Trusted Extensions 構成と管理

Part No: E25902
2011 年 12 月

ORACLE

120411@25097

目次

図目次

表目次

はじめに

『Trusted Extensions 構成と管理』では、Oracle Solaris オペレーティングシステム (Oracle Solaris OS) 上で Trusted Extensions 機能の有効化や初期構成を行うための手順を説明します。また、このマニュアルでは、Trusted Extensions システムで ユーザー、ゾーン、デバイス、およびホストを管理するための手順についても説明します。

注 – この Oracle Solaris のリリースでは、SPARC および x86 系列のプロセッサアーキテクチャーを使用するシステムをサポートしています。サポートされるシステムについては、Oracle Solaris OS: Hardware Compatibility Lists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。

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、Oracle 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 (『Trusted Extensions ユーザーガイド』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。

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

Trusted Extensions は、Oracle Solaris OS の上で動作します。Trusted Extensions ソフトウェアは Oracle Solaris OS を変更する場合があるので、Trusted Extensions では、Oracle Solaris のインストールオプションに関して特定の設定が必要になることがあります。このマニュアルのパート I では、Oracle Solaris OS を Trusted Extensions 用に準備する方法、Trusted Extensions を有効化する方法、およびこのソフトウェアの初期構成を行う方法について説明します。このマニュアルのパート II では、システムの Trusted Extensions 機能を一意に管理する方法について説明します。

Trusted Extensions マニュアルセットの構成

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

ガイドのタイトル	トピック	対象読者
『Trusted Extensions ユーザーガイド』	Trusted Extensions. の基本的な機能について説明しています。このマニュアルには用語集が含まれています。	エンドユーザー、管理者、開発者
『Trusted Extensions 構成と管理』	パート I では、Trusted Extensions の準備、有効化、および初期構成を行う方法について説明します。 パート II では、Trusted Extensions システムの管理方法について説明します。このマニュアルには用語集が含まれています。	管理者、開発者
『Trusted Extensions Developer's Guide』	Trusted Extensions を使ってアプリケーションを開発する方法について説明しています。	開発者、管理者
『Trusted Extensions Label Administration』	ラベルエンコーディングファイルでのラベルコンポーネントの指定方法について説明します。	管理者
『Compartmented Mode Workstation Labeling: Encodings Format 』	ラベルエンコーディングファイルで使用される構文について説明します。構文を使用することにより、適格な形式のラベルに関するさまざまな規則がシステムに適用されます。	管理者

関連するシステム管理マニュアル

次に示すマニュアルには、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
『SPARC プラットフォームでの Oracle Solaris のブートおよびシャットダウン』	システムのブートおよびシャットダウン、ブートサービスの管理、ブート動作の変更、ZFS からのブート、ブートアーカイブの管理、および SPARC プラットフォーム上でのブートのトラブルシューティング
『x86 プラットフォーム上の Oracle Solaris のブートおよびシャットダウン』	システムのブートおよびシャットダウン、ブートサービスの管理、ブート動作の変更、ZFS からのブート、ブートアーカイブの管理、および x86 プラットフォーム上でのブートのトラブルシューティング
『Oracle Solaris の管理: 一般的なタスク』	Oracle Solaris コマンドの使用、システムのブートとシャットダウン、ユーザーアカウントとグループの管理、サービス、ハードウェア障害、システム情報、システムリソース、およびシステムパフォーマンスの管理、ソフトウェアの管理、印刷、コンソールと端末、およびシステムやソフトウェアの問題のトラブルシューティング
『Oracle Solaris の管理: 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
『Oracle Solaris の管理: IP サービス』	TCP/IP ネットワーク管理、IPv4 および IPv6 アドレスの管理、DHCP、IPsec、IKE、IP フィルタ、および IPQoS
『Oracle Solaris Administration: Naming and Directory Services』	DNS、NIS、および LDAP ネームサービスおよびディレクトリサービス (NIS から LDAP への移行を含む)
『Oracle Solaris 管理: ネットワークインタフェースとネットワーク仮想化』	WiFi ワイヤレスを含む自動および手動の IP インタフェース構成、ブリッジ、VLAN、集積体、LLDP、および IPMP の管理、仮想 NIC とリソース管理
『Oracle 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
『Oracle Solaris のシステム管理 (Oracle Solaris ゾーン、Oracle Solaris 10 ゾーン、およびリソース管理)』	アプリケーションが使用可能なシステムリソースを使用する方法の制御を可能にするリソース管理機能、オペレーティングシステムのサービスを仮想化してアプリケーション実行用の隔離環境を作成する Oracle Solaris ゾーンソフトウェア区分技術、および Oracle Solaris 11 カーネル上で動作する Oracle Solaris 10 環境をホストする Oracle Solaris 10 ゾーン

マニュアルのタイトル	トピック
『Oracle Solaris の管理: セキュリティーサービス』	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、暗号化フレームワーク、鍵管理、特権、RBAC、SASL、Secure Shell、およびウィルススキャン
『Oracle Solaris Administration: SMB and Windows Interoperability 』	SMB クライアントから SMB 共有を使用できるように Oracle Solaris システムを構成することを可能にする SMB サービス、SMB 共有へのアクセスを可能にする SMB クライアント、および Oracle Solaris システムと Windows システムとの間でユーザーやグループの ID をマッピングできるようにするネイティブアイデンティティーマッピングサービス
『Oracle Solaris の管理: ZFS ファイルシステム』	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) を使用した ZFS ファイルの保護、ゾーンがインストールされた Oracle Solaris システム上での ZFS の使用
『Trusted Extensions 構成と管理』	Trusted Extensions に固有なシステムのインストール、構成、および管理
『Oracle Solaris 11 セキュリティーガイドライン』	Oracle Solaris システムのセキュリティー保護、およびゾーン、ZFS、Trusted Extensions などのセキュリティー機能の使用シナリオ
『Oracle Solaris 10 から Oracle Solaris 11 への移行』	Oracle Solaris 10 から Oracle Solaris 11 への移行に関するシステム管理情報や例の提供 (インストール、デバイス、ディスク、およびファイルシステムの管理、ソフトウェア管理、ネットワーキング、システム管理、セキュリティー、仮想化、デスクトップ機能、ユーザーアカウント管理とユーザー環境、エミュレートされたボリューム、トラブルシューティングとデータ回復の各分野)

関連資料

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

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。

関連するサードパーティーの Web サイト情報

このドキュメントにはオラクル社およびその関連会社が所有または管理しない Web サイトへのリンクが含まれている場合があります。

注 – オラクル社およびその関連会社は、それらの Web サイトのアクセシビリティに関しての評価や言及は行っておりません。このソフトウェアまたはハードウェア、そしてドキュメントは、第三者のコンテンツ、製品、サービスへのアクセス、あるいはそれらに関する情報を提供することがあります。オラクル社およびその関連会社は、第三者のコンテンツ、製品、サービスに関して一切の責任を負わず、いかなる保証もいたしません。オラクル社およびその関連会社は、第三者のコンテンツ、製品、サービスへのアクセスまたは使用によって損失、費用、あるいは損害が発生しても一切の責任を負いかねます。

Oracle サポートへのアクセス

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

表記上の規則

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。

表 P–1 表記上の規則 (続き)

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

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

- C シェル

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

- C シェルのスーパーユーザー

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

- Bash シェル、Korn シェル、および Bourne シェル

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

- Bash シェル、Korn シェル、および Bourne シェルのスーパーユーザー

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

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

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

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

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

パート I

Trusted Extensions の初期構成

このパートの各章では、Trusted Extensions を実行できるように Oracle Solaris システムを準備する方法について説明します。これらの章では、Trusted Extensions の有効化と初期構成のタスクについて説明します。

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

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

第 3 章「Oracle Solaris への Trusted Extensions 機能の追加 (手順)」では、Trusted Extensions ソフトウェア用に Oracle Solaris システムを準備する手順を示します。Trusted Extensions を有効化してログインする方法について説明します。

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

第 5 章「Trusted Extensions のための LDAP の構成 (手順)」では、Trusted Extensions システム上で LDAP ネームサービスを構成する手順を示します。

◆ ◆ ◆ 第 1 章

Trusted Extensions のセキュリティー計画

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

Trusted Extensions でのセキュリティー計画

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

Trusted Extensions の構成タスクのチェックリストについては、付録 B 「Trusted Extensions の構成チェックリスト」を参照してください。サイトのローカライズについては、30 ページの「英語以外のロケールで Trusted Extensions を使用するお客

様」を参照してください。評価された構成の実行については、28 ページの「サイトのセキュリティーポリシーについて」を参照してください。

Trusted Extensions について

Solaris Trusted Extensions の有効化および構成は、実行可能ファイルの読み込み、サイトのデータの指定、構成変数の設定などのタスクにとどまりません。高度な予備知識が必要です。Trusted Extensions ソフトウェアは、次の 2 つの Oracle Solaris 機能に基づいたラベル付き環境を実現します。

- ほとんどの UNIX 環境でスーパーユーザーに割り当てられる機能は、個別の管理役割によって処理されます。
- 特定のユーザーおよびアプリケーションがセキュリティーポリシーを上書きできるようにできます。

Trusted Extensions では、データへのアクセスは特殊なセキュリティータグによって制御されます。このようなタグをラベルと言います。ラベルはユーザー、プロセス、およびデータファイルやディレクトリなどのオブジェクトに割り当てられます。UNIX アクセス権つまり随意アクセス制御 (DAC) に加え、これらのラベルは必須アクセス制御 (MAC) を提供します。

サイトのセキュリティーポリシーについて

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

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

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

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

- `/etc/system` ファイルのカーネルスイッチの設定の変更。
- 監査またはデバイス割り当てのオフ。

- /usr ディレクトリの公開ファイル内のデフォルトエントリの変更。

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

Trusted Extensions の管理ストラテジの作成

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

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

管理ストラテジの一環として、次の事項を決定する必要があります。

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

ラベルストラテジの作成

ラベルを計画するには、機密ラベルの階層を定め、システム上の情報を分類する必要があります。label_encodings ファイルには、サイトについてのこの種の情報が含まれます。Trusted Extensions ソフトウェアで提供されている label_encodings ファイルのいずれかを使用できます。あるいは、その提供ファイルのいずれかを変更したり、サイト固有の label_encodings ファイルを新たに作成したりできます。このファイルには、Oracle 固有のローカルな拡張機能、少なくとも COLOR NAMES セクションを組み込んでください。

注意 – label_encodings ファイルを提供する場合のベストプラクティスは、ラベルがシステムによって検証される前にこのファイルの最終版をインストールしておくことです。ラベルの検証は、Trusted Extensions サービスを有効化したあとの最初のブート中に行われます。最初のゾーンやネットワークテンプレートを作成したあとで label_encodings ファイルを変更する場合は必ず、既存のゾーンやテンプレートも考慮に入れる必要があります。

ラベルの計画には、そのラベル構成の計画も含まれます。Trusted Extensions サービスの有効化が完了したら、複数のラベルでシステムにログインできるようにする必要があるのか、それとも 1 つのユーザーラベルのみを使用してシステムを構成することができるのかを決定する必要があります。たとえば、LDAP サーバーは、1 つのラベル付きゾーンを使用する場合の適切な候補になります。このサーバーのローカル管理を行うために、最小ラベルのゾーンを 1 つ作成します。システムを管理するには、管理者はログインし、ユーザーワークスペースから適切な役割になります。

詳細は、『Trusted Extensions Label Administration 』を参照してください。『Compartmented Mode Workstation Labeling: Encodings Format』も参照してください。

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

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

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

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

- 『Oracle Solaris 11 システムのインストール』、およびこのリリースの『リリースノート』の「インストール」の節で説明されている、Oracle Solaris リリースのインストールに関する推奨事項に従ってください。
- そこに示されるほかに、Trusted Extensions ではさらに追加される推奨事項があります。
  - 次のシステムでは、推奨される最小容量よりも多くのメモリーが必要です。
    - 複数の機密ラベルで実行されるシステム
    - 管理役割になれるユーザーが使用するシステム
  - 次のシステムではより多くのディスク容量が必要です。
    - 複数のラベルでファイルを格納するシステム
    - ユーザーが管理役割になれるシステム

トラステッドネットワークの計画

ネットワークハードウェアの計画については、『Oracle Solaris の管理: IP サービス』の第 1 章「ネットワーク配備の計画」を参照してください。

Trusted Extensions ソフトウェアは、cipso と unlabeled の 2 種類のホストを識別します。どちらの種類のホストにも、表 1–1 に示すデフォルトのセキュリティーテンプレートがあります。

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

ホストの種類	テンプレート名	目的
`unlabeled`	`admin_low`	大域ゾーンと通信可能な信頼できないホストを識別するために使用されます。そのようなホストはラベルを含まないパケットを送信します。詳細については、ラベルなしシステムを参照してください。
`cipso`	`cipso`	CIPSO パケットを送信するホストまたはネットワークを識別するために使用されます。CIPSO パケットはラベル付けされます。

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

ホスト、ゲートウェイ、およびネットワークのラベル付けについては、第 16 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。遠隔システムへのラベルの割り当ては、初期設定のあとで実行されます。

Trusted Extensions でのゾーン計画

Trusted Extensions ソフトウェアは、Oracle Solaris の大域ゾーンに追加されます。そのあとで、ラベル付きの非大域ゾーンを設定します。重複しないすべてのラベルに対してそれぞれ 1 つのラベル付きゾーンを作成できますが、`label_encodings` ファイル内のすべてのラベルに対してゾーンを作成する必要はありません。提供されているスクリプトを使用すれば、`label_encodings` ファイル内のデフォルトユーザーラベルとデフォルトユーザー認可上限に対応する 2 つのラベル付きゾーンを容易に作成できます。

ラベル付きゾーンを作成したあと、一般ユーザーは、構成されたシステムを使用できますが、ほかのシステムには接続されません。

- Trusted Extensions では、X サーバーに接続するためのローカルトランスポートは、UNIX ドメインソケットです。デフォルトでは、X サーバーは TCP 接続に対して待機しません。
- デフォルトでは、非大域ゾーンは信頼できないホストと通信できません。各ゾーンから到達可能な遠隔ホストの具体的な IP アドレスまたはネットワークマスクを指定する必要があります。

Trusted Extensions ゾーンと Oracle Solaris ゾーン

Trusted Extensions ゾーンつまりラベル付きゾーンは、Oracle Solaris ゾーンのブランドの 1 つです。ラベル付きゾーンは、主にデータを分けるために使用されます。Trusted Extensions では、一般ユーザーは、別のトラステッドシステム上の同一のラベルを持つゾーンからログインを行う場合を除き、遠隔でラベル付きゾーンにログインすることはできません。承認された管理者は、大域ゾーンからラベル付きゾーンにアクセスできます。ゾーンブランドの詳細については、`brands(5)` のマニュアルページを参照してください。

Trusted Extensions でのゾーン作成

Trusted Extensions でのゾーン作成は Oracle Solaris でのゾーン作成に似ています。Trusted Extensions には、このプロセスを案内する `txzonemgr` スクリプトが用意されています。このスクリプトには、ラベル付きゾーンの作成を自動化するためのコマンド行オプションがいくつかあります。

ラベル付きゾーンへのアクセス

適切に構成されたシステム上では、すべてのゾーンがネットワークアドレスを使用して同じラベルを共有するほかのゾーンと通信できる必要があります。次の各構成は、ラベル付きゾーンからほかのラベル付きゾーンへのアクセス機能を提供します。

- **all-zones** インタフェース – 1 つの `all-zones` アドレスが割り当てられます。このデフォルト構成で必要となる IP アドレスは、1 つだけです。大域ゾーンとラベル付きゾーンを含むすべてのゾーンは、この共有アドレス経由で遠隔システム上の同一のラベルを持つゾーンと通信できます。

  この構成の改良版として、大域ゾーンが排他的に使用するための 2 つ目の IP インスタンスを作成することが挙げられます。この 2 つ目のインスタンスは `all-zones` アドレスではありません。この IP インスタンスは、マルチレベルサービスをホストしたりプライベートへの経路を提供したりするために使用できる。
- **IP** インスタンス – Oracle Solaris OS と同様に、大域ゾーンを含むすべてのゾーンにそれぞれの IP アドレスが割り当てられています。これらのゾーンは IP スタックを共有します。もっとも単純な場合には、すべてのゾーンが同じ物理インタフェースを共有します。

ゾーンごとに別々のネットワーク情報カード (NIC) を割り当てれば、この構成がさらに改善されます。このような構成は、各 NIC に関連付けられている単一ラベルのネットワークを物理的に分離するために使用されます。

さらなる改良版として、ゾーンごとの IP インスタンスに加えて 1 つ以上の `all-zones` インタフェースを使用することが挙げられます。この構成では、`vni0` などの内部インタフェースを使用して大域ゾーンに到達できるため、遠隔攻撃から大域ゾーンを保護できます。たとえば、大域ゾーンで `vni0` のインスタンスにマルチレベルポートをバインドした特権付きサービスに内部から到達できるのは、共有スタックを使用しているゾーンだけです。

- 排他的 **IP** スタック – Oracle Solaris OS と同様に、大域ゾーンを含むすべてのゾーンにそれぞれの IP アドレスが割り当てられています。仮想ネットワークインタフェースカード (VNIC) がラベル付きゾーンごとに 1 つずつ作成されます。

  この構成の改良版として、各 VNIC をそれぞれ異なるネットワークインタフェース上に作成することが挙げられます。このような構成は、各 NIC に関連付けられている単一ラベルのネットワークを物理的に分離するために使用されます。排他的 IP スタックで構成されたゾーンは `all-zones` インタフェースを使用できません。

マルチレベルサービスの計画

デフォルトでは、Trusted Extensions はマルチレベルサービスを提供しません。ほとんどのサービスはゾーンからゾーンへのサービスとして、つまりシングルラベルサービスとして簡単に構成されます。たとえば、各ラベル付きゾーンは、そのラベル付きゾーンのラベルで実行されている NFS サーバーに接続できます。

サイトでマルチレベルサービスが必要になった場合、それらのサービスの構成先として最適なのは、少なくとも 2 つの IP アドレスを持つシステムです。マルチレベルサービスで必要になるマルチレベルポートは、大域ゾーンに関連付けられた IP アドレスに割り当てることができます。`all-zones` アドレスを使用すれば、ラベル付きゾーンからそれらのサービスに到達できます。

ヒント – ラベル付きゾーンのユーザーがマルチレベルサービスにアクセスできないようにする場合は、1 つの IP アドレスをシステムに割り当てることができます。この Trusted Extensions 構成は、主としてラップトップコンピュータで使用します。

Trusted Extensions での LDAP ネームサービスの計画

ラベル付きシステムのネットワークの構成を計画していない場合、この節は省略できます。LDAP を使用する予定の場合は、最初のラベル付きゾーンを追加する前にシステムを LDAP クライアントとして構成しておく必要があります。

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

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

Trusted Extensions での監査の計画

デフォルトでは、Trusted Extensions の初回ブート時に監査が有効化されます。したがってデフォルトでは、`login/logout` クラスのすべてのイベントが監査対象となります。システムを構成しようとするユーザーを監査するために、構成プロセスの最初の段階で役割を作成できます。それらの役割がシステムを構成する際に、その役割になったログインユーザーが監査レコードに含まれます。67 ページの「Trusted Extensions での役割とユーザーの作成」を参照してください。

Trusted Extensions での監査の計画は、Oracle Solaris OS の場合と同じです。詳細については、『Oracle Solaris の管理: セキュリティーサービス』のパート VII「Oracle Solaris での監査」を参照してください。Trusted Extensions は、クラス、イベント、および監査トークンを追加しますが、監査の管理方法は変更されません。監査に対する Trusted Extensions による追加については、第 22 章「Trusted Extensions での監査 (概要)」を参照してください。

Trusted Extensions でのユーザーセキュリティーの計画

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

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

ファイル名	キーワード	値
/etc/security/policy.conf	IDLECMD	lock | logout
	IDLETIME	30
	CRYPT_ALGORITHMS_ALLOW	1,2a,md5,5,6
	CRYPT_DEFAULT	sha256
	LOCK_AFTER_RETRIES	no | yes
	PRIV_DEFAULT	basic
	PRIV_LIMIT	all
	AUTHS_GRANTED	solaris.device.cdrw
	CONSOLE_USER	Console User
	PROFS_GRANTED	Basic Solaris User
/etc/security/tsol/label_encodings の LOCAL DEFINITIONS セクション	Default User Clearance	CNF INTERNAL USE ONLY
	Default User Sensitivity Label	PUBLIC

注 – IDLECMD 変数と IDLETIME 変数はログインユーザーのセッションに適用されます。ログインユーザーがある役割になると、その役割に対するユーザーの IDLECMD 値と IDLETIME 値が有効となります。

システム管理者は、すべてのユーザーに適切なシステムデフォルト値を設定するための標準ユーザーテンプレートを作成できます。たとえば、デフォルトでは各ユーザーの初期シェルは Bash シェルになります。システム管理者は、各ユーザーに対して pfbash シェルを設定したテンプレートを作成できます。

Trusted Extensions の構成ストラテジの作成

次に、もっとも安全な構成ストラテジから順に示します。

- 2 人のチームでソフトウェアを構成します。構成プロセスは監査されます。

  ソフトウェアを有効化するとき、2 人でコンピュータに向かいます。このチームは構成プロセスの初期段階で、個別の役割とそれらの役割になれるローカルユーザーを作成します。チームは、役割によって実行されるイベントを監査するための監査も設定します。ユーザーに役割が割り当てられ、コンピュータがリブートされたあと、ユーザーはログインし、制限された役割になります。このソ

フトウェアが役割によるタスク区分を実施します。監査証跡が構成プロセスの記録を提供します。安全な構成プロセスの図解については、図 1–1 を参照してください。

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

  構成プロセスの初期段階で、root 役割が追加の役割を作成します。root 役割は、役割によって実行されるイベントを監査するための監査も設定します。これらの追加の役割が最初のユーザーに割り当てられ、コンピュータがリブートされたあと、ユーザーはログインし、現在のタスクに適した役割になります。監査証跡が構成プロセスの記録を提供します。

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

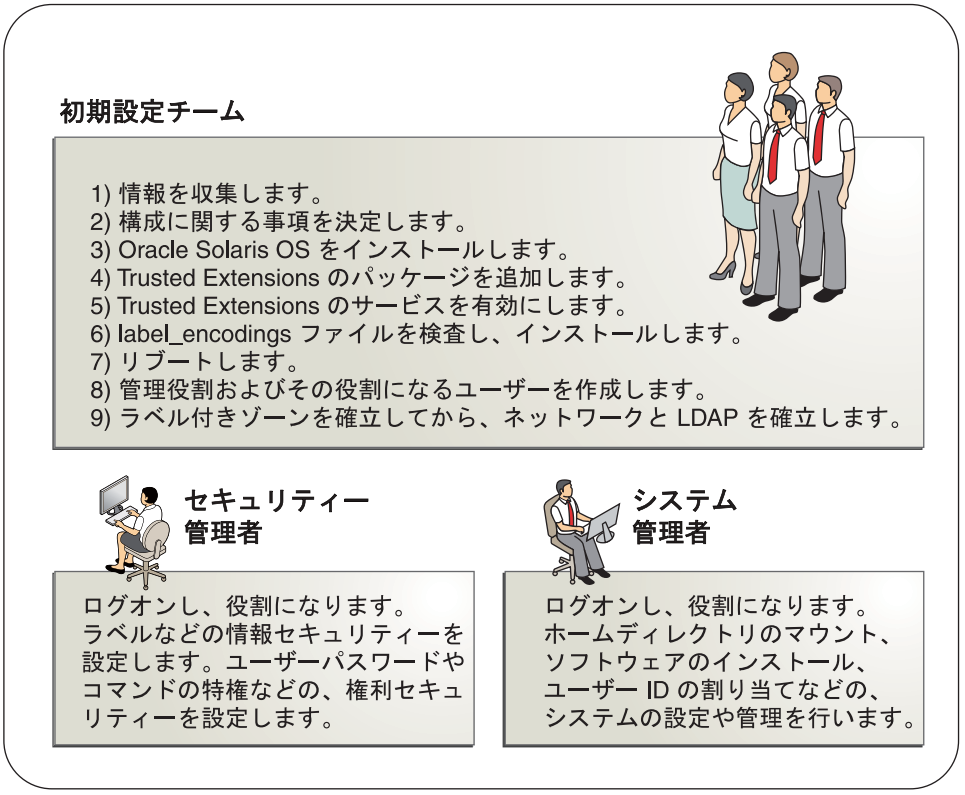
  このストラテジでは、構成プロセスは記録されません。

- 初期設定チームが root 役割をユーザーに変更します。

  このソフトウェアには、root として作業しているユーザーの名前に関するレコードは一切保持されません。この設定は、ヘッドレスシステムの遠隔管理で必要になる可能性があります。

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

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



Trusted Extensions 有効化前のその他の問題の解決

Trusted Extensions を構成する前に、システムを物理的に保護し、ゾーンに関連付けるラベルを決定し、セキュリティーに関するその他の問題を解決する必要があります。手順については、46 ページの「Trusted Extensions 有効化前のセキュリティー問題の解決」を参照してください。

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

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

管理者の立場から見たTrusted Extensionsの有効化の結果

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

- Oracle label_encodings ファイルがインストールされて構成されます。
- トラステッドデスクトップ Solaris Trusted Extensions (GNOME) によって、管理ワークスペースを提供するラベル付きウィンドウ表示環境が大域ゾーン内に作成されます。これらのワークスペースは、トラステッドストライプに表示されるトラステッドパスによって保護されます。
- Oracle Solaris OS と同様に、役割の権利プロファイルが定義されます。Oracle Solaris OS と同様に、`root` が唯一の定義済みの役割になります。

  追加の役割を使用して Trusted Extensions を管理するためには、その役割を作成する必要があります。構成時に、セキュリティー管理者役割を作成します。
- 3 つの Trusted Extensions ネットワークデータベース `tnrhdb`、 `tnrhtp`、および `tnzonecfg` が追加されます。`tncfg` コマンドを使用すると、管理者はこれらのトラステッドデータベースを表示および変更できます。
- Trusted Extensions に、システムを管理するための GUI が表示されます。完全な一覧については、第 7 章「Trusted Extensions 管理ツール」を参照してください。
  - `txzonemgr` スクリプトを使用すると、管理者は Trusted Extensions のゾーンやネットワークを構成できます。詳細については、`txzonemgr(1M)` のマニュアルページを参照してください。
  - デバイスマネージャーは、接続されたデバイスの割り当てやラベル付けを管理します。

◆ ◆ ◆ 第 2 章

Trusted Extensions の構成ロードマップ

この章では、Oracle Solaris の Trusted Extensions 機能を有効化および構成するための作業について概説します。

注意 – Trusted Extensions を遠隔で有効化および構成する場合は、Trusted Extensions 環境をブートする前に第 12 章「Trusted Extensions での遠隔管理 (手順)」をよく確認してください。

作業マップ: Trusted Extensions の準備と有効化

システムの準備と Trusted Extensions の有効化を行うには、次の作業を実行します。

作業	参照先
■ 既存の Oracle Solaris インストールを Trusted Extensions 用に準備します ■ Trusted Extensions を考慮して Oracle Solaris OS をインストールします。	■ 44 ページの「インストール済み Oracle Solaris システムを Trusted Extensions 用に準備する」 ■ 44 ページの「Oracle Solaris システムを安全にインストールする」
システムおよび Trusted Extensions ネットワークに関する情報を収集し、必要な事項を決定します。	46 ページの「Trusted Extensions 有効化前のセキュリティー問題の解決」
Trusted Extensions を有効にします。	48 ページの「Trusted Extensions を有効化してリブートする」

作業マップ:Trusted Extensions の構成の選択

次の作業マップのいずれかの方法を使用して、システムの Trusted Extensions を構成します。

作業	参照先
デモ用の Trusted Extensions システムを作成します。	40 ページの「作業マップ: 提供されたデフォルトを使用した Trusted Extensions の構成」
企業用の Trusted Extensions システムを作成します。	41 ページの「作業マップ: サイトの要件に応じた Trusted Extensions の構成」
遠隔システムで Trusted Extensions を構成します。	Trusted Extensions を有効化しますが、リブートは行いません。第 12 章「Trusted Extensions での遠隔管理 (手順)」の手順に従います。その後、モニターを備えたシステム用の手順に進みます。

作業マップ:提供されたデフォルトを使用した Trusted Extensions の構成

デフォルトの構成では、次の作業を順番に実行します。

作業	参照先
Trusted Extensions のパッケージを読み込みます。	45 ページの「Oracle Solaris システムに Trusted Extensions のパッケージを追加する」
Trusted Extensions を有効化してリブートします。	48 ページの「Trusted Extensions を有効化してリブートする」
ログインします。	49 ページの「Trusted Extensions にログインする」
2 つのラベル付きゾーンを作成します。	56 ページの「デフォルトの Trusted Extensions システムを作成する」 または 57 ページの「ラベル付きゾーンを対話形式で作成する」
ゾーンのラベル付きワークスペースを作成します。	59 ページの「2 つのゾーンワークスペースにラベルを割り当てる」

作業マップ: サイトの要件に応じた Trusted Extensions の構成

ヒント – 構成プロセスをセキュリティー保護するには、プロセスの初期段階で役割を作成します。

作業の順番は、次の作業マップに示されています。

- 56 ページの「ラベル付きゾーンの作成」の作業を行う必要があります。
- サイトの要件に応じて、その他の構成作業を実行します。

作業	参照先
大域ゾーンを構成します。	51 ページの「Trusted Extensions での大域ゾーンの設定」
ラベル付きゾーンを構成します。	56 ページの「ラベル付きゾーンの作成」
ほかのシステムと通信する場合は、ネットワークの設定を行います。	61 ページの「Trusted Extensions でのネットワークインタフェースの構成」
LDAP ネームサービスを構成します。 注 – LDAP を使用しない場合は省略してください。	第 5 章「Trusted Extensions のための LDAP の構成 (手順)」
システムの構成を完了します。	パート II「Trusted Extensions の管理」

◆ ◆ ◆ 第 3 章

Oracle Solaris への Trusted Extensions 機能の追加 (手順)

この章では、Oracle Solaris システム上で Trusted Extensions サービスの準備と有効化を行う方法について説明します。この章で扱う内容は、次のとおりです。

初期設定チームの担当

Trusted Extensions ソフトウェアは、別々のタスクを担当する 2 人によって構成されるように設計されています。このタスク区分は役割によって実現できます。Trusted Extensions のインストールが終了するまで個々の役割と追加のユーザーは作成されないので、有効化および構成は、少なくとも 2 人で構成される初期設定チームで行うことをお勧めします。

Oracle Solaris システムの準備と Trusted Extensions の追加

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

- Trusted Extensions を適切にサポートするには、基盤となる Oracle Solaris OS を確実にインストールする必要があります。Trusted Extensions に影響を与える Oracle Solaris インストールの選択肢については、44 ページの「Oracle Solaris システムを安全にインストールする」を参照してください。
- すでに Oracle Solaris OS を使用している場合は、現在の構成を Trusted Extensions の要件と比較してください。Trusted Extensions に影響する要因については、44 ページの「インストール済み Oracle Solaris システムを Trusted Extensions 用に準備する」を参照してください。

▼ Oracle Solaris システムを安全にインストールする

ここに示すタスクは、Oracle Solaris のフレッシュインストールの場合に該当します。アップグレードの場合は、44 ページの「インストール済み Oracle Solaris システムを Trusted Extensions 用に準備する」を参照してください。

1 **Oracle Solaris OS のインストール時にユーザーアカウントと root 役割アカウントを作成します。**

Trusted Extensions では、システムを構成する際に、ユーザーが作成した役割のほかに root 役割も使用します。

2 **Oracle Solaris への初回ログイン時に root 役割アカウントにパスワードを割り当てます。**

a. 端末ウィンドウを開きます。

b. **root の役割になります。**

プロンプトで、ユーザーアカウントのパスワードと異なるパスワードを入力します。

```
% su -
Your password has expired. Create a new password.
Enter new password:       Type a password for root
Retype the password:      Retype the root password
#
```

6 文字以上の英数字のパスワードを割り当てます。パスワードは推測が困難なものにする必要があります。そうすれば、攻撃者がパスワードを推測して承認されていないアクセス権を取得する可能性が低くなります。

次の手順 45 ページの「Oracle Solaris システムに Trusted Extensions のパッケージを追加する」に進みます。

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

ここに示すタスクは、すでに使用している Oracle Solaris システムがあり、その上で Trusted Extensions を実行する場合に該当します。

始める前に 大域ゾーンで root 役割になっている必要があります。

1 非大域ゾーンがシステムにインストールされている場合は、削除してください。
Trusted Extensions のラベル付きブランドは、ゾーンの排他的なブランドです。brands(5) および trusted_extensions(5) のマニュアルページを参照してください。

2 システムに **root** パスワードがない場合は作成します。

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

次の手順 45 ページの「Oracle Solaris システムに Trusted Extensions のパッケージを追加する」に進みます。

▼ Oracle Solaris システムに Trusted Extensions のパッケージを追加する

始める前に 44 ページの「インストール済み Oracle Solaris システムを Trusted Extensions 用に準備する」、44 ページの「Oracle Solaris システムを安全にインストールする」のいずれかを完了しています。

