細は、45 ページの「Trusted Extensions のラベルビルダー」を参照してください。

b. 「最大ラベル」ボタンをクリックして、最大ラベルを変更します。

6 変更を保存します。

a. 「構成」ダイアログボックスの「了解」をクリックします。

b. 「管理」ダイアログボックスの「了解」をクリックします。

7 デバイス割り当てマネージャーを閉じます。

Trusted Extensions の印刷制限の引き下げ (作業マップ)

以下のタスクは省略可能です。これらの手順では、Trusted Extensions のインストール時にデフォルトで設定される印刷のセキュリティーを引き下げます。

作業	説明	参照先
出力にラベルを付けないようプリンタを構成します。	本文ページにセキュリティー情報が印刷されないようにし、バナーページとトレーラページを削除します。	237 ページの「印刷出力からラベルを削除する」
シングルラベルでのプリンタをラベルなし出力に構成します。	特定のラベルで Solaris のプリンタに出力できるようにします。印刷ジョブはラベルでマークされません。	237 ページの「ラベルなしのプリンタサーバーにラベルを割り当てる」
本文ページの表示可能なラベルを削除します。	`tsol_separator.ps` ファイルを修正して、Trusted Extensions ホストから送信されるすべての印刷ジョブで、本文ページにラベルを付けないようにします。	238 ページの「すべての印刷ジョブからページラベルを削除する」
バナーページとトレーラページを抑制します。	特定のユーザーに、バナーページとトレーラページのないジョブの印刷を許可します。	240 ページの「特定のユーザーに対してバナーページとトレーラページを抑制する」
信頼できるユーザーにラベルなしのジョブを印刷できるようにします。	特定のユーザーまたは特定システムのすべてのユーザーに、ラベルなしのジョブの印刷を許可します。	239 ページの「特定のユーザーがページラベルを抑制できるようにする」

作業	説明	参照先
PostScript ファイルを印刷できるようにします。	特定のユーザーまたは特定システムのすべてのユーザーに、PostScript ファイルの印刷を許可します。	240 ページの「Trusted Extensions でユーザーが PostScript ファイルを印刷できるようにする」
印刷承認を割り当てます。	ユーザーがデフォルトの印刷制限をバイパスできるようにします。	98 ページの「便利な承認のための権利プロファイルを作成する」 89 ページの「policy.conf のデフォルトを修正する」

▼ 印刷出力からラベルを削除する

Trusted Extensions プリンタモデルスクリプトを持たないプリンタは、ラベル付きのバナーページまたはトレーラページを印刷しません。本文ページにもラベルは含まれません。

始める前に　大域ゾーンでセキュリティー管理者役割になります。

- 適切なラベルで、次のいずれかの操作を行います。
  - プリンタサーバーから、バナーの印刷を完全に停止します。

    ```
    % lpadmin -p printer -o nobanner=never
    ```

    本文ページにはまだラベルが付いたままです。
  - プリンタモデルスクリプトを **Solaris** スクリプトに設定します。

    ```
    % lpadmin -p printer  \
    -m { standard | netstandard | standard_foomatic | netstandard_foomatic }
    ```

    印刷出力にはラベルが表示されません。

▼ ラベルなしのプリンタサーバーにラベルを割り当てる

Solaris プリンタサーバーはラベルなしのプリンタサーバーですが、ラベルを割り当てることによって、Trusted Extensions がそのラベルでプリンタにアクセスできるようになります。ラベルなしのプリンタサーバーに接続されているプリンタは、そのプリンタサーバーに割り当てられているラベルでしかジョブを印刷できません。ジョブはラベルまたはトレーラページなしで印刷され、バナーページなしの場合もあります。ジョブがバナーページ付きで印刷される場合でも、そのページにセキュリティー情報は含まれません。

Trusted Extensions システムは、ラベルなしのプリンタサーバーで管理されるプリンタにジョブを送信するように構成することができます。ユーザーは、セキュリティー管理者がプリンタサーバーに割り当てたラベルでは、ラベルなしのプリンタでジョブを印刷できます。

始める前に　大域ゾーンでセキュリティー管理者役割になります。

1. 適切な有効範囲で **Solaris** 管理コンソールを開きます。
   詳細は、『Solaris Trusted Extensions 構成ガイド』の「Trusted Extensions で Solaris 管理コンソールサーバーを初期化する」を参照してください。
2. 「システム構成」で「コンピュータとネットワーク」ツールにナビゲートします。
   求められたらパスワードを入力します。
3. プリンタサーバーにラベルなしテンプレートを割り当てます。
   詳細は、193 ページの「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。
   ラベルを選択します。そのラベルで作業しているユーザーは、プリンタサーバーのラベルで Solaris プリンタに印刷ジョブを送信できます。ページはラベル付きで印刷されず、バナーページとトレーラページも印刷ジョブに含まれません。

例 15–3　ラベルなしプリンタへの公共印刷ジョブの送信

不特定多数の人が利用できるファイルは、ラベルなしプリンタでの印刷に適しています。この例では、マーケティングライターが、ページの最上部と最下部にラベルの印刷されない文書を作成しなければなりません。

セキュリティー管理者は、Solaris プリンタサーバーに、ラベルなしホストタイプのテンプレートを割り当てます。テンプレートについては、例 13–6 で説明されています。テンプレートの任意のラベルは `PUBLIC` です。このプリンタサーバーには、プリンタ `pr-nolabel1` が接続されています。`PUBLIC` ゾーンのユーザーからの印刷ジョブは、ラベルなしで `pr-nolabel1` プリンタ上で印刷されます。プリンタの設定によって、ジョブにはバナーページがあることもないこともあります。バナーページにセキュリティー情報は含まれません。

▼ すべての印刷ジョブからページラベルを削除する

この手順では、Trusted Extensions のプリンタでのすべての印刷ジョブで本文ページにラベルが表示されないようにします。

始める前に　大域ゾーンでセキュリティー管理者役割になります。

1 /usr/lib/lp/postscript/tsol_separator.ps ファイルを編集します。

トラステッドエディタを使用します。詳細は、59 ページの「Trusted Extensions の管理ファイルを編集する」を参照してください。

2 /PageLabel の定義を検索します。

検索するのは次の行です。

```
%% To eliminate page labels completely, change this line to
%% set the page label to an empty string: /PageLabel () def
/PageLabel Job_PageLabel def
```

注 – 値 Job_PageLabel は、サイトによって異なります。

---

3 /PageLabel の値を、1 組の空の括弧に置き換えます。

```
/PageLabel () def
```

▼ 特定のユーザーがページラベルを抑制できるようにする

この手順では、Trusted Extensions プリンタで、承認ユーザーまたは役割が各本文ページの最上部と最下部にラベルのないジョブを印刷できるようにします。ユーザーが作業できるすべてのラベルで、ページラベルが抑制されます。

始める前に 大域ゾーンでセキュリティー管理者役割になります。

1 ページラベルなしでジョブを印刷できるユーザーを特定します。

2 これらのユーザーおよび役割に、ページラベルなしでジョブを印刷できるよう許可します。

「ラベルなしで印刷」承認を含む権利プロファイルを、これらのユーザーおよび役割に割り当てます。詳細は、98 ページの「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。

3 ユーザーまたは役割に対し、印刷ジョブの送信時に lp コマンドを使用するように指示します。

```
% lp -o nolabels staff.mtg.notes
```

▼ 特定のユーザーに対してバナーページとトレーラページを抑制する

始める前に　「印刷マネージャー」ダイアログボックスの「バナーを常に印刷」チェックボックスには、チェックが付いていません。

大域ゾーンでセキュリティー管理者役割になります。

1. 「バナーなしで印刷」承認を含む権利プロファイルを作成します。
   バナーページとトレーラページなしの印刷を許可されている各ユーザーまたは役割に、そのプロファイルを割り当てます。
   詳細は、98 ページの「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。
2. ユーザーまたは役割に対し、印刷ジョブの送信時に `lp` コマンドを使用するように指示します。

```
% lp -o nobanner staff.mtg.notes
```

▼ Trusted Extensions でユーザーが PostScript ファイルを印刷できるようにする

始める前に　大域ゾーンでセキュリティー管理者役割になります。

- 次の 3 つの方法のいずれかで、ユーザーが PostScript ファイルを印刷できるようにします。
  - システムで PostScript 印刷を実行できるようにするには、`/etc/default/print` ファイルを修正します。
    a. `/etc/default/print` ファイルを作成または修正します。
       トラステッドエディタを使用します。詳細は、59 ページの「Trusted Extensions の管理ファイルを編集する」を参照してください。
    b. 次のエントリを入力します。

```
PRINT_POSTSCRIPT=1
```

c. ファイルを保存してエディタを終了します。

- すべてのユーザーがシステムから **PostScript** ファイルを印刷できるようにするには、`/etc/security/policy.conf` ファイルを修正します。

  a. `policy.conf` ファイルを修正します。
  トラステッドエディタを使用します。詳細は、59 ページの「Trusted Extensions の管理ファイルを編集する」を参照してください。

  b. `solaris.print.ps` 承認を追加します。
  `AUTHS_GRANTED=`*other-authorizations*`,solaris.print.ps`

  c. ファイルを保存してエディタを終了します。

- ユーザーまたは役割が任意のシステムから **PostScript** ファイルを印刷できるようにするには、そのユーザーまたは役割に適切な承認を付与します。
  「`Print Postscript`」承認を含むプロファイルを、これらのユーザーおよび役割に割り当てます。詳細は、98 ページの「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。

例 15–4 Public システムから PostScript 印刷を可能にする

次の例でセキュリティー管理者は、Public システムでの操作を `PUBLIC` ラベルに限定しています。システムには、興味のあるトピックを開くアイコンもあります。これらのトピックも印刷可能です。

セキュリティー管理者は、システムに `/etc/default/print` ファイルを作成します。このファイルには、PostScript ファイルの印刷を許可する 1 つのエントリだけがあります。ユーザーに「`Print Postscript`」承認は不要です。

```
# vi /etc/default/print

# PRINT_POSTSCRIPT=0
PRINT_POSTSCRIPT=1
```

◆ ◆ ◆ 第 16 章

Trusted Extensions のデバイス (概要)

この章では、Solaris Trusted Extensions で Solaris デバイスの保護に使用される拡張機能について説明します。

Trusted Extensions ソフトウェアによるデバイス保護

Solaris システムでは、割り当てと承認によってデバイスを保護することができます。デフォルトでは、デバイスは承認のない一般ユーザーにも利用可能です。Trusted Extensions ソフトウェアが設定されたシステムは、Solaris OS のデバイス保護メカニズムを使用します。

ただし、Trusted Extensions の場合、デフォルトでは、デバイスを使用するには割り当てが必要であり、デバイスを使用するユーザーに承認が必要です。さらに、デバイスはラベルによっても保護されます。Trusted Extensions には、デバイスを管理する管理者向けのグラフィカルユーザーインタフェース (GUI) が用意されています。ユーザーがデバイスを割り当てる際にも、同じインタフェースを使用します。

注 – Trusted Extensions では、ユーザーは `allocate` コマンドと `deallocate` コマンドを使用できません。ユーザーは、デバイス割り当てマネージャーを使用する必要があります。Solaris Trusted Extensions (JDS) では、GUI のタイトルはデバイスマネージャーです。

Solaris OS でのデバイス保護については、『System Administration Guide: Security Services』の第 4 章「Controlling Access to Devices (Tasks)」を参照してください。

Trusted Extensions が設定されたシステムでは、2 つの役割がデバイスを保護します。

- システム管理者役割は、周辺機器へのアクセスを制御します。

  システム管理者は、デバイスを割り当て可能にします。システム管理者が割り当て不可に設定したデバイスは、どのユーザーも使用できません。割り当て可能なデバイスは、承認ユーザーによってのみ割り当てられます。
- セキュリティー管理者役割は、デバイスにアクセスできるラベルを制限し、デバイスポリシーを設定します。セキュリティー管理者は、デバイス割り当てを承認されるユーザーを決定します。

Trusted Extensions ソフトウェアによるデバイス制御の主な機能は、次のとおりです。

- デフォルトでは、Trusted Extensions システムの未承認ユーザーは、テープドライブ、CD-ROM ドライブ、フロッピーディスクドライブなどのデバイスを割り当てることができません。