Software Installation 権利プロファイルが割り当てられている必要があります。

1 初期ユーザーとしてログインしたあと、端末ウィンドウで **root** 役割になります。

```
% su -
Enter Password:      Type root password
#
```

2 **Trusted Extensions** のパッケージをダウンロードしてインストールします。
コマンド行とパッケージマネージャー GUI のいずれかを使用します。

- 端末ウィンドウで **pkg install** コマンドを使用します。

```
$ pkg install system/trusted/trusted-extensions
```

トラステッドロケールをインストールするには、そのロケールの短縮名を指定します。たとえば、次のコマンドは日本語ロケールをインストールします。

```
$ pkg install system/trusted/locale/ja &
```

- 端末ウィンドウでパッケージマネージャー **GUI** を起動します。

  ```
  $ packagemanager &
  ```

  a. **Trusted Extensions** のパッケージを選択します。

     i. 「デスクトップ **(GNOME)**」カテゴリ内のカテゴリを表示します。

     ii. 「**Trusted Extensions**」カテゴリを選択します。

     iii. パッケージのリストで、**trusted-extensions** のチェックボックスをクリックします。

     iv. **(**省略可能**)** パッケージのリストで、インストールするすべてのロケールのチェックボックスをクリックします。

  b. パッケージを追加するには、「インストール/更新」アイコンをクリックします。

Trusted Extensions 有効化前のセキュリティー問題の解決

Trusted Extensions を構成するシステムごとに、構成に関する決定をいくつか行う必要があります。たとえば、Trusted Extensions のデフォルトの構成をインストールするのか、それとも構成をカスタマイズするのかを決定する必要があります。

▼ Trusted Extensions を有効化する前にシステムハードウェアのセキュリティー保護とセキュリティーに関する決定を行う

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

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

セキュリティー保護されたサイトでは、すべての Oracle Solaris システムで次の手順を実行します。

- SPARC システムの場合、PROM のセキュリティーレベルを選択し、パスワードを提供します。
- x86 システムの場合、BIOS を保護します。
- すべてのシステムで、`root` をパスワードで保護します。

2 **label_encodings** ファイルを準備します。

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

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

3 **label_encodings** ファイルのラベルのリストから、作成する予定のラベル付きゾーンのリストを作成します。

デフォルトの label_encodings ファイルの場合、ラベルは次のとおりであり、ゾーン名も同様にできます。

完全なラベル名	推奨ゾーン名
PUBLIC	public
CONFIDENTIAL: INTERNAL USE ONLY	internal
CONFIDENTIAL : NEED TO KNOW	needtoknow
CONFIDENTIAL : RESTRICTED	restricted

注 – 自動構成の方法では、public ゾーンと internal ゾーンが作成されます。

4 役割をいつ作成するかを決定します。

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

個別の役割を使用してシステムを構成する必要がない場合、root 役割でシステムを構成できます。この構成方法はあまり安全ではありません。root 役割がシステム上のすべてのタスクを実行できるのに対し、ほかの役割は通常より限定された一連のタスクを実行します。したがって、ユーザーが作成した役割を使って構成を実行すれば、構成がより細かく制御されます。

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

たとえば、次のようなセキュリティーに関する問題を検討します。

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

Trusted Extensions サービスの有効化とログイン

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

注 – ラップトップやワークステーションなど、ビットマップディスプレイが直接接続されたデスクトップを実行する際には、Trusted Extensions システムはネットワークを必要としません。他のシステムと通信するには、ネットワーク構成が必要です。

▼ Trusted Extensions を有効化してリブートする

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

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

始める前に　43 ページの「Oracle Solaris システムの準備と Trusted Extensions の追加」および 46 ページの「Trusted Extensions 有効化前のセキュリティー問題の解決」のタスクを完了しています。

大域ゾーンで `root` 役割になっている必要があります。

1. パネルを画面最上部から画面最下部に移動します。

注意 – パネルの移動に失敗した場合、Trusted Extensions へのログイン時にデスクトップのメインメニューやパネルに到達できない可能性があります。

a. 最上部のパネルで右クリックし、「プロパティー」を選択します。

b. 最上部のパネルの「向き」を「下」に変更します。

2 端末ウィンドウを開き、**labeld** サービスを有効化します。

```
# svcadm enable -s labeld
```

labeld サービスは、システムにラベルを追加し、デバイス割り当てサービスを起動します。

注意 – プロンプトにカーソルが戻るまで、システムでほかのタスクを実行しないでください。

3 サービスが使用可能になっていることを確認します。

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

注意 – Trusted Extensions の有効化や構成を遠隔で行う場合には、第 12 章「Trusted Extensions での遠隔管理 (手順)」をよく確認してください。遠隔管理が可能なようにシステムを構成するまでは、リブートしないでください。Trusted Extensions システムを遠隔管理用に構成しなかった場合、そのシステムには遠隔システムから到達できません。

4 システムをリブートします。

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

次の手順 49 ページの「Trusted Extensions にログインする」に進みます。

▼ Trusted Extensions にログインする

ログインすると、大域ゾーンになり、その環境では必須アクセス制御 (MAC) が認識されて実施されます。

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

始める前に　48 ページの「Trusted Extensions を有効化してリブートする」を完了しています。

1. インストール時に作成したユーザーアカウントを使用してログインします。
   ログインダイアログボックスで、*username* と入力してからパスワードを入力します。

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

2. マウスを使用して「状態」ウィンドウと「**Clearance**」ウィンドウを閉じます。

3. ラベル **PUBLIC** に対応するゾーンが存在しないことを示すダイアログボックスを閉じます。
   `root` 役割になったあとでゾーンを作成します。

4. **root** 役割になります。

   a. トラステッドストライプで自分の名前をクリックします。
      プルダウンメニューに `root` 役割が表示されます。

   b. **root** 役割を選択します。
      プロンプトが表示されたら、この役割の新しいパスワードを作成します。

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

次の手順　次のいずれかに進みます。

- デフォルトのシステムを構成する場合は、56 ページの「ラベル付きゾーンの作成」に進みます
- ラベル付きゾーンを作成する前にシステムをカスタマイズする場合は、51 ページの「Trusted Extensions での大域ゾーンの設定」に進みます。
- システムにグラフィック表示用のディスプレイがない場合は、第 12 章「Trusted Extensions での遠隔管理 (手順)」に進みます。

◆ ◆ ◆ 第 4 章

Trusted Extensions の構成 (手順)

この章では、モニターがあるシステムでの Trusted Extensions の構成方法について説明します。Trusted Extensions ソフトウェアが正しく機能するためには、ラベルとゾーンを構成する必要があります。また、ネットワーク通信、役割、および役割になれるユーザーも構成できます。

その他の構成タスクについては、パート II「Trusted Extensions の管理」を参照してください。

Trusted Extensions での大域ゾーンの設定

Trusted Extensions の構成をカスタマイズするには、次の作業マップの手順を実行します。デフォルトの構成をインストールするには、56 ページの「ラベル付きゾーンの作成」に進みます。

作業	説明	参照先
ハードウェアを保護します。	ハードウェア設定を変更する際にパスワードの入力を求めることによって、ハードウェアを保護します。	『Oracle Solaris の管理: セキュリティーサービス』の「システムハードウェアへのアクセスの制御 (タスク)」
ラベルを設定します。	ラベルはサイトに合わせて設定する必要があります。デフォルトの `label_encodings` ファイルを使用する場合、この手順は省略します。	52 ページの「ラベルエンコーディングファイルを検査およびインストールする」

作業	説明	参照先
IPv6 ネットワークを有効化します。	IP が IPv6 ネットワーク上のラベル付きパケットを認識できるようにします。	54 ページの「Trusted Extensions で IPv6 ネットワークを有効化する」
DOI を変更します。	1 でない解釈のドメイン (DOI) を指定します。	55 ページの「解釈のドメインを構成する」
LDAP サーバーを構成します。	Trusted Extensions LDAP ディレクトリサーバーを構成します。	第 5 章「Trusted Extensions のための LDAP の構成 (手順)」
LDAP クライアントを構成します。	このシステムを、Trusted Extensions LDAP ディレクトリサーバーのクライアントにします。	94 ページの「Trusted Extensions で大域ゾーンを LDAP クライアントにする」

▼ ラベルエンコーディングファイルを検査およびインストールする

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

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

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

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

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

`label_encodings` ファイルを編集するには、`root` 役割になる必要があります。

1. **`label_encodings` ファイルをディスクにコピーします。**

   ポータブルメディアからコピーするには、80 ページの「Trusted Extensions でポータブルメディアからファイルをコピーする」を参照してください。

2 端末ウィンドウでファイルの構文を検査します。

a. **chk_encodings** コマンドを実行します。

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

b. 出力を読み、次のいずれかを行います。

- エラーを解決します。

  コマンドによってエラーが報告された場合、続行する前に、そのエラーを解決しなければなりません。参考として、『Trusted Extensions Label Administration』の第 3 章「Creating a Label Encodings File (Tasks)」を参照してください。

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

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

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

例 4–1 コマンド行での label_encodings 構文の検査

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

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

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

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

---> VERSION = MYCOMPANY LABEL ENCODINGS  2.0 10/10/2010

---> CLASSIFICATIONS <---

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

---> COMPARTMENTS AND MARKINGS USAGE ANALYSIS <---
```

```
...
---> SENSITIVITY LABEL to COLOR MAPPING <---
...
```

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

```
# cp /var/encodings/label_encodings2 /etc/security/tsol/label.encodings.10.10.10
# cd /etc/security/tsol
# cp label_encodings label_encodings.tx.orig
# cp label.encodings.10.10.10 label_encodings
```

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

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

---> VERSION = MYCOMPANY LABEL ENCODINGS  2.0 10/10/2010
```

次の手順　ラベル付きゾーンを作成する前にシステムをリブートする必要があります。

▼ Trusted Extensions で IPv6 ネットワークを有効化する

注意 – txzonemgr スクリプトは IPv6 アドレスの構文をサポートしません。したがって、IPv6 ホストを Trusted Extensions ネットワークに追加するには tncfg コマンドを使用します。たとえば、206 ページの「トラステッドネットワーク代替メカニズム」 and 例 16–11を参照してください。

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

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

始める前に　大域ゾーンで root 役割になっています。

- **/etc/system** ファイルに次のエントリを入力します。

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

注意事項
- 起動中に IPv6 の構成が正しくないことを示すエラーメッセージが表示されたら、エントリを修正します。
  - エントリのスペルが正しいことを確認します。
  - `/etc/system` ファイルに正しいエントリを追加したあとにシステムがリブートされたことを確認します。
- すでに IPv6 が有効になっている Oracle Solaris システムに Trusted Extensions を追加して、`/etc/system` に IP エントリを追加できなかった場合、次のエラーメッセージが表示されます。 `t_optmgmt: System error: Cannot assign requested address` *time-stamp*

次の手順 ラベル付きゾーンを作成する前にシステムをリブートする必要があります。

▼ 解釈のドメインを構成する

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

サイトで 1 の DOI が使用されない場合は、すべてのセキュリティーテンプレートで `doi` 値を変更する必要があります。

始める前に 大域ゾーンで `root` 役割になっています。

- デフォルトのセキュリティーテンプレートで **DOI** 値を指定します。

```
# tncfg -t cipso set doi=n
# tncfg -t admin_low set doi=n
```

注 – すべてのセキュリティーテンプレートで DOI 値を指定する必要があります。

参照
- 203 ページの「Trusted Extensions のネットワークセキュリティー属性」
- 223 ページの「セキュリティーテンプレートを作成する」

次の手順 LDAP を使用する予定の場合は、第 5 章「Trusted Extensions のための LDAP の構成 (手順)」に進みます。ラベル付きゾーンを作成する前に LDAP を構成する必要があります。

それ以外の場合は、56 ページの「ラベル付きゾーンの作成」に進みます。

ラベル付きゾーンの作成

この節の手順では、ラベル付きゾーンを構成します。2 つのラベル付きゾーンを自動的に作成することも、ゾーンを手動で作成することもできます。

注 – LDAP を使用する予定の場合は、第 5 章「Trusted Extensions のための LDAP の構成 (手順)」に進みます。ラベル付きゾーンを作成する前に LDAP を構成する必要があります。

作業	説明	参照先
1a. デフォルトの Trusted Extensions 構成を作成します。	`txzonemgr -c` コマンドは、`label_encodings` ファイルから 2 つのラベル付きゾーンを作成します。	56 ページの「デフォルトの Trusted Extensions システムを作成する」
1b. GUI を使用してデフォルトの Trusted Extensions 構成を作成します。	`txzonemgr` スクリプトで、システムの構成時に適したタスクを提示する GUI を作成します。	57 ページの「ラベル付きゾーンを対話形式で作成する」
1c. ゾーン作成の手順を手動で実行します。	`txzonemgr` スクリプトで、システムの構成時に適したタスクを提示する GUI を作成します。	57 ページの「ラベル付きゾーンを対話形式で作成する」
2. 正常に動作するラベル付き環境を作成します。	デフォルトの構成では、2 つのワークスペースに `PUBLIC` と `INTERNAL USE ONLY` のラベルを付けます。	59 ページの「2 つのゾーンワークスペースにラベルを割り当てる」
3. (省略可能) ネットワーク上のほかのシステムにリンクします。	ラベル付きゾーンのネットワークインタフェースを構成し、大域ゾーンとラベル付きゾーンをほかのシステムに接続します。	61 ページの「Trusted Extensions でのネットワークインタフェースの構成」

▼ デフォルトの Trusted Extensions システムを作成する

この手順では、2 つのラベル付きゾーンを備えた正常に動作する Trusted Extensions システムを作成します。このシステムのセキュリティーテンプレートには遠隔ホストが割り当てられていないため、このシステムはどの遠隔ホストとも通信できません。

始める前に　49 ページの「Trusted Extensions にログインする」を完了しています。`root` 役割になっています。

1. 4 番目のワークスペースで端末ウィンドウを開きます。

2 (省略可能) **txzonemgr** のマニュアルページを確認します。

```
# man txzonemgr
```

3 デフォルトの構成を作成します。

```
# /usr/sbin/txzonemgr -c
```

このコマンドは、Oracle Solaris OS と Trusted Extensions ソフトウェアをあるゾーンにコピーし、そのゾーンのスナップショットを作成し、元のゾーンにラベルを付けたあと、そのスナップショットを使用して 2 番目のラベル付きゾーンを作成します。ゾーンがブートされます。

- 最初のラベル付きゾーンは、`label_encodings` ファイル内の `Default User Sensitivity Label` の値に基づいています。
- 2 番目のラベル付きゾーンは、`label_encodings` ファイル内の `Default User Clearance` の値に基づいています。

この手順は 20 分程度かかる可能性があります。このスクリプトでは、ゾーンをインストールするために、大域ゾーンの root パスワードがラベル付きゾーン用として使用されます。

次の手順 Trusted Extensions 構成を使用するには、59 ページの「2 つのゾーンワークスペースにラベルを割り当てる」に進みます。

▼ ラベル付きゾーンを対話形式で作成する

`label_encodings` ファイル中のラベルごとにゾーンを作成する必要はありませんが、作成することもできます。管理 GUI により、このシステムで GUI 用に作成されたゾーンを持つことのできるラベルが列挙されます。この手順では、2 つのラベル付きゾーンを作成します。Trusted Extensions の `label_encodings` ファイルを使用している場合は、デフォルトの Trusted Extensions 構成を作成します。

始める前に 49 ページの「Trusted Extensions にログインする」を完了しています。`root` 役割になっています。

ゾーンはまだ 1 つも作成していません。

1 オプションを一切指定せずに **txzonemgr** コマンドを実行します。

```
# txzonemgr &
```

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

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

ヒント – ゾーン完了の現在の状態を表示するには、Labeled Zone Manager の「Return to Main Menu」をクリックします。あるいは、「取消し」ボタンをクリックしてもかまいません。

2 次のいずれかの方法を選択してゾーンをインストールします。

- **2 つのラベル付きゾーンを作成するには、ダイアログボックスから「public and internal zones」を選択します。**
  - 最初のラベル付きゾーンは、`label_encodings` ファイル内の `Default User Sensitivity Label` の値に基づいています。
  - 2 番目のラベル付きゾーンは、`label_encodings` ファイル内の `Default User Clearance` の値に基づいています

  a. システムを識別するためのプロンプトに応答します。

  `public` ゾーンで排他的 IP スタックが使用されている場合や、そのゾーンが DNS で定義された IP アドレスを持つ場合は、DNS で定義されたホスト名を使用します。それ以外の場合は、システムの名前を使用します。

  b. **root** パスワードの入力を求めるプロンプトには応答しません。

  root パスワードはシステムのインストール時に設定されました。このプロンプトに対して入力すると、処理が失敗します。

  c. ゾーンのログインプロンプトで、ユーザーのログインとパスワードを入力します。

  次に、`svcs -x` コマンドを実行し、すべてのサービスが構成されていることを確認します。メッセージが何も表示されなければ、すべてのサービスが構成されています。

  d. ゾーンからログアウトし、ウィンドウを閉じます。

  プロンプトで exit と入力し、ゾーンのコンソールから「ウィンドウを閉じる」を選択します。

  別のウィンドウで 2 番目のゾーンのインストールが完了します。このゾーンはスナップショットから構築されるため、すぐに構築が終了します。

  e. **2** 番目のゾーンのコンソールにログインし、すべてのサービスが実行中であることを確認します。

```
# svcs -x
#
```

  メッセージが何も表示されなければ、すべてのサービスが構成されています。Labeled Zone Manager が表示されています。

f. **Labeled Zone Manager** で **internal** ゾーンをダブルクリックします。

「リブート」を選択したあと、「取消し」ボタンをクリックしてメイン画面に戻ります。すべてのゾーンが実行されています。ラベルなしのスナップショットは実行されていません。

- ゾーンを手動で作成するには、「メイン・メニュー」を選択したあと、「**Create a Zone**」を選択します。

  プロンプトに従います。GUI がゾーンの作成手順を案内します。

  このゾーンの作成とブートが完了したら、大域ゾーンに戻ってゾーンをさらに作成できます。これらのゾーンはスナップショットから作成されます。

例 4–2 別のラベル付きゾーンの作成

この例では、管理者が、デフォルトの `label_encodings` ファイルから制限されたゾーンを 1 つ作成します。

まず、管理者が `txzonemgr` スクリプトを対話モードで開きます。

```
# txzonemgr &
```

次に、管理者は大域ゾーンに移動し、`restricted` という名前のゾーンを作成します。

```
Create a new zone:restricted
```

次に、管理者は正しいラベルを適用します。

```
Select label:CNF : RESTRICTED
```

管理者はリストから、「クローン」オプションを選択したあと、新しいゾーンのテンプレートとして「`snapshot`」を選択します。

`restricted` ゾーンが使用可能になったあと、管理者は「ブート」をクリックしてこの 2 番目のゾーンをブートします。

`restricted` ゾーンにアクセスできるように、管理者は `label_encodings` ファイル内の `Default User Clearance` の値を `CNF RESTRICTED` に変更します。

▼ 2 つのゾーンワークスペースにラベルを割り当てる

この手順では、2 つのラベル付きワークスペースを作成し、各ラベル付きワークスペース内でラベル付きウィンドウを開きます。このタスクが完了すると、ネットワーク機能を持たない正常に動作する Trusted Extensions システムが作成されます。

始める前に　56 ページの「デフォルトの Trusted Extensions システムを作成する」、57 ページの「ラベル付きゾーンを対話形式で作成する」のいずれかを完了しています。

初期ユーザーです。

1 **PUBLIC** ワークスペースを作成します。

PUBLIC ワークスペースのラベルは Default User Sensitivity Label に対応しています。

a. 2 番目のワークスペースに切り替えます。

b. 右クリックして「ワークスペースラベルを変更」を選択します。

c. 「**PUBLIC**」を選択し、「了解」をクリックします。

2 プロンプトにパスワードを入力します。

PUBLIC ワークスペースにアクセスします。

3 端末ウィンドウを開きます。

ウィンドウには PUBLIC というラベルが表示されます。

4 **INTERNAL USE ONLY** ワークスペースを作成します。

サイト固有の label_encodings ファイルを使用する場合は、Default User Clearance の値からワークスペースを作成することになります。

a. 3 番目のワークスペースに切り替えます。

b. 右クリックして「ワークスペースラベルを変更」を選択します。

c. 「**INTERNAL USE ONLY**」を選択し、「了解」をクリックします。

5 プロンプトにパスワードを入力します。

INTERNAL ワークスペースに入ります。

6 端末ウィンドウを開きます。

ウィンドウには CONFIDENTIAL : INTERNAL USE ONLY というラベルが表示されます。

システムを使用する準備が整いました。ユーザーは 2 つのユーザーワークスペースと 1 つの役割ワークスペースを持ちます。この構成では、ラベル付きゾーンは、大域ゾーンと同じ IP アドレスを使用してほかのシステムとの通信を行います。それが可能なのは、デフォルトでこの IP アドレスが all-zones インタフェースとして共有されるからです。

次の手順　Trusted Extensions システムでほかのシステムとの通信を行う予定の場合は、61 ページの「Trusted Extensions でのネットワークインタフェースの構成」に進みます。

Trusted Extensions でのネットワークインタフェースの構成

ラップトップやワークステーションなど、ビットマップディスプレイが直接接続されたデスクトップを実行する際には、Trusted Extensions システムはネットワークを必要としません。ただし、ほかのシステムと通信するにはネットワークの構成が必要となります。`txzonemgr` GUI を使用すると、ほかのシステムに接続するようにラベル付きゾーンや大域ゾーンを簡単に構成できます。ラベル付きゾーンの構成オプションについては、32 ページの「ラベル付きゾーンへのアクセス」を参照してください。次の作業マップでは、ネットワーク構成タスクについて説明し、それらのタスクへのリンクを示します。

作業	説明	参照先
一般ユーザー向けのデフォルトシステムを構成します。	システムは 1 つの IP アドレスを持ち、1 つの `all-zones` インタフェースを使用してラベル付きゾーンや大域ゾーン間の通信を行います。その同じ IP アドレスが、遠隔システムとの通信に使用されます。	62 ページの「すべてのゾーンで単一の IP アドレスを共有する」
大域ゾーンに IP アドレスを追加します。	システムは複数の IP アドレスを持ち、大域ゾーンの排他的 IP アドレスを使用してプライベートサブネットに到達します。ラベル付きゾーンはこのサブネットに到達できません。	62 ページの「すべてのゾーンで単一の IP アドレスを共有する」
すべてのゾーンに IP アドレスを 1 つずつ割り当てます。ゾーンは IP スタックを共有します。	システムは複数の IP アドレスを持ちます。もっとも単純な場合には、ゾーンは 1 つの物理インタフェースを共有します。	63 ページの「ラベル付きゾーンに IP インスタンスを追加する」
ゾーンごとの IP インスタンスに `all-zones` インタフェースを追加します。	システムは自身のラベル付きゾーンに対し、遠隔攻撃から保護された特権付きサービスを提供できます。	63 ページの「ラベル付きゾーンに IP インスタンスを追加する」
すべてのゾーンに IP アドレスを 1 つずつ割り当てます。IP スタックは排他となります。	大域ゾーンを含むすべてのゾーンに、IP アドレスが 1 つずつ割り当てられます。ラベル付きゾーンごとに VNIC が 1 つずつ作成されます。	64 ページの「ラベル付きゾーンに仮想ネットワークインタフェースを追加する」
ゾーンを遠隔ゾーンに接続します。	このタスクでは、ラベル付きゾーンと大域ゾーンのネットワークインタフェースを構成することで、それらのゾーンが同じラベルの付いた遠隔システムに到達できるようにします。	65 ページの「Trusted Extensions システムをほかの Trusted Extensions システムに接続する」

作業	説明	参照先
ゾーンごとに異なる nscd デーモンを実行します。	このタスクでは、各サブネットが独自のネームサーバーを備えている環境で、ゾーンごとに nscd デーモンを 1 つずつ構成します。	66 ページの「ラベル付きゾーンごとに異なるネームサービスを構成する」

▼ すべてのゾーンで単一の IP アドレスを共有する

この手順を実行すれば、システムのすべてのゾーンが 1 つの IP アドレス、具体的には大域ゾーンの IP アドレスを使用して、ほかの同一のラベルを持つゾーンまたはホストに到達できるようになります。この構成がデフォルトです。ネットワークインタフェースを異なる方法で構成したあと、システムをデフォルトのネットワーク構成に戻す必要が生じた場合に、この手順を実行する必要があります。

始める前に　大域ゾーンで root 役割になっている必要があります。

1. オプションを一切指定せずに **txzonemgr** コマンドを実行します。

   ```
   # txzonemgr &
   ```

   Labeled Zone Manager にゾーンの一覧が表示されます。この GUI については、57 ページの「ラベル付きゾーンを対話形式で作成する」を参照してください。

2. 大域ゾーンをダブルクリックします。

3. 「**Configure Network Interfaces**」をダブルクリックします。

   インタフェースのリストが表示されます。次の特性が記載されたインタフェースを探します。

   - タイプ phys
   - ホスト名の IP アドレス
   - 状態 up

4. ホスト名に対応するインタフェースを選択します。

5. コマンドの一覧から「**Share with Shared-IP Zones**」を選択します。

   すべてのゾーンがこの共有 IP アドレスを使用して、自身と同じラベルの遠隔システムと通信できます。

6. 「取消し」をクリックしてゾーンコマンド一覧に戻ります。

次の手順　システムの外部ネットワークを構成するには、65 ページの「Trusted Extensions システムをほかの Trusted Extensions システムに接続する」に進みます。

▼ ラベル付きゾーンに IP インスタンスを追加する

共有 IP スタックとゾーンごとのアドレスを使用し、ラベル付きゾーンをネットワーク上のほかのシステムのラベル付きゾーンに接続する予定である場合に、この手順が必要となります。

この手順では、1 つ以上のラベル付きゾーンのために、IP インスタンスつまりゾーンごとのアドレスを作成します。ラベル付きゾーンは自身のゾーンごとのアドレスを使用して、ネットワーク上で同じラベルの付いたゾーンとの通信を行います。

始める前に　大域ゾーンで `root` 役割になっている必要があります。

Labeled Zone Manager にゾーンの一覧が表示されます。この GUI を開くには、57 ページの「ラベル付きゾーンを対話形式で作成する」を参照してください。構成対象のラベル付きゾーンは停止されている必要があります。

1. **Labeled Zone Manager** で、**IP** インスタンスを追加するラベル付きゾーンをダブルクリックします。
2. 「ネットワークインタフェースの構成」をダブルクリックします。
   構成オプションの一覧が表示されます。
3. 「**Add an IP instance**」を選択します。
4. システムに複数の **IP** アドレスがある場合は、目的のインタフェースを含むエントリを選択します。
5. このラベル付きゾーンの **IP** アドレスと接頭辞長を指定します。
   たとえば、`192.168.1.2/24` と入力します。接頭辞長を末尾に指定しなかった場合は、ネットマスクの入力を求められます。この例と同等のネットマスクは、`255.255.255.0` です。
6. 「了解」をクリックします。
7. デフォルトのルーターを追加するには、追加したばかりのエントリをダブルクリックします。
   プロンプトでルーターの IP アドレスを入力し、「了解」をクリックします。

注 – デフォルトのルーターを削除または変更するには、エントリを削除してから IP インスタンスを再度作成します。

---

8. 「取消し」をクリックしてゾーンコマンド一覧に戻ります。

次の手順　システムの外部ネットワークを構成するには、65 ページの「Trusted Extensions システムをほかの Trusted Extensions システムに接続する」に進みます。

▼ ラベル付きゾーンに仮想ネットワークインタフェースを追加する

排他的 IP スタックとゾーンごとのアドレスを使用し、ラベル付きゾーンをネットワーク上のほかのシステムのラベル付きゾーンに接続する予定である場合に、この手順が必要となります。

この手順では、VNIC を作成し、それをラベル付きゾーンに割り当てます。

始める前に　大域ゾーンで `root` 役割になっている必要があります。

Labeled Zone Manager にゾーンの一覧が表示されます。この GUI を開くには、57 ページの「ラベル付きゾーンを対話形式で作成する」を参照してください。構成対象のラベル付きゾーンは停止されている必要があります。

1. **Labeled Zone Manager** で、仮想インタフェースを追加するラベル付きゾーンをダブルクリックします。
2. 「ネットワークインタフェースの構成」をダブルクリックします。
   構成オプションの一覧が表示されます。
3. 「**Add a virtual interface (VNIC)**」をダブルクリックします。
   システムに複数の VNIC カードがある場合は、複数の選択肢が表示されます。目的のインタフェースを含むエントリを選択します。
4. ホスト名を割り当てるか、**IP** アドレスと接頭辞長を割り当てます。
   たとえば、`192.168.1.2/24` と入力します。接頭辞長を末尾に指定しなかった場合は、ネットマスクの入力を求められます。この例と同等のネットマスクは、`255.255.255.0` です。
5. デフォルトのルーターを追加するには、追加したばかりのエントリをダブルクリックします。
   プロンプトでルーターの IP アドレスを入力し、「了解」をクリックします。

注 – デフォルトのルーターを削除または変更するには、エントリを削除してから VNIC を再度作成します。

---

6 「取消し」をクリックしてゾーンコマンド一覧に戻ります。

VNIC のエントリが表示されます。`internal_0` のように、*zonename_n* という名前がシステムによって割り当てられます。

次の手順 システムの外部ネットワークを構成するには、65 ページの「Trusted Extensions システムをほかの Trusted Extensions システムに接続する」に進みます。

▼ Trusted Extensions システムをほかの Trusted Extensions システムに接続する

この手順では、Trusted Extensions システムから接続可能な遠隔ホストを追加することで、Trusted Extensions のネットワークを定義します。

始める前に Labeled Zone Manager が表示されています。この GUI を開くには、57 ページの「ラベル付きゾーンを対話形式で作成する」を参照してください。大域ゾーンで `root` 役割になっています。

1 **Labeled Zone Manager** で大域ゾーンをダブルクリックします。

2 「**Add Multilevel Access to Remote Host**」を選択します。

a. 別の **Trusted Extensions** システムの **IP** アドレスを入力します。

b. その別の **Trusted Extensions** システム上で対応するコマンドを実行します。

3 「取消し」をクリックしてゾーンコマンド一覧に戻ります。

4 **Labeled Zone Manager** でラベル付きゾーンをダブルクリックします。

5 「**Add Access to Remote Host**」を選択します。

a. 別の **Trusted Extensions** システム上の同じラベルの付いたゾーンの **IP** アドレスを入力します。

b. その別の **Trusted Extensions** システムのゾーン内で、対応するコマンドを実行します。

参照
- 第 15 章「トラステッドネットワーク (概要)」
- 220 ページの「ホストおよびネットワークへのラベル付け (作業マップ)」

▼ ラベル付きゾーンごとに異なるネームサービスを構成する

この手順では、各ラベル付きゾーンで、ネームサービスデーモン (nscd) を個別に構成できます。この構成は、評価された構成の条件を満たしません。評価された構成では、nscd デーモンは大域ゾーンでのみ実行されます。各ラベル付きゾーン内の door は、そのゾーンを大域の nscd デーモンに接続します。

この構成がサポートする環境では、各ゾーンがそのゾーンのラベルで動作するサブネットワークに接続されており、そのサブネットワークにはそのラベル用の独自のネームサーバーがあります。

注 – この構成では、高度なネットワークスキルが要求されます。

始める前に　Labeled Zone Manager が表示されています。この GUI を開くには、57 ページの「ラベル付きゾーンを対話形式で作成する」を参照してください。大域ゾーンで root 役割になっています。

1. **Labeled Zone Manager** で、「**Configure per-zone name service**」を選択し、「了解」をクリックします。

   注 – このオプションは、初期システム構成時に一度だけ使用されるように意図されています。

   ---

2. 各ゾーンの **nscd** サービスを構成します。
   補足情報については、nscd(1M) のマニュアルページを参照してください。

3. システムをリブートします。

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

4. ゾーンごとに、ルートとネームサービスデーモンを確認します。

   a. ゾーンコンソールで **nscd** サービスを表示します。

   ```
   zone-name # svcs -x name-service/cache
   svc:/system/name-service/cache:default (name service cache)
    State: online since September 10, 2011  10:10:11 AM PDT
      See: nscd(1M)
      See: /var/svc/log/system-name-service-cache:default.log
   Impact: None.
   ```

   b. サブネットワークへのルートを確認します。

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

例 4–3 各ラベル付きゾーンからのネームサービスキャッシュの削除

システム管理者が、ゾーンごとのネームサービスデーモンをテストしたあとで、ラベル付きゾーンからネームサービスデーモンを削除し、大域ゾーンでのみデーモンを実行することにしました。管理者はシステムをデフォルトのネームサービス構成に戻すために、`txzonemgr` GUI を開き、大域ゾーンを選択して、「`Unconfigure per-zone name service`」、「`OK`」の順に選択します。この選択により、すべてのラベル付きゾーンで `nscd` デーモンが削除されます。次に、管理者はシステムをリブートします。

次の手順 各ゾーンのユーザーおよび役割のアカウントを構成する場合の選択肢は、3 つあります。

- マルチレベルの LDAP ディレクトリサーバーに LDAP アカウントを作成できます。
- 個々の LDAP ディレクトリサーバー (ラベルごとに 1 つずつ) に LDAP アカウントを作成できます。
- ローカルアカウントを作成できます。

各ラベル付きゾーンでネームサービスデーモンを個別に構成すると、すべてのユーザーのパスワード処理に影響が及びます。ユーザーは、デフォルトラベルに対応するゾーンも含め、どのラベル付きゾーンにアクセスする際にも、自身を認証する必要があります。さらに、管理者が各ゾーン内でローカルにアカウントを作成する必要があるか、あるいは、ゾーンが LDAP クライアントになっている場合には LDAP ディレクトリ内にアカウントが存在している必要があります。

大域ゾーン内のアカウントが Labeled Zone Manager `txzonemgr` を実行しているような特殊な場合には、少なくともそのアカウントが各ゾーンにログインできるように、そのアカウントの情報が各ラベル付きゾーンにコピーされます。デフォルトでは、このアカウントが初期ユーザーアカウントになります。

Trusted Extensions での役割とユーザーの作成

Trusted Extensions での役割作成は、Oracle Solaris での役割作成と同じです。ただし、評価された構成ではセキュリティー管理者役割が必要となります。

作業	説明	参照先
セキュリティー管理者役割を作成します。	セキュリティー関連のタスクを処理する役割を作成します。	68 ページの「Trusted Extensions でセキュリティー管理者役割を作成する」
システム管理者役割を作成します。	セキュリティーに関係しないシステム管理タスクを処理する役割を作成します。	70 ページの「システム管理者役割を作成する」

作業	説明	参照先
管理役割になるユーザーを作成します。	役割になることができる 1 人または複数のユーザーを作成します。	70 ページの「Trusted Extensions で役割になれるユーザーを作成する」
役割が各自の作業を実行できることを確認します。	役割をテストします。	73 ページの「Trusted Extensions の役割が機能することを確認する」
ユーザーがラベル付きゾーンにログインできるようにします。	一般ユーザーがログインできるようにゾーンサービスを開始します。	73 ページの「ユーザーがラベル付きゾーンにログインできるようにする」

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

始める前に　大域ゾーンで root 役割になっています。

1 役割を作成するには、**roleadd** コマンドを使用します。

コマンドの詳細については、roleadd(1M) のマニュアルページを参照してください。次の情報を参考にしてください。

- 「役割名」– secadmin
- -c Local Security Officer

  専有情報は入力しないでください。
- -m *home-directory*
- -u *role-UID*
- -S *repository*
- -K *key=value*

  Information Security および User Security 権利プロファイルを割り当てます。

注 – 管理役割の場合は必ず、ラベル範囲で管理ラベルを使用し、pfexec コマンドの使用を監査し、lock_after_retries=no を設定し、パスワードの有効期限は設定しないでください。

```
# roleadd -c "Local Security Officer" -m \
-u 110 -K profiles="Information Security,User Security" -S files \
-K lock_after_retries=no \
-K min_label=ADMIN_LOW -K clearance=ADMIN_HIGH secadmin
```

2 役割の初期パスワードを提供します。

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

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

3 セキュリティー管理者役割を、ほかの役割を作成する際のガイドとして使用します。

可能な役割は、次のとおりです。

- admin 役割 – System Administrator 権利プロファイル
- oper 役割 – Operator 権利プロファイル

例 4–4 LDAP でのセキュリティー管理者役割の作成

管理者は、ローカルのセキュリティー管理者役割を使用して最初のシステムを構成したあと、LDAP リポジトリ内にセキュリティー管理者役割を作成します。このシナリオでは、LDAP に定義されたセキュリティー管理者役割が LDAP クライアントを管理できます。

```
# roleadd -c "Site Security Officer" -d server1:/rpool/pool1/BayArea/secadmin
-u 111 -K profiles="Information Security,User Security" -S ldap \
-K lock_after_retries=no -K audit_flags=lo,ex:no \
-K min_label=ADMIN_LOW -K clearance=ADMIN_HIGH secadmin
```

管理者は、役割の初期パスワードを指定します。

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

次の手順 ローカルユーザーにローカル役割を割り当てるには、70 ページの「Trusted Extensions で役割になれるユーザーを作成する」を参照してください。

▼ システム管理者役割を作成する

始める前に　大域ゾーンで root 役割になっています。

1. システム管理者権利プロファイルを役割に割り当てます。

```
# roleadd -c "Local System Administrator" -m -u 111  -K audit_flags=lo,ex:no\
-K profiles="System Administrator" -K lock_after_retries=no \
-K min_label=ADMIN_LOW -K clearance=ADMIN_HIGH sysadmin
```

2. 役割の初期パスワードを提供します。

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

▼ Trusted Extensions で役割になれるユーザーを作成する

サイトのセキュリティーポリシーで許可されるなら、1 人で複数の管理役割になれるようなユーザーを作成することもできます。

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

始める前に　大域ゾーンで root 役割になっている必要があります。また、責務分離が実施されている場合には、セキュリティー管理者とシステム管理者というそれぞれ別の役割になれるユーザーが存在しており、彼らがそれらの役割になって、この手順の該当する部分を実行する必要があります。

1. ユーザーを作成します。

   root 役割とシステム管理者役割のいずれかがこの手順を実行します。

   専有情報をコメント内に配置しないでください。

```
# useradd -c "Second User" -u 1201 -d /home/jdoe jdoe
```

2. ユーザーを作成したあと、ユーザーのセキュリティー属性を変更します。

   root 役割とセキュリティー管理者役割のいずれかがこの手順を実行します。

注 – 役割になれるユーザーの場合は、アカウントロックを無効にし、パスワードの有効期限は設定しません。さらに、pfexec コマンドの使用を監査します。

```
# usermod -K lock_after_retries=no -K idletime=5 -K idlecmd=lock \
-K audit_flags=lo,ex:no jdoe
```

注 – idletime と idlecmd の値は、ユーザーが役割になっても引き続き有効となります。詳細については、140 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。

3 6 文字以上の英数字のパスワードを割り当てます。

```
# passwd jdoe
New Password:       Type password
Re-enter new Password:      Retype password
```

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

4 役割をユーザーに割り当てます。

root 役割またはセキュリティー管理者役割がこの手順を実行します。

```
# usermod -R oper jdoe
```

5 ユーザーの環境をカスタマイズします。

a. 簡易認証の割り当て

サイトのセキュリティーポリシーを確認してから、簡易認証権利プロファイルを最初のユーザーに付与できます。このプロファイルによって、ユーザーはデバイスの割り当て、PostScript ファイルの印刷、ラベルなしの印刷、遠隔からのログイン、およびシステムのシャットダウンを行えます。プロファイルを作成するには、152 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。

b. ユーザー初期設定ファイルをカスタマイズします。

145 ページの「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)」を参照してください。

c. マルチレベルのコピーおよびリンクファイルを作成します。

マルチレベルシステムで、ほかのラベルにコピーまたはリンクするユーザー初期化ファイルをリストするファイルによって、ユーザーおよび役割を設定できます。詳細は、143 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。

例 4–5 ローカルユーザーを作成するための useradd コマンドの使用

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

このユーザーは、デフォルトのラベル範囲よりも広いラベル範囲を持つことになります。したがって、root 役割は、ユーザーの最下位ラベルおよび認可上限ラベルの 16 進数形式を確認します。

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

次に、root 役割は表 1–2 を確認してから、ユーザーを作成します。管理者はユーザーのホームディレクトリを、デフォルトの /export/home にではなく /export/home1 に配置します。

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

root 役割は初期パスワードを割り当てます。

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

最後に、root 役割は、セキュリティー管理者役割をユーザーの定義に追加します。役割は、68 ページの「Trusted Extensions でセキュリティー管理者役割を作成する」で作成されました。

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

▼ Trusted Extensions の役割が機能することを確認する

各役割を確認するには、その役割になります。次に、その役割だけが実行できるタスクを実行し、その役割が実行を許可されていないタスクの実行を試みます。

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

1. 役割ごとに、その役割になれるユーザーとしてログインします。
2. その役割になります。
   次のトラステッドストライプ内では、ユーザー名は `tester` です。

   a. トラステッドストライプでユーザーの名前をクリックします。

   b. 割り当てられた役割の一覧から、役割を選択します。
3. その役割をテストします。
   ユーザーのプロパティーを変更するために必要となる承認については、`passwd(1)` のマニュアルページを参照してください。
   - システム管理者役割は、ユーザーを作成したり、ユーザーのログインシェルなど、`solaris.user.manage` 承認を必要とするユーザープロパティーを変更したりできるはずです。システム管理者役割は、`solaris.account.setpolicy` 承認を必要とするユーザープロパティーを変更できないはずです。
   - セキュリティー管理者役割は、`solaris.account.setpolicy` 承認を必要とするユーザープロパティーを変更できるはずです。セキュリティー管理者は、ユーザーを作成したり、ユーザーのログインシェルを変更したりできないはずです。

▼ ユーザーがラベル付きゾーンにログインできるようにする

システムがリブートされると、デバイスと基礎のストレージとの関連付けも再設定されなければなりません。

始める前に　少なくとも 1 つのラベル付きゾーンが作成されています。システムを構成したあと、リブートしました。`root` 役割になれます。

1 ログインし、**root** 役割になります。

2 ゾーンサービスの状態を検査します。

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

3 サービスを再起動します。

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

4 ログアウトします。

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

Trusted Extensions での集中管理ホームディレクトリの作成

Trusted Extensions では、ユーザーは、ユーザーが作業するすべてのラベルでホームディレクトリにアクセスする必要があります。デフォルトでは、各ゾーン内で実行されているオートマウンタによってホームディレクトリが自動作成されます。ただし、NFS サーバーを使用してホームディレクトリを集中管理する場合は、ホームディレクトリへのアクセスをユーザーのすべてのラベルで有効化する必要があります。

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

始める前に 大域ゾーンで root 役割になっています。

1 **Trusted Extensions** ソフトウェアをホームディレクトリサーバーに追加し、そのラベル付きゾーンを構成します。

- ユーザーがログイン可能なすべてのラベルでホームディレクトリが必要になるため、すべてのユーザーラベルでホームディレクトリサーバーを作成します。たとえば、デフォルトの構成を作成する場合は、PUBLIC ラベル用と INTERNAL ラベル用のホームディレクトリサーバーを 1 つずつ作成します。

2 ラベル付きゾーンごとに、**193** 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」の自動マウント手順に従います。そのあと、この手順に戻ります。

3. ホームディレクトリが作成されていることを確認します。

   a. ホームディレクトリサーバーからログアウトします。

   b. 一般ユーザーとしてホームディレクトリサーバーにログインします。

   c. ログインゾーンで端末を開きます。

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

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

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

4. ホームディレクトリサーバーからログアウトします。

▼ 各 NFS サーバーにログインすることでユーザーがすべてのラベルで遠隔ホームディレクトリにアクセスできるようにする

この手順では、ユーザーが各ホームディレクトリサーバーに直接ログインできるようにすることで、ユーザーが各ラベルのホームディレクトリを作成できるようにします。中央サーバー上に各ホームディレクトリが作成されると、ユーザーは自身のホームディレクトリに任意のシステムからアクセスできるようになります。

あるいは、管理者としてスクリプトを実行してからオートマウンタを変更することで、各ホームディレクトリサーバー上にマウントポイントを作成することもできます。この方法については、76 ページの「各サーバーでオートマウンタを構成することでユーザーが遠隔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。

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

- ユーザーが各ホームディレクトリサーバーに直接ログインできるようにします。
  通常、NFS サーバーはラベルごとに 1 つずつ作成されています。

  a. 各 NFS サーバーにそのサーバーのラベルでログインするように、各ユーザーに指示します。

b. ログインが成功したら、サーバーからログアウトするようユーザーに指示します。

ログインが成功すると、サーバーのラベルにあるユーザーのホームディレクトリが使用可能になります。

c. 通常のワークステーションからログインするよう、ユーザーに指示します。

デフォルトラベルのホームディレクトリが、ホームディレクトリサーバーから使用可能になります。ユーザーがセッションのラベルを変更したり、異なるラベルでワークスペースを追加したりすると、そのラベルのユーザーのホームディレクトリがマウントされます。

次の手順　デフォルトラベルとは異なるラベルでログインするには、ログイン時にラベルビルダーから異なるラベルを選択します。

▼ 各サーバーでオートマウンタを構成することでユーザーが遠隔ホームディレクトリにアクセスできるようにする

この手順では、各 NFS サーバーでホームディレクトリのマウントポイントを作成するスクリプトを実行します。次に、そのサーバーのラベルで `auto_home` エントリを変更してマウントポイントを追加します。これでユーザーがログインできるようになります。

始める前に　Trusted Extensions ドメインのホームディレクトリサーバーが LDAP クライアントとして構成されました。`-S ldap` オプション付きの `useradd` コマンドを使用して、LDAP サーバー上にユーザーアカウントが作成されています。`root` 役割になっている必要があります。

1 すべてのユーザーのホームディレクトリマウントポイントを作成するためのスクリプトを作成します。

サンプルスクリプトでは次のことを仮定しています。

- LDAP サーバーは NFS ホームディレクトリサーバーとは異なるサーバーである。
- クライアントシステムも異なるシステムである。
- `hostname` エントリは、ゾーンつまりそのラベルに対する NFS ホームディレクトリサーバーの外部 IP アドレスを指定している。

- このスクリプトは、NFS サーバー上で、そのラベルのクライアントにサービスを提供するゾーン内で実行される。

```
#!/bin/sh
hostname=$(hostname)
scope=ldap

for j in $(getent passwd|tr ' ' _); do
    uid=$(echo $j|cut -d: -f3)
    if [ $uid -ge 100 ]; then
        home=$(echo $j|cut -d: -f6)
        if [[ $home == /home/* ]]; then
            user=$(echo $j|cut -d: -f1)
            echo Updating home directory for $user
            homedir=/export/home/$user
            usermod -md ${hostname}:$homedir -S $scope $user
            mp=$(mount -p|grep  " $homedir zfs" )
            dataset=$(echo $mp|cut -d" " -f1)
            if [[ -n $dataset ]]; then
                zfs set sharenfs=on $dataset
            fi
        fi
    fi
done
```

2 各 **NFS** サーバー上で、そのラベルのクライアントにサービスを提供するラベル付きゾーン内で、前述のスクリプトを実行します。

Trusted Extensions の構成のトラブルシューティング

デスクトップの構成が間違っていると、システムを使用できなくなる可能性があります。

▼ デスクトップパネルを画面最下部に移動する

注 – デスクトップパネルのデフォルトの位置は、画面最上部です。ところが、Trusted Extensions では、画面最上部はトラステッドストライプで覆われます。このため、パネルはワークスペースの側面か最下部に配置する必要があります。デフォルトのワークスペースには 2 つのデスクトップパネルが含まれます。

始める前に　システムのデスクトップパネルの位置を変更するには、`root` 役割になっている必要があります。

1. 画面最下部にデスクトップパネルが 1 つ表示されている場合は、次のいずれかのアクションを実行します。

   - マウスの右ボタンを使用して、表示されているパネルにアプレットを追加します。
   - 次の手順を実行して、2 番目の隠れているデスクトップパネルを画面最下部に移動します。

2. それ以外の場合、このログインのみで、またはシステムのすべてのユーザーで、最下部デスクトップパネルを作成します。

   - このログインのみでパネルを移動するには、ホームディレクトリ内の **top_panel_screen***n* ファイルを編集します。

     a. パネルの位置を定義するファイルを含むディレクトリに移ります。

     ```
     % cd $HOME/.gconf/apps/panel/toplevels
     % ls
     %gconf.xml    bottom_panel_screen0/   top_panel_screen0/
     % cd top_panel_screen0
     % ls
     %gconf.xml             top_panel_screen0/
     ```

     b. 最上部パネルの位置を定義する **%gconf.xml** ファイルを編集します。

     ```
     % vi %gconf.xml
     ```

     c. 方向に関するすべての行を探し、文字列 **top** を **bottom** で置き換えます。
     たとえば、方向に関する行を次のようにします。

     ```
     /toplevels/orientation" type="string">
                    <stringvalue>bottom</stringvalue>
     ```

   - システムのすべてのユーザーでパネルを移動するには、デスクトップの構成を変更します。

     root 役割の端末ウィンドウで次のコマンドを実行します。

     ```
     # export SETUPPANEL="/etc/gconf/schemas/panel-default-setup.entries"
     # export TMPPANEL="/tmp/panel-default-setup.entries"
     # sed 's/<string>top<\/string>/<string>bottom<\/string>/' $SETUPPANEL > $TMPPANEL
     # cp $TMPPANEL $SETUPPANEL
     # svcadm restart gconf-cache
     ```

3. システムからログアウトしたあと、再度ログインします。
   デスクトップパネルが複数存在している場合、それらのパネルは画面最下部に重ね合わせられます。

その他の Trusted Extensions 構成タスク

次の 2 つのタスクでは、構成ファイルの正確なコピーをサイトのすべての Trusted Extensions システムに転送できます。最後のタスクでは、Trusted Extensions のカスタマイズを Oracle Solaris システムから削除できます。

▼ Trusted Extensions でファイルをポータブルメディアにコピーする

ポータブルメディアにコピーする場合、情報と同じ機密ラベルをメディアに付けます。

注 – root 役割は Trusted Extensions の構成時に、label_encodings ファイルをすべてのシステムに転送するためにポータブルメディアを使用する可能性があります。このメディアには Trusted Path のラベルを付けます。

始める前に　管理ファイルをコピーするには、大域ゾーンで root 役割になっている必要があります。

1. 適切なデバイスを割り当てます。

   デバイスマネージャーを使用し、何も記録されていないメディアを挿入します。詳細は、『Trusted Extensions ユーザーガイド』の「Trusted Extensions でデバイスを割り当てる」を参照してください。

   ファイルブラウザにそのクリーンメディアの内容が表示されます。

2. 別のファイルブラウザを開きます。

3. コピーするファイルがあるフォルダに移動します。

4. 各ファイルに対して次を行います。

   a. ファイルのアイコンを強調表示します。

   b. ポータブルメディアのファイルブラウザにファイルをドラッグします。

5. デバイスの割り当てを解除します。

   詳細は、『Trusted Extensions ユーザーガイド』の「Trusted Extensions でデバイスの割り当てを解除する」を参照してください。

6. ポータブルメディアのファイルブラウザで、「ファイル」メニューから「取り出し」を選択します。

注 – コピーしたファイルの機密ラベルを示した物理的なラベルを、メディアに必ず貼り付けてください。

例 4–6 構成ファイルをすべてのシステムで同一にする

システム管理者は、同じ設定ですべてのシステムを確実に構成しようと思っています。そのためには、最初に構成するシステムで、管理者はリブートによって削除されないディレクトリを作成します。そのディレクトリに、管理者はすべてのシステムで同一のファイルまたはほとんど同じファイルを配置します。

たとえば管理者は、このサイトの `policy.conf` ファイルや、デフォルトの `login` および `passwd` ファイルを変更します。したがって、管理者は次のファイルを永続ディレクトリにコピーします。

```
# mkdir /export/commonfiles
# cp  /etc/security/policy.conf \
# cp  /etc/default/login \
# cp  /etc/default/passwd \
# cp  /etc/security/tsol/label_encodings \
/export/commonfiles
```

管理者はデバイスマネージャーを使用して、大域ゾーンで CD-ROM を割り当て、ファイルを CD に転送し、`Trusted Path` のラベルを付けます。

▼ Trusted Extensions でポータブルメディアからファイルをコピーする

ファイルを置き換える前に、元の Trusted Extensions ファイルの名前を変更しておくと安全です。システムを構成する際に、`root` 役割が管理ファイルの名前の変更およびコピーを行います。

始める前に 管理ファイルをコピーするには、大域ゾーンで `root` 役割になっている必要があります。

1. 適切なデバイスを割り当てます。

   詳細は、『Trusted Extensions ユーザーガイド』の「Trusted Extensions でデバイスを割り当てる」を参照してください。

   ファイルブラウザに内容が表示されます。

2. 管理ファイルを含むメディアを挿入します。

3 システムに同じ名前のファイルがある場合、元のファイルを新しい名前でコピーします。

たとえば、元のファイルの名前の後ろに .orig を追加します。

```
# cp /etc/security/tsol/label_encodings /etc/security/tsol/label_encodings.orig
```

4 ファイルブラウザを開きます。

5 **/etc/security/tsol** などのコピー先ディレクトリに移動します。

6 コピーするそれぞれのファイルに対して、次を行います。

a. マウントされたメディアのファイルブラウザで、ファイルのアイコンを強調表示します。

b. 別のファイルブラウザのコピー先ディレクトリにファイルをドラッグします。

7 デバイスの割り当てを解除します。

詳細は、『Trusted Extensions ユーザーガイド』の「Trusted Extensions でデバイスの割り当てを解除する」を参照してください。

8 プロンプトが表示されたら、メディアを取り出します。

▼ Trusted Extensions をシステムから削除する

Oracle Solaris システムから Trusted Extensions 機能を削除するには、特定の手順を実行する必要があります。

始める前に 大域ゾーンで root 役割になっています。

1 保持する必要のあるラベル付きゾーン内のデータをすべてアーカイブします。

ポータブルメディアでは、アーカイブされた各ゾーンに、ゾーンの機密ラベルを持つ物理的なステッカーを付けます。

2 システムからラベル付きゾーンを削除します。

詳細は、『Oracle Solaris のシステム管理 (Oracle Solaris ゾーン、Oracle Solaris 10 ゾーン、およびリソース管理)』の「非大域ゾーンを削除する方法」を参照してください。

3 **Trusted Extensions** サービスを無効化します。

```
# svcadm disable labeld
```

4 デバイス割り当てを無効にします。

```
# svcadm disable allocate
```

5 (省略可能) システムをリブートします。

6 システムを構成します。

さまざまなサービスを Oracle Solaris システム用に構成する必要があります。たとえば、基本的なネットワーキング、ネームサービス、ファイルシステムのマウントなどが挙げられます。

◆ ◆ ◆ 第 5 章

Trusted Extensions のための LDAP の構成 (手順)

この章では、Trusted Extensions で使用するための Oracle Directory Server Enterprise Edition (Directory Server) を構成する方法について説明します。Directory Server は LDAP サービスを提供します。LDAP は、Trusted Extensions の対応ネームサービスです。末尾の節、94 ページの「Trusted Extensions LDAP クライアントの作成」では、LDAP クライアントを構成する方法について説明します。

Directory Server の構成には、2 つの選択肢があります。Trusted Extensions システムに LDAP サーバーを構成するか、Trusted Extensions プロキシサーバーを使用して既存のサーバーに接続します。

LDAP サーバーを構成するには、次のいずれかの作業マップの手順に従います。

- 83 ページの「Trusted Extensions ネットワークでの LDAP の構成 (作業マップ)」
- 84 ページの「Trusted Extensions システムでの LDAP プロキシサーバーの構成 (作業マップ)」

Trusted Extensions ネットワークでの LDAP の構成 (作業マップ)

作業	説明	参照先
Trusted Extensions LDAP サーバーを設定します。	既存の Oracle Directory Server Enterprise Edition がない場合、最初の Trusted Extensions システムを Directory Server にします。このシステムにラベル付きゾーンはありません。 その他の Trusted Extensions システムは、このサーバーのクライアントになります。	85 ページの「LDAP 用に Directory Server の情報を収集する」 86 ページの「Oracle Directory Server Enterprise Edition をインストールする」 89 ページの「Oracle Directory Server Enterprise Edition のログを構成する」

作業	説明	参照先
Trusted Extensions データベースをサーバーに追加します。	Trusted Extensions システムファイルのデータを LDAP サーバーに入力します。	91 ページの「Oracle Directory Server Enterprise Edition にデータを入力する」
その他のすべての Trusted Extensions システムを、このサーバーのクライアントとして構成します。	別のシステムに Trusted Extensions を構成する場合、そのシステムをこの LDAP サーバーのクライアントにします。	94 ページの「Trusted Extensions で大域ゾーンを LDAP クライアントにする」

Trusted Extensions システムでの LDAP プロキシサーバーの構成 (作業マップ)

Oracle Solaris システムで実行されている既存の Oracle Directory Server Enterprise Edition がある場合、この作業マップを使用します。

作業	説明	参照先
Trusted Extensions データベースをサーバーに追加します。	Trusted Extensions ネットワークデータベースの `tnrhdb` および `tnrhtp` は、LDAP サーバーに追加する必要があります。	91 ページの「Oracle Directory Server Enterprise Edition にデータを入力する」
LDAP プロキシサーバーを設定します。	1 つの Trusted Extensions システムをその他の Trusted Extensions システムのプロキシサーバーにします。これらのその他のシステムは、このプロキシサーバーを使用して LDAP サーバーにアクセスします。	93 ページの「LDAP プロキシサーバーを作成する」
プロキシサーバーに LDAP 用のマルチレベルポートを構成します。	Trusted Extensions プロキシサーバーが特定ラベルで LDAP サーバーと通信できるようにします。	91 ページの「Oracle Directory Server Enterprise Edition のマルチレベルポートを設定する」
その他のすべての Trusted Extensions システムを LDAP プロキシサーバーのクライアントとして構成します。	別のシステムに Trusted Extensions を構成する場合、そのシステムを LDAP プロキシサーバーのクライアントにします。	94 ページの「Trusted Extensions で大域ゾーンを LDAP クライアントにする」

Trusted Extensions システムでの Oracle Directory Server Enterprise Edition の構成

LDAP ネームサービスは、Trusted Extensions の対応ネームサービスです。サイトで LDAP ネームサービスがまだ実行されていない場合、Trusted Extensions が構成されているシステムで Oracle Directory Server Enterprise Edition (Directory Server) を構成します。

サイトですでに Directory Server が実行されている場合、Trusted Extensions データベースをサーバーに追加する必要があります。Directory Server にアクセスするために、Trusted Extensions システムで LDAP プロキシを設定します。

注 – この LDAP サーバーを NFS サーバーとして使用しない場合は、このサーバーにラベル付きゾーンをインストールする必要はありません。

▼ LDAP 用に Directory Server の情報を収集する

- 次の項目の値を決定します。

  各項目は、Sun Java Enterprise System のインストールウィザードに表示される順序で記載されています。

インストールウィザードのプロンプト	対応または情報
Oracle Directory Server Enterprise Edition *version*	
「管理者ユーザー ID」	デフォルト値は「`admin`」です。
「管理者ユーザーパスワード」	「`admin123`」のようなパスワードを作成します。
「ディレクトリマネージャ DN」	デフォルト値は「`cn=Directory Manager`」です。
「ディレクトリマネージャパスワード」	「`dirmgr89`」のようなパスワードを作成します。
「Directory Server ルート」	デフォルト値は「`/var/opt/mps/serverroot`」です。プロキシソフトウェアをインストールする場合、このパスはあとでも使用されます。
「サーバー識別子」	デフォルト値はローカルシステムです。

インストールウィザードのプロンプト	対応または情報
「サーバーポート」	Directory Server を使用して標準的な LDAP ネームサービスをクライアントシステムに提供する場合は、デフォルト値「389」を使用します。 Directory Server を使用してプロキシサーバーの今後のインストールをサポートする場合は、「10389」など標準以外のポートを入力します。
「サフィックス」	「dc=example-domain,dc=com」のように、ドメインコンポーネントを含めます。
「管理ドメイン」	「example-domain.com」のように、サフィックスに対応させて作成します。
「システムユーザー」	デフォルト値は「root」です。
「システムグループ」	デフォルト値は「root」です。
「データの保存場所」	デフォルト値は「このサーバーに設定データを保存します。」です。
「データの保存場所」	デフォルト値は「このサーバーにユーザー/グループデータを保存します。」です。
「Administration Port」	デフォルト値はサーバーポートです。デフォルトを変更するために推奨される慣例は、ソフトウェアバージョンに 1000 を掛けた数値です。ソフトウェアバージョン 5.2 の場合、この慣例ではポート 5200 になります。

▼ Oracle Directory Server Enterprise Edition をインストールする

Directory Server のパッケージは Oracle web site for Sun Software Products (http://www.oracle.com/us/sun/sun-products-map-075562.html) から入手できます。

始める前に　大域ゾーンを含む Trusted Extensions システムで作業しています。システムにラベル付きゾーンはありません。大域ゾーンで root 役割になっている必要があります。

Trusted Extensions LDAP サーバーは、pam_unix を使用して LDAP リポジトリに対する認証を行うクライアントのために構成されています。pam_unix を使用する場合、パスワード操作と、その結果としてのパスワードポリシーは、クライアントによって決定されます。すなわち、LDAP サーバーによって設定されたポリシーは使用されません。クライアントで設定できるパスワードパラメータについては、『Oracle Solaris の管理: セキュリティーサービス』の「パスワード情報の管理」を参照してください。pam_unix の詳細については、pam.conf(4) のマニュアルページを参照してください。

注 – LDAP クライアントで pam_ldap を使用する構成は、Trusted Extensions では評価されていません。

1 **Directory Server** パッケージをインストールする前に、システムのホスト名エントリに **FQDN** を追加します。

FQDN とは「完全指定のドメイン名 (Fully Qualified Domain Name)」のことです。この名前は、次のようにホスト名と管理ドメインの組み合わせになります。

```
## /etc/hosts
...
192.168.5.5 myhost myhost.example-domain.com
```

2 **Oracle Directory Server Enterprise Edition** のパッケージを **Oracle web site for Sun Software Products (http://www.oracle.com/us/sun/sun-products-map-075562.html)** からダウンロードします。

プラットフォームに適した最新のソフトウェアを選択します。

3 **Directory Server** パッケージをインストールします。

85 ページの「LDAP 用に Directory Server の情報を収集する」からの情報を使って質問に答えます。質問、デフォルト値、推奨される回答の詳細な一覧については、『Oracle Solaris Administration: Naming and Directory Services』の第 11 章「Setting Up Oracle Directory Server Enterprise Edition With LDAP Clients (Tasks)」と『Oracle Solaris Administration: Naming and Directory Services』の第 12 章「Setting Up LDAP Clients (Tasks)」を参照してください。

4 (省略可能) 自身のパスに **Directory Server** の環境変数を追加します。

```
# $PATH
/usr/sbin:.../opt/SUNWdsee/dsee6/bin:/opt/SUNWdsee/dscc6/bin:/opt/SUNWdsee/ds6/bin:
/opt/SUNWdsee/dps6/bin
```

5 (省略可能) **MANPATH** に **Directory Server** のマニュアルページを追加します。

```
/opt/SUNWdsee/dsee6/man
```

6 **cacaoadm** プログラムを有効にして、プログラムが有効になったことを確認します。

```
# /usr/sbin/cacaoadm enable
# /usr/sbin/cacaoadm start
start: server (pid n) already running
```

7 起動するたびに **Directory Server** も起動されるようにします。

Directory Server 用の SMF サービスのテンプレートが、Oracle Directory Server Enterprise Edition パッケージ内に含まれています。

- **Trusted Extensions Directory Server** で、サービスを有効にします。

```
# dsadm stop /export/home/ds/instances/your-instance
# dsadm enable-service -T SMF /export/home/ds/instances/your-instance
```

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

dsadm コマンドについては、dsadm(1M) のマニュアルページを参照してください。

- プロキシ **Directory Server** で、サービスを有効にします。

```
# dpadm stop /export/home/ds/instances/your-instance
# dpadm enable-service -T SMF /export/home/ds/instances/your-instance
# dpadm start /export/home/ds/instances/your-instance
```

dpadm コマンドについては、dpadm(1M) のマニュアルページを参照してください。

8 インストールを確認します。

```
# dsadm info /export/home/ds/instances/your-instance
Instance Path:          /export/home/ds/instances/your-instance
Owner:                  root(root)
Non-secure port:        389
Secure port:            636
Bit format:             32-bit
State:                  Running
Server PID:             298
DSCC url:               -
SMF application name:   ds--export-home-ds-instances-your-instance
Instance version:       D-A00
```

注意事項　LDAP 構成の問題を解決する方針については、『Oracle Solaris Administration: Naming and Directory Services』の第 13 章「LDAP Troubleshooting (Reference)」を参照してください。

▼ Directory Server 用の LDAP クライアントの作成

このクライアントを使用して、LDAP 用の Directory Server にデータを入力します。このタスクは、Directory Server にデータを入力する前に実行する必要があります。

一時的に Trusted Extensions Directory Server 上にクライアントを作成してからサーバー上のクライアントを移動することも、独立したクライアントを作成することもできます。

始める前に　大域ゾーンで root 役割になっています。

1 **Trusted Extensions** ソフトウェアをシステムに追加します。

Trusted Extensions Directory Server を使用することも、別個のシステムに Trusted Extensions を追加することもできます。

2 クライアント上の **name-service/switch** サービスで **LDAP** を構成します。

a. 現在の構成を表示します。

```
# svccfg -s name-service/switch listprop config
config                      application
config/value_authorization  astring       solaris.smf.value.name-service.switch
config/default              astring       "files ldap"
config/host                 astring       "files dns"
config/netgroup             astring       ldap
config/printer              astring       "user files ldap"
```

b. 次のプロパティーをデフォルトから変更します。

```
# svccfg -s name-service/switch setprop config/host = astring: "files ldap dns"
```