  「デバイスの割り当て」承認を持つ一般ユーザーは、そのユーザーがデバイスを割り当てるラベルで情報をインポートまたはエクスポートすることができます。
- ユーザーが直接ログインしている場合は、デバイス割り当てマネージャーを起動してデバイスを割り当てます。デバイスを遠隔で割り当てるには、ユーザーが大域ゾーンにアクセスできる必要があります。通常は、役割だけが大域ゾーンにアクセスできます。
- 各デバイスのラベル範囲は、セキュリティー管理者によって制限されます。一般ユーザーがアクセスできるのは、そのユーザーが作業を許可されているラベルを含むラベル範囲を持つデバイスだけです。デバイスのデフォルトのラベル範囲は、`ADMIN_LOW` から `ADMIN_HIGH` までです。
- 割り当て可能なデバイスにも、割り当て不可のデバイスにも、ラベル範囲を制限することができます。割り当て不可のデバイスは、フレームバッファーやプリンタなどのデバイスです。

デバイスのラベル範囲

ユーザーが機密情報をコピーできないように、割り当て可能な各デバイスにはラベル範囲があります。割り当て可能なデバイスを使用するには、ユーザーが現在そのデバイスのラベル範囲で操作している必要があります。それ以外のユーザーには、割り当てが拒否されます。ユーザーの現在のラベルは、デバイスがそのユーザーに割り当てられている間にインポートまたはエクスポートされるデータに適用されます。エクスポートされたデータのラベルは、デバイスが割り当て解除されるときに表示されます。エクスポートされたデータを含むメディアには、ユーザーが物理的にラベルを付ける必要があります。

デバイスに対するラベル範囲の効果

コンソールによる直接ログインアクセスを制限するために、セキュリティー管理者はフレームバッファーに制限付きのラベル範囲を設定することができます。

たとえば、制限付きのラベル範囲を指定して、公共アクセス可能なシステムへのアクセスを制限することもできます。ラベル範囲を使用すると、ユーザーはそのフレームバッファーのラベル範囲内でのみシステムにアクセスできるようになります。

ホストにローカルプリンタがある場合、プリンタに制限付きのラベル範囲を設定することによって、プリンタで印刷できるジョブを制限できます。

デバイスアクセスポリシー

Trusted Extensions は、Solaris OS と同じデバイスポリシーに従います。セキュリティー管理者は、デフォルトのポリシーを変更し、新しいポリシーを定義することができます。`getdevpolicy` コマンドでデバイスポリシーに関する情報を取り出し、`update_drv` コマンドでデバイスポリシーを変更します。詳細は、『System Administration Guide: Security Services』の「Configuring Device Policy (Task Map)」を参照してください。`getdevpolicy(1M)` および `update_drv(1M)` のマニュアルページも参照してください。

デバイスクリーンスクリプト

デバイスクリーンスクリプトは、デバイスを割り当てるとき、または割り当て解除するときに実行されます。Solaris OS には、テープドライブ、CD-ROM ドライブ、およびフロッピーディスクドライブ用のスクリプトが用意されています。サイトで割り当て可能なデバイスタイプをシステムに追加した場合、追加したデバイスにスクリプトが必要な場合があります。既存のスクリプトを確認する場合は、`/etc/security/lib` ディレクトリに移動します。詳細は、『System Administration Guide: Security Services』の「Device-Clean Scripts」を参照してください。

Trusted Extensions ソフトウェアの場合、デバイスクリーンスクリプトは一定の要件を満たさなくてはなりません。この要件については、`device_clean(5)` のマニュアルページを参照してください。

デバイス割り当てマネージャー GUI

デバイス割り当てマネージャーは、割り当て可能デバイスと割り当て不可デバイスを管理する際に管理者が使用します。一般ユーザーがデバイスを割り当てる、または割り当て解除するときにもデバイス割り当てマネージャーを使用します。ユーザーには、「デバイスの割り当て」承認が必要です。Solaris Trusted Extensions (CDE) ワークスペースでは、デバイス割り当てマネージャーはフロントパネルから開きます。アイコンは次のように表示されます。

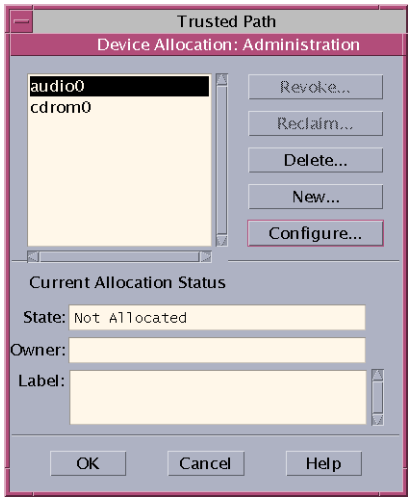
デバイス割り当て 

Solaris Trusted Extensions (JDS) ワークスペースでは、GUI はデバイスマネージャーと呼ばれます。この GUI は、トラステッドパスメニューから「デバイスの割り当て」を選択することによって起動します。Trusted CDE では、トラステッドパスメニューから GUI を起動することもできます。次の図は、`audio` デバイスを割り当てることのできるユーザーがデバイス割り当てマネージャーを開いたところです。

図 16–1 ユーザーが開いたデバイス割り当てマネージャー

デバイスの割り当てを承認されていないユーザーには、空のリストが表示されます。または、リストが空の場合、割り当て可能なデバイスが現在ほかのユーザーによって割り当てられているか、エラー状態である可能性もあります。「使用可能デバイス」リストにデバイスが表示されない場合、ユーザーは責任管理者に連絡する必要があります。

デバイス管理機能は、デバイスの管理に必要な承認を 1 つまたは両方持っている役割が使用できます。管理に必要な承認は、「デバイス属性の構成」と「デバイスの解除または再利用」です。次の図は、「デバイスの割り当て管理」ダイアログボックスを示したものです。



Solaris Trusted Extensions (JDS) では、「デバイス管理」ボタンは「管理」と呼ばれます。

Trusted Extensions でのデバイスセキュリティーの実施

セキュリティー管理者は、デバイスを割り当てることのできるユーザーを決定し、デバイスの使用を承認されているユーザーがトレーニングを受けていることを確認します。ユーザーは、次の操作を行うと信頼されています。

- 機密情報が不正なユーザーに利用されることのないよう、エクスポートされた機密情報を含むメディアを適切にラベル付けし、扱うこと。

  たとえば、NEED TO KNOW ENGINEERING のラベルの情報がフロッピーディスクに保存される場合、その情報をエクスポートしたユーザーはそのディスクに NEED TO KNOW ENGINEERING という物理的なラベルを付けてください。フロッピーディスクは、この情報を知る必要のあるエンジニアグループのメンバーだけがアクセスできる場所に保管する必要があります。
- これらのデバイス上のメディアからインポートされる (読み込まれる) 情報について、ラベルが適切に管理されるようにすること。

  承認ユーザーは、インポートする情報と同じラベルでデバイスを割り当てる必要があります。たとえば、PUBLIC でフロッピーディスクドライブを割り当てる場合、そのユーザーは PUBLIC というラベルの情報だけをインポートしてください。

セキュリティー管理者は、セキュリティー要件の適切な遵守についても責任があります。

Trusted Extensions のデバイス (リファレンス)

Trusted Extensions のデバイス保護では、Solaris インタフェースと Trusted Extensions インタフェースを使用します。

Solaris のコマンド行インタフェースについては、『System Administration Guide: Security Services』の「Device Protection (Reference)」を参照してください。

デバイス割り当てマネージャーにアクセスできない管理者は、コマンド行を使用して割り当て可能デバイスを管理できます。allocate コマンドと deallocate コマンドには、管理用のオプションがあります。たとえば、『System Administration Guide: Security Services』の「Forcibly Allocating a Device」と『System Administration Guide: Security Services』の「Forcibly Deallocating a Device」を参照してください。

Trusted Extensions のコマンド行インタフェースについては、add_allocatable(1M) および remove_allocatable(1M) のマニュアルページを参照してください。

◆ ◆ ◆ 第 17 章

Trusted Extensions でのデバイス管理 (手順)

この章では、Solaris Trusted Extensions が設定されたシステムでデバイスを管理し使用する方法について説明します。

Trusted Extensions でのデバイスの扱い (作業マップ)

周辺機器を取り扱う管理者とユーザーの作業マップは、次のとおりです。

作業	説明	参照先
デバイスを使用します。	役割として、または一般ユーザーとしてデバイスを使用します。	250 ページの「Trusted Extensions でのデバイスの使用法 (作業マップ)」
デバイスを管理します。	一般ユーザーのためにデバイスを構成します。	250 ページの「Trusted Extensions でのデバイスの管理 (作業マップ)」
デバイス承認をカスタマイズします。	セキュリティー管理者役割が、新しい承認を作成してデバイスにその承認を追加し、承認を権利プロファイルに配置して、このプロファイルをユーザーに割り当てます。	260 ページの「Trusted Extensions でのデバイス承認のカスタマイズ (作業マップ) 」

Trusted Extensions でのデバイスの使用法 (作業マップ)

Trusted Extensions では、すべての役割がデバイスの割り当てを承認されています。ユーザーと同様、役割もデバイス割り当てマネージャーを使う必要があります。Solaris の `allocate` コマンドは、Trusted Extensions では機能しません。ユーザーがデバイスを使用して管理タスクを行う手順は、次の作業マップのとおりです。

作業	参照先
デバイスの割り当ておよび割り当ての解除を行います。	『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」 『Solaris Trusted Extensions ユーザーズガイド』の「ワークスペーススイッチ領域」
ポータブルメディアを使用してファイルを転送します。	『Solaris Trusted Extensions 構成ガイド』の「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」 『Solaris Trusted Extensions 構成ガイド』の「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」

Trusted Extensions でのデバイスの管理 (作業マップ)

次の作業マップでは、サイトのデバイスを保護する手順について説明します。

作業	説明	参照先
デバイスポリシーを設定または修正します。	デバイスへのアクセスに必要な特権を変更します。	『System Administration Guide: Security Services』の「Configuring Device Policy (Task Map)」
ユーザーによるデバイス割り当てを承認します。	セキュリティー管理者役割が、「デバイスの割り当て」承認のあるプロファイルをユーザーに割り当てます。	『System Administration Guide: Security Services』の「How to Authorize Users to Allocate a Device」
	セキュリティー管理者役割が、サイト固有の承認のあるプロファイルをユーザーに割り当てます。	260 ページの「Trusted Extensions でのデバイス承認のカスタマイズ (作業マップ)」
デバイスを構成します。	セキュリティー機能を選択してデバイスを保護します。	251 ページの「Trusted Extensions でデバイスを構成する」

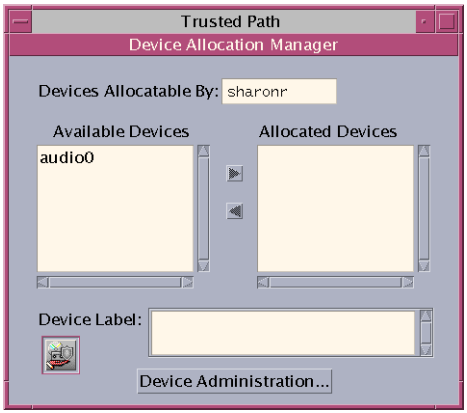
作業	説明	参照先
デバイスを解除または再利用します。	デバイス割り当てマネージャーを使用して、デバイスを利用できるようにします。	254 ページの「Trusted Extensions でデバイスを解除または再利用する」
	Solaris コマンドを使用して、デバイスを利用可能または利用不可にします。	『System Administration Guide: Security Services』の「Forcibly Allocating a Device」 『System Administration Guide: Security Services』の「Forcibly Deallocating a Device」
割り当て可能なデバイスへのアクセスを禁止します。	デバイスへのきめ細かいアクセス制御を提供します。	例 17–4
	割り当て可能なデバイスへのすべてのアクセスを禁止します。	例 17–1
プリンタとフレームバッファーを保護します。	割り当て不可のデバイスが割り当て可能にならないようにします。	255 ページの「Trusted Extensions で割り当て不可のデバイスを保護する」
シリアルログインデバイスを構成します。	シリアルポートによるログインを可能にします。	256 ページの「ログイン用のシリアル回線を構成する」
CD プレイヤプログラムを使用可能にします。	音楽 CD を挿入したときにオーディオプレイヤプログラムが自動的に開くようにします。	257 ページの「Trusted CDE でオーディオプレイヤプログラムを使用できるように構成する」
ファイルマネージャーの表示を禁止します。	デバイスの割り当て後にファイルマネージャーが表示されないようにします。	258 ページの「デバイスの割り当て後にファイルマネージャーが表示されないようにする」
新しいデバイスクリーンスクリプトを使用します。	新しいスクリプトを適切な場所に配置します。	259 ページの「Trusted Extensions で Device_Clean スクリプトを追加する」

▼ Trusted Extensions でデバイスを構成する

デフォルトで割り当て可能なデバイスは、ラベル範囲が `ADMIN_LOW` から `ADMIN_HIGH` であり、使用するには割り当てられる必要があります。また、ユーザーはデバイス割り当てを承認されている必要があります。これらのデフォルトは、変更可能です。

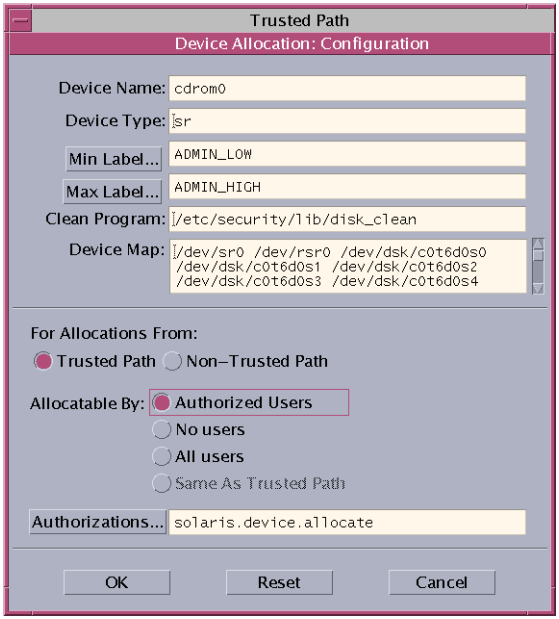
始める前に　大域ゾーンでセキュリティー管理者役割になります。

1. 「トラステッドパス」メニューから「デバイスの割り当て」を選択します。
   デバイス割り当てマネージャーが表示されます。



2 デフォルトのセキュリティー設定を表示します。

「デバイス管理」をクリックして、デバイスを強調表示します。次の図は、CD-ROM ドライブのデフォルトのセキュリティー設定を示しています。



3 (省略可能) デバイスのラベル範囲を制限します。

a. 最小ラベルを設定します。

「最小ラベル...」ボタンをクリックします。ラベルビルダーから最小ラベルを選択します。ラベルビルダーの詳細は、45 ページの「Trusted Extensions のラベルビルダー」を参照してください。

b. 最大ラベルを設定します。

「最大ラベル...」ボタンをクリックします。ラベルビルダーから最大ラベルを選択します。

4 デバイスがローカルに割り当て可能かどうかを指定します。

「トラステッドパスからの割り当て」の「デバイス割り当て構成」ダイアログボックスで、「割り当てを行えるユーザー」リストからオプションを選択します。デフォルトでは、「承認されたユーザー」オプションがチェックされています。したがって、デバイスは割り当て可能であり、ユーザーは承認が必要です。

- デバイスを割り当て不可にするには、「なし」をクリックします。

  プリンタ、フレームバッファーなど、割り当て可能にしてはいけないデバイスを構成する場合は、「なし」を選択します。

- デバイスを割り当て可能だが承認不要にするには、「すべてのユーザー」をクリックします。

5 デバイスが遠隔で割り当て可能かどうかを指定します。

「信頼できないパスからの割り当て」セクションで、「割り当てを行えるユーザー」リストからオプションを選択します。デフォルトでは、「トラステッドパスと同じ」オプションがチェックされています。

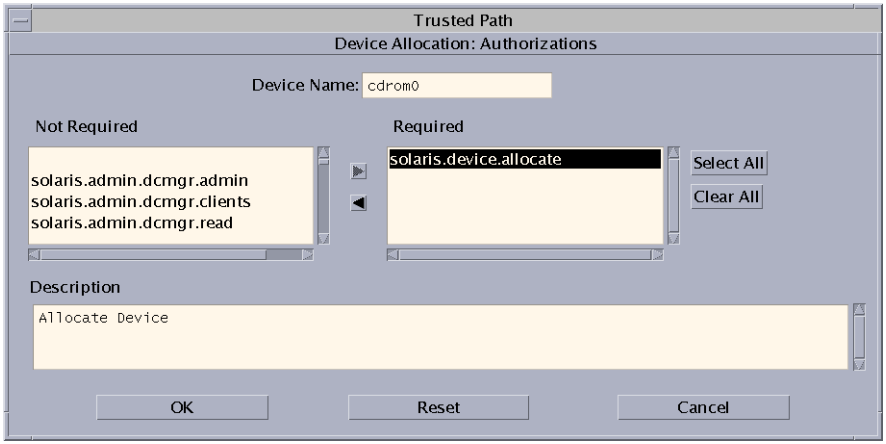
- ユーザー承認を必要にするには、「承認されたユーザーによって割り当て可能」を選択します。

- 遠隔ユーザーによる割り当てを不可にするには、「なし」を選択します。

- 任意のユーザーがデバイスを割り当てできるようにするには、「すべてのユーザー」を選択します。

6 デバイスが割り当て可能であり、かつサイトで新しいデバイス承認を作成してある場合、適切な承認を選択します。

次のダイアログボックスは、`cdrom0` デバイスを割り当てるために `solaris.device.allocate` 承認が必要であることを示しています。



サイト固有のデバイス承認の作成と使用法については、260 ページの「Trusted Extensions でのデバイス承認のカスタマイズ (作業マップ)」を参照してください。

7 「了解」をクリックして変更を保存します。

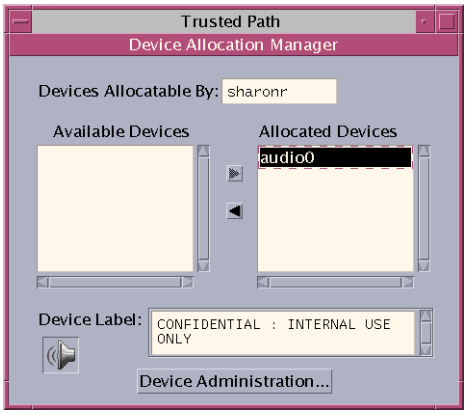
▼ Trusted Extensions でデバイスを解除または再利用する

デバイスがデバイス割り当てマネージャーに表示されていない場合、すでに割り当てられているか、割り当てエラー状態である可能性があります。システム管理者は、利用できるようにデバイスを回復することができます。

始める前に 大域ゾーンで、システム管理者役割になっている必要があります。この役割には、`solaris.device.revoke` 承認が含まれています。

1 「トラステッドパス」メニューから「デバイスの割り当て」を選択します。

次の図では、オーディオデバイスがすでにユーザーに割り当てられています。



2 「デバイス管理」ボタンをクリックします。

3 デバイスの状態をチェックします。
デバイス名を選択し、「状態」フィールドを確認します。

- 「状態」フィールドが「割り当てエラーの状態」の場合は、「再利用」ボタンをクリックします。
- 「状態」フィールドが「割り当て済み」の場合は、次のいずれかの操作を行います。
  - 「所有者」フィールドのユーザーに、デバイスの割り当て解除を依頼する。
  - 「解除」ボタンを押して、デバイスを強制的に割り当て解除する。

4 デバイス割り当てマネージャーを閉じます。

▼ Trusted Extensions で割り当て不可のデバイスを保護する

「デバイス割り当て: 構成」ダイアログボックスの「割り当てを行えるユーザー」セクションの「なし」オプションは、フレームバッファーとプリンタでもっとも頻繁に使用されます。これらのデバイスは割り当てせずに利用できるからです。

始める前に 大域ゾーンでセキュリティー管理者役割になります。

1 「トラステッドパス」メニューから「デバイスの割り当て」を選択します。

2 デバイス割り当てマネージャーで、「デバイス管理」ボタンをクリックします。

3 新しいプリンタまたはフレームバッファーを選択します。

a. デバイスを割り当て不可にするには、「なし」をクリックします。

b. (省略可能) デバイスのラベル範囲を制限します。

i. 最小ラベルを設定します。

「最小ラベル...」ボタンをクリックします。ラベルビルダーから最小ラベルを選択します。ラベルビルダーの詳細は、45 ページの「Trusted Extensions のラベルビルダー」を参照してください。

ii. 最大ラベルを設定します。

「最大ラベル...」ボタンをクリックします。ラベルビルダーから最大ラベルを選択します。

例 17–1 オーディオデバイスの遠隔割り当ての禁止

「割り当てを行えるユーザー」セクションの「なし」オプションを使用すると、遠隔ユーザーは遠隔システム周辺の会話を聞くことができません。

セキュリティー管理者は、デバイス割り当てマネージャーで次のようにオーディオデバイスを構成します。

```
Device Name: audio
For Allocations From: Trusted Path
Allocatable By: Authorized Users
Authorizations: solaris.device.allocate

Device Name: audio
For Allocations From: Non-Trusted Pathh
Allocatable By: No Users
```

▼ ログイン用のシリアル回線を構成する

始める前に 大域ゾーンでセキュリティー管理者役割になります。

1 ファイルの有効範囲で **Solaris** 管理コンソールを開きます。

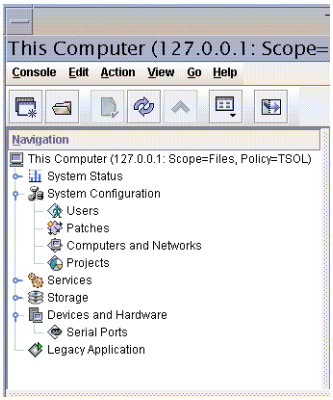


図 17–1 Solaris 管理コンソールのシリアルポートツール

2 「デバイスおよびハードウェア」で、「シリアルポート」にナビゲートします。

求められたらパスワードを入力します。 オンラインヘルプに従って、シリアルポートを構成します。

3 デフォルトのラベル範囲を変更するには、デバイス割り当てマネージャーを開きます。

デフォルトのラベル範囲は、`ADMIN_LOW` から `ADMIN_HIGH` までです。

例 17–2 シリアルポートのラベル範囲の制限

シリアルログインデバイスを作成後、セキュリティー管理者はシリアルポートのラベル範囲をシングルラベル `Public` に制限します。管理者は、「デバイス管理」ダイアログボックスで次の値を設定します。

```
Device Name: /dev/term/[a|b]
Device Type: tty
Clean Program: /bin/true
Device Map: /dev/term/[a|b]
Minimum Label: Public
Maximum Label: Public
Allocatable By: No Users
```

▼ Trusted CDE でオーディオプレイヤプログラムを使用できるように構成する

次の手順では、ユーザーが音楽 CD を挿入したときオーディオプレイヤがTrusted CDE ワークスペースで自動的に開くようにします。ユーザーの手順について

は、『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」の例を参照してください。

注 – Trusted JDS ワークスペースでは、ユーザーはリムーバブルメディアの動作を、非トラステッドワークスペースで指定するのと同じように指定します。

始める前に　大域ゾーンで、システム管理者役割になっている必要があります。

1. `/etc/rmmount.conf` ファイルを編集します。
   トラステッドエディタを使用します。詳細は、59 ページの「Trusted Extensions の管理ファイルを編集する」を参照してください。
2. サイトの CD プレイヤプログラムを、ファイルの `cdrom` アクションに追加します。
   `action` *media* `action_`*program*`.so` *path-to-program*

例 17–3 オーディオプレイヤプログラムを使用できるように構成

次の例でシステム管理者は、システムのユーザーすべてが `workman` プログラムを使えるようにします。`workman` プログラムは、オーディオプレイヤプログラムです。

```
# /etc/rmmount.conf file
action cdrom action_workman.so /usr/local/bin/workman
```

▼ デバイスの割り当て後にファイルマネージャーが表示されないようにする

デフォルトでは、デバイスをマウントすると、ファイルマネージャーが表示されます。ファイルシステムのあるデバイスをマウントしない場合、ファイルマネージャーを表示されないようにすることができます。

始める前に　大域ゾーンで、システム管理者役割になっている必要があります。

1. `/etc/rmmount.conf` ファイルを編集します。
   トラステッドエディタを使用します。詳細は、59 ページの「Trusted Extensions の管理ファイルを編集する」を参照してください。
2. 次の `filemgr` アクションを探します。

```
action cdrom action_filemgr.so
action floppy action_filemgr.so
```