3 大域ゾーンで **ldapclient init** コマンドを実行します。

この例では、LDAP クライアントは `example-domain.com` ドメイン内にあります。サーバーの IP アドレスは `192.168.5.5` です。

```
# ldapclient init -a domainName=example-domain.com -a profileName=default \
> -a proxyDN=cn=proxyagent,ou=profile,dc=example-domain,dc=com \
> -a proxyDN=cn=proxyPassword={NS1}ecc423aad0 192.168.5.5
System successfully configured
```

4 サーバーの **enableShadowUpdate** パラメータに **TRUE** を設定します。

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

`enableShadowUpdate` パラメータについては、『Oracle Solaris Administration: Naming and Directory Services』の「enableShadowUpdate Switch」と、`ldapclient(1M)` のマニュアルページを参照してください。

▼ Oracle Directory Server Enterprise Edition のログを構成する

この手順では次の 3 種類のログを構成します。 アクセスログ、監査ログ、およびエラーログです。次のデフォルト設定は変更されません。

- すべてのログが有効化およびバッファリングされます。
- 各ログは対応する `/export/home/ds/instances/`*your-instance*`/logs/`*LOG_TYPE* ディレクトリ内に配置されます。
- イベントはログレベル 256 でロギングされます。
- ログは `600` ファイルアクセス権で保護されます。
- アクセスログは毎日ローテーションされます。
- エラーログは毎週ローテーションされます。

この手順の設定は次の要件を満たします。

- 監査ログは毎日ローテーションされます。
- 3 か月よりも古いログファイルは期限切れになります。
- すべてのログファイルで最大 20,000M バイトのディスク容量を使用します。
- 各ファイル最大 500M バイトの、最大 100 のログファイルが保持されます。
- ディスク容量の空きが 500M バイトを下回ると古いログから削除されます。
- エラーログでは追加情報が収集されます。

始める前に　大域ゾーンで `root` 役割になっている必要があります。

1 アクセスログを構成します。

アクセスの *LOG_TYPE* は `ACCESS` です。ログを構成するための構文は、次のとおりです。

```
dsconf set-log-prop LOG_TYPE property:value
```

```
# dsconf set-log-prop ACCESS max-age:3M
# dsconf set-log-prop ACCESS max-disk-space-size:20000M
# dsconf set-log-prop ACCESS max-file-count:100
# dsconf set-log-prop ACCESS max-size:500M
# dsconf set-log-prop ACCESS min-free-disk-space:500M
```

2 監査ログを構成します。

```
# dsconf set-log-prop AUDIT max-age:3M
# dsconf set-log-prop AUDIT max-disk-space-size:20000M
# dsconf set-log-prop AUDIT max-file-count:100
# dsconf set-log-prop AUDIT max-size:500M
# dsconf set-log-prop AUDIT min-free-disk-space:500M
# dsconf set-log-prop AUDIT rotation-interval:1d
```

監査ログのローテーション間隔は、デフォルトで 1 週間です。

3 エラーログを構成します。

この構成では、エラーログで追加データが収集されるように指定します。

```
# dsconf set-log-prop ERROR max-age:3M
# dsconf set-log-prop ERROR max-disk-space-size:20000M
# dsconf set-log-prop ERROR max-file-count:30
# dsconf set-log-prop ERROR max-size:500M
# dsconf set-log-prop ERROR min-free-disk-space:500M
# dsconf set-log-prop ERROR verbose-enabled:on
```

4 (省略可能) さらにログを構成します。

ログごとに次の設定を行うことも可能です。

```
# dsconf set-log-prop LOG_TYPE rotation-min-file-size:undefined
# dsconf set-log-prop LOG_TYPE rotation-time:undefined
```

`dsconf` コマンドについては、`dsconf(1M)` のマニュアルページを参照してください。

▼ Oracle Directory Server Enterprise Edition のマルチレベルポートを設定する

Trusted Extensions で作業するには、Directory Server のサーバーポートを大域ゾーンのマルチレベルポート (MLP) として設定する必要があります。

始める前に　大域ゾーンで root 役割になっている必要があります。

1. **txzonemgr** を起動します。

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

2. **TCP** プロトコル用のマルチレベルポートを大域ゾーンに追加します。
   ポート番号は 389 です。

3. **UDP** プロトコル用のマルチレベルポートを大域ゾーンに追加します。
   ポート番号は 389 です。

▼ Oracle Directory Server Enterprise Edition にデータを入力する

ラベル構成、ユーザー、および遠隔システムに関する Trusted Extensions データを保持するために、複数の LDAP データベースが作成および変更されています。この手順では、Directory Server データベースに Trusted Extensions 情報を取り込みます。

始める前に　大域ゾーンで root 役割になっている必要があります。シャドウ更新が有効になっている LDAP クライアントで作業しています。前提条件については、88 ページの「Directory Server 用の LDAP クライアントの作成」を参照してください。

1. ネームサービスデータベースにデータを入力するために使用するファイルのステージング領域を作成します。

   ```
   # mkdir -p /setup/files
   ```

2. サンプルの **/etc** ファイルをステージング領域にコピーします。

   ```
   # cd /etc
   # cp aliases group networks netmasks protocols /setup/files
   # cp rpc services auto_master /setup/files

   # cd /etc/security/tsol
   # cp tnrhdb tnrhtp /setup/files
   ```

注意 – *attr ファイルはコピーしないでください。代わりに、ユーザー、役割、および権利プロファイルを LDAP リポジトリに追加するコマンドで、-S ldap オプションを使用します。これらのコマンドは、user_attr、auth_attr、exec_attr、および prof_attr データベース用のエントリを追加します。詳細は、user_attr(4) および useradd(1M) のマニュアルページを参照してください。

3 **/setup/files/auto_master** ファイルから **+auto_master** エントリを削除します。

4 ステージング領域にゾーン自動マップを作成します。

```
# cp /zone/public/root/etc/auto_home_public /setup/files
# cp /zone/internal/root/etc/auto_home_internal /setup/files
# cp /zone/needtoknow/root/etc/auto_home_needtoknow /setup/files
# cp /zone/restricted/root/etc/auto_home_restricted /setup/files
```

次の自動マップのリストで、各ペアの最初の行はファイルの名前を示します。2 行めはファイルの内容を示します。ゾーン名は、Trusted Extensions ソフトウェアに含まれているデフォルトの label_encodings ファイルからのラベルを特定します。

- ここに示された行のゾーン名を実際のゾーン名に置き換えてください。
- *myNFSserver* でホームディレクトリの NFS サーバーを特定します。

```
/setup/files/auto_home_public
 * myNFSserver_FQDN:/zone/public/root/export/home/&

/setup/files/auto_home_internal
 * myNFSserver_FQDN:/zone/internal/root/export/home/&

/setup/files/auto_home_needtoknow
 * myNFSserver_FQDN:/zone/needtoknow/root/export/home/&

/setup/files/auto_home_restricted
 * myNFSserver_FQDN:/zone/restricted/root/export/home/&
```

5 **ldapaddent** コマンドを使用して、ステージング領域のすべてのファイルを利用して **Directory Server** にデータを入力します。

たとえば、次のコマンドでは、ステージング領域の hosts ファイルからサーバーにデータが入力されます。

```
# /usr/sbin/ldapaddent -D "cn=directory manager" \
-w dirmgr123 -a simple -f /setup/files/hosts hosts
```

6 **Trusted Extensions Directory Server** で **ldapclient** コマンドを実行する場合は、システム上のクライアントを無効にします。

大域ゾーンで ldapclient uninit コマンドを実行します。詳細出力を使用して、そのシステムが LDAP クライアントではなくなっていることを確認します。

```
# ldapclient -v uninit
```

詳細については、ldapclient(1M) のマニュアルページを参照してください。

7 **LDAP の Trusted Extensions ネットワークデータベースにデータを設定するには、`-S ldap` オプション付きの `tncfg` コマンドを使用します。**

手順については、220 ページの「ホストおよびネットワークへのラベル付け (作業マップ)」を参照してください。

既存の Oracle Directory Server Enterprise Edition のための Trusted Extensions プロキシの作成

最初に、Oracle Solaris システムの既存の Directory Server に Trusted Extensions データベースを追加する必要があります。次に、Trusted Extensions システムが Directory Server にアクセスできるように、Trusted Extensions システムが LDAP プロキシサーバーになるよう構成する必要があります。

▼ LDAP プロキシサーバーを作成する

サイトに LDAP サーバーがすでに存在する場合、Trusted Extensions システムにプロキシサーバーを作成します。

始める前に `enableShadowUpdate` パラメータに `TRUE` を設定するように変更したクライアントから、LDAP サーバーにデータを入力しました。要件については、88 ページの「Directory Server 用の LDAP クライアントの作成」を参照してください。

また、`enableShadowUpdate` パラメータに `TRUE` を設定したクライアントから、Trusted Extensions の情報を含むデータベースを LDAP サーバーに追加しました。詳細は、91 ページの「Oracle Directory Server Enterprise Edition にデータを入力する」を参照してください。

大域ゾーンで `root` 役割になっている必要があります。

1 **Trusted Extensions が設定されているシステムで、プロキシサーバーを作成します。**

注 – 2 つの `ldapclient` コマンドを実行する必要があります。`ldapclient init` コマンドを実行したら、`ldapclient modify` コマンドを実行して、`enableShadowUpdate` パラメータに `TRUE` を設定します。

次にサンプルのコマンドを示します。`ldapclient init` コマンドはプロキシ値を定義します。

```
# ldapclient init \
-a proxyDN=cn=proxyagent,ou=profile,dc=west,dc=example,dc=com \
-a domainName=west.example.com \
```

```
-a profileName=pit1 \
-a proxyPassword=test1234 192.168.0.1
System successfully configured
```

`ldapclient mod` コマンドはシャドウ更新を有効にします。

```
# ldapclient mod -a enableShadowUpdate=TRUE \
-a adminDN=cn=admin,ou=profile,dc=west,dc=example,dc=com \
-a adminPassword=admin-password
System successfully configured
```

詳細は、『Oracle Solaris Administration: Naming and Directory Services』の第 12 章「Setting Up LDAP Clients (Tasks)」を参照してください。

2 **Trusted Extensions データベースがプロキシサーバーで表示できることを確認します。**

```
# ldaplist -l database
```

注意事項 LDAP 構成の問題を解決する方針については、『Oracle Solaris Administration: Naming and Directory Services』の第 13 章「LDAP Troubleshooting (Reference)」を参照してください。

Trusted Extensions LDAP クライアントの作成

次の手順では、既存の Trusted Extensions Directory Server 用の LDAP クライアントを作成します。

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

この手順では、LDAP クライアント上で大域ゾーンの LDAP ネームサービス構成を確立します。

`txzonemgr` スクリプトを使用します。

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

始める前に Oracle Directory Server Enterprise Edition つまり Directory Server が存在しなければなりません。Trusted Extensions データベースのデータがサーバーに入力されていて、このクライアントシステムがサーバーと通信できなければなりません。したがって、Directory Server によってセキュリティーテンプレートがこのクライアントに割り当てられている必要があります。明示的な割り当ては不要であり、ワイルドカード割り当てで十分です。

大域ゾーンで root 役割になっている必要があります。

1 **DNS を使用する場合は、name-service/switch の構成に dns を追加します。**
LDAP 用の標準的なネームサービスのスイッチファイルは限定的であるため、Trusted Extensions には使用できません。

a. 現在の構成を表示します。

```
# svccfg -s name-service/switch listprop config
config                      application
config/value_authorization  astring       solaris.smf.value.name-service.switch
config/default              astring       files ldap
config/netgroup             astring       ldap
config/printer              astring       "user files ldap"
```

b. **host** プロパティーに **dns** を追加し、サービスを更新します。

```
# svccfg -s name-service/switch setprop config/host = astring: "files dns ldap"
# svccfg -s name-service/switch:default refresh
```

c. 新しい構成を確認します。

```
# svccfg -s name-service/switch listprop config
config                      application
config/value_authorization  astring       solaris.smf.value.name-service.switch
config/default              astring       files ldap
config/host                 astring       files dns ldap
config/netgroup             astring       ldap
config/printer              astring       "user files ldap"
```

Trusted Extensions データベースはデフォルトの構成 files ldap を使用しているため、表示されません。

2 **LDAP クライアントを作成するには、オプションを一切指定せずに txzonemgr コマンドを実行します。**

```
# txzonemgr &
```

a. 大域ゾーンをダブルクリックします。

b. 「**Create LDAP Client**」を選択します。

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

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

d. 表示された値を確定するか取り消します。

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

ユーザーが確認すると、txzonemgr スクリプトは ldapclient init コマンドを実行します。

3 シャドウ更新を有効化してクライアントの構成を完了します。

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

4 サーバーに関する情報が正しいことを確認します。

a. 端末ウィンドウを開き、**LDAP** サーバーを照会します。

```
# ldapclient list
```

出力表示は次のようになります。

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

b. エラーを修正します。

エラーが発生した場合は、手順 2 から手順 4 までをやり直します。たとえば、次のエラーが表示される場合、LDAP サーバーにシステムのエントリがない可能性があります。

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

このエラーを修正するには、LDAP サーバーを確認する必要があります。

パート II

Trusted Extensions の管理

このパートの各章では、Trusted Extensions の管理方法について説明します。

第 6 章「Trusted Extensions の管理の概念」では、Trusted Extensions 機能の概要を説明します。

第 7 章「Trusted Extensions 管理ツール」では、Trusted Extensions に固有の管理プログラムについて説明します。

第 8 章「Trusted Extensions システムのセキュリティー要件 (概要)」では、Trusted Extensions で必要となるセキュリティー要件や構成可能なセキュリティー要件について説明します。

第 9 章「Trusted Extensions での一般的なタスクの実行 (手順)」では、Trusted Extensions 管理の概要を説明します。

第 10 章「Trusted Extensions でのユーザー、権利、および役割 (概要)」では、Trusted Extensions での役割に基づくアクセス制御 (RBAC) の概要を説明します。

第 11 章「Trusted Extensions でのユーザー、権利、役割の管理 (手順)」では、Trusted Extensions の一般ユーザーを管理する手順を示します。

第 12 章「Trusted Extensions での遠隔管理 (手順)」では、Trusted Extensions の遠隔管理を行う手順を示します。

第 13 章「Trusted Extensions でのゾーンの管理 (手順)」では、ラベル付きゾーンを管理する手順を示します。

第 14 章「Trusted Extensions でのファイルの管理とマウント (手順)」では、システムを管理、マウント、バックアップする手順、および Trusted Extensions のその他のファイル関連タスクを示します。

第 15 章「トラステッドネットワーク (概要)」では、Trusted Extensions でのネットワークデータベースや経路指定の概要を説明します。

第 16 章「Trusted Extensions でのネットワークの管理 (手順)」では、Trusted Extensions でネットワークデータベースや経路指定を管理する手順を示します。

第 18 章「Trusted Extensions でのマルチレベルメール (概要)」では、Trusted Extensions でのメール固有の問題について説明します。

第 19 章「ラベル付き印刷の管理 (手順)」では、Trusted Extensions で印刷を処理する手順を示します。

第 20 章「Trusted Extensions のデバイス (概要)」では、Trusted Extensions で提供されている、Oracle Solaris のデバイス保護に対する拡張について説明します。

第 21 章「Trusted Extensions でのデバイス管理 (手順)」では、デバイスマネージャーを使用してデバイスを管理する手順を示します。

第 22 章「Trusted Extensions での監査 (概要)」では、監査に関する Trusted Extensions 固有の情報を提供します。

第 23 章「Trusted Extensions のソフトウェア管理 (リファレンス)」では、Trusted Extensions システムでアプリケーションを管理する方法について説明します。

◆ ◆ ◆ 第 6 章

Trusted Extensions の管理の概念

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

Trusted Extensions と Oracle Solaris OS

Trusted Extensions ソフトウェアは、Oracle 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 Oracle 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 Oracle Solaris のその他のセキュリティー機能を使用します。Secure Shell、BART、暗号フレームワーク、IPsec、および IP フィルタを、Trusted Extensions で使用できます。Trusted Extensions では、スナップショットや暗号化も含め、ZFS ファイルシステムのすべての機能が使用可能です。

Trusted Extensions と Oracle Solaris OS の相違点

Trusted Extensions ソフトウェアは、Oracle Solaris OS を拡張します。次のリストに概要を示します。付録 C「Trusted Extensions 管理の手引き」も参照してください。

- 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、つまり随意アクセス制御 (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。

  Oracle 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、Oracle 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、Oracle Solaris システムでオプションとされている機能の中に有効化されるものがあります。たとえば、Trusted Extensions を構成する多くのサイトでは、ユーザーを作成したりセキュリティー属性を割り当てたりする際に、責務分離が必要となります。
- Trusted Extensions では、Oracle Solaris 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 が構成されたシステムでは、デバイス割り当てが必要になります。
- Trusted Extensions では、利用できる選択肢が Oracle Solaris よりも制限される場合があります。たとえば、Trusted Extensions では、すべてのゾーンがラベル付きゾーンです。Oracle Solaris 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 は、マルチレベル版の Oracle Solaris デスクトップである Solaris Trusted Extensions (GNOME) を提供します。この名称は Trusted GNOME 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マネージャー GUI が用意されています。また、`updatehome` コマンドは、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 が構成されたシステムでは、ラベル付きゾーンを管理する際に、`zonecfg` コマンドのほかに Labeled Zone Manager も使用されます。
- 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。デフォルトでは、一般ユーザーはシステムをシャットダウンできません。

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いちばん下のモニターに表示されます。

マルチヘッドシステムのモニターにそれぞれ異なるワークスペースが表示されている場合、Trusted GNOME はモニターごとにトラステッドストライプを 1 つずつ表示します。

Trusted Extensions の基本概念

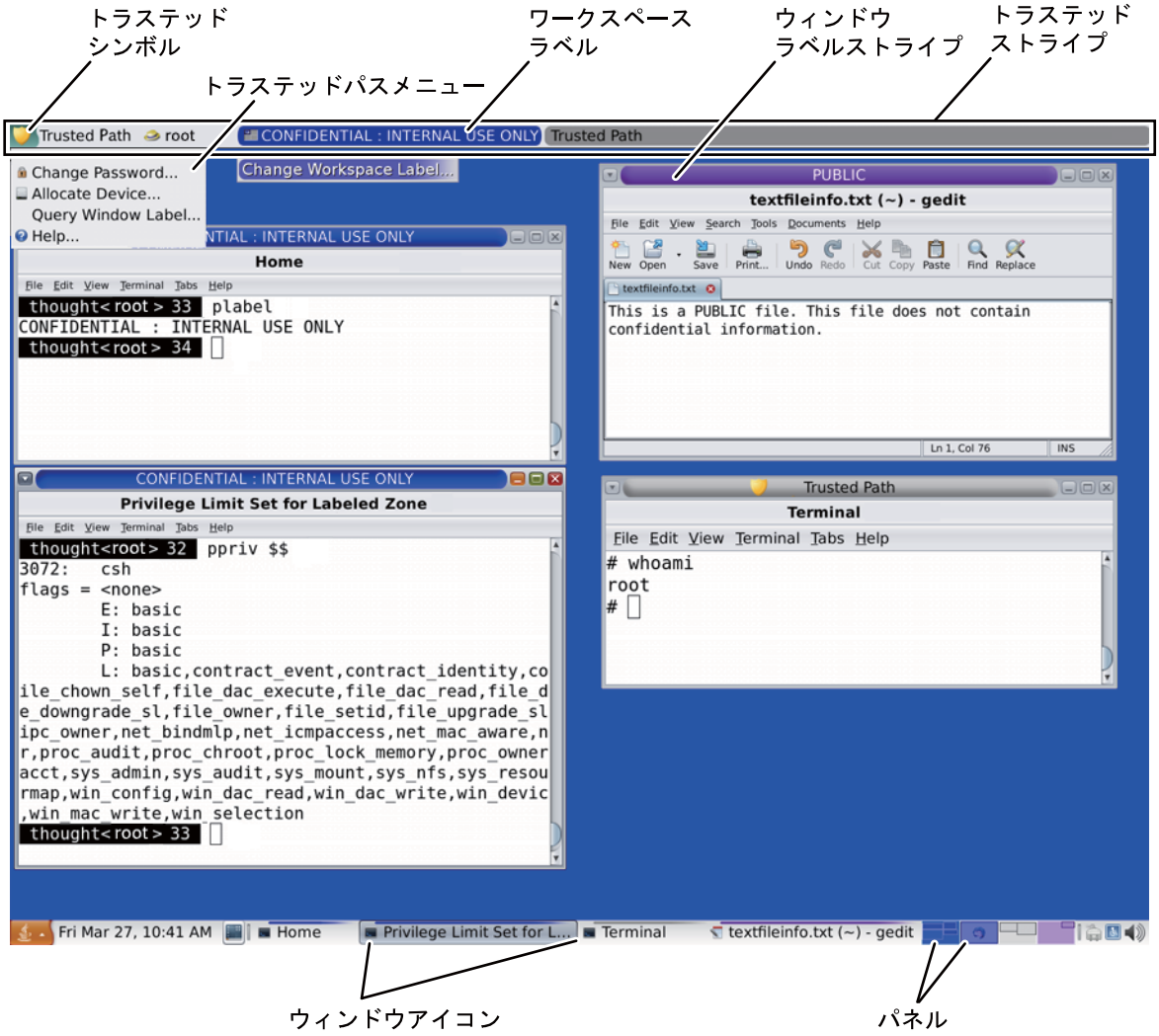
Trusted Extensions ソフトウェアにより、Oracle Solaris システムにラベルが追加されます。また、ラベル付きワークスペースと、ラベルビルダーやデバイスマネージャーなどのトラステッドアプリケーションも追加されます。この節で説明する概念は、ユーザーと管理者の両方にとって、Trusted Extensions を理解するために必要な知識です。『Trusted Extensions ユーザーガイド』でも、これらの概念をユーザーを対象として説明しています。

Trusted Extensions が提供する保護

Trusted Extensions ソフトウェアは Oracle Solaris OS の保護を強化します。Oracle Solaris 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となるほか、役割をログインアカウントとして使用することはできません。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 GNOME では、ストライプ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 6–1 を参照してください。

図 6–1 Trusted Extensions マルチレベルデスクトップ



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。ユーザーはパスワードを変更する場合などに、TCB ソフトウェアと対話できます。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 はどちらも、Oracle Solaris が提供する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。

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」コンポーネントと任意の数の「コンパートメント」コンポーネントから構成されます。格付けコンポーネントは、`TOP SECRET`、`SECRET`、`PUBLIC` など、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、別のシステムなど、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コンポーネントが、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 6–1 ラベル関係の例

ラベル 1	メンバーシップ	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`
`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、共有されているだれ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、『Trusted Extensions Label Administration』と『Compartmented Mode Workstation Labeling: Encodings Format』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。ユーザーにもリソース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。
- **IPsec** および **IKE** – IPsec のセキュリティーアソシエーションと IKE の規則にラベルが付けられます。
- 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セキュリティーテンプレートが割り当てられます。ラベルなしホストにも、Trusted Extensions システムとの通信によってデフォルトラベルが割り当てられます。
- 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 19 章「ラベル付き印刷の管理 (手順)」と『Trusted Extensions Label Administration』の「Labels on Printed Output」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、図 6–1 に示したように、ワークスペースパネル上と、ウィンドウタイトルバーの上側に表示されます。

  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。そのウィンドウから起動されたプロセスは、元のラベルで実行されます。
- 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。

役割と Trusted Extensions

Oracle 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。

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。

Oracle Solaris と同様、権利プロファイルは役割の機能の基本です。権利プロファイルや役割については、『Oracle Solaris の管理: セキュリティーサービス』の第 8 章「役割と特権の使用 (概要)」を参照してください。

◆ ◆ ◆ 第 7 章

7 Trusted Extensions 管理ツール

この章では、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、Oracle 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 7–1 Trusted Extensions 管理ツール

ツール	説明	参照先
/usr/sbin/txzonemgr	ネットワークを含め、ラベル付きゾーンを作成および構成するための Labeled Zone Manager GUI を作成します。	56 ページの「ラベル付きゾーンの作成」と、txzonemgr(1M) のマニュアルページを参照してください。
	コマンド行オプションを使用すると、ユーザーが指定したゾーンを自動作成できます。	txzonemgr は zenity (1) スクリプトです。

表 7–1 Trusted Extensions 管理ツール (続き)

ツール	説明	参照先
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。	113 ページの「デバイスマネージャー」および 279 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。
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、152 ページの「ユーザーのラベル範囲を変更する」を参照してください。
選択マネージャー	これも、データのセキュリティーレベルの変更を承認されているユーザー用のツールです。プログラムがユーザーに対してデータのセキュリティーレベルの変更を要求する場合に表示されます。	ユーザーを承認するには、157 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。図については、『Trusted Extensions ユーザーガイド』の「ラベル間でデータを移動する」を参照してください。
Trusted Extensions コマンド	管理タスクを実行するために使用されます。	管理用のコマンドや構成ファイルの一覧については、付録 D 「Trusted Extensions マニュアルページのリスト」を参照してください。

txzonemgr スクリプト

`/usr/sbin/txzonemgr` コマンドは 2 つのモードを提供します。

- CLI では、このコマンドはラベル付きゾーンを既存のファイルから作成します。`-c` コマンドオプションを指定してこの CLI を実行すると、2 つのラベル付きゾーンが作成およびブートされます。`-d` オプションを指定すると、すべてのラベル付きゾーンが削除されます。
- GUI では、スクリプトは Labeled Zone Manager というタイトルのダイアログボックスを表示します。この GUI は、ラベル付きゾーンを作成してブートする手順を案内します。このスクリプトには、ゾーンのクローンを作成してスナップショットを作成する機能が含まれています。さらにこの GUI には、ネットワーク、ネームサービス、および LDAP の構成メニューも用意されています。

`txzonemgr` コマンドは `zenity(1)` スクリプトを実行します。「Labeled Zone Manager」ダイアログボックスには、ラベル付きゾーンの現在の構成ステータスで有効な選択肢のみが表示されます。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。

デバイスマネージャー

「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。

デバイスマネージャーの「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。

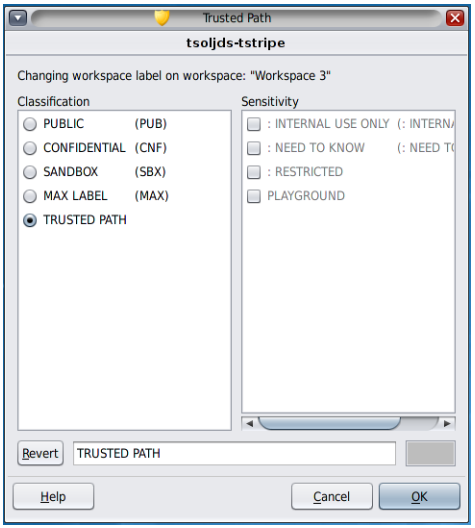
Trusted Extensions でのデバイス保護については、第 21 章「Trusted Extensions でのデバイス管理 (手順)」を参照してください。

Trusted Extensions の選択マネージャー

選択マネージャー GUI は、あるオブジェクトまたは選択範囲のラベルを変更しようとすると表示されます。詳細は、123 ページの「データのセキュリティーレベルを変更する際の規則」を参照してください。

Trusted Extensions のラベルビルダー

ラベルビルダー GUI 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の選択肢を提供します。たとえば、ラベルビルダーはログイン時に表示されます (『Trusted Extensions ユーザーガイド』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 コンポーネント名は、`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 `SENSITIVITY` セクションの下にある `WORDS` セクションに対応します。

開発者は `tgnome-selectlabel` コマンドを使用することで、自身のアプリケーションのラベルビルダーを構築できます。オンラインヘルプを表示するには、`tgnome-selectlabel -h` と入力します。『Trusted Extensions Developer's Guide』の第 6 章「Label Builder GUI」も参照してください。

Trusted Extensions のコマンド行ツール

Trusted Extensions に固有のコマンドや Trusted Extensions によって変更されるコマンドは、『Oracle Solaris Reference Manual』に含まれています。`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。コマンドの説明、Trusted Extensions ドキュメントセット内の例へのリンク、およびマニュアルページへのリンクについては、付録 D 「Trusted Extensions マニュアルページのリスト」を参照してください。

Trusted Extensions の構成ファイル

/etc/inet/ike/config ファイルは、ラベル情報を含むように Trusted Extensions によって拡張されます。ike.config(4) のマニュアルページでは、label_aware グローバルパラメータと 3 つのフェーズ 1 変換パラメータ single_label、multi_label、および wire_label について説明しています。

注 – IKE の構成ファイルに含まれるキーワード label は、フェーズ 1 の IKE 規則を一意にするために使用されます。IKE のキーワード label は、Trusted Extensions のラベルとは異なります。

◆ ◆ ◆ 第 8 章

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

この章では、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。

構成可能なセキュリティー機能

Trusted Extensions には Oracle Solaris 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、Oracle 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。

Trusted Extensions が Oracle Solaris と異なる点は、通常ある役割になることでシステムを管理するという点です。Oracle Solaris OS と同様に、構成ファイルは `root` 役割によって変更されます。

Trusted Extensions の役割

Trusted Extensions では、通常、役割を使用してシステムを管理します。スーパーユーザーは `root` 役割であり、監査フラグの設定、アカウントのパスワードの変更、システムファイルの編集など、いくつかのタスクで必要となります。役割は Oracle Solaris の場合とまったく同様に作成されます。

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 – Oracle Solaris のインストール時に作成されます
- 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 – 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

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。

Trusted Extensions で役割を作成する処理は、Oracle Solaris と同じです。デフォルトでは、`ADMIN_HIGH` から `ADMIN_LOW` の管理ラベル範囲が役割に割り当てられます。

- 役割の作成の概要については、『Oracle Solaris の管理: セキュリティーサービス』の「RBAC の使用 (タスク)」を参照してください。
- 役割を作成するには、『Oracle Solaris の管理: セキュリティーサービス』の「役割を作成する方法」を参照してください。

Trusted Extensions での役割の引き受け

トラステッドデスクトップ上で、割り当てられた役割になるには、トラステッドストライプのユーザー名をクリックして役割の選択肢を表示します。役割のパスワードの確認が完了すると、現在のワークスペースが役割ワークスペースに変更されます。役割ワークスペースは大域ゾーンに存在し、トラステッドパスの属性を持ちます。役割ワークスペースは管理ワークスペースです。

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

Trusted Extensions では既存のセキュリティー機能を拡張できます。さらに、Trusted Extensions は固有のセキュリティー機能も提供します。

Trusted Extensions による Oracle Solaris セキュリティー機能の拡張

Oracle Solaris が提供する次のセキュリティーメカニズムは、Trusted Extensions でも Oracle Solaris と同様に拡張可能です。

- 監査クラス – 監査クラスの追加については、『Oracle Solaris の管理: セキュリティーサービス』の第 28 章「監査の管理 (タスク)」で説明しています。

注 – 監査イベントを追加する必要のあるベンダーは、Oracle Solaris の担当者に連絡を取り、イベント番号の予約と監査インタフェースへのアクセス権の取得を行う必要があります。

- 役割と権利プロファイル – 役割や権利プロファイルの追加については、『Oracle Solaris の管理: セキュリティーサービス』の第 9 章「役割に基づくアクセス制御の使用 (タスク)」で説明しています。
- 承認 – 新しい承認の追加例については、288 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。

Oracle Solaris と同様に、特権は拡張できません。

Trusted Extensions 固有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。ワークスペースとそのオブジェクトにラベルが付けられます。
- デバイスマネージャー – 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 – このメニューを使用すると、ユーザーまたは役割のパスワードを変更できます。
- 「ワークスペースラベルを変更」メニュー – マルチレベルセッションのユーザーはワークスペースのラベルを変更できます。ユーザーが別のラベルのワークスペースに入る際にパスワードの入力を要求することが可能です。

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。

サイトから追加の提案を提供される可能性があります。

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、ユーザーに警告してください。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。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。
- `auth_attr` ファイル – カスタムの承認が含まれます。`auth_attr(4)` のマニュアルページを参照してください。
- `prof_attr` ファイル – カスタムの権利プロファイルが含まれます。`prof_attr(4)` のマニュアルページを参照してください。

- exec_attr ファイル – サイトで権利プロファイルに追加されたセキュリティー属性を持つコマンドが含まれます。exec_attr(4) のマニュアルページを参照してください。
- **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。

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/share/gnome/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/bin/tsoljdsselmgr` 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＆ドロップが対象です。

表 8–1 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
ファイルブラウザ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
	ダウングレード情報	同一 UID	`solaris.label.file.downgrade`
	アップグレード情報	同一 UID	`solaris.label.file.upgrade`
	ダウングレード情報	異なる UID	`solaris.label.file.downgrade`
	アップグレード情報	異なる UID	`solaris.label.file.upgrade`