3 適切なアクションをコメントアウトします。

次の例は、cdrom デバイスと diskette デバイスの両方で action_filemgr.so アクションをコメントアウトしています。

```
# action cdrom action_filemgr.so
# action floppy action_filemgr.so
```

CD-ROM またはフロッピーディスクを割り当てた場合、ファイルマネージャーは表示されません。

▼ Trusted Extensions で Device_Clean スクリプトを追加する

デバイスの作成時に device_clean スクリプトが指定されていない場合、デフォルトスクリプトの /bin/true が使用されます。

始める前に 使用可能なデータをすべて物理デバイスから削除し、成功の場合は 0 を返すスクリプトを用意します。リムーバブルメディアを使用するデバイスの場合、メディアの取り出しをユーザーが行わないと、代わりにスクリプトが試行します。メディアが取り出されない場合、スクリプトによってデバイスは割り当てエラー状態になります。要件については、device_clean(5) のマニュアルページを参照してください。

大域ゾーンで、システム管理者役割になっている必要があります。

1 スクリプトを /etc/security/lib ディレクトリにコピーします。

2 「デバイス管理」ダイアログボックスで、スクリプトへのフルパスを指定します。

a. デバイス割り当てマネージャーを開きます。

b. 「デバイス管理」ボタンをクリックします。

c. デバイスの名前を選択し、「構成」ボタンをクリックします。

d. 「clean プログラム」フィールドに、スクリプトへのフルパスを入力します。

3 変更を保存します。

Trusted Extensions でのデバイス承認のカスタマイズ (作業マップ)

次の作業マップでは、サイトでデバイス承認を変更する手順について説明します。

作業	説明	参照先
新しいデバイス承認を作成します。	サイト固有の承認を作成します。	260 ページの「新しいデバイス承認を作成する」
デバイスへの承認を追加します。	選択したデバイスにサイト固有の承認を追加します。	263 ページの「Trusted Extensions でサイト固有の承認をデバイスに追加する」
ユーザーおよび役割へデバイス承認を割り当てます。	ユーザーと役割が新しい承認を使えるようにします。	264 ページの「デバイス承認を割り当てる」

▼ 新しいデバイス承認を作成する

デバイスの作成時に承認が指定されない場合、デフォルトではすべてのユーザーがデバイスを使用できます。承認が指定される場合、デフォルトでは承認されたユーザーのみがデバイスを使用できます。

承認を使わずに、割り当て可能なデバイスへのアクセスをすべて回避する方法については、例 17–1 を参照してください。

始める前に　大域ゾーンでセキュリティー管理者役割になります。

1. `auth_attr` ファイルを編集します。

   トラステッドエディタを使用します。詳細は、59 ページの「Trusted Extensions の管理ファイルを編集する」を参照してください。

2. 新しい承認の見出しを作成します。

   組織のインターネットドメイン名の逆順を使い、必要に応じて、そのあとに会社名などの任意のコンポーネントを付けます。複数のコンポーネントはドットで区切ります。見出し名はドットで終わります。

   domain-suffix`.`*domain-prefix*`.`*optional*`.:::`*Company* `Header::help=`*Company*`.html`

3. 新しい承認エントリを追加します。

   1 行に 1 つずつ承認を追加します。行は表示のために分割されています。承認には、管理者による新しい承認の割り当てを可能にする grant 承認を含めます。

   ```
   domain-suffix.domain-prefix.grant:::Grant All Company Authorizations::
   help=CompanyGrant.html
   domain-suffix.domain-prefix.grant.device:::Grant Company Device Authorizations::
   help=CompanyGrantDevice.html
   domain-suffix.domain-prefix.device.allocate.tape:::Allocate Tape Device::
   help=CompanyTapeAllocate.html
   domain-suffix.domain-prefix.device.allocate.floppy:::Allocate Floppy Device::
   help=CompanyFloppyAllocate.html
   ```

4. ファイルを保存してエディタを終了します。

5. ネームサービスとして **LDAP** を使用している場合は、**Sun Java System Directory Server (LDAP サーバー)** 上の auth_attr エントリを更新します。

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

6. 新しい承認を適切な権利プロファイルに追加します。次に、そのプロファイルをユーザーと役割に割り当てます。

   Solaris 管理コンソールを使用します。セキュリティー管理者役割になり、Solaris の手順『System Administration Guide: Security Services』の「How to Create or Change a Rights Profile」に従います。

7. 承認を使用して、テープドライブとフロッピーディスクドライブへのアクセスを制限します。

   デバイス割り当てマネージャーで、新しい承認を、必須の承認リストに追加します。手順については、263 ページの「Trusted Extensions でサイト固有の承認をデバイスに追加する」を参照してください。

例 17–4 きめ細かいデバイス承認の作成

NewCo のセキュリティー管理者は、自社のため、きめ細かいデバイス承認を構築する必要があります。

最初に、管理者は次のヘルプファイルを書き、そのファイルを /usr/lib/help/auths/locale/C ディレクトリに配置します。

```
Newco.html
NewcoGrant.html
NewcoGrantDevice.html
NewcoTapeAllocate.html
NewcoFloppyAllocate.html
```

次に、管理者は、auth_attr ファイルで newco.com に対するすべての承認用のヘッダーを追加します。

```
# auth_attr file
com.newco.:::NewCo Header::help=Newco.html
```

次に、承認エントリをファイルに追加します。

```
com.newco.grant:::Grant All NewCo Authorizations::
help=NewcoGrant.html
com.newco.grant.device:::Grant NewCo Device Authorizations::
help=NewcoGrantDevice.html
com.newco.device.allocate.tape:::Allocate Tape Device::
help=NewcoTapeAllocate.html
com.newco.device.allocate.floppy:::Allocate Floppy Device::
help=NewcoFloppyAllocate.html
```

行は表示のために分割されています。

auth_attr エントリでは、次の承認が作成されます。

- NewCo のすべての承認を付与する承認
- NewCo のデバイス承認を付与する承認
- テープドライブを割り当てる承認
- フロッピーディスクドライブを割り当てる承認

例 17–5 トラステッドパス承認と非トラステッドパス承認の作成

デフォルトでは、「デバイスの割り当て」承認によって、トラステッドパスからもトラステッドパス以外からも割り当てが可能です。

次の例では、サイトのセキュリティーポリシーが遠隔 CD-ROM の割り当て制限を要求しています。セキュリティー管理者は、com.someco.device.cdrom.local 承認を作成します。この承認は、トラステッドパスによって割り当てられる CD-ROM ドライブ用です。com.someco.device.cdrom.remote 承認は、トラステッドパス以外からの CD-ROM ドライブ割り当てを許可される少数のユーザー用です。

セキュリティー管理者は、ヘルプファイルを作成し、auth_attr データベースに承認を追加し、その承認をデバイスに追加して、権利プロファイルに配置します。これらのプロファイルを、デバイスの割り当てを許可するユーザーに割り当てます。

- auth_attr データベースエントリは次のとおりです。

```
com.someco.:::SomeCo Header::help=Someco.html
com.someco.grant:::Grant All SomeCo Authorizations::
help=SomecoGrant.html
com.someco.grant.device:::Grant SomeCo Device Authorizations::
help=SomecoGrantDevice.html
```

```
com.someco.device.cdrom.local:::Allocate Local CD-ROM Device::
help=SomecoCDAllocateLocal.html
com.someco.device.cdrom.remote:::Allocate Remote CD-ROM Device::
help=SomecoCDAllocateRemote.html
```

- デバイス割り当てマネージャーの割り当ては次のとおりです。

  トラステッドパスでは、承認されたユーザーがローカルの CD-ROM ドライブを割り当てるときにデバイス割り当てマネージャーを使用できます。

  ```
  Device Name: cdrom_0
  For Allocations From: Trusted Path
  Allocatable By: Authorized Users
  Authorizations: com.someco.device.cdrom.local
  ```

  非トラステッドパスでは、ユーザーが `allocate` コマンドを使用して遠隔でデバイスを割り当てることができます。

  ```
  Device Name: cdrom_0
  For Allocations From: Non-Trusted Path
  Allocatable By: Authorized Users
  Authorizations: com.someco.device.cdrom.remote
  ```

- 権利プロファイルエントリは次のとおりです。

  ```
  # Local Allocator profile
  com.someco.device.cdrom.local

  # Remote Allocator profile
  com.someco.device.cdrom.remote
  ```

- 承認されたユーザーの権利プロファイルは次のとおりです。

  ```
  # List of profiles for regular authorized user
  Local Allocator Profile
  ...

  # List of profiles for role or authorized user
  Remote Allocator Profile
  ...
  ```

▼ Trusted Extensions でサイト固有の承認をデバイスに追加する

始める前に　セキュリティー管理者役割であるか、「デバイス属性の構成」承認を持つ役割である必要があります。あらかじめサイト固有の承認を作成してあることが必要です。詳細は、260 ページの「新しいデバイス承認を作成する」を参照してください。

1. 251 ページの「Trusted Extensions でデバイスを構成する」の手順に従います。
   a. 新しい承認で保護する必要のあるデバイスを選択します。
   b. 「デバイス管理」ダイアログボックスを開きます。
   c. 「デバイス割り当て:構成」ダイアログボックスで、「承認」ボタンをクリックします。
      新しい承認は「必須でない」リストに表示されます。
   d. 新しい承認を承認の「必須」リストに追加します。
2. 「了解」をクリックして変更を保存します。

▼ デバイス承認を割り当てる

「デバイスの割り当て」承認は、ユーザーがデバイスを割り当てられるようにします。「デバイスの割り当て」承認と、「デバイスの解除または再利用」承認は、管理役割に適しています。

始める前に　大域ゾーンでセキュリティー管理者役割になります。

既存のプロファイルが適切でない場合、セキュリティー管理者が新しいプロファイルを作成できます。例については、98 ページの「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。

- ユーザーに、「デバイスの割り当て」承認を含む権利プロファイルを割り当てます。
  詳細は、オンラインヘルプを参照してください。詳細な手順については、『System Administration Guide: Security Services』の「How to Change the RBAC Properties of a User」を参照してください。
  次のプロファイルでは、役割がデバイスを割り当てることができます。
  - All Authorizations
  - Device Management
  - Media Backup
  - Media Restore
  - Object Label Management
  - Software Installation

  次のプロファイルでは、役割がデバイスを解除または再利用できます。
  - All Authorizations
  - Device Management

次のプロファイルでは、役割がデバイスを作成または構成できます。

- All Authorizations
- Device Security

例 17–6 新しいデバイス承認の割り当て

この例では、セキュリティー管理者がシステムの新しいデバイス承認を構成し、新しい承認を持つ権利プロファイルを信頼できるユーザーに割り当てます。セキュリティー管理者は次の操作を行います。

1. 260 ページの「新しいデバイス承認を作成する」に従って、新しいデバイス承認を作成します。
2. デバイス割り当てマネージャーで、テープドライブとフロッピーディスクドライブに新しいデバイス承認を追加します。
3. 新しい承認を、権利プロファイル NewCo Allocation に配置します。
4. テープドライブとフロッピーディスクドライブの割り当てを承認されるユーザーと役割のプロファイルに、NewCo Allocation 権利プロファイルを追加します。

これで、承認されたユーザーと役割はこのシステムでテープドライブとフロッピーディスクドライブを使えるようになります。

◆ ◆ ◆ 第 18 章

18 Trusted Extensions での監査 (概要)

この章では、Solaris Trusted Extensions で提供される監査の追加機能について説明します。

Trusted Extensions と監査

Trusted Extensions ソフトウェアが設定されたシステムでは、監査の構成と管理は Solaris システムでの監査の場合と類似しています。ただし、次の相違点があります。

- Trusted Extensions ソフトウェアは、監査クラス、監査イベント、監査トークン、および監査ポリシーオプションをシステムに追加します。
- Trusted Extensions ソフトウェアでは、デフォルトで監査が有効になっています。
- Solaris のゾーン別の監査はサポートされていません。Trusted Extensions では、すべてのゾーンがあらゆる点で同じように監査されます。
- Trusted Extensions には、ユーザーの監査特性を管理し、監査ファイルを編集するための管理ツールがあります。
- Trusted Extensions での監査の構成と管理には、システム管理者とセキュリティー管理者の 2 つの役割が使用されます。