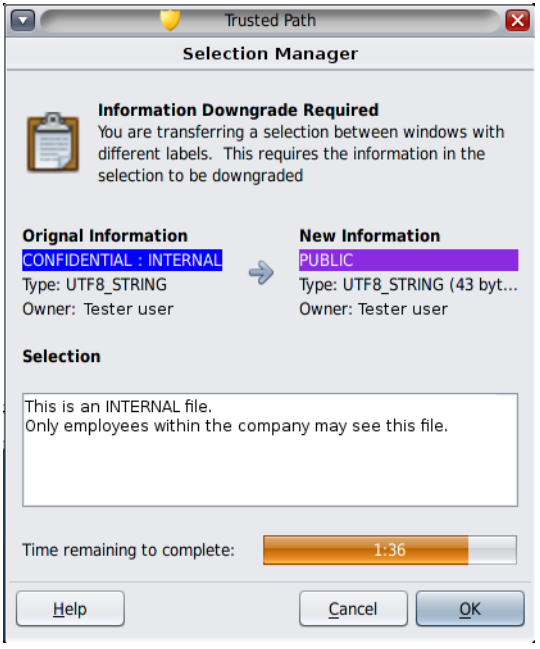
ウィンドウ内やファイル内の選択範囲には、異なる規則が適用されます。「選択範囲」のドラッグ＆ドロップでは、常にラベルと所有者が同じである必要があります。ウィンドウ間のドラッグ＆ドロップは、`sel_config` ファイルではなく、選択マネージャーアプリケーションを介して行われます。

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 8–2 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
	ダウングレード情報	同一 UID	`solaris.label.win.downgrade`
	アップグレード情報	同一 UID	`solaris.label.win.upgrade`
	ダウングレード情報	異なる UID	`solaris.label.win.downgrade`
	アップグレード情報	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 2 行の選択範囲を示しています。



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

/usr/share/gnome/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

◆ ◆ ◆ 第 9 章

Trusted Extensions での一般的なタスクの実行 (手順)

この章では、Trusted Extensions システムの管理について紹介し、これらのシステムで一般的に実行されるタスクについて説明します。

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
Trusted Extensions システムにログインします。	安全にログインします。	『Trusted Extensions ユーザーガイド』の「Trusted Extensions へのログイン」
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 のマニュアルページの使用	『Trusted Extensions ユーザーガイド』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	『Trusted Extensions ユーザーガイド』の「トラステッドアクションの実行」

作業	説明	参照先
役割になります。	大域ゾーンで役割になります。すべての管理タスクは大域ゾーンで実行されます。	128 ページの「Trusted Extensions の大域ゾーンに入る」
ユーザーワークスペースを選択します。	大域ゾーンから退出します。	128 ページの「Trusted Extensions の大域ゾーンを終了する」

▼ 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、150 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　管理役割が割り当てられています。118 ページの「Trusted Extensions での役割の作成」を参照してください。

1. トラステッドストライプで *account-name* をクリックします。
   一覧から役割を選択します。

   Trusted Extensions デスクトップの各機能の位置については、図 6–1 を参照してください。これらの機能の説明については、『Trusted Extensions ユーザーガイド』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。

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。
   認証後、現在のワークスペースが役割ワークスペースに切り替わります。

▼ Trusted Extensions の大域ゾーンを終了する

始める前に　大域ゾーンにいます。

1. 画面最下部のデスクトップパネルからユーザーワークスペースを選択します。

2. あるいは、トラステッドストライプで役割名をクリックしてからユーザー名を選択します。
   現在のワークスペースがユーザーワークスペースに変わります。このワークスペースでこれ以降にユーザーが作成するウィンドウはすべて、そのユーザーのユーザーラベルで作成されます。

役割ワークスペースで作成されたウィンドウは、その役割のラベルのプロセスをサポートし続けます。これらのウィンドウで起動されたプロセスは、大域ゾーン内で管理特権付きで実行されます。

詳細は、『Trusted Extensions ユーザーガイド』の「ラベル付きシステムでの作業」を参照してください。

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 での一般的な管理手順について説明します。

作業	説明	参照先
root のパスワードを変更します。	root 役割の新しいパスワードを指定します。	130 ページの「root ユーザーのパスワードを変更する」
ラベル付きゾーンでパスワードの変更を反映させます。	パスワードが変更されたことをゾーンに通知するために、ゾーンをリブートします。	130 ページの「ラベル付きゾーンで新しいローカルユーザーパスワードを有効にする」
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。	131 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。	132 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。	133 ページの「可読のラベルを 16 進形式から取得する」
デバイスを割り当てます。	ユーザーがデバイスを割り当てられるようにします。 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。	『Oracle Solaris の管理: セキュリティーサービス』の「ユーザーによるデバイス割り当てを承認する方法」 『Trusted Extensions ユーザーガイド』の「Trusted Extensions でデバイスを割り当てる」
システムを遠隔で管理します。	遠隔システムから Trusted Extensions システムを管理します。	第 12 章「Trusted Extensions での遠隔管理 (手順)」

▼ root ユーザーのパスワードを変更する

Trusted Extensions には、パスワードを変更するための GUI が用意されています。

1. **root** 役割になります。
   手順については、128 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. トラステッドストライプの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を開きます。
3. 「**Change Login Password**」を選択します。
   ゾーンごとに異なるパスワードが作成されている場合は、メニューに「Change Workspace Password」と表示されます。
4. パスワードを変更し、変更を確定します。

▼ ラベル付きゾーンで新しいローカルユーザーパスワードを有効にする

次の場合は、ラベル付きゾーンをリブートする必要があります。

- 1 人以上のローカルユーザーがパスワードを変更した。
- ネームサービスキャッシュデーモン (`nscd`) の単一インスタンスをすべてのゾーンが使用している。
- システムが LDAP ではなくファイルで管理されている。

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

- パスワードの変更を有効にするには、ユーザーがアクセスできるラベル付きゾーンをリブートします。
  次のいずれかの方法を使用します。
  - **`txzonemgr` GUI** を使用します。
    ```
    # txzonemgr &
    ```
    Labeled Zone Manager でラベル付きゾーンに移動し、コマンドの一覧から、「停止」を選択したあと「ブート」を選択します。
  - 大域ゾーンの端末ウィンドウでゾーン管理コマンドを使用します。
    システムのシャットダウンまたは停止を選択できます。
    - `zlogin` コマンドは、ゾーンを正常にシャットダウンします。

```
# zlogin labeled-zone shutdown -i 0
# zoneadm -z labeled-zone boot
```

- `halt` サブコマンドは、シャットダウンスクリプトを無視します。

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

注意事項 ラベル付きゾーンのユーザーパスワードを自動的に更新するには、LDAP を構成するか、ゾーンごとにネームサービスを 1 つずつ構成する必要があります。その両方を構成することもできます。

- LDAP を構成するには、第 5 章「Trusted Extensions のための LDAP の構成 (手順)」を参照してください。
- ゾーンごとにネームサービスを 1 つずつ構成するには、高度なネットワークスキルが必要となります。手順については、66 ページの「ラベル付きゾーンごとに異なるネームサービスを構成する」を参照してください。

▼ 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 9–1 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 9–2 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、128 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 : INTERNAL USE ONLY"
    0x0004-08-48
    ```

    文字列では大文字と小文字は区別されませんが、空白は正確でなければいけません。たとえば、次の引用符付き文字列では、16 進値のラベルが返されます。

    - `"CONFIDENTIAL : INTERNAL USE ONLY"`
    - `"cnf : Internal"`
    - `"confidential : internal"`

    次の引用符付き文字列では、解析エラーが返されます。

    - `"confidential:internal"`
    - `"confidential: internal"`

- 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。

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 9–3 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 Oracle Solaris と同じく、root アカウントはシステム上のデフォルトのセキュリティー値を変更できます。

セキュリティー値は、/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。詳細は、『Oracle Solaris の管理: セキュリティーサービス』の第 3 章「システムアクセスの制御 (タスク)」を参照してください。

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 root 役割になっている必要があります。

- システムファイルを編集します。

  次の表に、セキュリティーファイルと各ファイル内で変更可能なセキュリティー値の一覧を示します。

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。	『Oracle Solaris の管理: セキュリティーサービス』の「すべてのログイン失敗操作を監視する方法」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。	『Oracle Solaris の管理: セキュリティーサービス』の「システムのアボートシーケンスを無効にする方法」 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。 kadb(1M) のマニュアルページ
/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 10 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、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、67 ページの「Trusted Extensions での役割とユーザーの作成」を参照してください。

Trusted Extensions 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 権利プロファイルのコマンドは、ラベル属性を持ちます。コマンドは、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、Oracle Solaris 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。

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。

- 『Oracle Solaris の管理: 一般的なタスク』の「ユーザーアカウントの設定と管理 (作業マップ)」
- 『Oracle Solaris の管理: セキュリティーサービス』のパート III「役割、権利プロファイル、特権」

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
- 初期パスワードの割り当て
- ユーザーと役割のプロパティーの修正 (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、`root` 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。

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、Trusted Extensions のユーザーが実行可能なアクションや、必要とされる作業量に影響を与えます。一部の決定事項は、Oracle 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最初に設定されています。デフォルトの説明については、139 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、148 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、USB ドライブなどの周辺デバイス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、292 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を作成するには、288 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、140 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。決定は、29 ページの「ラベルストラテジの作成」と、『Trusted Extensions Label Administration』の例に基づいています。

セキュリティー管理者が個々のユーザーに対して明示的に設定したラベル値は、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

/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値が含まれています。Trusted Extensions はこのファイルに 2 つのキーワードを追加します。値をシステム全体で変更するには、これらの *keyword=value* ペアをファイルに追加します。次の表に、これらのキーワードのデフォルト値と可能な値を示します。

表 10–1　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	注意事項
IDLECMD	LOCK	LOCK | LOGOUT	ログインユーザーに適用されます。
IDLETIME	30	0 から 120 分	ログインユーザーに適用されます。

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。

34 ページの「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

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、2 つのヘルパーファイル .copy_files と .link_files を設定する場合があります。詳細は、143 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は、新しいユーザーのセキュリティー属性を変更できます。デフォルト値を含むファイルについては、139 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。次の表に、ユーザーに割り当て可能なセキュリティー属性とそれぞれの割り当ての効果を示します。

表 10–2 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	割り当ての効果
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	カーネル	任意	ユーザーはシステムデフォルト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は、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。

ユーザーにセキュリティー属性を割り当てるときには、次の情報を考慮してください。

パスワードの割り当て
: システム管理者は、ユーザーアカウントの作成時にアカウントにパスワードを割り当てることができます。この初期割り当てのあと、セキュリティー管理者またはユーザーはパスワードを変更できます。

  Oracle Solaris 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
: Oracle Solaris OS と同様、承認をユーザーに割り当てると、これらの承認は既存の承認に追加されます。ベストプラクティスは、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ることです。

権利プロファイルの割り当て
: Oracle Solaris OS と同様に、権利プロファイルの順序は重要です。プロファイルメカニズムでは、承認を除いて、割り当て済みセキュリティー属性の最初のインスタンスの値が使用されます。詳細は、『Oracle Solaris の管理: セキュリティーサービス』の「割り当てられたセキュリティー属性の検索順序」を参照してください。

  プロファイルの整列順を利用できます。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、権利プロファイルは機能できません。

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、156 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
: Oracle Solaris OS と同様に、ユーザーに監査クラスを割り当てると、そのユーザーの事前選択マスクが変更されます。監査の詳細については、『Oracle Solaris の管理: セキュリティーサービス』のパート VII「Oracle Solaris での監査」 and 第 22 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、148 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          .bashrc.user     .login
.aliases         .cshrc           .mailrc
.bashrc          .emacs           .mime_types
```

```
.newsrc                    .signature                 .soffice
```

◆ ◆ ◆ 第 11 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 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。これらのタスクの多くは、一般ユーザーがログインできるようになる前に実行します。

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。	146 ページの「デフォルトのユーザーラベル属性を修正する」
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。	146 ページの「`policy.conf` のデフォルトを修正する」
	システムのアイドル状態が設定された時間だけ続いた場合に、スクリーンセーバーを有効にするかユーザーをログアウトさせます。	例 11–1
	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 11–2

作業	説明	参照先
	パブリックキオスクの印刷出力でラベルが表示されないようにします。	例 11–3
ユーザーの初期設定ファイルを構成します。	.bashrc、.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。	148 ページの「Trusted Extensions のユーザーの起動ファイルを構成する」
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。	150 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できます。変更はすべての Trusted Extensions システムにコピーする必要があります。

注意 – 一般ユーザーがシステムにアクセスする前にこのタスクを実行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、128 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。
   詳細は、表 1–2 in 34 ページの「Trusted Extensions でのユーザーセキュリティーの計画」 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。
3. ファイルのコピーを各 **Trusted Extensions** システムに配布します。

注意 – label_encodings ファイルは、すべてのシステムで同一である必要があります 配布方法については、79 ページの「Trusted Extensions でファイルをポータブルメディアにコピーする」と 80 ページの「Trusted Extensions でポータブルメディアからファイルをコピーする」を参照してください。

▼ 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、Oracle Solaris 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と同じです。システムのすべてのユーザーのデフォルトを変更するには、この手順を使用します。

始める前に　大域ゾーンで root 役割になっている必要があります。詳細は、128 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 10–1 を参照してください。

2　設定を修正します。

例 11–1　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、root 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、root 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。

ログインユーザーがある役割になると、その役割に対するユーザーの IDLECMD 値と IDLETIME 値が有効となります。

例 11–2　各ユーザーの基本的な特権セットの修正

この例では、大規模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、root 役割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、次のようにコメントを外して修正します。

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

例 11–3　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、サイトセキュリティーが、パブリックキオスクコンピュータがラベルなしで印刷することを許可します。パブリックキオスクの root 役割が、/etc/security/policy.conf ファイル内の AUTHS_GRANTED の値を変更します。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。管理者はさらに policy.conf エントリを変更します。

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

パブリックキオスクのリブート後、すべての印刷ジョブがラベルなしになり、バナーページやトレーラページもなくなります。

▼ 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、128 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. エディタで、**.copy_files** ファイルへのフルパス名を入力します。

      ```
      # vi /etc/skel/.copy_files
      ```

   b. **.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。
      143 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 11–4 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. エディタで、**.link_files** ファイルへのフルパス名を入力します。

      ```
      # vi /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。

- 起動ファイルにどのファイルを含めるかについては、『Oracle Solaris の管理: 一般的なタスク』の「ユーザーの作業環境のカスタマイズ」を参照してください。
- 詳細は、『Oracle Solaris の管理: 一般的なタスク』の「ユーザー初期設定ファイルをカスタマイズする方法」を参照してください。

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 11–4 ユーザーの起動ファイルのカスタマイズ

この例では、システム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。

システム管理者は、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
.bashrc
.bashrc.user
.cshrc
.login
:wq

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

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 .bashrc .bashrc.user .cshrc \
.login .profile .mailrc /etc/skelC
$ cp .copy_files .link_files .ksh .profile .mailrc \
/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。

▼ 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. ログイン画面でユーザー名を入力します。

2. 画面最下部で、デスクトップメニューから「**Solaris Trusted Extensions Failsafe Session**」を選択します。
3. プロンプトが表示されたら、パスワードを入力します。
4. 追加のパスワードを求めるプロンプトが表示されたら、**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。

ユーザーと権利の管理 (作業マップ)

Trusted Extensions でユーザー、承認、権利、および役割を管理するには、セキュリティー管理者役割になります。次の作業マップでは、ラベル付きの環境で操作するユーザーに対して実行する一般的な作業について説明します。

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。	152 ページの「ユーザーのラベル範囲を変更する」
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。	152 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」
ユーザーをいくつかのアプリケーションに制限するデスクトップを作成します。	デスクトップ上に表示されるアプリケーションのみをユーザーが開けるようにする権利プロファイルを割り当てます。コマンド行は使用できないか、必要に応じて少数のコマンドのみを受け入れます。	153 ページの「デスクトップアプリケーションにユーザーを制限する」
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。	156 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。	156 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。	157 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。	157 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」

▼ ユーザーのラベル範囲を変更する

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が、ある特定のラベルで実行されているシステムの一覧を表示できるようになります。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。

- 次のいずれかを行います。
  - 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割り当てます。

    ```
    # usermod -K min_label=INTERNAL -K clearance=ADMIN_HIGH jdoe
    ```

    また、最小ラベルを下げることでユーザーのラベル範囲を拡張することもできます。

    ```
    # usermod -K min_label=PUBLIC -K clearance=INTERNAL jdoe
    ```

    詳細は、usermod(1M) および user_attr(4) のマニュアルページを参照してください。
  - 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。

    ```
    # usermod -K min_label=INTERNAL -K clearance=INTERNAL jdoe
    ```

▼ 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、146 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. 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、『Oracle Solaris の管理: セキュリティーサービス』の「権利プロファイルを作成または変更する方法」を参照してください。

ユーザーにとって便利な可能性のある承認を次に示します。

- `solaris.device.allocate` – マイクロフォンや CD-ROM などの周辺デバイスの割り当てをユーザーに承認します。

  デフォルトでは、Oracle 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。
- `solaris.label.file.downgrade` – 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。
- `solaris.label.file.upgrade` – 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。
- `solaris.label.win.downgrade` – 上位レベルファイルからの情報の選択と、下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。
- `solaris.label.win.noview` – 移動対象の情報を表示せずに移動することを、ユーザーに承認します。
- `solaris.label.win.upgrade` – 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。
- `solaris.login.remote` – 遠隔ログインをユーザーに承認します。
- `solaris.print.ps` – PostScript ファイルの印刷をユーザーに承認します。
- `solaris.print.nobanner` – 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。
- `solaris.print.unlabeled` – 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。
- `solaris.system.shutdown` – 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。

2. 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。

   詳細な手順については、『Oracle Solaris の管理: セキュリティーサービス』の「ユーザーの RBAC プロパティーを変更する方法」を参照してください。

▼ デスクトップアプリケーションにユーザーを制限する

サイトのセキュリティーによっては、デスクトップアイコンから開けるアプリケーションのみにユーザーがアクセスできるようにしなければいけない場合があります。この手順では、必要なアプリケーションのみにユーザーを制限する権利プロファイルを割り当てます。

注 – Trusted Extensions デスクトップでは、コマンドの実行は常に権利プロファイルに基づいて行われます。

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、146 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 **Oracle Solaris** ユーザーがデスクトップ上の基本的なアプレットを実行できるようにする **Desktop Applets** という名前の権利プロファイルを作成します。

手順については、『Oracle Solaris の管理: セキュリティーサービス』の「ユーザーをデスクトップアプリケーションに制限する方法」を参照してください。

2 **Trusted Extensions** ユーザーがデスクトップ上の必要なトラステッドアプレットを実行できるようにする別の権利プロファイルを作成します。

行は表示のために折り返されています。

```
# profiles -p "Trusted Desktop Applets"
profiles:Trusted Desktop Applets>
set desc="Can use trusted desktop applications except terminal"
profiles:Trusted Desktop Applets> add cmd=/usr/dt/config/tsoljds-migration;end
profiles:Trusted Desktop Applets> add cmd=/usr/bin/tsoljds-xagent;end
profiles:Trusted Desktop Applets> commit
```

3 **Desktop Applets** プロファイルを補助的な権利プロファイルとして、**Trusted Desktop Applets** プロファイルに追加します。

この権利プロファイルは手順 2 で作成済みです。

```
profiles:Trusted Desktop Applets> add profiles="Desktop Applets"
profiles:Trusted Desktop Applets> commit
profiles:Trusted Desktop Applets> exit
```

4 **Trusted Desktop Applets** 権利プロファイルに正しいエントリが含まれていることを確認します。

エントリにタイプミスや抜け、重複などの誤りが含まれていないか確認します。

```
# profiles -p "Trusted Desktop Applets" info
Found profile in files repository.
name=Trusted Desktop Applets
desc=Can use trusted desktop applications except terminal
profiles=Desktop Applets
cmd=/usr/dt/config/tsoljds-migration
cmd=/usr/bin/tsoljds-xagent
```

ヒント – デスクトップアイコンを持つアプリケーションまたはアプリケーションクラスの権利プロファイルを作成できます。その後、Trusted Desktop Applets 権利プロファイルを、デスクトップアクセスのための補助的な権利プロファイルとして追加します。

5 **Trusted Desktop Applets** および **Stop** 権利プロファイルをユーザーに割り当てます。

```
# usermod -P "Trusted Desktop Applets,Stop" username
```

このユーザーは、トラステッドデスクトップを使用することはできますが、端末ウィンドウを起動したり、コンソールユーザーとして振る舞ったり、Basic Solaris User 権利プロファイルに含まれる権利を持ったりすることはできません。

例 11–5 デスクトップユーザーが端末ウィンドウを開けるようにする

この例の管理者は、デスクトップユーザーが端末ウィンドウを開けるようにします。管理者はすでに、Oracle Solaris デスクトップユーザー用の Desktop Applets 権利プロファイルと Trusted Extensions デスクトップユーザー用の Trusted Desktop Applets 権利プロファイルを、LDAP リポジトリに作成済みです。

まず、管理者は Terminal Window 権利プロファイルを作成し、その内容を確認します。

```
# profiles -p "Terminal Window" -S ldap
profiles:Terminal Window> set desc="Can open a terminal window"
profiles:Terminal Window> add cmd=/usr/bin/gnome-terminal;end
profiles:Terminal Window> commit
profiles:Terminal Window> exit
# profiles -p "Terminal Window" info
Found profile in ldap repository.
name=Terminal Window
desc=Can open a terminal window
cmd=/usr/bin/gnome-terminal
```

次に、管理者はこの権利プロファイルと All 権利プロファイルを、タスク実行時に端末ウィンドウを必要とするデスクトップユーザーに割り当てます。All 権利プロファイルがなければ、`ls` や `cat` などの特権を必要としない UNIX コマンドを、ユーザーは実行することができません。

```
# usermod -P "Trusted Desktop Applets,Terminal Window,All,Stop" -S ldap jdoe
```

この一連の権利プロファイルにより、ユーザー `jdoe` は、デスクトップや端末ウィンドウを使用できますが、コンソールユーザーとして振る舞ったり、Basic Solaris User 権利プロファイルに含まれる権利を持ったりすることはできません。

▼ 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。

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。

- **basic** セットにある 1 つ以上の特権を削除します。

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できません。

```
# usermod -K defaultpriv=basic,!proc_info,!proc_session,!file_link_any
```

proc_info 特権を削除することにより、ユーザーは自分が開始元でないプロセスを一切検査できなくなります。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。

参照　権利プロファイル内の特権制限を収集する例については、『Oracle Solaris の管理: セキュリティーサービス』の「権利プロファイルを作成または変更する方法」のあとの例を参照してください。

システム上のすべてのユーザーの特権を制限するには、例 11–2 を参照してください。

▼ ユーザーのアカウントロックを禁止する

この手順は、役割になれるすべてのユーザーで実行します。

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。

- ローカルユーザーのアカウントロックを無効にします。

```
# usermod -K lock_after_retries=no jdoe
```

LDAP ユーザーのアカウントロックを無効にするには、LDAP リポジトリを指定します。

```
# usermod -S ldap -K lock_after_retries=no jdoe
```

▼ 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または選択されたテキスト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、181 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. 152 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. そのプロファイルを適切なユーザーや役割に割り当てます。

   詳細な手順については、『Oracle Solaris の管理: セキュリティーサービス』の「ユーザーの RBAC プロパティーを変更する方法」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　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. 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. ユーザーアカウントを削除します。

```
# userdel -r jdoe
```

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。

その他の考慮点については、122 ページの「ユーザーの削除について」を参照してください。

◆ ◆ ◆ 第 12 章

Trusted Extensions での遠隔管理 (手順)

この章では、遠隔管理が可能なように Trusted Extensions システムを設定する方法と、そうしたシステムにログインして管理する方法について説明します。

注 – ヘッドレスシステムやその他の遠隔システムで必要とされる構成方法は、評価された構成の基準を満たしません。詳細は、28 ページの「サイトのセキュリティーポリシーについて」を参照してください。

Trusted Extensions での遠隔管理

遠隔管理には重大なセキュリティーリスクが伴います。信頼できないシステム上のユーザーからの遠隔管理では特にそうです。デフォルトの Trusted Extensions では、どのシステムからも遠隔管理は行えません。

ネットワークが構成されるまでは、すべての遠隔ホストに `admin_low` セキュリティーテンプレートが割り当てられます。つまり、それらのホストはラベルなしホストとして認識されます。ラベル付きゾーンが構成されるまで、使用可能なゾーンは大域ゾーンだけになります。Trusted Extensions では、大域ゾーンが管理ゾーンです。これにアクセスできるのは役割だけです。具体的には、大域ゾーンに到達するには、アカウントに `ADMIN_LOW` から `ADMIN_HIGH` のラベル範囲が含まれている必要があります。

この初期状態の間、Trusted Extensions 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。それらのメカニズムには、netservices の値、デフォルトの ssh ポリシー、デフォルトのログインポリシー、デフォルトの PAM ポリシーなどがあります。

- インストール時には、Secure Shell 以外の遠隔サービスは有効化されず、ネットワーク上で待機しません。

  ただし、ssh ポリシー、ログインポリシー、および PAM ポリシーが存在しているため、root や役割が ssh サービスを使用して遠隔ログインを行うことはできません。

- root は役割であるため、root アカウントを使用して遠隔ログインを行うことはできません。PAM の制限により、役割はログインできません。

  root をユーザーアカウントに変更しても、デフォルトのログインポリシーと ssh ポリシーにより、root ユーザーによる遠隔ログインは禁止されます。

- 2 つのデフォルトの PAM 値によって遠隔ログインが禁止されます。

  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と遠隔ログインを拒否します。

  Trusted Extensions PAM モジュール pam_tsol_account は、CIPSO プロトコルを使用しないかぎり、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。

このため、Oracle Solaris システムの場合と同様に、遠隔管理を構成する必要があります。Trusted Extensions では、大域ゾーンへの到達に必要なラベル範囲と pam_tsol_account モジュールという、2 つの構成要件が追加されます。

Trusted Extensions での遠隔システムの管理方式

Trusted Extensions では、ssh プロトコルとホストベースの認証を使用して遠隔システムに到達し、管理する必要があります。ホストベースの認証を使用すると、同じ名前を持つユーザーアカウントが遠隔 Trusted Extensions 上で役割になることができます。

ホストベースの認証を使用する場合、ssh クライアントは、元のユーザー名と役割名の両方を遠隔システムであるサーバーに送信します。サーバーはこの情報に基づいて、ユーザーアカウントがサーバーにログインしなくても役割になれるだけの内容を、pam_roles モジュールに渡すことができます。

Trusted Extensions では、次の遠隔管理方式が可能です。

- **Trusted Extensions** システムからの管理 – もっとも安全な遠隔管理を行えるように、両方のシステムで、相手のシステムを CIPSO セキュリティーテンプレートに割り当てます。例 12–1 を参照してください。
- ラベルなしシステムからの管理 – Trusted Extensions システムによる管理が実用的でない場合は、`pam.conf` ファイルで `pam_tsol_account` モジュールに `allow_unlabeled` オプションを指定することにより、ネットワークプロトコルのポリシーを引き下げることができます。

  このポリシーを引き下げた場合、任意のシステムが大域ゾーンに到達できないようにデフォルトのセキュリティーテンプレートを変更する必要があります。`admin_low` テンプレートはひかえめに使用するようにし、ワイルドカードアドレス `0.0.0.0` のデフォルトを `ADMIN_LOW` ラベルにしないようにする必要があります。詳細は、233 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。

どちらの管理シナリオの場合も、`root` 役割を使用して遠隔ログインを行うには、`pam_roles` モジュールに `allow_remote` オプションを指定して PAM ポリシーを引き下げる必要があります。

通常、管理者は `ssh` コマンドを使用することで、コマンド行から遠隔システムを管理します。`-X` オプションを指定すれば、Trusted Extensions の管理 GUI を使用できます。

また、Xvnc サーバーで遠隔 Trusted Extensions を構成することもできます。その場合、仮想ネットワークコンピューティング (VNC) 接続を使用することで、遠隔マルチレベルデスクトップの表示とシステムの管理を行うことができます。164 ページの「遠隔アクセス用に Xvnc で Trusted Extensions システムを構成する」を参照してください。

Trusted Extensions での遠隔システムの構成および管理 (作業マップ)

遠隔管理を有効にしたあと、遠隔システムをリブートして Trusted Extensions を有効にする前に、仮想ネットワークコンピューティング (VNC) または `ssh` プロトコルを使用してシステムを構成できます。

作業	説明	参照先
Trusted Extensions システムの遠隔管理を有効にします。	指定された `ssh` クライアントからの Trusted Extensions システムの管理を有効にします。	162 ページの「遠隔 Trusted Extensions システムの遠隔管理を有効にする」

作業	説明	参照先
仮想ネットワークコンピューティング (Virtual Network Computing、VNC) を有効にします。	任意のクライアントから、遠隔 Trusted Extensions システムで Xvnc サーバーを使用して、クライアントにサーバーのマルチレベルセッションを表示します。	164 ページの「遠隔アクセス用に Xvnc で Trusted Extensions システムを構成する」
Trusted Extensions システムに遠隔でログインします。	遠隔システム上の役割になってそのシステムを管理します。	166 ページの「遠隔 Trusted Extensions システムにログインして管理する」

注 – セキュリティーポリシーを確認して、サイトで許可されている遠隔管理の方法を判定します。

▼ 遠隔 Trusted Extensions システムの遠隔管理を有効にする

この手順では、ある Oracle Solaris 遠隔システム上でホストベースの認証を有効にしたあと、そのシステムに Trusted Extensions 機能を追加します。遠隔システムは ssh サーバーです。

始める前に　遠隔システムに Oracle Solaris がインストールされており、そのシステムにアクセスできます。

1. 両方のシステムでホストベースの認証を有効にします。

   手順については、『Oracle Solaris の管理: セキュリティーサービス』の「ホストに基づく認証を Secure Shell に設定する方法」を参照してください。

   注 – cat コマンドは使用しないでください。ssh 接続経由で公開鍵をコピー & ペーストします。ssh クライアントが Oracle Solaris システムでない場合は、プラットフォームの手順に従って、ホストベースの認証で ssh クライアントを構成します。

   この手順が完了すると、root 役割になれるユーザーアカウントが両方のシステム上に存在しています。これらのアカウントには同じ UID、GID、および役割割り当てが割り当てられています。また、生成された公開/非公開鍵ペアと共有公開鍵も存在しています。

2. **ssh サーバーで、ssh ポリシーを引き下げて root が遠隔ログインを行えるようにします。**

   ```
   # vi /etc/ssh/sshd_config
   ## Permit remote login by root
   PermitRootLogin yes
   ```

   あとの手順で、root ログインを特定のシステムとユーザーに制限します。

注 – 管理者は root 役割になるので、遠隔 root ログインを禁止するログインポリシーを引き下げる必要はありません。

3 **ssh** サーバーで **ssh** サービスを再起動します。

```
# svcadm restart ssh
```

4 **ssh** サーバーの **root** のホームディレクトリ内で、ホストベースの認証のためのホストとユーザーを指定します。

```
# cd
# vi .shosts
client-host username
```

この .shosts ファイルは、公開/非公開鍵が共有されている状態で、*client-host* システム上の *username* がサーバー上の root 役割になれるようにします。

5 **ssh** サーバーで **2** つの **PAM** ポリシーを引き下げます。

a. 役割による遠隔ログインを許可します。

```
# vi /etc/pam.conf
...
# Default definition for Account management
# Used when service name is not explicitly mentioned for account management
#
# other   account requisite    pam_roles.so.1
# Enable remote role assumption
other   account requisite    pam_roles.so.1   allow_remote
...
```

このポリシーは、*client-host* システム上の *username* がサーバー上で役割になれるようにします。

b. ラベルなしホストから **Trusted Extensions** 遠隔システムへの接続を許可します。

```
# vi /etc/pam.conf
# Default definition for Account management
# Used when service name is not explicitly mentioned for account management
#
# other   account requisite    pam_roles.so.1
# Enable remote role assumption
other   account requisite    pam_roles.so.1   allow_remote
#
other   account required     pam_unix_account.so.1
# other   account required     pam_tsol_account.so.1
# Enable unlabeled access to TX system
other   account required     pam_tsol_account.so.1  allow_unlabeled
```

c. 変更済みの **pam.conf** ファイルを **pam.conf.site** にコピーします。

```
# cp /etc/pam.conf /etc/pam.conf.site
```

6 この構成をテストします。

a. 遠隔システムで新しい端末を開きます。

b. *client-host* 上の *username* が所有するウィンドウ内で、遠隔システム上の **root** 役割になります。

```
% ssh -l root remote-system
```

7 構成が正しく機能することがわかったら、遠隔システムで **Trusted Extensions** を有効にし、リブートします。

```
# svcadm enable -s labeld
# /usr/sbin/reboot
```

例 12–1 遠隔管理のための CIPSO ホストタイプの割り当て

この例では、管理者は Trusted Extensions システムを使用して遠隔 Trusted Extensions ホストを構成します。管理者はそのために、各システム上で `tncfg` コマンドを使用して、ピアシステムのホストタイプを定義します。

remote-system `# tncfg -t cipso add host=192.168.1.12` *Client-host*

client-host `# tncfg -t cipso add host=192.168.1.22` *Remote system*

ラベルなしシステムも遠隔 Trusted Extensions ホストを構成できるので、管理者は遠隔システムの `pam.conf` ファイル内に `allow_unlabeled` オプションを残します。

注意事項 管理者が新しいリリースの Oracle Solaris OS にアップグレードしても、新しい `pam.conf` ファイルはインストールされません。アップグレード時の `preserve=true` ファイルアクションの説明については、`pkg`(5) のマニュアルページを参照してください。

▼ 遠隔アクセス用に Xvnc で Trusted Extensions システムを構成する

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 が実行されている Xvnc サーバーに接続して、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。

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。

始める前に　Xvnc サーバーとして使用されるこのシステム上で、Trusted Extensions のインストールと構成が完了しています。このシステムの大域ゾーンは固定 IP アドレスを持ちます。つまりこのゾーンでは、netcfg(1M) のマニュアルページで説明されている自動ネットワーク構成プロファイルは使用されていません。

このシステムは、VNC クライアントをホスト名か IP アドレスで認識します。具体的には、admin_low セキュリティーテンプレート内で、このサーバーの VNC クライアントになれるシステムが、明示的に特定されるかワイルドカードを使用して特定されます。接続を安全に構成する方法の詳細については、233 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。

現在、将来の Trusted Extensions Xvnc サーバーのコンソールの GNOME セッションで実行している場合は、デスクトップ共有を有効にする必要はありません。

将来の Trusted Extensions Xvnc サーバーの大域ゾーンで root 役割になっています。

1. **Xvnc ソフトウェアを読み込むか更新します。**

   ```
   # packagemanager &
   ```

   パッケージマネージャー GUI で「vnc」を検索し、使用可能なサーバーから選択します。オプションの 1 つとして、TigerVNC X11/VNC サーバーソフトウェアがあります。

2. **X ディスプレイマネージャーの制御プロトコルを有効にします。**

   GNOME ディスプレイマネージャー (gdm) のカスタム構成ファイルを変更します。/etc/gdm/custom.conf ファイルの [xdmcp] 見出しの下に、Enable=true と入力します。

   ```
   [xdmcp]
   Enable=true
   ```

3. **/etc/gdm/Xsession ファイルの 27 行目あたりに、次の行を挿入します。**

   ```
   DISPLAY=unix:$(echo $DISPLAY|sed -e s/::ffff://|cut -d: -f2)
   ```

4. **Xvnc サーバーのサービスを有効にします。**

   ```
   # svcadm enable xvnc-inetd
   ```

5. **このサーバー上のアクティブな GNOME セッションをすべてログアウトさせます。**

   ```
   # svcadm restart gdm
   ```

   デスクトップマネージャーが再起動するまで約 1 分間待ちます。これで、VNC クライアントが接続可能となります。

6. **Xvnc ソフトウェアが有効になっていることを確認します。**

   ```
   # svcs | grep vnc
   ```

7 この **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。Oracle Solaris リポジトリの VNC ソフトウェアを使用できます。

8 **Xvnc** サーバーのワークスペースを **VNC** クライアント上で表示するには、次の手順を実行します。

a. 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
```

コマンドのオプションについては、`vncviewer(1)` のマニュアルページを参照してください。

b. 表示されるウィンドウで、ユーザー名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、『Trusted Extensions ユーザーガイド』の「Trusted Extensions へのログイン」を参照してください。

▼ 遠隔 Trusted Extensions システムにログインして管理する

この手順を実行すると、コマンド行と `txzonemgr` GUI を使用して遠隔 Trusted Extensions システムを管理できます。

始める前に 162 ページの「遠隔 Trusted Extensions システムの遠隔管理を有効にする」の説明に従って、ローカルシステム上と遠隔システム上でユーザー、役割、および役割割り当てがまったく同様に定義されています。

1 デスクトップシステムで、遠隔システムからのプロセスが表示されるようにします。

```
desktop $ xhost + remote-sys
```

2 両方のシステムで同じ名前が付けられたユーザーになっている必要があります。

3 端末ウィンドウから遠隔システムにログインします。

`ssh` コマンドを使用してログインします。

```
desktop $ ssh -X -l identical-username remote-sys
Password:       Type the user's password
remote-sys $
```

`-X` オプションは GUI の表示を可能にします。

4 同じ端末ウィンドウで、両方のシステムでまったく同様に定義された役割になります。

たとえば、root の役割になります。

```
remote-sys $ su - root
Password:      Type the root password
```

大域ゾーンにいます。これで、この端末ウィンドウを使用してコマンド行から遠隔システムを管理できるようになりました。画面上に GUI が表示されます。例については、例 12–2 を参照してください。

例 12–2 遠隔システムでのラベル付きゾーンの設定

この例では、管理者が txzonemgr GUI を使用して、ラベル付きデスクトップシステムからラベル付き遠隔システム上のラベル付きゾーンを設定します。Oracle Solaris と同様に、管理者は ssh コマンドに -X オプションを使用して、デスクトップシステムへの X サーバーのアクセスを許可します。ユーザー jandoe は両方のシステムで同じように定義されているので、役割 remoterole になることができます。

```
TXdesk1 $ xhost + TXnohead4

TXdesk1 $ ssh -X -l jandoe TXnohead4
Password: Ins1PwD1
TXnohead4 $
```

管理者は大域ゾーンに到達するために、jandoe アカウントを使用して役割 remoterole になります。この役割は、両方のシステムで同じように定義されています。

```
TXnohead4 # su - remoterole
Password: abcd1EFG
```

同じ端末で、管理者は remoterole 役割と l して txzonemgr GUI を起動します。

```
TXnohead4 $ /usr/sbin/txzonemgr &
```

Labeled Zone Manager は遠隔システム上で実行され、ローカルシステム上に表示されます。

例 12–3 遠隔ラベル付きゾーンへのログイン

管理者は、遠隔システム上の PUBLIC ラベルの構成ファイルを変更する必要があります。

管理者には 2 つの選択肢が用意されています。

- 大域ゾーンに遠隔ログインして遠隔大域ゾーンを表示したあと、PUBLIC ラベルに切り替え、端末ウィンドウを開き、ファイルを編集します。
- PUBLIC 端末ウィンドウから ssh コマンドを使用して PUBLIC ゾーンに遠隔ログインしたあと、ファイルを編集します。

遠隔システムですべてのゾーンに対して 1 つのネームサービスデーモン (nscd) が実行されていて、なおかつその遠隔システムでファイルネームサービスが使用されている場合、遠隔ゾーンのパスワードは、そのゾーンが最後にブートされたときに有効だったパスワードになります。遠隔 PUBLIC ゾーンのパスワードを変更しても、変更後にそのゾーンをブートしなければ、元のパスワードでアクセスが許可されます。

注意事項 -X オプションが機能しない場合は、パッケージをインストールしなければいけない可能性があります。xauth バイナリがインストールされていないと、X11 転送が無効になります。このバイナリを読み込むコマンドを次に示します: **pkg install pkg:/x11/session/xauth**

◆ ◆ ◆ 第 13 章

Trusted Extensions でのゾーンの管理 (手順)

この章では、非大域ゾーンまたはラベル付きゾーンが Trusted Extensions システム上でどのように動作するかについて説明します。また、ラベル付きゾーンに固有の手順も含まれています。

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。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 システムでは、大域ゾーンは完全に管理ゾーンになります。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できます。

Trusted Extensions システムで、ゾーンのファイルシステムは通常、大域ゾーンで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。

各ゾーンはそれぞれ独立した ZFS ファイルシステムです。各ゾーンは、関連付けられた IP アドレスとセキュリティー属性を持つことができます。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 14 章「Trusted Extensions でのファイルの管理とマウント (手順)」および 189 ページの「ラベル付き ZFS データセットのマウント」を参照してください。

Trusted Extensions のゾーンは、Oracle Solaris ゾーン製品の上に構築されます。参考情報として、『Oracle Solaris のシステム管理 (Oracle Solaris ゾーン、Oracle Solaris 10 ゾーン、およびリソース管理)』のパート II「Oracle Solaris ゾーン」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。彼らは 32 ページの「ラベル付きゾーンへのアクセス」で説明した 3 種類の構成を考慮し、その概要は次のとおりです。

- 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。

  このデフォルト構成は、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。

- 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ネットワーク接続された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。

Oracle Solaris では、排他 IP インスタンスと呼ばれる 4 つ目の構成タイプが、非大域ゾーンで使用可能になっています。この構成では、非大域ゾーンに独自の IP インスタンスが割り当てられ、各ゾーンは独自の物理インタフェースを管理します。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。その説明については、『Oracle Solaris のシステム管理 (Oracle Solaris ゾーン、Oracle Solaris 10 ゾーン、およびリソース管理)』の「ゾーンネットワークインタフェース」を参照してください。

Trusted Extensions で排他 IP インスタンスを構成した場合、各ラベル付きゾーンは、独立したシングルレベルシステムであるか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。このマニュアルでは、ネットワークが完全に大域ゾーンによって制御されるものと仮定しています。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。Trusted Extensions システムと通信を行うことで、IP アドレスにセキュリティーテンプレートが割り当てられます。セキュリティー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のラベル範囲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デフォルト構成では、ssh サービス用の MLP を 1 つのゾーンに追加できます。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。

例については、238 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。

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。ラベル付きファイルシステムを共有する場合は、191 ページの「ラベル付きゾーンのファイルシステムを共有する」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

ゾーン管理タスクはコマンド行から実行できます。ただし、ゾーンを管理するもっとも単純な方法は、Trusted Extensions が提供するシェルスクリプト /usr/sbin/txzonemgr を使用することです。このスクリプトは、ゾーンの作成、インストール、初期化、およびブート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。txzonemgr は zenity コマンドを使用します。詳細については、txzonemgr(1M) と zenity(1) のマニュアルページ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、Oracle 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へのリンクも示します。

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。	175 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。	176 ページの「マウントされたファイルのラベルを表示する」
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。	177 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。	178 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。	181 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」
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。	179 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。	57 ページの「ラベル付きゾーンを対話形式で作成する」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。	238 ページの「ゾーンにマルチレベルポートを作成する」 例 16–19
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。	195 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」
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。	『Oracle Solaris のシステム管理 (Oracle Solaris ゾーン、Oracle Solaris 10 ゾーン、およびリソース管理)』の「非大域ゾーンを削除する方法」

▼ 作成済みまたは実行中のゾーンを表示する

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. **txzonemgr &** コマンドを実行します。
   ゾーンの名前、ステータス、およびラベルが GUI に表示されます。

2. または、**zoneadm list -v** コマンドを使用します。

```
# zoneadm list -v
ID NAME       STATUS     PATH              BRAND       IP
 0 global     running    /                 ipkg        shared
 5 internal   running    /zone/internal    labeled     shared
 6 public     running    /zone/public      labeled     shared
```

   ゾーンのラベルは出力に表示されません。

▼ 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. エディタで **getmounts** スクリプトを作成します。

   `/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_HIGH
/dev:   ADMIN_HIGH
/system/contract:        ADMIN_HIGH
/proc:                   ADMIN_HIGH
/system/volatile:        ADMIN_HIGH
/system/object:          ADMIN_HIGH
/lib/libc.so.1:          ADMIN_HIGH
/dev/fd:        ADMIN_HIGH
/tmp:           ADMIN_HIGH
/etc/mnttab:    ADMIN_HIGH
/export:        ADMIN_HIGH
/export/home:   ADMIN_HIGH
/export/home/jdoe:   ADMIN_HIGH
/zone/public:        ADMIN_HIGH
/rpool:              ADMIN_HIGH
/zone:               ADMIN_HIGH
/home/jdoe:          ADMIN_HIGH
/zone/public:        ADMIN_HIGH
/zone/snapshot:      ADMIN_HIGH
/zone/internal:      ADMIN_HIGH
...
```

例 13–1　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` ゾーンのサンプル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/jdoe:   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
   ```

3. ゾーンを起動します。

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

例 13–2 /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 13–3 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かぎり、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する必要があります。大域ゾーンで root 役割になっている必要があります。

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. **データセットを共有できるようにします。**

   `# zfs set sharenfs=on` *datasetdir/subdir*

5 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、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。

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 13–4 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、管理者はデータセットを共有します。

```
# zfs set sharenfs=on 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
```

次に、管理者は needtoknow ゾーンをブートします。

```
# 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 ゾーンは needtoknow ゾーンよりも優位であり、ユーザーは /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 構成する予定のゾーンを停止する必要があります。大域ゾーンでセキュリティー管理者役割になります。

1. **Labeled Zone Manager を開きます。**

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

2. 再ラベル付けできるようにゾーンを構成します。

   a. ゾーンをダブルクリックします。

   b. 一覧から「**Permit Relabeling**」を選択します。

3. 「ブート」を選択してゾーンを再起動します。

4. 「取消し」をクリックしてゾーン一覧に戻ります。

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、157 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 13–5 internal ゾーンからのダウングレードの禁止

この例では、セキュリティー管理者は、以前ファイルをダウングレードするために使用されていたシステム上で、`CNF: INTERNAL USE ONLY` ファイルのダウングレードを禁止します。

管理者は Labeled Zone Manager を使用して、`internal` ゾーンを停止したあと、`internal` ゾーンのメニューから「Deny Relabeling」を選択します。

◆ ◆ ◆ 第 14 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、NFS、および ZFS 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、Oracle Solaris 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 はすべての非大域ゾーンに一意のラベルを付けるため、そのゾーンに属するファイルやファイルシステムはすべて、そのゾーンのラベルでマウントされます。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 Oracle Solaris マウントと類似しています。違いは、MAC ポリシーの実施にあります。さらに、`txzonemgr` スクリプトは、ホームディレクトリが `/export/home` としてマウントされるものと仮定します。

Trusted Extensions の NFS 共有は、大域ゾーンの Oracle 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、Oracle Solaris 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、オートマウンタと `mount` コマンドを使用できます。ファイルの共有には、ZFS データセットの `sharenfs` プロパティーが使用されます。
- 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、Oracle Solaris 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、オートマウンタと `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 `auto_home_`*zone-name* 構成ファイルが存在します。
- ラベル付きゾーンでの共有 – ラベル付きゾーン内のファイルは、ZFS 共有プロパティーを使用してそのゾーンのラベルで共有できます。詳細は、172 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 システムが別の Trusted Extensions システムのファイルシステムをマウントできるためには、サーバーとクライアントが互換性のある `cipso` タイプの遠隔ホストテンプレートを持っている必要があります。

  Trusted Extensions クライアントが NFS マウントされたファイルシステムに書き込みできるためには、そのファイルシステムが読み取り/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。
- Trusted Extensions システムがラベルなしシステムのファイルシステムをマウントできるためには、Trusted Extensions システムによってラベルなしシステムに割り当てられたシングルラベルが、Trusted Extensions システムのラベルに一致する必要があります。

  同様に、ラベル付きゾーンがラベルなしシステムのファイルシステムをマウントできるためには、Trusted Extensions システムによってラベルなしシステムに割り当てられたシングルラベルが、ラベル付きゾーンのラベルに一致する必要があります。

- マウント先のゾーンとは異なるラベルを持つファイルシステムが LOFS でマウントされた場合、そのファイルシステムは表示はできますが、変更はできません。NFS マウントについては、186 ページの「Trusted Extensions での NFS マウントされたファイルシステムへのアクセス」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できます。詳細は、186 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、管理者は下位レベルのファイルシステムをユーザーから隠すことができます。詳細は、178 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 アクセスできないかぎ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

Oracle Solaris の非大域ゾーンはファイルシステムを共有できます。同様に、Trusted Extensions のラベル付きゾーンはファイルシステムを共有できます。ラベル付きゾーンのファイルシステムを共有するには、ファイルシステムの ZFS 共有プロパティーを有効にします。

ラベル付きゾーンのステータスが `ready` または `running` の場合、そのゾーンのラベルでファイルシステムが共有されます。手順については、191 ページの「ラベル付きゾーンのファイルシステムを共有する」を参照してください。

Trusted Extensions での NFS マウントされたファイルシステムへのアクセス

NFS マウントされた低いレベルのディレクトリが高いレベルのゾーン内のユーザーに表示されるようにするには、次の準備が必要になります。

- サーバーの構成 – NFS サーバー上で、共有プロパティーを設定することで ZFS ファイルシステムをエクスポートします。手順については、191 ページの「ラベル付きゾーンのファイルシステムを共有する」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、193 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。

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、187 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。ただし、そのホームディレクトリは、ホームディレクトリサーバーの大域ゾーン内に作成されます。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 – 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、157 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を作成するには、75 ページの「各

NFS サーバーにログインすることでユーザーがすべてのラベルで遠隔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-level* 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
*    public-zone-IP-address:/export/home/&
```

txzonemgr スクリプトは、この PUBLIC エントリを大域ゾーンの auto_master ファイル内で設定します。

```
+auto_master
/net        -hosts        -nosuid,nobrowse
/home        auto_home    -nobrowse
/zone/public/home      auto_home_public      -nobrowse
```

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

Trusted Extensions ソフトウェアは、NFS Version 3 (NFSv3) と 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 Oracle Solaris 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、例 16–19を参照してください。

Trusted Extensions システムはそ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。ラベルなしシステムにエクスポートされたファイルシステムは、そのラベルが、エクスポート元のゾーンによってその遠隔システムに割り当てられたラベルと等しい場合に、書き込み可能となります。ラベルなしホストにエクスポートされるファイルシステムは、そのラベルよりも優位のラベルが遠隔システムに割り当て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相手側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。遠隔ファイルシステムの `mount` コマンドに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 ZFS データセットのマウント

ZFS で提供されるセキュリティーラベル属性 mlslabel には、データセット内のデータのラベルが含まれます。mlslabel プロパティーは継承可能です。明示的なラベルを持つ ZFS データセットは、Trusted Extensions が構成されていない Oracle Solaris システムではマウントできません。

mlslabel プロパティーが未定義の場合、そのデフォルト値は、ラベルなしを示す文字列 none になります。

ZFS データセットをラベル付きゾーンでマウントすると、次のことが起こります。

- データセットにラベルが付いていない、つまり mlslabel プロパティーが未定義の場合は、mlslabel プロパティーの値が、マウント先となるゾーンのラベルに変更されます。

  大域ゾーンの場合、mlslabel プロパティーは自動的には設定されません。admin_low というラベルが明示的に付けられたデータセットは、読み取り専用でマウントする必要があります。
- データセットにラベルが付いている場合、カーネルは、そのデータセットのラベルがマウント先となるゾーンのラベルと一致するか確認します。ラベルが一致しない場合には、ゾーンで下位読み取りマウントが許可されていないかぎり、マウントは失敗します。ゾーンで下位読み取りマウントが許可されている場合、低いレベルのファイルシステムは読み取り専用でマウントされます。

コマンド行から mlslabel プロパティーを設定するには、次のような内容を入力します。

```
# zfs set mlslabel=public export/publicinfo
```

初期ラベルを設定したり、デフォルト以外のラベルを高いレベルのラベルに変更したりする場合は、file_upgrade_sl 特権が必要となります。ラベルを削除する、つまりラベルを none に設定する場合は、file_downgrade_sl 特権が必要となります。この特権は、デフォルト以外のラベルを低いレベルのラベルに変更する場合にも必要となります。

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ファイルシステム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。	ユーザーのデータをアーカイブします。	190 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。	191 ページの「Trusted Extensions でファイルを復元する」
ラベル付きファイルシステムを共有します。	ほかのシステム上のユーザーがラベル付きファイルシステムにアクセスできるようにします。	191 ページの「ラベル付きゾーンのファイルシステムを共有する」
ラベル付きゾーンによって共有されているファイルシステムをマウントします。	ファイルシステムの内容を、同じラベルのラベル付きゾーンで読み取り/書き込み権付きで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。	193 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すべてのラベル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。	75 ページの「各 NFS サーバーにログインすることでユーザーがすべてのラベルで遠隔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。	低いレベルの情報を高いレベルで表示できないようにします。	178 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。	195 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

始める前に　Media Backup 権利プロファイルが割り当てられている必要があります。大域ゾーンにいます。

- 使用可能な方法については、『Oracle Solaris の管理: ZFS ファイルシステム』の「ZFS データを送信および受信する」を参照してください。

注意 – ラベルを保持できるのは次のコマンドだけです。

- 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

  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

始める前に　大域ゾーンで root 役割になっています。

- 使用可能な方法については、『Oracle Solaris の管理: ZFS ファイルシステム』の「ZFS データを送信および受信する」を参照してください。

注意 – ラベルを保持できるのは次のコマンドだけです。

- 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

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。

▼ ラベル付きゾーンのファイルシステムを共有する

ラベル付きゾーンで作成されたディレクトリをマウントまたは共有するには、そのファイルシステムに適切な ZFS 共有プロパティーを設定したあと、ゾーンを再起動してその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　ZFS File System Management 権利プロファイルが割り当てられている必要があります。

1. 共有しようとしているファイルシステムのラベルで、ワークスペースを作成します。

   詳細は、『Trusted Extensions ユーザーガイド』の「自分の最下位ラベルでワークスペースを追加する方法」を参照してください。

2. ゾーン内でファイルシステムを作成します。

```
# zfs create rpool/wdocs1
```

3 **ZFS 共有プロパティーを設定してファイルシステムを共有します。**

たとえば、次の一連のコマンドを実行すると、ライター向けの文書ファイルシステムが共有されます。このファイルシステムは、ライターがこのサーバー上のドキュメントを変更できるように、読み取り/書き込み権付きで共有されます。`setuid` プログラムは許可されません。

```
# zfs set share=name=wdocs1,path=/wdocs1,prot=nfs,setuid=off,
exec=off,devices=off rpool/wdocs1
# zfs set sharenfs=on rpool/wdocs1
```

コマンド行は、表示の都合上、折り返して記載されています。

4 **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ファイルシステムを共有できます。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、ゾーンをリブートします。

  ```
  # zoneadm -z zone-name reboot
  ```

5 **システムから共有されているファイルシステムを表示します。**

大域ゾーンの `root` 役割として次のコマンドを実行します。

```
# zfs get all rpool
```

詳細は、『Oracle Solaris の管理: ZFS ファイルシステム』の「ZFS ファイルシステムの情報のクエリー検索を行う」を参照してください

6 **共有されているファイルシステムをクライアントがマウントできるようにする方法は、193 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 14–1 PUBLIC ラベルで /export/share ファイルシステムを共有する

`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/reference` ファイルシステムにある文書を読めるようにします。

まず、管理者はワークスペースのラベルを public ワークスペースに変更し、端末ウィンドウを開きます。管理者はこのウィンドウ内で、選択された share プロパティーを /reference ファイルシステムに設定します。次のコマンドは、表示の都合上、折り返して記載されています。

```
# zfs set share=name=reference,path=/reference,prot=nfs,
setuid=off,exec=off,devices=off,rdonly=on rpool/wdocs1
```

次に、管理者はファイルシステムを共有します。

```
# zfs set sharenfs=on rpool/reference
```

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。ユーザーはこのファイルサーバー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システムを共有します。

```
# zoneadm -z public ready
```

共有されたファイルシステムがユーザーのシステムにマウントされると、ユーザーはそのファイルシステムにアクセスできるようになります。

▼ 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システムは、Trusted Extensions のラベル付きシステムにマウントできます。システムは、マウント先ゾーンのラベルでファイルサーバーへの経路を持っている必要があります。

- シングルラベルホストのファイルを読み取り/書き込み権付きでマウントするには、その遠隔ホストに割り当てられたラベルがマウント先ゾーンのラベルと一致する必要があります。2 つの遠隔ホスト構成が可能です。
  - マウント先のゾーンと同じラベルが遠隔ホストに割り当てられている。
  - 遠隔ホストがマルチレベルサーバーであり、マウント先ゾーンのラベルを含んでいる。
- 上位ゾーンによってマウントされるファイルシステム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、Oracle Solaris と同じマウントインタフェースが使用されます。

- デフォルトでは、ファイルシステムは起動時にマウントされます。
- ファイルシステム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。

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。マウントするファイルシステムが共有されていることを確認します。オートマウンタを使用する場合を除き、File System Management 権利プロファイルが割り当てられている必要があります。下位レベルのサーバーからマウントする場合、このクライアント上のゾーンを `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、『Trusted Extensions ユーザーガイド』の「自分の最下位ラベルでワークスペースを追加する方法」を参照してください。

- 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。

- ゾーンの起動時にファイルをマウントします。

- 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。

▼ 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システムのラベルでゾーン内にいる必要があります。root 役割である必要があります。

1. NFS サーバーのファイルシステムが共有されていることを確認します。
2. NFS サーバーのセキュリティー属性を確認します。
   a. **tninfo** または **tncfg** コマンドを使用して、その NFS サーバーの IP アドレスまたはそのサーバーを含む IP アドレス範囲を見つけます。
      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。
3. 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。
4. 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 15 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。

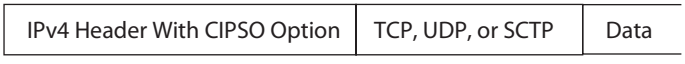
一般的にトラステッドネットワークでは、ラベルは送信側ホストによって生成され、受信側ホストによって処理されます。ただし、信頼されたルーターは、トラステッドネットワークでパケットを転送するときにラベルを追加したり取り除くことができます。機密ラベルは、転送の前に CIPSO ラベルにマップされます。CIPSO ラベルは IP パケットに埋め込まれます。通常、パケットの送信側と受信側は、同じラベルで操作を行います。

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。

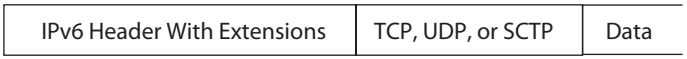
Trusted Extensions のデータパケット

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。



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、拡張されたヘッダー内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。



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。ネットワークの構成には、`txzonemgr` GUI と `tncfg` コマンドが使用されます。

Trusted Extensions ソフトウェアを実行しているシステムは、Trusted Extensions システムと次のタイプのホスト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、ほかのホスト
- 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ホスト (Oracle 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ホスト

Oracle 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、Oracle Solaris OS 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 はトラステッドネットワークの管理用として、コマンドを追加し、GUI を提供します。また、Trusted Extensions は Oracle Solaris OS 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、200 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。

  これらのインタフェースは、3 つの Trusted Extensions ネットワーク構成データベース `tnzonecfg`、`tnrhdb`、および `tnrhtp` を管理します。詳しくは、201 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 は、ネームサービススイッチ SMF サービス `svc:/system/name-service/switch` のプロパティーに、`tnrhtp` および `tnrhdb` データベースを追加します。
- パート I「Trusted Extensions の初期構成」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。追加の手順については、第 16 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 IKE 構成ファイル `/etc/inet/ike/config` を拡張します。詳細は、214 ページの「ラベル付き IPsec の管理」と、`ike.config(4)` のマニュアルページ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。

- `tncfg` – このコマンドは、Trusted Extensions ネットワークの構成を作成、変更、および表示します。`tncfg -t` コマンドは、指定されたセキュリティーテンプレートを表示、作成、または変更するために使用します。`tncfg -z` コマンドは、指定されたゾーンのネットワークプロパティーを表示または変更するために使用します。詳細は、`tncfg(1M)` のマニュアルページを参照してください。
- `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割り当て (`tnrhdb`)、またはゾーンの構成 (`tnzonecfg`) を `txzonemgr` または `tncfg` コマンドを使用して変更するたびに呼び出されます。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。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 ディレクトリおよびローカルファイルから `tnrhdb` および `tnrhtp` 情報を取得します。検索の順序は、`name-service/switch` SMF サービスによって決定されます。`tnd` デーモンはブート時に、`svc:/network/tnd` サービスによって起動されます。このサービスは `svc:/network/ldap/client` に依存します。

  LDAP ネットワークでは、`tnd` 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 Oracle Solaris ネットワークコマンドにオプションを追加します。

- `ipadm` – `all-zones` アドレスプロパティーは、指定されたインタフェースをシステム上のすべてのゾーンから使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。詳細は、`ipadm(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、Oracle 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 Oracle 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` – Oracle Solaris 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。
- `ipseckey` – Trusted Extensions では、IPsec で保護されたパケットにラベルを付けるために、次の拡張が使用可能となっています: `label` *label*、`outer-label` *label*、および `implicit-label` *label*。詳細については、`ipseckey(1M)` のマニュアルページ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。`tncfg` コマンドが、このデータベースへのアクセスや変更を行うためのインタフェースです。

  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)` 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、171 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。tncfg コマンドが、このデータベースへのアクセスや変更を行うためのインタフェースです。

  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、202 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。
- tnrhdb – このデータベースには、このシステムとの通信を許可されたすべてのホストに対応する IP アドレスや IP アドレス範囲が格納されます。tncfg コマンドが、このデータベースへのアクセスや変更を行うためのインタフェースです。

  各ホストまたは各 IP アドレス範囲には、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。

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、同じプロトコルと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、遠隔システム (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、これらを遠隔システムに割り当てます。遠隔システムにテンプレートが割り当てられていない場合、そのシステムとの通信は一切行えません。

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。204 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。

詳細は、203 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 システムのインストール時には、遠隔ホストのラベルプロパティーを定義するために使用されるセキュリティーテンプレートのデフォルトセットが追加されます。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、セキュリティー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。テンプレートが割り当てられていないホストは、Trusted Extensions が設定されたホストと通信できません。テンプレートはローカルに格納されます。

セキュリティーテンプレートにホストを追加する場合、IP アドレスを指定することも、IP アドレス範囲の一部として指定することもできます。詳細は、206 ページの「トラステッドネットワーク代替メカニズム」を参照してください。

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 システム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、ホストタイプ `unlabeled` に固有です。詳細は、204 ページの「セキュリティーテンプレートのデフォルトラベル」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。`unlabeled` 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。
- 補助ラベルセット – 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。補助ラベルセットが指定されたテンプレートに追加されたホストは、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。指定できる最大の補助ラベル数は 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、Oracle 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、そのセキュリティー属性は制限が少なすぎるため、通常のシステム操作には向かない可能性があります。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、Oracle 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。これらのホストを「シングルラベル」と呼ぶ技術上の理由は、これらのホストに `admin_high` ラベルと `admin_low` ラベルが含まれないことにあります。

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。

デフォルト値と異なる DOI 値をサイトで使用する場合には、55 ページの「解釈のドメインを構成する」の説明に従ってすべてのセキュリティーテンプレートでこの値を使用する必要があります。

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補助ラベル

補助ラベルセットは、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、補助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メカニズム

ホストの IP アドレスは、セキュリティーテンプレートに直接的に追加することも、間接的に追加することもできます。直接割り当てでは、ホストの IP アドレスを追加します。間接割り当てでは、ホストを含む IP アドレス範囲を追加します。ある特定のホストに一致させる場合、トラステッドネットワークソフトウェアはまず特定の IP アドレスを検索します。この検索でホストに固有のエントリが見つからない場合、「最長接頭辞一致」で検索が行われます。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。例については、表 15–1 を参照してください。

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メカニズムは使用されません。

表 15–1 Trusted Extensions ホストアドレスと代替メカニズムのエントリ

IP バージョン	host_type=cipso のホストエントリ	含まれる IP アドレス
IPv4	192.168.118.57	192.168.118.57
	192.168.118.57/32	/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	192.168.118.0 ～ 192.168.118.63
	192.168.118.0	192.168.118. サブネット上のすべてのアドレス。
	192.168.118.0/24	
	192.168.0.0/24	192.168.0. サブネット上のすべてのアドレス。
	192.168.0.0	192.168. サブネット上のすべてのアドレス。
	192.168.0.0/16	
	192.0.0.0	192. サブネット上のすべてのアドレス。
	192.0.0.0/8	
	192.168.118.0/32	ホストアドレス 192.168.118.0。アドレス範囲ではありません。
	192.168.0.0/32	ホストアドレス 192.168.0.0。アドレス範囲ではありません。
	192.0.0.0/32	ホストアドレス 192.0.0.0。アドレス範囲ではありません。
	0.0.0.0/32	ホストアドレス 0.0.0.0。アドレス範囲ではありません。
	0.0.0.0	全ネットワーク上の全アドレス。
IPv6	2001\:DB8\:22\:5000\:\:21f7	2001:DB8:22:5000::21f7
	2001\:DB8\:22\:5000\:\:0/52	2001:DB8:22:5000::0 ～ 2001:DB8:22:5fff:ffff:ffff:ffff:ffff
	0\:\:0/0	全ネットワーク上の全アドレス。

0.0.0.0/32 アドレスは、アドレス 0.0.0.0 に一致することに注意してください。0.0.0.0/32 エントリをシステムのラベルなしセキュリティーテンプレートに追加すると、特定のアドレス 0.0.0.0 を持つホストがシステムに接続できるようになります。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アプリケーションの tnrhdb エントリを作成するには、例 16–16 を参照してください。0.0.0.0:admin_low ネットワーク

が、admin_low ラベルなしホストテンプレートのデフォルトエントリです。このデフォルトを変更する必要が生じるセキュリティー上の問題については、233 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」を確認してください。