  セキュリティー管理者は、監査の対象と、イベントとクラスとのサイト固有のマッピングを計画します。Solaris OS の場合と同じく、システム管理者は監査ファイルのためのディスク容量要件を計画し、監査管理サーバーを作成して、監査構成ファイルをインストールします。

Trusted Extensions の役割による監査の管理

Trusted Extensions での監査には、Solaris OS の場合と同様の計画が必要です。計画については、『System Administration Guide: Security Services』の第 29 章「Planning for Solaris Auditing」を参照してください。

監査管理のための役割の設定

Trusted Extensions では、監査を担当する役割が 2 つあります。 システム管理者役割は、ディスクと監査ストレージのネットワークを設定します。セキュリティー管理者役割は、監査の対象を決定し、監査構成ファイルに情報を指定します。Solaris OS の場合と同じく、管理者がソフトウェアで役割を作成します。これら 2 つの役割に対する権利プロファイルが用意されています。初期設定チームは、初期構成中にセキュリティー管理者役割を作成しました。詳細は、『Solaris Trusted Extensions 構成ガイド』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。

注 – システムは、監査構成ファイルによってシステムが記録するように設定されている (事前選択の) セキュリティー関連イベントのみを記録します。したがって、後続の監査見直しでは、記録されたイベントしか考慮しません。設定に誤りがあると、システムのセキュリティーに対する侵入の試みが検出されなかったり、セキュリティー侵入の責任があるユーザーを管理者が特定できなくなる可能性があります。管理者は定期的に監査証跡を分析して、セキュリティー侵入をチェックする必要があります。

Trusted Extensions での監査タスク

Trusted Extensions で監査を構成し管理する手順は、Solaris での手順と少し異なります。

- 監査の構成は、2 つの管理役割のいずれかが大域ゾーンで行います。その後、システム管理者はカスタマイズされたそれぞれの監査ファイルを大域ゾーンから各ラベル付きゾーンにコピーします。この手順に従うことにより、ユーザーアクションは大域ゾーンとラベル付きゾーンで同じように監査されます。

  詳細は、269 ページの「セキュリティー管理者の監査タスク」 and 269 ページの「システム管理者の監査タスク」を参照してください。
- Trusted Extensions 管理者はトラステッドエディタを使用して、監査構成ファイルを編集します。Trusted CDE の場合、Trusted Extensions 管理者は CDE アクションを使用して、トラステッドエディタを起動します。アクションのリストについては、37 ページの「Trusted CDE アクション」を参照してください。

- Trusted Extensions 管理者は Solaris 管理コンソールを使用して、特定のユーザーを設定します。ユーザー固有の監査特性は、このツールで指定できます。ユーザーの特性を指定する必要があるのは、そのユーザーの監査特性が、作業中のシステムの監査特性と異なる場合だけです。このツールについては、40 ページの「Solaris 管理コンソールツール」を参照してください。

セキュリティー管理者の監査タスク

次のタスクはセキュリティー関連であり、セキュリティー管理者が担当します。Solaris に関する指示に従いますが、Trusted Extensions の管理ツールを使用してください。

作業	Solaris に関する指示	Trusted Extensions に関する指示
監査ファイルを設定します。	『System Administration Guide: Security Services』の「Configuring Audit Files (Task Map)」	トラステッドエディタを使用します。詳細は、59 ページの「Trusted Extensions の管理ファイルを編集する」を参照してください。
(省略可能) デフォルトの監査ポリシーを変更します。	『System Administration Guide: Security Services』の「How to Configure Audit Policy」	トラステッドエディタを使用します。
監査を無効にし、再度有効にします。	『System Administration Guide: Security Services』の「How to Disable the Auditing Service」	監査機能はデフォルトで有効になります。
監査を管理します。	『System Administration Guide: Security Services』の「Solaris Auditing (Task Map)」	トラステッドエディタを使用します。 ゾーンごとの監査タスクを無視します。

システム管理者の監査タスク

次のタスクは、システム管理者が担当します。Solaris に関する指示に従いますが、Trusted Extensions の管理ツールを使用してください。

作業	Solaris に関する指示	Trusted Extensions に関する指示
監査パーティションおよび監査管理サーバーを作成、監査パーティションをエクスポート、監査パーティションをマウントします。 `audit_warn` 別名を作成します。	『System Administration Guide: Security Services』の「Configuring and Enabling the Auditing Service (Tasks)」	大域ゾーンですべての管理を実行します。 トラステッドエディタを使用します。

作業	Solaris に関する指示	Trusted Extensions に関する指示
カスタマイズされた監査ファイルをラベル付きゾーンにコピーまたはループバックマウントします。	『System Administration Guide: Security Services』の「Configuring the Auditing Service in Zones (Tasks)」	最初のラベル付きゾーンにファイルをコピーしてから、そのゾーンをコピーします。 あるいは、ラベル付きゾーンが作成されたあとで、それぞれのゾーンにファイルをループバックマウントまたはコピーします。
(省略可能) 監査構成ファイルを配布します。	指示なし	『Solaris Trusted Extensions 構成ガイド』の「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」を参照してください。
監査を管理します。	『System Administration Guide: Security Services』の「Solaris Auditing (Task Map)」	ゾーンごとの監査タスクを無視します。
ラベル別の監査レコードを選択する	『System Administration Guide: Security Services』の「How to Select Audit Events From the Audit Trail」	ラベル別のレコードを選択するには、`auditreduce` コマンドと `-l` オプションを使用します。

Trusted Extensions の監査のリファレンス

Trusted Extensions ソフトウェアは、監査クラス、監査イベント、監査トークン、および監査ポリシーのオプションを Solaris OS に追加します。いくつかの監査コマンドが、ラベル処理のために拡張されています。Trusted Extensions の監査レコードには、次の図に示すようにラベルが含まれています。

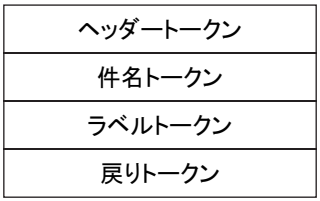


図 18–1 ラベル付きシステムでの一般的な監査レコード

Trusted Extensions の監査クラス

Trusted Extensions ソフトウェアで Solaris OS に追加される監査クラスの一覧を次の表にアルファベット順に示します。これらのクラスは、`/etc/security/audit_class` ファイルに一覧されています。監査クラスについては、`audit_class(4)` のマニュアルページを参照してください。

表 18–1　X サーバー監査クラス

短い名前	長い名前	監査マスク
xc	X - オブジェクトの作成/破棄	0x00800000
xp	X - 特権/管理操作	0x00400000
xs	X - 失敗した場合、常にメッセージを表示せずにエラーになる操作	0x02000000
xx	X - xl、xc、xp、および xs クラスのすべての X イベント (メタクラス)	0x03e00000

X サーバー監査イベントは、次の条件に従ってこれらのクラスにマップされます。

- **xc –** このクラスは、サーバーオブジェクトの作成と破棄を監査します。たとえば、このクラスで `CreateWindow()` を監査します。
- **xp –** このクラスは特権の使用を監査します。特権の使用は、成功と失敗のいずれかになります。たとえば、クライアントがほかのクライアントのウィンドウの属性を変更しようとするときは、`ChangeWindowAttributes()` が監査されます。このクラスには、`SetAccessControl()` などの管理ルーチンも含まれています。
- **xs –** このクラスは、セキュリティー属性が原因で失敗したときにクライアントに X エラーメッセージを返さないルーチンを監査します。たとえば `GetImage()` は、特権がないためにウィンドウからの読み取りに失敗しても、`BadWindow` エラーを返しません。

  これらのイベントは、成功した場合にのみ監査するよう選択してください。失敗した場合の xs イベントを選択すると、監査証跡が無関係のレコードでいっぱいになります。
- **xx –** このクラスには、X 監査クラスがすべて含まれます。

Trusted Extensions の監査イベント

Trusted Extensions ソフトウェアでは、システムに監査イベントが追加されます。新しい監査イベントと、そのイベントが属する監査クラスは、`/etc/security/audit_event` ファイルに一覧されています。Trusted Extensions の監査イベント番号は、9000 から 10000 の間です。監査クラスについては、`audit_event(4)` のマニュアルページを参照してください。

Trusted Extensions の監査トークン

Trusted Extensions ソフトウェアで Solaris OS に追加される監査トークンを、次の表にアルファベット順に一覧しています。トークンは、`audit.log(4)` マニュアルページにも一覧されています。

表 18–2　Trusted Extensions の監査トークン

トークン名	説明
272 ページの「`label` トークン」	機密ラベル
273 ページの「`xatom` トークン」	X ウィンドウのアトム ID
273 ページの「`xclient` トークン」	X クライアント ID
274 ページの「`xcolormap` トークン」	X ウィンドウのカラー情報
274 ページの「`xcursor` トークン」	X ウィンドウのカーソル情報
274 ページの「`xfont` トークン」	X ウィンドウのフォント情報
275 ページの「`xgc` トークン」	X ウィンドウのグラフィカルコンテキスト情報
275 ページの「`xpixmap` トークン」	X ウィンドウのピクセルマッピング情報
275 ページの「`xproperty` トークン」	X ウィンドウのプロパティー情報
276 ページの「`xselect` トークン」	X ウィンドウのデータ情報
277 ページの「`xwindow` トークン」	X ウィンドウのウィンドウ情報

`label` トークン

`label` トークンは、機密ラベルを含みます。次のフィールドがあります。

- トークン ID
- 機密ラベル

トークン形式は次の図のとおりです。

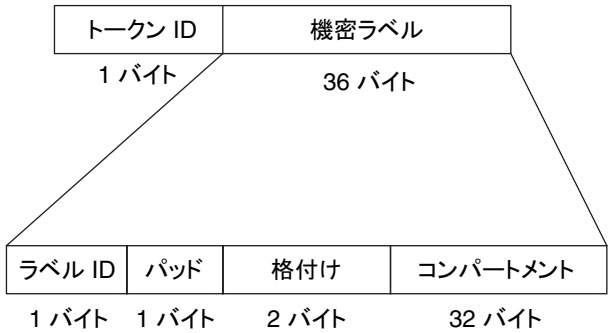


図 18–2 label トークン形式

label トークンは、praudit コマンドによって次のように表示されます。

```
sensitivity label,ADMIN_LOW
```

xatom トークン

xatom トークンは、X アトムに関する情報を含みます。次のフィールドがあります。

- トークン ID
- 文字列長
- アトムを識別するテキスト文字列

xatom トークンは、praudit によって次のように表示されます。

```
X atom,_DT_SAVE_MODE
```

xclient トークン

xclient トークンは、X クライアントに関する情報を含みます。次のフィールドがあります。

- トークン ID
- クライアント ID

xclient トークンは、praudit によって次のように表示されます。

```
X client,15
```

xcolormap トークン

xcolormap トークンは、カラーマップに関する情報を含みます。次のフィールドがあります。

- トークン ID
- X サーバー識別子
- 作成者のユーザー ID

トークン形式は次の図のとおりです。

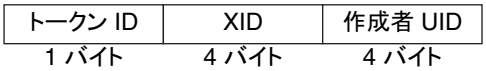


図 18–3 xcolormap、 xcursor、xfont、xgc、xpixmap 、xwindow トークンの形式

xcolormap トークンは、praudit によって次のように表示されます。

```
X color map,0x08c00005,srv
```

xcursor トークン

xcursor トークンは、カーソルに関する情報を含みます。次のフィールドがあります。

- トークン ID
- X サーバー識別子
- 作成者のユーザー ID

トークン形式は、図 18–3 のとおりです。

xcursor トークンは、praudit によって次のように表示されます。

```
X cursor,0x0f400006,srv
```

xfont トークン

xfont トークンは、フォントに関する情報を含みます。次のフィールドがあります。

- トークン ID
- X サーバー識別子
- 作成者のユーザー ID

トークン形式は、図 18–3 のとおりです。

xfont トークンは、praudit によって次のように表示されます。

```
X font,0x08c00001,srv
```

xgc トークン

xgc トークンは、xgc に関する情報を含みます。次のフィールドがあります。

- トークン ID
- X サーバー識別子
- 作成者のユーザー ID

トークン形式は、図 18–3 のとおりです。

xgc トークンは、praudit によって次のように表示されます。

```
Xgraphic context,0x002f2ca0,srv
```

xpixmap トークン

xpixmap トークンは、ピクセルマッピングに関する情報を含みます。次のフィールドがあります。

- トークン ID
- X サーバー識別子
- 作成者のユーザー ID

トークン形式は、図 18–3 のとおりです。

xpixmap トークンは、praudit によって次のように表示されます。

```
X pixmap,0x08c00005,srv
```

xproperty トークン

xproperty トークンは、ウィンドウの各種プロパティーに関する情報を含みます。次のフィールドがあります。

- トークン ID
- X サーバー識別子
- 作成者のユーザー ID
- 文字列長
- アトムを識別するテキスト文字列

xproperty トークン形式は次の図のとおりです。

トークン ID	XID	作成者 UID	文字列長	文字列 (アトム長)
1 バイト	4 バイト	4 バイト	2 バイト	N バイト

図 18–4 xproperty トークン形式

xproperty トークンは、praudit によって次のように表示されます。

```
X property,0x000075d5,root,_MOTIF_DEFAULT_BINDINGS
```

xselect トークン

xselect トークンは、ウィンドウ間で移動するデータを含みます。このデータは、内部構造を想定されないバイトストリームと、プロパティー文字列です。次のフィールドがあります。