IPv4 および IPv6 アドレスの接頭辞長の詳細については、『Oracle Solaris の管理: IP サービス』の「ネットワークの IP アドレス指定形式の決定」および『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、Oracle 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。Trusted Extensions は Oracle Solaris と違って、動的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 Oracle 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 Oracle 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補助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ホスト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、セキュリティーテンプレート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、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。
- すべての宛先について、送信パケットのラベルが、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。
- 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、パケットはセキュリティーテンプレート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、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。
  - すべての宛先について、送信パケット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。
  - 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 システム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、パケットはセキュリティーテンプレート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。サイトのセキュリティーポリシーで要求されるレベルのセキュリティーを実現す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。この制限を実現するには、これらのサイトで、外部ネットワークに接続されているゲートウェイのネットワークインタフェースを、シングルラベルテンプレートに追加します。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。

- 『Oracle Solaris の管理: IP サービス』の「IPv4 ルーターの構成」
- 『Oracle Solaris の管理: IP サービス』の「ネットワーク上のコンポーネントシステムの構成」
- 『Oracle Solaris の管理: IP サービス』の「主な TCP/IP 管理タスク (タスクマップ)」
- `netcfg`(1M)

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経路指定テーブルが拡張されます。属性については、209 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。

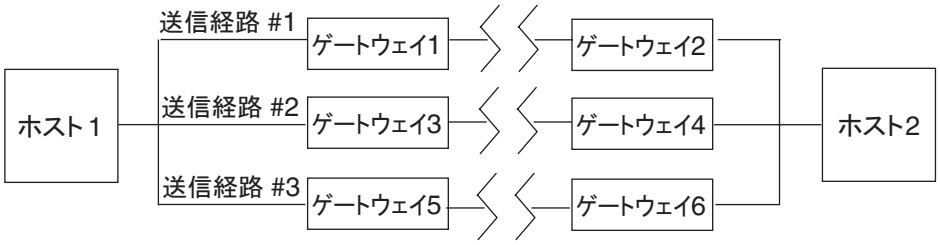
経路指定ソフトウェアは、経路指定テーブルで宛先ホストへの送信経路を探します。ホストが明示的に定義されていない場合、経路指定ソフトウェアは、ホストが配置されているサブネットのエントリを探します。ホストとサブネットのどちらも定義されていない場合、デフォルトゲートウェイが定義されていれば、ホストはデフォルトゲートウェイにパケットを送信します。複数のデフォルトゲートウェイを定義可能で、それぞれが同等に扱われます。

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」として静的に定義できます。

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 15–1 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、そのセキュリティー属性は、ゲートウェイ 5 のセキュリティーテンプレートから派生します。

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 Oracle 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。

Trusted Extensions には、経路指定テーブルエントリを変更するためのインタフェースとして、次のものが用意されています。

- txzonemgr GUI は、インタフェースにデフォルトの経路を割り当てる場合に使用できます。
- add または delete オプション付きの route -p コマンドは、経路指定テーブルエントリを変更する場合に使用できます。

例については、237 ページの「デフォルト経路を追加する」を参照してください。

ラベル付き IPsec の管理

Trusted Extensions システムは、ラベル付きネットワークパケットを IPsec で保護できます。IPsec パケットの送信時には、明示的または暗黙的な Trusted Extensions ラベルを付加できます。ラベルを明示的に送信する場合は CIPSO IP オプションを使用し、暗黙的に送信する場合はラベル付き IPsec セキュリティーアソシエーション (SA) を使用します。さらに、さまざまな暗黙的ラベルを持つ IPsec 暗号化パケットは、ラベルなしネットワーク上でトンネリングさせることができます。

IPsec の一般的な概念や構成手順については、『Oracle Solaris の管理: IP サービス』のパート III「IP セキュリティー」を参照してください。Trusted Extensions での IPsec 手順の変更点については、240 ページの「ラベル付き IPsec の構成 (作業マップ)」を参照してください。

IPsec で保護された交換のためのラベル

Trusted Extensions システムでのすべての通信は、IPsec で保護された通信も含め、セキュリティーラベルの認可検査に合格する必要があります。これらの検査については、209 ページの「Trusted Extensions の認可検査」で説明しています。

これらの検査をパスする必要のある、ラベル付きゾーン内のアプリケーションからの IPsec パケットのラベルは、内部ラベル、ワイヤーラベル、および鍵管理ラベルです。

- アプリケーションセキュリティーラベル – アプリケーションが存在しているゾーンのラベル。
- 内部ラベル – IPsec の AH または ESP ヘッダーが適用される前の暗号化されていないメッセージデータのラベル。`SO_MAC_EXEMPT` ソケットオプション (MAC-exempt) またはマルチレベルポート (MLP) 機能を使用する場合、このラベルはアプリケーションセキュリティーラベルと異なる可能性があります。ラベルによって制約されるセキュリティーアソシエーション (SA) と IKE 規則を選択した場合、IPsec と IKE でこの内部ラベルが使用されます。

  デフォルトでは、内部ラベルはアプリケーションセキュリティーラベルと同じになります。通常、両端のアプリケーションのラベルは同じになります。ただし、MAC-exempt または MLP 通信ではこの条件が成立しない可能性があります。IPsec 構成設定では、内部ラベルをネットワーク経由でどのようにして伝達するかを定義できます。つまり、この設定ではワイヤーラベルを定義できます。IPsec 構成設定では、内部ラベルの値は定義できません。
- ワイヤーラベル – IPsec の AH または ESP ヘッダーが適用されたあとの暗号化されたメッセージデータのラベル。IKE および IPsec 構成ファイルの内容によっては、ワイヤーラベルは内部ラベルと異なる可能性があります。

- 鍵管理ラベル – 2 つのノード間のすべての IKE ネゴシエーションは、ネゴシエーションを起動したアプリケーションメッセージのラベルにかかわらず、シングルラベルで制御されます。IKE ネゴシエーションのラベルは、`/etc/inet/ike/config` ファイル内で IKE 規則ごとに定義されます。

IPsec セキュリティーアソシエーション用のラベル拡張

IPsec のラベル拡張は、Trusted Extensions システム上で、セキュリティーアソシエーション (SA) の内側で伝送されるトラフィックにラベルを関連付けるために使用されます。デフォルトでは、IPsec ではラベル拡張が使用されないため、ラベルは無視されます。2 つのシステム間のトラフィックはすべて、Trusted Extensions のラベルにかかわらず、ある単一の SA 内を流れます。

ラベル拡張を使用すると次のことが行えます。

- 各 Trusted Extensions ラベルで使用するための IPsec SA を個別に構成する。この構成は事実上、2 つのマルチレベルシステム間を行き来するトラフィックのラベルを伝達するための追加メカニズムを提供します。
- 暗号化されていない形式のテキストとは異なる IPsec 暗号化メッセージのテキストのための、ワイヤー上のラベルを指定する。この構成は、安全性の低いネットワーク経由での暗号化された機密データの伝送をサポートします。
- IP パケット内での CIPSO IP オプションの使用を抑制する。この構成では、ラベル付きのトラフィックが、CIPSO を認識しないネットワークや CIPSO 非対応のネットワーク内を移動できます。

ラベル拡張を使用するかどうかの指定は、216 ページの「IKE 用のラベル拡張」での説明に従って IKE 経由で自動的に行うことも、`ipseckey` コマンドを使用して手動で行うこともできます。ラベル拡張機能の詳細については、`ipseckey(1M)` のマニュアルページを参照してください。

ラベル拡張を使用する場合、アウトバウンドトラフィックの SA 選択には、内部機密ラベルがその一致の一部として含まれます。インバウンドトラフィックのセキュリティーラベルは、受信パケットの SA のセキュリティーラベルによって定義されます。

IKE 用のラベル拡張

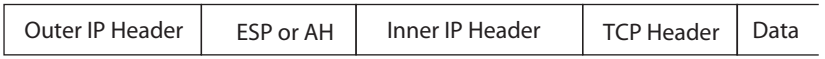
Trusted Extensions システムの IKE では、ラベルを認識するピアとの SA 用ラベルのネゴシエーションがサポートされています。このメカニズムを制御するには、`/etc/inet/ike/config` ファイル内で次のキーワードを使用します。

- **label_aware** – `in.iked` デーモンによる Trusted Extensions ラベルインタフェースの使用と、ピアとのラベルのネゴシエーションを可能にします。
- **single_label** – ピアが SA 用ラベルのネゴシエーションをサポートしないことを示します。
- **multi_label** – ピアが SA 用ラベルのネゴシエーションをサポートすることを示します。IKE は、2 つのノード間のトラフィック内で新しいラベルを検出するたびに、新しい SA を作成します。
- **wire_label inner** – ワイヤーラベルが内部ラベルと同じであるようなラベル付き SA を、`in.iked` デーモンに作成させます。デーモンが `cipso` ピアとネゴシエーションを行う場合の鍵管理ラベルは、`ADMIN_LOW` になります。デーモンがラベルなしピアとネゴシエーションを行う場合の鍵管理ラベルは、そのピアのデフォルトラベルになります。伝送パケットに CIPSO IP オプションを追加する際には、通常の Trusted Extensions 規則に従います。
- **wire_label** *label* – 内部ラベルの値にかかわらず、ワイヤーラベルが *label* に設定されたラベル付き SA を `in.iked` デーモンに作成させます。`in.iked` デーモンは、指定されたラベルで鍵管理のネゴシエーションを実行します。伝送パケットに CIPSO IP オプションを追加する際には、通常の Trusted Extensions 規則に従います。
- **wire_label none** *label* – `wire_label` *label* に似た動作になりますが、SA の下で伝送される IKE パケットやデータパケットで CIPSO IP オプションが抑制される点が異なります。

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

トンネルモード IPsec でのラベルと認可

アプリケーションのデータパケットがトンネルモードの IPsec によって保護される場合、パケットには複数の IP ヘッダーが含まれます。



IKE プロトコルの IP ヘッダーには、アプリケーションデータパケットの外部 IP ヘッダーと同じ発信元アドレスと宛先アドレスのペアが含まれます。

Outer IP Header	UDP Header	IKE Key Management Protocol

Trusted Extensions は、内部 IP ヘッダーのアドレスを使用して内部ラベルの認可検査を行います。Trusted Extensions は、外部 IP ヘッダーのアドレスを使用してワイヤーラベルと鍵管理ラベルの検査を実行します。認可検査については、209 ページの「Trusted Extensions の認可検査」を参照してください。

ラベル拡張による機密性保護と完全性保護

次の表では、ラベル拡張のさまざまな構成で、IPsec の機密性保護や完全性保護がセキュリティーラベルにどのように適用されるかについて説明します。

セキュリティーアソシエーション	機密性	完全性
ラベル拡張なし	ラベルは CIPSO IP オプション内で可視となります。	CIPSO IP オプション内のメッセージラベルは、ESP ではなく AH で保護されます。「注」を参照してください。
ラベル拡張あり	CIPSO IP オプションは可視ですが、ワイヤーラベルを表します。これは、内部メッセージラベルとは異なる可能性があります。	ラベルの完全性は、ラベル固有の SA の存在によって暗黙的に保護されます。 ワイヤー上の CIPSO IP オプションは AH で保護されます。「注」を参照してください。
ラベル拡張あり、CIPSO IP オプション抑制	メッセージラベルは可視ではありません。	ラベルの完全性は、ラベル固有の SA の存在によって暗黙的に保護されます。

注 – メッセージがネットワーク内を移動するときに、CIPSO を認識するルーターが CIPSO IP オプションを取り除いたり追加したりする可能性がある場合には、IPsec AH 完全性保護を使用して CIPSO IP オプションを保護することはできません。CIPSO IP オプションが少しでも変更されるとそのメッセージは無効となり、AH で保護されたパケットが宛先でドロップされることになります。

◆ ◆ ◆ 第 16 章

Trusted Extensions でのネットワークの管理 (手順)

この章では、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。

トラステッドネットワークの管理 (作業マップ)

一般的な Trusted Extensions 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
ホストやネットワークにラベルを割り当てます。	遠隔ホストテンプレートを作成し、ホストをセキュリティーテンプレートに割り当てます。	220 ページの「ホストおよびネットワークへのラベル付け (作業マップ)」
デフォルトルーターを割り当て、マルチレベルポート (MLP) を構成します。	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。 ラベル付きゾーンや大域ゾーンにプライベート MLP と共有 MLP を追加します。	237 ページの「経路およびマルチレベルポートの構成 (手順)」
IPsec を有効にしてラベル付きパケットを保護します。	ラベル付きパケットを IPsec で保護します。	240 ページの「ラベル付き IPsec の構成 (作業マップ)」

作業	説明	参照先
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。	245 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)」

ホストおよびネットワークへのラベル付け (作業マップ)

Trusted Extensions システムは、そのシステム上でほかのホストのセキュリティー属性が定義されたあとではじめて、それらのホストに接続できるようになります。遠隔ホストのセキュリティー属性は互いに似ている可能性があるため、Trusted Extensions には、ホストの追加先として使用可能なセキュリティーテンプレートが用意されています。

次の作業マップでは、セキュリティーテンプレートを追加したり、それらを遠隔ホストに適用したりする場合に使用可能なタスクについて説明します。

作業	説明	参照先
セキュリティーテンプレートを表示します。	使用可能なセキュリティーテンプレートを表示します。	222 ページの「セキュリティーテンプレートを表示する」
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。	223 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」
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。	227 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」

作業	説明	参照先
セキュリティーテンプレートを作成します。	トラステッドネットワークのセキュリティー属性を定義するセキュリティーテンプレートを作成します。	223 ページの「セキュリティーテンプレートを作成する」
	このセキュリティーテンプレートは、DOI を 1 以外の値に変更します。	55 ページの「解釈のドメインを構成する」
	このセキュリティーテンプレートは、特定のラベルを遠隔ホストに割り当てます。	例 16–1
	シングルラベルゲートウェイとして動作する遠隔ホスト用のセキュリティーテンプレートです。	例 16–2
	狭いラベル範囲内にトラフィックを制限する遠隔ホスト用のセキュリティーテンプレートです。	例 16–3
	別個のラベルを持つ遠隔ホスト用のセキュリティーテンプレートです。	例 16–4
	ラベルなし遠隔ホストおよびネットワーク用のセキュリティーテンプレートです。	例 16–5
	ネットワークの残りの部分から切り離されたラベルを持つ 2 つの遠隔ホスト用のセキュリティーテンプレートです。	例 16–6
セキュリティーテンプレートにホストを追加します。	セキュリティーテンプレートに IP アドレスを追加します。	228 ページの「セキュリティーテンプレートにホストを追加する」 例 16–7 例 16–8 例 16–9 例 16–10
セキュリティーテンプレートに連続する IP アドレスを追加します。	セキュリティーテンプレートに IP アドレスの範囲を追加します。	231 ページの「セキュリティーテンプレートにホストの範囲を追加する」 例 16–12 例 16–13
セキュリティーテンプレートからホストを削除します。	ホストのセキュリティー定義を削除します。	例 16–11

作業	説明	参照先
admin_low ラベルで通信可能なホストを指定します。	セキュリティーを高めるため、システムがブート時に接続できるホストを指定します。	233 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」
	セキュリティーを高めるため、システムがブート時に接続できるラベル付きホストのネットワークを指定します。	例 16–14
ホストアドレス 0.0.0.0/32 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アプリケーションサーバーを構成します。	例 16–16

▼ セキュリティーテンプレートを表示する

セキュリティーテンプレートの一覧と各テンプレートの内容を表示できます。この手順で示す例は、デフォルトのセキュリティーテンプレートです。

1 使用可能なセキュリティーテンプレートを一覧表示します。

```
# tncfg list
   cipso
   admin_low
```

2 一覧表示されたテンプレートの内容を表示します。

```
# tncfg -t cipso info
   name=cipso
   host_type=cipso
   doi=1
   min_label=ADMIN_LOW
   max_label=ADMIN_HIGH
   host=127.0.0.1/32
```

この cipso セキュリティーテンプレートの 127.0.0.1/32 エントリにより、このシステムがラベル付きとして識別されます。ピアが host_type cipso の遠隔ホストテンプレートにこのシステムを割り当てた場合、その 2 つのシステムはラベル付きパケットを交換できます。

```
# tncfg -t admin_low info
   name=admin_low
   host_type=unlabeled
   doi=1
   def_label=ADMIN_LOW
   min_label=ADMIN_LOW
   max_label=ADMIN_HIGH
   host=0.0.0.0/0
```

この admin_low セキュリティーテンプレートの 0.0.0.0/0 エントリは、セキュリティーテンプレートに明示的に割り当てられていないすべてのホストがこのシステムに接続できるようにします。これらのホストはラベルなしとして認識されます。

- このエントリの利点は、サーバーやゲートウェイなど、ブート時にこのシステムで必要となるすべてのホストを検出できることです。
- このエントリの欠点は、このシステムのネットワーク上の任意のホストがこのシステムに接続できることです。このシステムに接続できるホストを制限するには、233 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。

▼ 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** のセキュリティーテンプレートを十分に理解します。
   使用可能なセキュリティーテンプレートを表示するには、222 ページの「セキュリティーテンプレートを表示する」の手順に従います。
2. 通信相手となるホストに対して次のいずれかを行う必要がある場合は、新しいセキュリティー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。
   - ADMIN_LOW 以外のラベルのシングルラベルホストを作成します。
   - 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。
   - 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。

次の手順　デフォルトのセキュリティーテンプレートにホストを追加する場合は、228 ページの「セキュリティーテンプレートにホストを追加する」に進みます。

それ以外の場合は、223 ページの「セキュリティーテンプレートを作成する」に進みます。

▼ セキュリティーテンプレートを作成する

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、セキュリティー値を修正できます。セキュリティー管理者役割には、これらの権利プロファイルが含まれています。

1 (省略可能) **ADMIN_HIGH** と **ADMIN_LOW** 以外の任意のラベルの 16 進バージョンを確認します。

PUBLIC などのラベルでは、ラベル文字列、0x0002-08-08 などの 16 進値のどちらも、ラベル値として使用できます。tncfg コマンドはどちらの形式も受け入れます。

```
# atohexlabel "confidential : internal use only"
0x0004-08-48
```

詳細は、132 ページの「ラベルの 16 進値を求める」を参照してください。

2 デフォルトのセキュリティーテンプレートは変更しません。

サポートの目的上、デフォルトのセキュリティーテンプレートは削除しないでください。これらのテンプレートは、コピーして変更できます。そして、これらのテンプレートに割り当てられたホストを削除したりホストを追加したりできます。例については、233 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 セキュリティーテンプレートを作成します。

tncfg -t コマンドには、新しいテンプレートを作成するための方法が 3 つ用意されています。

- セキュリティーテンプレートを新規に作成します。

  tncfg コマンドを対話モードで使用します。info サブコマンドは、デフォルトで提供された値を表示します。Tab キーを使用すると、部分的なプロパティーや値が補完されます。

  ```
  # tncfg -t newunlabeled
  tncfg:newtemplate> info
     name=newunlabeled
     host_type=unlabeled
     doi=1
     def_label=ADMIN_LOW
     min_label=ADMIN_LOW
     max_label=ADMIN_HIGH
  tncfg:newunlabeled> set m<Tab>
  set max_label=" set min_label="
  tncfg:newunlabeled> set ma<Tab>
  tncfg:newunlabeled> set max_label=ADMIN_LOW
  ...
  ```

  セキュリティーテンプレートの完全な属性リストをコマンド行で指定することもできます。複数の set サブコマンドはセミコロンで区切ります。省略されたプロパティーではデフォルト値が使用されます。

  ```
  # tncfg -t newunlabeled set host_type=unlabeled;set doi=1; \
  set min_label=ADMIN_LOW;set max_label=ADMIN_LOW
  ```

- 既存のセキュリティーテンプレートをコピーして変更します。

  ```
  # tncfg -t cipso
  tncfg:cipso> set name=newcipso
  tncfg:newcipso> info
  ```

```
name=newcipso
host_type=cipso
doi=1
min_label=ADMIN_LOW
max_label=ADMIN_HIGH
```

既存のセキュリティーテンプレートに割り当てられているホストは、新しいテンプレートにコピーされません。

- **export** サブコマンドによって作成されたテンプレートファイルを使用します。

```
# tncfg -f unlab_1 -f template-file
tncfg: unlab1> set host_type=unlabeled
...
# tncfg -f template-file
```

インポート用のソーステンプレートの作成例については、tncfg(1M) のマニュアルページを参照してください。

例 16–1 1 つのラベルでパケットを処理するゲートウェイ用の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はラベル 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定義します。

```
# tncfg -t cipso_public
tncfg:cipso_public> set host_type=cipso
tncfg:cipso_public> set doi=1
tncfg:cipso_public> set min_label="public"
tncfg:cipso_public> set max_label="public"
tncfg:cipso_public> commit
tncfg:cipso_public> exit
```

次に、セキュリティー管理者はセキュリティーテンプレートにゲートウェイホストを追加します。追加方法については、例 16–7 を参照してください。

例 16–2 ラベル付きパケットの経路指定を行う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。

セキュリティー管理者はテンプレートを新規に作成します。

```
# tncfg -t unl_public
tncfg:unl_public> set host_type=unlabeled
tncfg:unl_public> set doi=1
```

```
tncfg:unl_public> set def_label="PUBLIC"
tncfg:unl_public> set min_label=ADMIN_LOW
tncfg:unl_public> set max_label=ADMIN_HIGH
tncfg:unl_public> exit
```

次に、セキュリティー管理者はセキュリティーテンプレートにルーターを追加します。追加方法については、例 16–8 を参照してください。

例 16–3 制限されたラベル範囲を持つゲートウェイ用の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は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。管理者はセキュリティーテンプレートを作成し、そのセキュリティーテンプレートにあとでゲートウェイホストを割り当てます。

```
# tncfg -t cipso_iuo_rstrct
tncfg:cipso_iuo_rstrct> set host_type=cipso
tncfg:cipso_iuo_rstrct> set doi=1
tncfg:cipso_iuo_rstrct> set min_label=0x0004-08-48
tncfg:cipso_iuo_rstrct> set max_label=0x0004-08-78
tncfg:cipso_iuo_rstrct> add host=192.168.131.78
tncfg:cipso_iuo_rstrct> exit
```

次に、セキュリティー管理者はセキュリティーテンプレートにゲートウェイホストを追加します。追加方法については、例 16–9 を参照してください。

例 16–4 不連続な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は `confidential : internal use only` と `confidential : restricted` の 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。その他のトラフィックはすべて拒否されます。

まず、管理者は注意しながらラベルを正確に入力します。ソフトウェアは、ラベルで大文字と小文字のどちらが使用されていても、また短縮名が使用されていてもラベルを認識しますが、空白が不正確なラベルは認識しません。たとえば、ラベル `confidential :restricted` は有効なラベルではありません。

```
# tncfg -t cipso_int_and_rst
tncfg:cipso_int_and_rst> set host_type=cipso
tncfg:cipso_int_and_rst> set doi=1
tncfg:cipso_int_and_rst> set min_label="cnf : internal use only"
tncfg:cipso_int_and_rst> set max_label="cnf : internal use only"
tncfg:cipso_int_and_rst> set aux_label="cnf : restricted"
tncfg:cipso_int_and_rst> exit
```

例 16–5 ラベル PUBLIC でのラベルなし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は `PUBLIC` ラベルのパケットのみを送受信できるホスト用のシングルラベルテンプレートを作成します。このテンプレート

は、Trusted Extensions システムが PUBLIC ラベルでマウントする必要のあるファイルシステムを含むホストに割り当てることができます。

```
# tncfg -t public
tncfg:public> set host_type=unlabeled
tncfg:public> set doi=1
tncfg:public> set def_label="public"
tncfg:public> set min_sl="public"
tncfg:public> set max_sl="public"
tncfg:public> exit
```

次に、セキュリティー管理者はセキュリティーテンプレートにホストを追加します。追加方法については、例 16–13 を参照してください。

例 16–6 開発者用のラベル付き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は cipso_sandbox テンプレートを作成します。このセキュリティーテンプレートは、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。開発者のテストがほかのラベル付きホストに影響を与え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。

```
# tncfg -t cipso_sandbox
tncfg:cipso_sandbox> set host_type=cipso
tncfg:cipso_sandbox> set doi=1
tncfg:cipso_sandbox> set min_sl="SBX"
tncfg:cipso_sandbox> set max_sl="SBX"
tncfg:cipso_sandbox> exit
```

▼ システムの既知のネットワークにホストを追加する

ホストやホストのグループをシステムの /etc/hosts ファイルに追加すると、それらのホストはシステムに認識されます。セキュリティーテンプレートに追加できるのは、既知のホストだけです。

始める前に 大域ゾーンで root 役割になっています。

1 個々のホストを **/etc/hosts** ファイルに追加します。

```
# vi /etc/hosts

...
192.168.111.121   ahost
```

2 ホストのグループを **/etc/hosts** ファイルに追加します。

```
# vi /etc/hosts

...
192.168.111.0   111-network
```

次の手順 228 ページの「セキュリティーテンプレートにホストを追加する」に進みます。

▼ セキュリティーテンプレートにホストを追加する

始める前に 次のことが必要になります。

- セキュリティーテンプレートが存在している必要があります。手順については、223 ページの「セキュリティーテンプレートを作成する」を参照してください。
- IP アドレスが `/etc/hosts` ファイル内に存在しているか、DNS で解決可能である必要があります。

  `hosts` ファイルについては、227 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。

  DNS については、『Oracle Solaris Administration: Naming and Directory Services』の第 3 章「Managing DNS (Tasks)」を参照してください。
- ラベルのエンドポイントが一致する必要があります。規則については、208 ページの「Trusted Extensions の経路指定の概要」を参照してください。
- 大域ゾーンでセキュリティー管理者役割になります。

1 ホスト名または **IP** アドレスをセキュリティーテンプレートに追加します。

たとえば、IP アドレス `192.168.1.2` を追加します。

```
# tncfg -t cipso
tncfg:cipso> add host=192.168.1.2
```

別のテンプレートに以前追加されたホストを追加した場合、そのセキュリティーテンプレート割り当てが置換されるという旨の通知が表示されます。例:

```
# tncfg -t cipso
tncfg:cipso> add host=192.168.1.22
192.168.1.2 previously matched the admin_low template
tncfg:cipso> info
...
host=192.168.1.2/32
tncfg:cipso> exit
```

2 変更後のセキュリティーテンプレートを表示します。

たとえば、`cipso` テンプレートに追加されたアドレス `192.168.1.2` を次に示します。

```
tncfg:cipso> info
...
   host=192.168.1.2/32
```

接頭辞長 /32 は、このアドレスが厳密なアドレスであることを示しています。

3 変更をコミットしてセキュリティーテンプレートを終了します。

```
tncfg:cipso> commit
tncfg:cipso> exit
```

ホストのエントリを削除する場合は、例 16–11 を参照してください。

例 16–7 1 つのラベルでパケットを処理するゲートウェイの作成

例 16–1 では管理者が、ラベル PUBLIC のパケットのみを通過させることのできるゲートウェイを定義したセキュリティーテンプレートを作成します。この例では、セキュリティー管理者はゲートウェイホストの IP アドレスが解決可能であることを確認します。

```
# arp 192.168.131.75
gateway-1.example.com (192.168.131.75) at 0:0:0:1:ab:cd
```

arp コマンドは、このホストがシステムの /etc/hosts ファイルに定義されているか、あるいは DNS で解決可能であることを検査します。

次に、管理者は gateway-1 ホストをセキュリティーテンプレートに追加します。

```
# tncfg -t cipso_public
tncfg:cipso_public> add host=192.168.131.75
tncfg:cipso_public> exit
```

システムはすぐに、gateway-1 経由で public パケットの送受信を行えます。

例 16–8 ラベル付きパケットの経路指定を行うラベルなしルーターの作成

例 16–2 では、管理者がルーター用のセキュリティーテンプレートを作成します。この例では、管理者はルーターの IP アドレスが解決可能であることを確認します。

```
# arp 192.168.131.82
router-1.example.com (192.168.131.82) at 0:0:0:2:ab:cd
```

arp コマンドは、このホストがシステムの /etc/hosts ファイルに定義されているか、あるいは DNS で解決可能であることを示します。

次に、管理者はルーターをセキュリティーテンプレートに追加します。

```
# tncfg -t unl_public
tncfg:unl_public> add host=192.168.131.82
tncfg:unl_public> exit
```

システムはすぐに、router-1 経由ですべてのラベルのパケットの送受信を行えます。

例 16–9 制限されたラベル範囲を持つゲートウェイの作成

例 16–3 では、管理者は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を作成します。この例では、セキュリティー管理者はゲートウェイホストの IP アドレスが解決可能であることを確認します。

```
# arp 192.168.131.78
gateway-ir.example.com (192.168.131.78) at 0:0:0:3:ab:cd
```

arp コマンドは、このホストがシステムの /etc/hosts ファイルに定義されているか、あるいは DNS で解決可能であることを示します。

次に、管理者はゲートウェイをセキュリティーテンプレートに追加します。

```
# tncfg -t cipso_iuo_rstrct
tncfg:cipso_iuo_rstrct> add host=192.168.131.78
tncfg:cipso_iuo_rstrct> exit
```

システムはすぐに、ラベル internal または restricted の付いたパケットの送受信を gateway-ir 経由で行えます。

例 16–10 開発者用のラベル付きホストの作成

例 16–6 では、管理者は cipso_sandbox セキュリティーテンプレートを作成します。この例では、セキュリティー管理者は 2 つのホストをテンプレートに追加します。

```
# tncfg -t cipso_sandbox
tncfg:cipso_sandbox> add host=196.168.129.102
tncfg:cipso_sandbox> add host=196.168.129.129
tncfg:cipso_sandbox> exit
```

196.168.129.102 システムと 196.168.129.129 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。

例 16–11 セキュリティーテンプレートからのいくつかのホストの削除

この例では、セキュリティー管理者は cipso セキュリティーテンプレートからいくつかのホストを削除します。管理者は、info サブコマンドを使用してホストを表示したあと、remove と入力し、4 つの host= エントリをコピー&ペーストします。

```
# tncfg -t cipso info
   name=cipso
   host_type=cipso
   doi=1
   min_label=ADMIN_LOW
   max_label=ADMIN_HIGH
   host=127.0.0.1/32
   host=192.168.1.2/32
```

```
   host=192.168.113.0/24
   host=192.168.113.100/25
   host=2001:a08:3903:200::0/56

# tncfg -t cipso
tncfg:cipso> remove host=192.168.1.2/32
tncfg:cipso> remove host=192.168.113.0/24
tncfg:cipso> remove host=192.168.113.100/25
tncfg:cipso> remove host=2001:a08:3903:200::0/56
tncfg:cipso> info
...
   max_label=ADMIN_HIGH
   host=127.0.0.1/32
   host=192.168.75.0/24
```

管理者は、ホストを削除したあとで変更をコミットし、セキュリティーテンプレートを終了します。

```
tncfg:cipso> commit
tncfg:cipso> exit
#
```

▼ セキュリティーテンプレートにホストの範囲を追加する

始める前に　要件については、228 ページの「セキュリティーテンプレートにホストを追加する」を参照してください

1. サブネットにセキュリティーテンプレートを割り当てるには、そのサブネットアドレスをテンプレートに追加します。

   たとえば、2 つのサブネットを cipso テンプレートに追加したあと、このセキュリティーテンプレートを表示します。

```
# tncfg -t cipso
tncfg:cipso> add host=192.168.75.0
tncfg:cipso> add host=192.168.113.0
tncfg:cipso> info
...
host=192.168.75.0/24
host=192.168.113.0/24
tncfg:cipso> exit
```

   接頭辞長 /24 は、.0 で終わるこのアドレスがサブネットであることを示しています。

注 – 別のテンプレートに以前追加されたホスト範囲を追加する場合、そのセキュリティーテンプレート割り当てが置換されるという旨の通知が表示されます。

```
# tncfg -t cipso
tncfg:cipso> add host=192.168.113.100/25
192.168.113.100/25 previously matched the admin_low template
```

2 連続する IP アドレスの範囲にセキュリティーテンプレートを割り当てるには、その IP アドレスと接頭辞長を指定します。

次の例の接頭辞長は、192.168.113.0 から 192.168.113.127 までのアドレス範囲をカバーしています。このアドレスには、192.168.113.100 が含まれます。

```
# tncfg -t cipso
tncfg:cipso> add host=192.168.113.100/25
tncfg:cipso> exit
```

次の例の接頭辞長は、2001:a08:3903:200::0 から 2001:a08:3903:2ff:ffff:ffff:ffff:ffff までの連続する IPv6 アドレスをカバーしています。このアドレスには、2001:a08:3903:201:20e:cff:fe08:58c が含まれます。

```
# tncfg -t cipso
tncfg:cipso> add host=2001:a08:3903:200::0/56
tncfg:cipso> info
...
host=2001:a08:3903:200::0/56
tncfg:cipso> exit
```

エントリを間違って入力した場合は、次のようなメッセージが表示されます。

```
# tncfg -t cipso
tncfg:cipso> add host=2001:a08:3903::0/56
Invalid host: 2001:a08:3903::0/56
```

別のテンプレートに以前追加されたホストを追加した場合、そのセキュリティーテンプレート割り当てが置換されるという旨の通知が表示されます。例:

```
# tncfg -t cipso
tncfg:cipso> add host=192.168.113.100/32
192.168.113.100/32 previously matched the admin_low template
tncfg:cipso> info
...
host=192.168.113.100/32
tncfg:cipso> exit
```