- トークン ID
- プロパティー文字列の長さ
- プロパティー文字列
- プロパティータイプの長さ
- プロパティータイプ文字列
- データのバイト数を示す長さフィールド
- データを含むバイト文字列

トークン形式は次の図のとおりです。

トークン ID	プロパティー文字列長	プロパティー文字列	プロパティータイプ長	プロパティータイプ	データ長	ウィンドウデータ
1 バイト	2 バイト	N バイト	2 バイト	N バイト	2 バイト	N バイト

図 18–5 xselect トークン形式

xselect トークンは、praudit によって次のように表示されます。

```
X selection,entryfield,halogen
```

xwindow トークン

xwindow トークンは、ウィンドウに関する情報を含みます。次のフィールドがあります。

- トークン ID
- X サーバー識別子
- 作成者のユーザー ID

トークン形式は、図 18–3 のとおりです。

xwindow トークンは、praudit によって次のように表示されます。

```
X window,0x07400001,srv
```

Trusted Extensions での監査ポリシーオプション

Trusted Extensions は、既存の Solaris 監査ポリシーオプションに 2 つの監査ポリシーオプションを追加します。追加の監査ポリシーを確認するには、ポリシーを一覧表示します。

```
$ auditconfig -lspolicy
...
windata_down Include downgraded window information in audit records

windata_up   Include upgraded window information in audit records
```

Trusted Extensions の監査コマンドの拡張

auditconfig、auditreduce、および bsmrecord の各コマンドは、Trusted Extensions 情報を処理できるように拡張されています。

- auditconfig コマンドには、Trusted Extensions の監査ポリシーが含まれます。詳細は、auditconfig(1M) のマニュアルページを参照してください。
- auditreduce コマンドでは、ラベルに従ってレコードをフィルタする -l オプションが追加されています。詳細は、auditreduce(1M) のマニュアルページを参照してください。
- bsmrecord コマンドには、Trusted Extensions の監査イベントが含まれます。詳細は、bsmrecord(1M) のマニュアルページを参照してください。

◆ ◆ ◆ 第 19 章

Trusted Extensions のソフトウェア管理 (手順)

この章では、Solaris Trusted Extensions が設定されたシステムで、他社製のソフトウェアを信頼できる方法で実行する方法について説明します。

Trusted Extensions へのソフトウェアの追加

Solaris システムに追加できるソフトウェアは、Trusted Extensions が設定されたシステムにも追加できます。また、Trusted Extensions API を使用するプログラムも追加できます。Trusted Extensions システムへのソフトウェアの追加は、非大域ゾーンを実行している Solaris システムにソフトウェアを追加する場合と同様です。

たとえば、パッケージの問題は、非大域ゾーンをインストールしたシステムに影響します。パッケージのパラメータにより、次のことが定義されます。

- パッケージのゾーンの有効範囲 – この範囲では、特定のパッケージをインストールできるゾーンの種類を決定します。
- パッケージの可視性 – 可視性は、パッケージをすべてのゾーンにインストールする必要があるかどうか、およびすべてのゾーンで同一にする必要があるかどうかを決定します。
- パッケージの制限 – 制限の 1 つに、パッケージを現在のゾーンのみにインストールする必要があるかどうかがあります。

Trusted Extensions では、プログラムは一般ユーザーがラベル付きのゾーンで使用できるように、一般的に大域ゾーンにインストールされます。ゾーンでのパッケージのインストールについては、『System Administration Guide: Solaris Containers-Resource Management and Solaris Zones』の第 24 章「About Packages and Patches on a Solaris System With Zones Installed (Overview)」を参照してください。また、`pkgadd(1M)` のマニュアルページも参照してください。

Trusted Extensions サイトでは、システム管理者とセキュリティー管理者がソフトウェアをインストールします。セキュリティー管理者は、セキュリティーポリシーを厳守するために、ソフトウェアの追加を評価します。ソフトウェアの実行に特権や承認が必要な場合、セキュリティー管理者役割はソフトウェアのユーザーに適切な権利プロファイルを割り当てます。

リムーバブルメディアからソフトウェアをインポートするには、承認が必要です。「デバイスの割り当て」承認を持つアカウントは、リムーバブルメディアを使用したデータのインポートやエクスポートを実行できます。データには実行可能コードが含まれることがあります。一般ユーザーは、ユーザーの認可上限内のラベルでデータをインポートすることのみ可能です。

システム管理者役割は、セキュリティー管理者が承認したプログラムを追加します。

Solaris のソフトウェアセキュリティー機構

Trusted Extensions は、Solaris OS と同じセキュリティー機構を使用します。セキュリティー機構には、次の機能が含まれます。

- 承認 – プログラムのユーザーに、特定の承認を要求することができます。承認については、『System Administration Guide: Security Services』の「Solaris RBAC Elements and Basic Concepts」を参照してください。また、`auth_attr(4)` および `getauthattr(3SECDB)` のマニュアルページも参照してください。
- 特権 – プログラムとプロセスには特権を割り当てることができます。特権については、『System Administration Guide: Security Services』の第 8 章「Using Roles and Privileges (Overview)」を参照してください。また、`privileges(5)` のマニュアルページも参照してください。

  `ppriv` コマンドはデバッグユーティリティーを提供します。詳細は、`ppriv(1)` のマニュアルページを参照してください。非大域ゾーンで動作するプログラムでこのユーティリティーを使用する場合の説明は、『System Administration Guide: Solaris Containers-Resource Management and Solaris Zones』の「Using the ppriv Utility」を参照してください。
- 権利プロファイル – 権利プロファイルは、ユーザーまたは役割に割り当てるために、セキュリティー属性をまとめたものです。権利プロファイルについては、『System Administration Guide: Security Services』の「RBAC Rights Profiles」を参照してください。Trusted Extensions では、セキュリティー属性を割り当てることができる実行可能ファイルのタイプに、CDE アクションが追加されます。
- トラステッドライブラリ – `setuid`、`setgid`、および特権プログラムが使用する、動的な共有ライブラリです。特権プログラムはトラステッドディレクトリからのみロードできます。Solaris OS と同様、`crle` コマンドを使用して、特権プログラムの共有ライブラリディレクトリをトラステッドディレクトリに追加できます。詳細は、`crle(1)` のマニュアルページを参照してください。

ソフトウェアのセキュリティーの評価

ソフトウェアに特権が割り当てられた場合や、代替のユーザー ID またはグループ ID での実行時には、そのソフトウェアが「トラステッド」とみなされます。信頼されたソフトウェアは、Trusted Extensions のセキュリティーポリシーによる制約を必ずしも受けません。信頼できないソフトウェアでも、「トラステッド」にできることに注意してください。慎重な調査によってソフトウェアが信頼できる方法で特権を使用することが明らかになるまで、セキュリティー管理者はソフトウェアに特権を与えることを保留します。

トラステッドシステムでは、プログラムは次の 3 つのカテゴリに分類されます。

- セキュリティー属性を必要としないプログラム – 一部のプログラムはシングルのレベルで動作し、特権を必要としません。これらのプログラムは、`/usr/local` などの公開ディレクトリにインストールできます。アクセスするには、ユーザーと役割の権利プロファイルにプログラムをコマンドとして割り当てます。
- **root** ユーザーとして動作するプログラム – 一部のプログラムは、`setuid 0` で実行されます。これらのプログラムには、権利プロファイルで `0` の実効 UID を割り当てることができます。セキュリティー管理者は、プロファイルを管理役割に割り当てます。

  ヒント – アプリケーションが信頼できる方法で特権を使用できる場合は、アプリケーションに必要な特権を割り当てます。プログラムを `root` として実行しないでください。

- 特権が必要なプログラム – 明らかな理由がないにもかかわらず、特権が必要とされるプログラムもあります。システムのセキュリティーポリシーに違反すると思われる機能を実行していないプログラムでも、内部的な動作がセキュリティーに違反している可能性があります。たとえば、プログラムが共有されたログファイルを使用していたり、`/dev/kmem` から読み取りを行なっている可能性があります。セキュリティーに関する注意は、mem(7D) のマニュアルページを参照してください。

  内部的なポリシーの上書きが、アプリケーションの正常な動作にとって特に重要でない場合もあります。このような上書きは、ユーザーへの便宜のために提供されているに過ぎません。

  組織としてソースコードにアクセスできる場合は、アプリケーションのパフォーマンスに影響を与えずに、ポリシーの上書きを必要とする操作を削除できるかどうかを確認してください。

トラステッドプログラムを作成する開発者の役割

プログラムの開発者がソースコードで特権のセットを操作できても、セキュリティー管理者が必要な特権をプログラムに割り当てていなければ、プログラムは正

常に動作しません。トラステッドプログラムの作成では、開発者とセキュリティー管理者が共同で作業する必要があります。

トラステッドプログラムを作成する開発者には、次のタスクが必要です。

1. プログラムを正常に動作させるために、どこで特権が必要かを理解する。
2. 特権ブラケットなどの、プログラムで特権を安全に使用するための技術を習得して使用する。
3. 特権をプログラムに割り当てるときに、セキュリティーの関連性に注意する。プログラムはセキュリティーポリシーに違反してはならない。
4. トラステッドディレクトリからプログラムにリンクされた共有ライブラリを使用して、プログラムをコンパイルする。

   詳しくは、『Solaris セキュリティーサービス開発ガイド』を参照してください。Trusted Extensions のコード例については、『Solaris Trusted Extensions 開発ガイド』を参照してください。

トラステッドプログラムにおけるセキュリティー管理者の役割

セキュリティー管理者は、新しいソフトウェアをテストおよび評価します。ソフトウェアを信頼できると判断したら、セキュリティー管理者はプログラムの権利プロファイルとその他のセキュリティーに関する属性を構成します。

セキュリティー管理者には次のような責任があります。

1. プログラマやプログラム配布プロセスが信頼できることを確認する。
2. 次の情報源のいずれかから、プログラムに必要な特権を決定する。
   - プログラマに確認する。
   - ソースコードを調べて、プログラムが使用する予定の特権を検索する。
   - ソースコードを調べて、プログラムがユーザーに要求する承認を検索する。
   - `ppriv` コマンドにデバッグオプションを使用して、特権の使用を検索する。この例は、`ppriv(1)` のマニュアルページを参照してください。
3. ソースコードを調査し、プログラムの動作に必要な特権に関して信頼できる方法で処理していることを確認します。

   プログラムが信頼できる方法で特権を使用していない場合、プログラムのソースコードを修正できるときはコードを修正します。セキュリティーについて熟知しているセキュリティーコンサルタントや開発者は、コードを修正できます。修正には、特権ブラケットや承認の検査が含まれる場合があります。

   特権の割り当ては、手動で行う必要があります。特権の不足によりエラーが発生するプログラムには、特権を割り当てることができます。また、セキュリティー管理者が、特権を不要にする実効 UID または実効 GID を割り当てるように決定する場合もあります。

ウィンドウシステムでのトラステッドプロセス

Solaris Trusted Extensions (CDE) では、次のウィンドウシステムのプロセスが信頼されます。

- フロントパネル
- フロントパネルのサブパネル
- ワークスペースメニュー
- ファイルマネージャー
- アプリケーションマネージャー

ウィンドウシステムのトラステッドプロセスはだれでも利用できますが、管理アクションへのアクセスは大域ゾーンの役割に制限されます。

アクションがアカウントのプロファイルのいずれにもない場合、ファイルマネージャーにアクションのアイコンは表示されません。ワークスペースメニューでは、アクションがアカウントのプロファイルのいずれにもない場合、アクションは表示されますが、アクションを実行するとエラーが表示されます。

Trusted CDE では、ウィンドウマネージャーの `dtwm` が `Xtsolusersession` スクリプトを呼び出します。このスクリプトはウィンドウマネージャーとともに動作し、ウィンドウシステムから起動されるアクションを呼び出します。`Xtsolusersession` スクリプトは、アカウントがアクションを起動しようとしたときに、アカウントの権利プロファイルを確認します。いずれの場合も、アクションが割り当てられた権利プロファイルに指定されている場合、アクションはプロファイルに指定されているセキュリティー属性で実行されます。

Trusted CDE アクションの追加

Trusted Extensions で CDE アクションを作成および使用する手順は、Solaris OS における手順と同様です。アクションの追加については、『Solaris Common Desktop Environment: Advanced User's and System Administrator's Guide』の第 4 章「Adding and Administering Applications」で説明されています。

Solaris OS と同様、アクションの使用は権利プロファイルで管理できます。Trusted Extensions では、管理役割の権利プロファイルで、いくつかのアクションにセキュリティー属性が割り当てられています。セキュリティー管理者は、「権利」ツールを使用して、新しいアクションにセキュリティー属性を割り当てることもできます。

次の表では、管理者がアクションを作成し使用する場合の、Solaris システムと Solaris Trusted Extensions システムの主な相違点について説明します。

表 19–1 Trusted Extensions での CDE アクションの制約

Solaris CDE アクション	Trusted CDE アクション
新しいアクションは、だれでも自分のホームディレクトリ内に作成できます。 作成者は、新しいアクションを自動的に使用できるようになります。	アクションは、ユーザーに割り当てられた権利プロファイルである場合のみ使用可能です。アクションの検索パスは異なります。ユーザーのホームディレクトリにあるアクションは、最初ではなく最後に処理されます。したがって、既存のアクションをカスタマイズすることはできません。 ユーザーは自分のホームディレクトリに新しいアクションを作成できますが、アクションを使用できない場合があります。 All プロファイルを持つユーザーは、作成したアクションを使用することができます。それ以外の場合は、セキュリティー管理者が、アカウントの権利プロファイルのいずれかに新しいアクションの名前を追加する必要があります。 アクションを起動するには、ユーザーはファイルマネージャーを使用します。システム管理者は、アクションを公開ディレクトリに配置できます。
アクションはフロントパネルにドラッグ&ドロップできます。	フロントパネルはトラステッドパスの一部です。ウィンドウマネージャーは、`/usr/dt` と `/etc/dt` サブディレクトリにある、管理者が追加したアクションだけを認識します。All プロファイルが割り当てられていても、ユーザーはフロントパネルに新しいアクションをドラッグできません。ユーザーのホームディレクトリにあるアクションは、ウィンドウマネージャーでは認識されません。マネージャーは公開ディレクトリだけを確認します。
`root` によって実行された場合、アクションは特権処理を実行できます。	ユーザーに割り当てられた権利プロファイルでアクションに特権が割り当てられている場合、アクションは特権を必要とする処理を実行できます。
アクションは Solaris 管理コンソール では管理されません。	アクションは Solaris 管理コンソール の「権利」ツールで権利プロファイルに割り当てられます。新しいアクションが追加されると、セキュリティー管理者は新しいアクションを利用可能にすることができます。

Trusted Extensions でのソフトウェアの管理 (手順)

Trusted Extensions でのソフトウェアの管理は、非大域ゾーンがインストールされた Solaris システムでのソフトウェアの管理タスクと同様です。ゾーンの詳細は、『System Administration Guide: Solaris Containers-Resource Management and Solaris Zones』のパート II「Zones」を参照してください。

▼ Trusted Extensions でソフトウェアパッケージを追加する

始める前に　デバイスを割り当てることができる役割になる必要があります。

1. 適切なワークスペースで作業を開始します。
   - ソフトウェアパッケージを大域ゾーンにインストールする場合は、大域ゾーンで作業します。
   - ソフトウェアパッケージをラベル付きゾーンにインストールする場合は、そのラベルでワークスペースを作成します。
     詳細は、『Solaris Trusted Extensions ユーザーズガイド』の「ワークスペースのラベルを変更する」を参照してください。
2. **CD-ROM** ドライブを割り当てます。
   詳細は、『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。
3. ソフトウェアをインストールします。
   詳細は、『System Administration Guide: Basic Administration』の「Where to Find Software Management Tasks」を参照してください。
4. 転送が終了したら、デバイスの割り当てを解除します。
   詳細は、『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。

▼ Trusted Extensions で Java Archive ファイルをインストールする

この手順では、Java™ archive (JAR) ファイルを大域ゾーンにダウンロードします。大域ゾーンから、管理者はファイルを一般ユーザーが利用できるようにできます。

始める前に　セキュリティー管理者は、Java プログラムのソースが信頼できること、配信方法が安全であること、およびプログラムを信頼できる方法で実行できることを確認しています。

大域ゾーンでセキュリティー管理者役割になります。Software Installation 権利プロファイルに、Java コードの「開く」アクションが含まれています。

1. **JAR ファイルを /tmp ディレクトリにダウンロードします。**
   たとえば、http://www.sunfreeware.com からソフトウェアを選択する場合、サイトの「Web Start Wizard Installation of Freeware」の指示に従います。
2. ファイルマネージャーを開き、/tmp ディレクトリに移動します。
3. ダウンロードしたファイルをダブルクリックします。
4. ダイアログボックスの質問に答えて、ソフトウェアをインストールします。
5. インストールログを確認します。

例 19–1 ユーザーラベルへの JAR ファイルのダウンロード

セキュリティーリスクを小さくするため、システム管理者は一般ユーザーの認可範囲内でシングルラベルにソフトウェアをダウンロードします。続いてセキュリティー管理者は、そのラベルで JAR ファイルをテストします。このソフトウェアがテストに合格したら、セキュリティー管理者はラベルを ADMIN_LOW にダウングレードします。システム管理者は、このソフトウェアを NFS サーバーにインストールし、すべてのユーザーが利用できるようにします。

1. 最初に、システム管理者は、ユーザーラベルでワークスペースを作成します。
2. システム管理者は、作成したワークスペースで、JAR ファイルをダウンロードします。
3. ユーザーラベルで、セキュリティー管理者は JAR ファイルをテストします。
4. 次に、セキュリティー管理者は、このファイルのラベルを ADMIN_LOW に変更します。
5. 最後に、システム管理者は、ラベルが ADMIN_LOW の NFS サーバーにこのファイルをコピーします。

◆ ◆ ◆ 付 録 A

Trusted Extensions 管理の手引き

Solaris Trusted Extensions インタフェースは Solaris OS を拡張します。この付録は、これらの相違の手引きです。ライブラリルーチンとシステムコールを含む、インタフェースの詳細なリストについては、付録 B 「Trusted Extensions マニュアルページのリスト」を参照してください。

Trusted Extensions の管理インタフェース

Trusted Extensions には、ソフトウェアのインタフェースが用意されています。次のインタフェースは、Trusted Extensions ソフトウェアが実行されている場合にのみ利用できます。

`txzonemgr` スクリプト	ラベル付きゾーンの作成、インストール、初期化、および起動を行うためのメニューベースのウィザードを提供します。このメニューのタイトルは「Labeled Zone Manager」です。また、このスクリプトには、ネットワークオプションやネームサービスオプション用のメニュー項目や、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用意されています。
Trusted CDE アクション	Trusted CDE では、「ワークスペースメニュー」->「アプリケーションマネージャー」->「Trusted_Extensions」に、ファイルの構成、ゾーンのインストールと起動、およびそのほかの Trusted Extensions のタスクの簡素化を行う CDE アクションが含まれています。これらのアクションが実行するタスクについては、37 ページの「Trusted CDE アクション」を参照し

	てください。Trusted CDE のオンラインヘルプでも、これらのアクションについて説明しています。
管理エディタ	システムファイルの編集には、このトラステッドエディタが使用されます。Trusted CDE では、「ワークスペースメニュー」->「アプリケーションマネージャー」->「Trusted_Extensions」->「管理エディタ」により、管理エディタが呼び出されます。Trusted JDS では、このエディタはコマンド行から呼び出されます。管理者は、編集するファイルを次のように引数として指定します。 `/usr/dt/bin/trusted_edit` *filename*
デバイス割り当てマネージャー	Trusted Extensions では、この GUI はデバイスを管理するために使用します。「デバイス管理」ダイアログボックスは、デバイスを構成する管理者が使用します。 デバイス割り当てマネージャーは、デバイスを割り当てるために、役割と一般ユーザーが使用します。GUI は、トラステッドパスメニューから利用できます。
ラベルビルダー	このアプリケーションは、ユーザーがラベルまたは認可上限を選択できるときに起動されます。また、このアプリケーションは、役割がラベルまたはラベル範囲をデバイス、ゾーン、ユーザー、または役割に割り当てるときにも表示されます。
選択マネージャー	このアプリケーションは、承認されたユーザーまたは承認された役割が、情報のアップグレードまたはダウングレードを試みているときに起動されます。
トラステッドパスメニュー	このメニューは、Trusted Computing Base (TCB) とのやり取りを処理します。たとえば、このメニューには「パスワードを変更」メニュー項目が表示されます。Trusted CDE では、ワークスペーススイッチ領域からトラステッドパスメニューにアクセスします。Trusted JDS では、トラステッドストライプの左にあるトラステッドシンボルをクリックして、トラステッドパスメニューにアクセスします。

管理コマンド

Trusted Extensions には、ラベルを取得したり、ほかのタスクを行うためのコマンドが用意されています。コマンドのリストについては、46 ページの「Trusted Extensions のコマンド行ツール」を参照してください。

Trusted Extensions による Solaris インタフェースの拡張

Trusted Extensions は、既存の Solaris 構成ファイル、コマンド、および GUI を拡張します。

管理コマンド

Trusted Extensions は、一部の Solaris コマンドにオプションを追加します。リストについては、表 2–5 を参照してください。

構成ファイル

Trusted Extensions は、`net_mac_aware` と `net_mlp` の 2 つの特権を追加します。`net_mac_aware` の使用法については、150 ページの「Trusted Extensions で NFS マウントされたディレクトリへのアクセス」を参照してください。

Trusted Extensions は、`auth_attr` データベースに承認を追加します。リストについては、『Solaris Trusted Extensions 移行ガイド』の「Trusted Extensions におけるその他の権限と承認」を参照してください。

Trusted Extensions は、`exec_attr` データベースに CDE アクションを含む実行可能ファイルを追加します。

Trusted Extensions は、`prof_attr` データベースの既存の権利プロファイルを修正します。また、データベースにプロファイルを追加します。

Trusted Extensions は、`exec_attr` データベースで特権を設定できる実行可能ファイルに、CDE アクションを追加します。

Trusted Extensions は、`policy.conf` データベースにフィールドを追加します。フィールドについては、82 ページの「Trusted Extensions の `policy.conf` ファイルのデフォルト」を参照してください。

	Trusted Extensions は、監査トークン、監査イベント、監査クラス、および監査ポリシーオプションを追加します。リストについては、270 ページの「Trusted Extensions の監査のリファレンス」を参照してください。
Solaris 管理コンソール	Trusted Extensions は、「コンピュータとネットワーク」ツールセットに「セキュリティーテンプレート」ツールを追加します。 Trusted Extensions は、「コンピュータとネットワーク」ツールセットに「トラステッドネットワークゾーン」ツールを追加します。 Trusted Extensions は、「ユーザー」ツールと「管理役割」ツールに「Trusted Extensions の属性」タブを追加します。
ゾーンからのディレクトリ共有	Trusted Extensions では、ラベル付きゾーンからディレクトリを共有できます。このディレクトリは、大域ゾーンから `/etc/dfs/dfstab` ファイルを作成することにより、ゾーンのラベルで共有されます。

Trusted Extensions の厳密なセキュリティーデフォルト

Trusted Extensions は、Solaris OS よりも厳密なセキュリティーデフォルトを確立します。

監査	デフォルトで監査は有効です。 管理者は監査をオフにできます。ただし、Trusted Extensions をインストールするサイトでは、一般的に監査が必要です。
デバイス	デフォルトでは、デバイス割り当ては有効です。 デフォルトで、デバイス割り当てには承認が必要です。したがって、一般ユーザーはデフォルトでリムーバブルメディアを使用できません。 管理者は、承認の要件を削除できます。ただし、Trusted Extensions をインストールするサイトでは、一般的にデバイスの割り当てが必要です。
印刷	一般ユーザーは、プリンタのラベル範囲にユーザーのラベルが含まれるプリンタのみで印刷が可能です。

デフォルトでは、トレーラとバナーページが出力されます。これらのページと本文ページには、印刷ジョブのラベルが含まれます。

デフォルトでは、ユーザーは PostScript ファイルを印刷できません。

役割

Solaris OS でも役割を使用できますが、使用は任意です。Trusted Extensions では、適切な管理に役割が必須です。

root ユーザーを役割にすることは、Solaris OS でも可能です。Trusted Extensions では、root ユーザーとして操作しているユーザーを詳細に監査するために、root ユーザーを役割にします。

Trusted Extensions で制限されるオプション

Trusted Extensions では、構成の選択肢の幅が Solaris よりも制限されています。

デスクトップ

Trusted Extensions は、Solaris Trusted Extensions (CDE) と Solaris Trusted Extensions (JDS) の 2 つのデスクトップを提供します。

ネームサービス

LDAP ネームサービスがサポートされます。すべてのゾーンは、1 つのネームサービスから管理される必要があります。

ゾーン

大域ゾーンは、管理用のゾーンです。root ユーザーまたは役割だけが、大域ゾーンに入ることができます。したがって、Solaris の一般ユーザーが使用できる管理インタフェースを、Trusted Extensions の一般ユーザーは使用できません。たとえば、Trusted Extensions では、ユーザーは Solaris 管理コンソールを起動できません。

非大域ゾーンはラベル付きゾーンです。ユーザーはラベル付きゾーンで作業します。

すべてのゾーンは、1 つのネームサービスから管理される必要があります。

◆ ◆ ◆ 付 録 B

Trusted Extensions マニュアルページのリスト

Solaris Trusted Extensions は、Solaris OS の構成要素のひとつです。この付録では、Trusted Extensions に関する情報が含まれている Solaris のマニュアルページについて簡単に説明します。

Trusted Extensions マニュアルページ (アルファベット順)

次のマニュアルページでは、Solaris システム上での Trusted Extensions ソフトウェアについて記載されています。これらのマニュアルページは、Trusted Extensions が構成されているシステムにのみ該当します。

Solaris マニュアルページ	機能説明
add_allocatable(1M)	割り当てデータベースへのエントリの追加
atohexlabel(1M)	人が認識できるラベルの内部テキスト形式への変換
blcompare(3TSOL)	バイナリラベルの比較
blminmax(3TSOL)	2 つのラベルの境界の判定
chk_encodings(1M)	ラベルエンコーディングファイルの構文の検査
dtappsession(1)	新規アプリケーションマネージャーセッションの起動
fgetlabel(2)	ファイルのラベルの取得
getdevicerange(3TSOL)	デバイスのラベル範囲の取得
getlabel(1)	ファイルラベルの表示
getlabel(2)	ファイルラベルの取得
getpathbylabel(3TSOL)	ゾーンのパス名の取得

getplabel(3TSOL)	プロセスラベルの取得
getuserrange(3TSOL)	ユーザーのラベル範囲の取得
getzoneidbylabel(3TSOL)	ゾーンラベルからのゾーン ID の取得
getzonelabelbyid(3TSOL)	ゾーン ID を使用したゾーンラベルの取得
getzonelabelbyname(3TSOL)	ゾーン名を使用したゾーンラベルの取得
getzonepath(1)	指定したラベルに対応するゾーンのルートパスの表示
getzonerootbyid(3TSOL)	ゾーンのルート ID を使用したゾーンのルートパス名の取得
getzonerootbylabel(3TSOL)	ゾーンラベルからのゾーンのルートパス名の取得
getzonerootbyname(3TSOL)	ゾーン名を使用したゾーンのルートパス名の取得
hextoalabel(1M)	内部テキストラベルの人が認識できる形式への変換
labelbuilder(3TSOL)	有効なラベルまたは認可上限を対話形式で構築するための Motif ベースのユーザーインタフェースの作成
labelclipping(3TSOL)	バイナリラベルの変換および指定された幅へのクリッピング
label_encodings(4)	ラベルエンコーディングファイルの説明
label_to_str(3TSOL)	ラベルを人が認識できる文字列へ変換
labels(5)	Solaris Trusted Extensions ラベル属性の説明
libtsnet(3LIB)	Solaris Trusted Extensions ネットワークライブラリ
libtsol(3LIB)	Solaris Trusted Extensions ライブラリ
m_label(3TSOL)	新規ラベル用のリソースの割り当てと解放
pam_tsol_account(5)	ラベルに関連したアカウント制限の検査
plabel(1)	プロセスラベルの取得
remove_allocatable(1M)	割り当てデータベースからのエントリの削除
sel_config(4)	コピー、カット、ペースト、およびドラッグ＆ドロップ操作時の選択規則

setflabel(3TSOL)	対応する機密ラベルを持つゾーンへのファイルの移動
smtnrhdb(1M)	Trusted Extensions ネットワークデータベース内のエントリの管理
smtnrhtp(1M)	Trusted Extensions ネットワーキング用のテンプレートデータベース内のエントリの管理
smtnzonecfg(1M)	非大域ゾーンでの Trusted Extensions ネットワーキング用の構成データベース内のエントリの管理
str_to_label(3TSOL)	人が認識できる文字列からラベルへの構文解析
tnctl(1M)	Trusted Extensions ネットワークパラメータの設定
tnd(1M)	トラステッドネットワークデーモン
tninfo(1M)	カーネルレベルの Trusted Extensions ネットワーク情報と統計の表示
trusted_extensions(5)	Trusted Extensions の概要
TrustedExtensionsPolicy(4)	Trusted Extensions X サーバー拡張用の構成ファイル
tsol_getrhtype(3TSOL)	Trusted Extensions ネットワーク情報からのホストタイプの取得
updatehome(1M)	現在のラベル用のホームディレクトリのコピーファイルとリンクファイルの更新
XTSOLgetClientAttributes(3XTSOL)	X クライアントのラベル属性の取得
XTSOLgetPropAttributes(3XTSOL)	ウィンドウプロパティーのラベル属性の取得
XTSOLgetPropLabel(3XTSOL)	ウィンドウプロパティーのラベルの取得
XTSOLgetPropUID(3XTSOL)	ウィンドウプロパティーの UID の取得
XTSOLgetResAttributes(3XTSOL)	ウィンドウまたはピクセルマップのすべてのラベル属性の取得
XTSOLgetResLabel(3XTSOL)	ウィンドウ、ピクセルマップ、またはカラーマップのラベルの取得
XTSOLgetResUID(3XTSOL)	ウィンドウまたはピクセルマップの UID の取得
XTSOLgetSSHeight(3XTSOL)	画面ストライプの高さの取得

XTSOLgetWorkstationOwner(3XTSOL)	ワークステーションの所有権の取得
XTSOLIsWindowTrusted(3XTSOL)	ウィンドウがトラステッドクライアントにより作成されたものかどうかのテスト
XTSOLMakeTPWindow(3XTSOL)	このウィンドウをトラステッドパスウィンドウにする
XTSOLsetPolyInstInfo(3XTSOL)	多インスタンス化情報の設定
XTSOLsetPropLabel(3XTSOL)	ウィンドウプロパティーのラベルの設定
XTSOLsetPropUID(3XTSOL)	ウィンドウプロパティーの UID の設定
XTSOLsetResLabel(3XTSOL)	ウィンドウまたはピクセルマップのラベルの設定
XTSOLsetResUID(3XTSOL)	ウィンドウ、ピクセルマップ、またはカラーマップの UID の設定
XTSOLsetSessionHI(3XTSOL)	セッション最上位機密ラベルをウィンドウサーバーに設定
XTSOLsetSessionLO(3XTSOL)	セッション最下位機密ラベルをウィンドウサーバーに設定
XTSOLsetSSHeight(3XTSOL)	画面ストライプの高さの設定
XTSOLsetWorkstationOwner(3XTSOL)	ワークステーションの所有権の設定

Trusted Extensions によって変更される Solaris マニュアルページ

Solaris Trusted Extensions では、Solaris の次のマニュアルページに情報が追加されます。

Solaris マニュアルページ	**Trusted Extensions** による修正
allocate(1)	ゾーン内のデバイスの割り当てと、ウィンドウ環境内でのデバイスのクリーニングをサポートするためのオプションの追加
auditconfig(1M)	ラベル付き情報のためのウィンドウポリシーの追加
audit_class(4)	X サーバー監査クラスの追加
audit_event(4)	監査イベントの追加
auditreduce(1M)	ラベル選択子の追加

auth_attr(4)	ラベル承認の追加
automount(1M)	下位レベルのホームディレクトリをマウントおよび参照するための機能の追加
cancel(1)	ユーザーの印刷ジョブを取り消す能力へのラベル制限の追加
deallocate(1)	ゾーン内のデバイスの解放、ウィンドウ環境でのデバイスのクリーニング、解放するデバイスの種類の指定をサポートするオプションの追加
device_clean(5)	Trusted Extensions でデフォルトで呼び出される
exec_attr(4)	プロファイルオブジェクトの一種としての CDE アクションの追加
getpflags(2)	プロセスフラグ NET_MAC_AWARE および NET_MAC_AWARE_INHERIT の認識
getsockopt(3SOCKET)	ソケットの必須のアクセス制御状態 SO_MAC_EXEMPT の取得
getsockopt(3XNET)	ソケットの必須のアクセス制御状態 SO_MAC_EXEMPT の取得
ifconfig(1M)	all-zones インタフェースの追加
is_system_labeled(3C)	システムに Trusted Extensions が構成されているかどうかを判定
ldaplist(1)	Trusted Extensions ネットワークデータベースの追加
list_devices(1)	デバイスに関連するラベルなどの属性の追加
lp(1)	-nolabels オプションの追加
lpadmin(1M)	管理者の印刷管理能力へのラベル制限の追加
lpmove(1M)	管理者の印刷ジョブ移動能力へのラベル制限の追加
lpq(1B)	印刷待ち行列情報の表示へのラベル制限の追加
lprm(1B)	呼び出し元の印刷要求の削除能力へのラベル制限の追加
lpsched(1M)	管理者の印刷サービスの停止と再起動能力へのラベル制限の追加
lpstat(1)	印刷サービス状態の表示へのラベル制限の追加
netstat(1M)	拡張セキュリティー属性を表示するための -R オプションの追加

privileges(5)	PRIV_FILE_DOWNGRADE_SL などの Trusted Extensions 特権の追加
prof_attr(4)	オブジェクトラベル管理などの権利プロファイルの追加
route(1M)	拡張セキュリティー属性を経路に追加するための -secattr オプションの追加
setpflags(2)	NET_MAC_AWARE プロセスフラグの設定
setsockopt(3SOCKET)	SO_MAC_EXEMPT オプションの設定
setsockopt(3XNET)	ソケットの必須のアクセス制御 SO_MAC_EXEMPT の設定
smexec(1M)	CDE アクションの種類をサポートするためのオプションの追加
smrole(1M)	役割のラベルをサポートするためのオプションの追加
smuser(1M)	ユーザーのラベルまたは許可されるアイドル時間などのセキュリティー属性をサポートするためのオプションの追加
socket.h(3HEAD)	ラベルなし接続先のための SO_MAC_EXEMPT オプションのサポート
tar(1)	tar ファイルへのラベルの追加と、ラベルに従ったファイルの抽出の追加
tar.h(3HEAD)	ラベル付き tar ファイルで使用する属性の種類の追加
ucred_getlabel(3C)	ユーザー証明書上のラベル値の取得の追加
user_attr(4)	Trusted Extensions 固有のユーザーセキュリティー属性の追加

索引

N

O

P

R

S

T

U

V

X

Z

あ

こ

さ

し

そ

た

ち

つ

て

と

な

に

ら

り

る

ろ

わ