206 ページの「トラステッドネットワーク代替メカニズム」で説明したように、以前の割り当てがこの明示的な割り当てで上書きされることが、Trusted Extensions の代替メカニズムによって保証されます。

例 16–12 不連続なラベルのホストの作成

例 16–4 では、管理者は 2 つのラベルを認識するセキュリティーテンプレートを作成します。この例では、セキュリティー管理者は各ホストの IP アドレスが解決可能であることを確認します。

```
# arp 192.168.132.21
host-auxset1.example.com (192.168.132.21) at 0:0:0:4:ab:cd
```

```
# arp 192.168.132.22
host-auxset2.example.com (192.168.132.22) at 0:0:0:5:ab:cd
# arp 192.168.132.23
host-auxset3.example.com (192.168.132.23) at 0:0:0:6:ab:cd
# arp 192.168.132.24
host-auxset4.example.com (192.168.132.24) at 0:0:0:7:ab:cd
```

arp コマンドは、このホストがシステムの /etc/hosts ファイルに定義されているか、あるいは DNS で解決可能であることを示します。

次に、管理者は接頭辞長を使用して、IP アドレスの範囲をセキュリティーテンプレートに割り当てます。

```
# tncfg -t cipso_int_rstrct
tncfg:cipso_int_rstrct> set host=192.168.132.0/24
```

例 16–13 ラベル PUBLIC でのラベルなしサブネットワークの作成

例 16–5 では、管理者はシングルラベルの PUBLIC ホストを定義するセキュリティーテンプレートを作成します。この例で、セキュリティー管理者はあるサブネットワークを PUBLIC ラベルに割り当てます。トラステッドシステム上のユーザーは、このサブネットワーク内のファイルシステムをラベル PUBLIC でマウントできます。

```
# tncfg -t public
tncfg:public> add host=10.10.0.0/16
tncfg:public> exit
```

このサブネットワークにはラベル PUBLIC ですぐに到達できます。

▼ 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と、admin_low デフォルトセキュリティーテンプレート内にネットワーク上のすべてのホストが定義されています。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トラステッドネットワーク値は、ブート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遠隔ホスト (0.0.0.0/0) 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 0.0.0.0/0 ワイルドカードエントリを削除できます。このエントリは、ブート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、0.0.0.0/0 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、およびルーターをテンプレートに明示的に追加する必要があります。

アプリケーションが最初にクライアントをホストアドレス 0.0.0.0/32 で認識する場合は、0.0.0.0/32 ホストエントリを admin_low テンプレートに追加する必要があります。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。

ブート時に接続されるすべてのホストは、/etc/hosts ファイル内に存在している必要があります。

1 **ブート時に接続する必要のあるすべてのラベルなしホストに、admin_low テンプレートを割り当てます。**

- ブート時に接続する必要のあるすべてのラベルなしホストを含めます。
- このシステム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。
- 0.0.0.0/0 の割り当てを削除します。

2 **cipso テンプレートにホストを追加します。**

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。

- このシステムが通信時に経由する必要のある、Trusted Extensions を実行している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。
- ブート時に接続する必要のあるラベル付きホストの範囲を含めます。

サンプルデータベースについては、例 16–15 を参照してください。

3 **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 16–14 IP アドレス 0.0.0.0/0 のラベルの変更

この例では、管理者は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 0.0.0.0/0 ホストエントリを削除し、ラベルなし public テンプレートに 0.0.0.0/0 ホストエントリを追加します。システムは、別のセキュリティーテンプレートに明示的に割り当てられていないすべてのホストを、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。

```
# tncfg -t admin_low info
tncfg:admin_low> remove host=0.0.0.0      Wildcard address
tncfg:admin_low> exit

# tncfg -t public
tncfg:public> set host_type=unlabeled
tncfg:public> set doi=1
tncfg:public> set def_label="public"
tncfg:public> set min_sl="public"
tncfg:public> set max_sl="public"
tncfg:public> add host=0.0.0.0     Wildcard address
tncfg:public> exit
```

例 16–15 ブート時に接続するコンピュータの列挙

この例では、管理者は 2 つのネットワークインタフェースを備えた Trusted Extensions システムのトラステッドネットワークを構成します。システムは、ほかのネットワークおよびルーターと通信します。遠隔ホストは、3 つのテンプレート cipso、admin_low、public のいずれかに割り当てられます。次のコマンドには注釈を付けています。

```
# tncfg -t cipso
tncfg:admin_low> add host=127.0.0.1     Loopback address
tncfg:admin_low> add host=192.168.112.111      Interface 1 of this host
tncfg:admin_low> add host=192.168.113.111      Interface 2 of this host
tncfg:admin_low> add host=192.168.113.6     File server
tncfg:admin_low> add host=192.168.112.255      Subnet broadcast address
tncfg:admin_low> add host=192.168.113.255      Subnet broadcast address
tncfg:admin_low> add host=192.168.113.1     Router
tncfg:admin_low> add host=192.168.117.0/24      Another Trusted Extensions network
tncfg:admin_low> exit

# tncfg -t public
tncfg:public> add host=192.168.112.12      Specific network router
tncfg:public> add host=192.168.113.12      Specific network router
tncfg:public> add host=224.0.0.2      Multicast address
tncfg:admin_low> exit
```

```
# tncfg -t admin_low
tncfg:admin_low> add host=255.255.255.255      Broadcast address
tncfg:admin_low> exit
```

管理者は、ブート時に接続するホストを指定し終わると、admin_low テンプレートから 0.0.0.0/0 エントリを削除します。

```
# tncfg -t admin_low
tncfg:admin_low> remove host=0.0.0.0
tncfg:admin_low> exit
```

例 16–16 ホストアドレス 0.0.0.0/32 を有効な初期アドレスにする

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アプリケーションサーバーを構成します。

管理者は、サーバーのトラステッドネットワークを構成します。サーバーとクライアントのエントリには注釈を付けています。

```
# tncfg -t cipso info
   name=cipso
   host_type=cipso
   doi=1
   min_label=ADMIN_LOW
   max_label=ADMIN_HIGH
   host=127.0.0.1/32
   host=192.168.128.1/32       Application server address
   host=192.168.128.0/24       Application's client network
     Other addresses to be contacted at boot time
```

```
# tncfg -t admin_low info
   name=cipso
   host_type=cipso
   doi=1
   def_label=ADMIN_LOW
   min_label=ADMIN_LOW
   max_label=ADMIN_HIGH
   host=192.168.128.0/24       Application's client network
   host=0.0.0.0/0       Wildcard address
     Other addresses to be contacted at boot time
```

テストがこの段階まで成功すると、管理者は構成をロックダウンするために、デフォルトのワイルドカードアドレス 0.0.0.0/0 を削除して変更をコミットしたあと、特定のアドレスを追加します。

```
# tncfg -t admin_low info
tncfg:admin_low> remove host=0.0.0.0
tncfg:admin_low> commit
tncfg:admin_low> add host=0.0.0.0/32      For initial client contact
tncfg:admin_low> exit
```

admin_low の最終的な構成は、次のようになります。

```
# tncfg -t admin_low
   name=cipso
   host_type=cipso
   doi=1
   def_label=ADMIN_LOW
   min_label=ADMIN_LOW
   max_label=ADMIN_HIGH
   192.168.128.0/24       Application's client network
   host=0.0.0.0/32        For initial client contact
     Other addresses to be contacted at boot time
```

`0.0.0.0/32` エントリは、アプリケーションのクライアントのみがアプリケーションサーバーに到達できるようにします。

経路およびマルチレベルポートの構成 (手順)

静的送信経路を使用すると、ラベル付きパケットがラベル付きまたはラベルなしゲートウェイ経由で宛先に到達できます。MLP は、アプリケーションが 1 つのエントリポイントを使用してすべてのゾーンに到達できるようにします。

▼ デフォルト経路を追加する

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。

宛先の各ホスト、ネットワーク、ゲートウェイのセキュリティーテンプレートへの追加が完了しています。詳細は、228 ページの「セキュリティーテンプレートにホストを追加する」 and 231 ページの「セキュリティーテンプレートにホストの範囲を追加する」を参照してください。

1. **txzonemgr GUI を使用してデフォルト経路を作成します。**

   ```
   # txzonemgr &
   ```

2. デフォルト経路を設定するゾーンをダブルクリックしたあと、その **IP** アドレスエントリをダブルクリックします。

   ゾーンに複数の IP アドレスがある場合は、目的のインタフェースを含むエントリを選択します。

3. プロンプトでルーターの **IP** アドレスを入力し、「了解」をクリックします。

注 – デフォルトルーターを削除または変更するには、エントリを削除し、IP エントリを作成し直してルーターを追加します。ゾーンに IP アドレスが 1つしかない場合、エントリを削除するには IP インスタンスを削除する必要があります。

例 16–17 route コマンドを使用した大域ゾーンのデフォルト経路の設定

この例では、管理者は route コマンドを使用して大域ゾーンのデフォルト経路を作成します。

```
# route add default 192.168.113.1 -static
```

▼ ゾーンにマルチレベルポートを作成する

ラベル付きゾーンや大域ゾーンにプライベート MLP と共有 MLP を追加できます。

この手順は、あるラベル付きゾーンで実行されているアプリケーションが、そのゾーンと通信するためにマルチレベルポート (MLP) を必要とする場合に使用します。この手順では、Web プロキシがゾーンと通信します。

始める前に 大域ゾーンで root 役割になっている必要があります。システムに少なくとも 2 つの IP アドレスが存在していなければならず、ラベル付きゾーンが停止されています。

1. プロキシホストと **Web** サービスホストを **/etc/hosts** ファイルに追加します。

```
## /etc/hosts file
...
proxy-host-name  IP-address
web-service-host-name IP-address
```

2. ゾーンを構成します。

   たとえば、PUBLIC というラベルが明示的に付けられたパケットを認識するように、public ゾーンを構成します。この構成では、セキュリティーテンプレートの名前は webprox です。

```
# tncfg -t webprox
tncfg:public> set name=webprox
tncfg:public> set host_type=cipso
tncfg:public> set min_label=public
tncfg:public> set max_label=public
tncfg:public> add host=mywebproxy.oracle.com      host name associated with public zone
tncfg:public> add host=10.1.2.3/16      IP address of public zone
tncfg:public> exit
```

3. **MLP** を構成します。

   たとえば、Web プロキシサービスは 8080/tcp インタフェース経由で PUBLIC ゾーンと通信を行うとします。

```
# tncfg -z public add mlp_shared=8080/tcp
# tncfg -z public add mlp_private=8080/tcp
```

4. **MLP** をカーネルに追加するには、ゾーンをブートします。

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

5 大域ゾーンで、新しいアドレスの経路を追加します。
経路を追加するには、237 ページの「デフォルト経路を追加する」を実行します。

例 16–18 txzonemgr GUI を使用した MLP の構成

管理者は、Web プロキシサービスを構成するために Labeled Zone Manager を開きます。

```
# txzonemgr &
```

管理者は、PUBLIC ゾーンをダブルクリックしたあと、「Configure Multilevel Ports」をダブルクリックします。次に、管理者は「Private interfaces」行を選択してダブルクリックします。選択領域が次のような入力フィールドに変わります。

```
Private interfaces:111/tcp;111/udp
```

管理者は、セミコロン区切り文字を使用して Web プロキシの入力を開始します。

```
Private interfaces:111/tcp;111/udp;8080/tcp
```

プライベートの入力が完了したら、管理者は「Shared interfaces」フィールドに Web プロキシを入力します。

```
Shared interfaces:111/tcp;111/udp;8080/tcp
```

public ゾーンのマルチレベルポートは次回のゾーンブート時に有効になることを示すポップアップメッセージが表示されます。

例 16–19 udp 経由 NFSv3 用のプライベートマルチレベルポートの構成

この例では、管理者は udp 経由の NFSv3 下位読み取りマウントを有効にします。管理者は tncfg コマンドを使用できます。

```
# tncfg -z global add mlp_private=2049/udp
```

また、txzonemgr GUI を使用して MLP を定義することもできます。

Labeled Zone Manager で、管理者は global ゾーンをダブルクリックしたあと、「Configure Multilevel Ports」をダブルクリックします。MLP のメニューで、管理者は「Private interfaces」行を選択してダブルクリックし、ポート/プロトコルを追加します。

```
Private interfaces:111/tcp;111/udp;8080/tcp
```

global ゾーンのマルチレベルポートは次回ブート時に有効になることを示すポップアップメッセージが表示されます。

例 16–20 システム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
```

ラベル付き IPsec の構成 (作業マップ)

この作業マップでは、IPsec 保護にラベルを追加するために使用されるタスクについて説明します。

作業	説明	参照先
IPsec を Trusted Extensions とともに使用します。	IPsec 保護にラベルを追加します。	241 ページの「マルチレベル Trusted Extensions ネットワークで IPsec 保護を適用する」
信頼できないネットワーク上で、IPsec を Trusted Extensions とともに使用します。	信頼できないネットワーク上でラベル付き IPsec パケットをトンネリングします。	243 ページの「信頼できないネットワーク上でトンネルを構成する」

▼ マルチレベル Trusted Extensions ネットワークで IPsec 保護を適用する

この手順では、次の条件に対応できるように、2 つの Trusted Extensions システムで IPsec を構成します。

- 2 つのシステム enigma と partym は、マルチレベルネットワーク内で動作しているマルチレベル Trusted Extensions システムです。
- アプリケーションデータは暗号化され、ネットワーク内での承認されていない変更から保護されます。
- データのセキュリティーラベルは、enigma システムと partym システム間のパス上にあるマルチレベルルーターやセキュリティーデバイスで使用される CIPSO IP オプションの形で可視となります。
- enigma と partym の間で交換されるセキュリティーラベルは、承認されていない変更から保護されます。

始める前に　大域ゾーンで root 役割になっています。

1. **enigma** ホストと **partym** ホストを **CIPSO** セキュリティーテンプレートに追加します。
   220 ページの「ホストおよびネットワークへのラベル付け (作業マップ)」の手順に従います。CIPSO ホストタイプのテンプレートを使用します。

2. **enigma** システムと **partym** システムで **IPsec** を構成します。
   手順については、『Oracle Solaris の管理: IP サービス』の「IPsec で 2 つのシステム間のトラフィックを保護するには」を参照してください。鍵管理については、次の手順で説明するように IKE を使用します。

3. **IKE** ネゴシエーションにラベルを追加します。
   『Oracle Solaris の管理: IP サービス』の「事前共有鍵により IKE を構成する方法」の手順に従ったあと、ike/config ファイルを次のように変更します。

   a. **enigma** システムの **/etc/inet/ike/config** ファイルにキーワード **label_aware**、**multi_label**、および **wire_label inner** を追加します。
      結果となるファイルは次のようになります。ラベルの追加箇所が強調表示されています。

```
    ### ike/config file on enigma, 192.168.116.16
    ## Global parameters
    #
## Use IKE to exchange security labels.
    label_aware
  #
        ## Defaults that individual rules can override.
    p1_xform
```

```
        { auth_method preshared oakley_group 5 auth_alg sha encr_alg 3des }
    p2_pfs 2
    #
## The rule to communicate with partym
    # Label must be unique
    { label "enigma-partym"
        local_addr 192.168.116.16
        remote_addr 192.168.13.213
        multi_label
        wire_label inner
        p1_xform
         { auth_method preshared oakley_group 5 auth_alg sha1 encr_alg aes }
        p2_pfs 5
    }
```

b. **partym** システムの **ike/config** ファイルにも同じキーワードを追加します。

```
    ### ike/config file on partym, 192.168.13.213
    ## Global Parameters
    #
## Use IKE to exchange security labels.
    label_aware
    #
        p1_xform
          { auth_method preshared oakley_group 5 auth_alg sha encr_alg 3des }
    p2_pfs 2
    ## The rule to communicate with enigma
    # Label must be unique
    { label "partym-enigma"
        local_addr 192.168.13.213
        remote_addr 192.168.116.16
        multi_label
        wire_label inner
    p1_xform
           { auth_method preshared oakley_group 5 auth_alg sha1 encr_alg aes }
        p2_pfs 5
    }
```

4 **CIPSO IP** オプションの **AH** 保護がネットワーク上で使用できない場合は、**ESP** 認証を使用します。

認証を処理する方法として、`/etc/inet/ipsecinit.conf` ファイルで `auth_algs` の代わりに `encr_auth_algs` を使用します。ESP 認証は、IP ヘッダーや IP オプションを保護しませんが、ESP ヘッダーのあとの情報をすべて認証します。

```
{laddr enigma raddr partym} ipsec {encr_algs any encr_auth_algs any sa shared}
```

注 – 証明書で保護されたシステムにラベルを追加することもできます。Trusted Extensions システムでは、公開鍵証明書は大域ゾーンで管理されます。『Oracle Solaris の管理: IP サービス』の「公開鍵証明書による IKE の構成」の手順を実行したあと、`ike/config` ファイルを同じように変更します。

▼ 信頼できないネットワーク上でトンネルを構成する

この手順では、公開ネットワーク上で 2 つの Trusted Extensions VPN ゲートウェイシステムの間で IPsec トンネルを構成します。この手順で使用する例は、『Oracle Solaris の管理: IP サービス』の「IPsec で VPN を保護するタスクのためのネットワークトポロジの説明」の図に示された構成に基づいています。

この図に次の変更を行ったものと仮定します。

- `10` サブネットは、マルチレベルトラステッドネットワークです。CIPSO IP オプションのセキュリティーラベルは、これらの LAN 上で可視となります。
- `192.168` サブネットは、`PUBLIC` ラベルで動作するシングルラベルの信頼できないネットワークです。これらのネットワークは CIPSO IP オプションをサポートしません。
- `euro-vpn` と `calif-vpn` との間のラベル付きトラフィックは、承認されていない変更から保護されます。

始める前に　大域ゾーンで `root` 役割になっています。

1. 220 ページの「ホストおよびネットワークへのラベル付け (作業マップ)」の手順に従って次の定義を行います。

   a. **`10.0.0.0/8` IP アドレスをラベル付きセキュリティーテンプレートに追加します。**
   CIPSO ホストタイプのテンプレートを使用します。デフォルトのラベル範囲、`ADMIN_LOW` から `ADMIN_HIGH` を維持します。

   b. **`192.168.0.0/16` IP アドレスをラベルなしセキュリティーテンプレートにラベル `PUBLIC` で追加します。**
   ラベルなしホストタイプのテンプレートを使用します。デフォルトラベルを `PUBLIC` に設定します。デフォルトのラベル範囲、`ADMIN_LOW` から `ADMIN_HIGH` を維持します。

   c. **`Calif-vpn` と `Euro-vpn` のインターネット側アドレス `192.168.13.213` と `192.168.116.16` を、CIPSO テンプレートに追加します。**
   デフォルトのラベル範囲を維持します。

2. **IPsec トンネルを作成します。**
   『Oracle Solaris の管理: IP サービス』の「トンネルモードの IPsec で VPN を保護する方法」の手順に従います。鍵管理については、次の手順で説明するように IKE を使用します。

3 **IKE** ネゴシエーションにラベルを追加します。

『Oracle Solaris の管理: IP サービス』の「事前共有鍵により IKE を構成する方法」の手順に従ったあと、`ike/config` ファイルを次のように変更します。

a. **euro-vpn** システムの **/etc/inet/ike/config** ファイルにキーワード **label_aware**、**multi_label**、および **wire_label none PUBLIC** を追加します。

結果となるファイルは次のようになります。ラベルの追加箇所が強調表示されています。

```
        ### ike/config file on euro-vpn, 192.168.116.16
    ## Global parameters
    #
## Use IKE to exchange security labels.
    label_aware
    #
        ## Defaults that individual rules can override.
    p1_xform
          { auth_method preshared oakley_group 5 auth_alg sha encr_alg 3des }
    p2_pfs 2
    #
   ## The rule to communicate with calif-vpn
       # Label must be unique
    { label "eurovpn-califvpn"
          local_addr 192.168.116.16
          remote_addr 192.168.13.213
          multi_label
          wire_label none PUBLIC
          p1_xform
           { auth_method preshared oakley_group 5 auth_alg sha1 encr_alg aes }
          p2_pfs 5
        }
```

b. **calif-vpn** システムの **ike/config** ファイルにも同じキーワードを追加します。

```
    ### ike/config file on calif-vpn, 192.168.13.213
    ## Global Parameters
    #
## Use IKE to exchange security labels.
    label_aware
    #
        p1_xform
          { auth_method preshared oakley_group 5 auth_alg sha encr_alg 3des }
    p2_pfs 2
    ## The rule to communicate with euro-vpn
    # Label must be unique
    { label "califvpn-eurovpn"
          local_addr 192.168.13.213
          remote_addr 192.168.116.16
          multi_label
          wire_label none PUBLIC
    p1_xform
           { auth_method preshared oakley_group 5 auth_alg sha1 encr_alg aes }
        p2_pfs 5
    }
```

注 – 証明書で保護されたシステムにラベルを追加することもできます。『Oracle Solaris の管理: IP サービス』の「公開鍵証明書による IKE の構成」の手順を実行したあと、`ike/config` ファイルを同じように変更します。

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、Trusted Extensions ネットワークのデバッグを支援するタスクについて説明します。

作業	説明	参照先
システムと遠隔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。	245 ページの「システムのインタフェースが稼働していることを確認する」
	システムと遠隔ホストが互いに通信できない場合はデバッグツールを使用します。	246 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。	249 ページの「LDAP サーバーへのクライアントの接続をデバッグする」

▼ システム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　ネットワーク属性値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、これらの値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。

システムのインタフェースを表示するには、Labeled Zone Manager GUI または `ipadm` コマンドを使用します。

- **Labeled Zone Manager** を開いたあと、目的のゾーンをダブルクリックします。

```
# txzonemgr &
```

「ネットワークインタフェースの構成」を選択し、ゾーンの「Status」列の値が「Up」になっていることを確認します。

- あるいは、**ipadm show-addr** コマンドを使用します。

```
# ipadm show-addr
...
ADDROBJ           TYPE      STATE        ADDR
lo0/v4            static    ok           127.0.0.1/8
net0/_a           dhcp      down         10.131.132.133/23
net0:0/_a         dhcp      down         10.131.132.175/23
```

net0 インタフェースの値が ok になっているはずです。ipadm コマンドの詳細については、ipadm(1M) のマニュアルページを参照してください。

2 インタフェースが稼働していない場合は、稼働状態にします。

a. **Labeled Zone Manager GUI** で、停止しているインタフェースを含むゾーンをダブルクリックします。

b. 「ネットワークインタフェースの構成」を選択します。

c. 状態が「**Down**」になっているインタフェースをダブルクリックします。

d. 「稼働状態にする」を選択してから「了解」をクリックします。

e. 「取消し」または「了解」をクリックします。

▼ 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 Oracle 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 Oracle 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、付録 D 「Trusted Extensions マニュアルページのリスト」を参照してください。

- ラベル付きゾーンを接続するときの問題については、174 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、195 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。

始める前に　ネットワーク属性値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、これらの値をチェックできます。ファイルを編集できるのは、root 役割だけです。

1 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. 各システム上で、**name-service/switch SMF** サービスの **Trusted Extensions** データベースの値を確認します。

```
# svccfg -s name-service/switch listprop config
config/value_authorization  astring  solaris.smf.value.name-service.switch
config/default              astring  ldap
...
config/tnrhtp               astring  "files ldap"
config/tnrhdb               astring  "files ldap"
```

b. ホスト間で値が異なっている場合は、問題のホスト上で値を修正します。

```
# svccfg -s name-service/switch setprop config/tnrhtp="files ldap"
# svccfg -s name-service/switch setprop config/tnrhdb="files ldap"
```

c. 次に、それらのホスト上でネームサービスデーモンを再起動します。

```
# svcadm restart name-service/switch
```

2 各ホストが正しく定義されていることを確認するため、伝送にかかわる発信元ホスト、宛先ホスト、およびゲートウェイホストのセキュリティー属性を表示します。

コマンド行を使用してネットワーク情報が正しいことを確認します。各ホストの割り当てがネットワーク上のほかのホストの割り当てと一致していることを確認します。必要な表示形式に応じて `tncfg` コマンド、`tninfo` コマンド、`txzonemgr` GUI のいずれかを使用します。

- テンプレート定義を表示します。

  `tninfo -t` コマンドは、ラベルを文字列形式と 16 進形式で表示します。

```
$ 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
```

- テンプレートと、そのテンプレートに割り当てられたホストを表示します。

  `tncfg -t` コマンドは、ラベルを文字列形式で表示し、割り当てられているホストを一覧表示します。

```
$ tncfg -t template info
   name=<template-name>
   host_type=<one of cipso or unlabeled>
   doi=1
   min_label=<minimum-label>
   max_label=<maximum-label>
   host=127.0.0.1/32            /** Localhost **/
   host=192.168.1.2/32          /** LDAP server **/
   host=192.168.1.22/32         /** Gateway to LDAP server **/
```

```
host=192.168.113.0/24          /** Additional network **/
host=192.168.113.100/25          /** Additional network **/
host=2001:a08:3903:200::0/56     /** Additional network **/
```

- ある特定のホストの **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` コマンドは、指定されたホストの IP アドレスと、そのホストに割り当てられたセキュリティーテンプレートの名前を表示します。

  ```
  $ tninfo -h hostname
  IP Address: IP-address
  Template: template-name
  ```

  `tncfg get host=` コマンドは、指定されたホストを定義するセキュリティーテンプレートの名前を表示します。

  ```
  $ tncfg get host=hostname|IP-address[/prefix]
  template-name
  ```

- ゾーンのマルチレベルポート **(MLP)** を表示します。

  `tncfg -z` コマンドは、MLP を 1 行に 1 つずつ一覧表示します。

  ```
  $ tncfg -z zone-name info [mlp_private | mlp_shared]
  mlp_private=<port/protocol-that-is-specific-to-this-zone-only>
  mlp_shared=<port/protocol-that-the-zone-shares-with-other-zones>
  ```

  `tninfo -m` コマンドは、1 行目にプライベート MLP を、2 行目に共有 MLP をそれぞれ表示します。各 MLP はセミコロンで区切られます。

  ```
  $ tninfo -m zone-name
  private: ports-that-are-specific-to-this-zone-only
  shared: ports-that-the-zone-shares-with-other-zones
  ```

  MLP を GUI で表示するには、`txzonemgr` コマンドを使用します。ゾーンをダブルクリックしたあと、「マルチレベルポートを構成」を選択します。

3 正しくない情報があれば修正します。

a. ネットワークのセキュリティー情報を変更または確認するには、トラステッドネットワークの管理コマンド **tncfg** と **txzonemgr** を使用します。データベースの構文を検査するには、**tnchkdb** コマンドを使用します。

たとえば次の出力は、テンプレート名 `internal_cipso` が未定義であることを示しています。

```
# tnchkdb
     checking /etc/security/tsol/tnrhtp ...
     checking /etc/security/tsol/tnrhdb ...
tnchkdb: unknown template name: internal_cipso at line 49
tnchkdb: unknown template name: internal_cipso at line 50
tnchkdb: unknown template name: internal_cipso at line 51
     checking /etc/security/tsol/tnzonecfg ...
```

このエラーから、internal_cipso セキュリティーテンプレートの作成や割り当てを行うときに、tncfg コマンドや txzonemgr コマンドが使用されなかったことがわかります。

修復するには、tnrhdb ファイルを元のファイルで置き換えたあと、tncfg コマンドを使用してセキュリティーテンプレートの作成や割り当てを行います。

b. カーネルキャッシュをクリアーするには、リブートします。

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。SMF サービス name-service/switch によって、カーネルへのデータ設定時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が決まります。

4 デバッグに役立つ伝送情報を収集します。

a. 経路指定構成を確認します。

```
$ 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。

b. パケットのラベル情報を表示します。

```
$ snoop -v
```

-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できます。詳細は、snoop(1M) のマニュアルページを参照してください。

c. 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 -aR
```

-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。

```
$ netstat -rR
```

-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の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。

a. **tncfg** または **tninfo** コマンドを使用して情報を表示します。

```
# tncfg get host=LDAP-server
# tncfg get host=gateway-to-LDAP-server

# tninfo -h LDAP-server
# tninfo -h gateway-to-LDAP-server
```

b. サーバーへの経路を確認します。

```
# route get LDAP-server
```

間違ったテンプレート割り当てが見つかった場合は、ホストを正しいテンプレートに追加します。

2 **/etc/hosts** ファイルを確認し、必要であれば修正します。

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可能性があります。

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` ファイルから `LServer-zones` を削除します。

3 **DNS** を使用している場合は、**svc:/network/dns/client** サービスの構成を確認します。

```
# svccfg -s dns/client listprop config
config                          application
config/value_authorization      astring       solaris.smf.value.name-service.dns.switch
config/nameserver               astring       192.168.8.25 192.168.122.7
```

4 値を変更するには、**svccfg** コマンドを使用します。

```
# svccfg -s dns/client setprop config/search = astring: example1.domain.com
# svccfg -s dns/client setprop config/nameserver = net_address: 192.168.8.35
# svccfg -s dns/client:default refresh
# svccfg -s dns/client:default validate
# svcadm enable dns/client
# svcadm refresh name-service/switch
# nslookup some-system
Server:         192.168.135.35
Address:        192.168.135.35#53

Name:   some-system.example1.domain.com
Address: 10.138.8.22
```

```
Name:    some-system.example1.domain.com
Address: 10.138.8.23
```

5 **name-service/switch** サービスの **tnrhdb** エントリと **tnrhtp** エントリが正確であることを確認します。

次の出力では、tnrhdb および tnrhtp エントリが表示されていません。したがって、これらのデータベースではデフォルトの files ldap ネームサービスがこの順番で使用されます。

```
# svccfg -s name-service/switch listprop config
config                          application
config/value_authorization      astring       solaris.smf.value.name-service.switch
config/default                  astring       "files ldap"
config/host                     astring       "files dns"
config/netgroup                 astring       ldap
```

6 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
```

7 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
```

8 現在実行中のすべてのゾーンから **LDAP** サーバーに接続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
...
```

9 **LDAP** を構成してリブートします。

a. 手順については、94 ページの「**Trusted Extensions** で大域ゾーンを **LDAP** クライアントにする」を参照してください。

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、リブートします。

```
# zoneadm list
zone1
zone2
,
,
,
# zoneadm -z zone1 halt
# zoneadm -z zone2 halt
.
.
.
# reboot
```

代わりに txzonemgr GUI を使用してラベル付きゾーンを停止してもかまいません。

◆ ◆ ◆ 第 17 章

Trusted Extensions と LDAP (概要)

この章では、Trusted Extensions が設定されたシステムでの Oracle Directory Server Enterprise Edition (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。`svc:/system/name-service/switch` サービスによって、どのネームサービスが使用されるかが決まります。LDAP は、Trusted Extensions で推奨されるネームサービスです。

ディレクトリサーバーは、Trusted Extensions および Oracle Solaris クライアントに LDAP ネームサービスを提供できます。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がシステム構成時にマルチレベルポートを指定します。

Trusted Extensions は、ディレクトリサーバーに 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。

- Oracle Solaris での LDAP ネームサービスの使用方法については、『Oracle Solaris Administration: Naming and Directory Services』を参照してください。
- Trusted Extensions に対するディレクトリサーバーの設定については、第 5 章「Trusted Extensions のための LDAP の構成 (手順)」を参照してください。Trusted Extensions システムを Oracle Solaris ディレクトリサーバーのクライアントにするには、Trusted Extensions で構成されたディレクトリサーバープロキシを使用します。

- Trusted Extensions ディレクトリサーバーのクライアントの設定方法については、94 ページの「Trusted Extensions LDAP クライアントの作成」を参照してください。

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

ローカルで管理される 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、システム、ネットワークの構成情報がすべてのシステム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 つのシステムで行なった変更は、すべてのシステムで行う必要があります。

ローカルで管理されている Trusted Extensions システムでは、構成情報は `/etc`、`/etc/security`、および `/etc/security/tsol` ディレクトリ内のファイルに格納されます。

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 Oracle Solaris 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 構成の問題を解決する方針については、『Oracle Solaris Administration: Naming and Directory Services』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、249 ページの「LDAP サーバーへのクライアントの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、『Oracle Solaris Administration: Naming and Directory Services』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
```

- Oracle Directory Server Enterprise Edition ソフトウェアのバージョン 6 または 7 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
```

- Oracle Directory Server Enterprise Edition ソフトウェアの 6 または 7 でプロキシ 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。

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

◆ ◆ ◆ 第 18 章

Trusted Extensions でのマルチレベルメール (概要)

この章では、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できます。詳細については、148 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 ではシステム管理者役割が、『Oracle Solaris のシステム管理 (ネットワークサービス)』の第 13 章「メールサービス (手順)」の手順に従ってメールサーバーの設定や管理を行います。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かぎり、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 に追加できます。これらのファイルについては、updatehome(1) 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、143 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、Thunderbird 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 Thunderbird 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。

- 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。この検査については、このリストと209 ページの「Trusted Extensions の認可検査」で説明しています。
  - 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 19 章

19 ラベル付き印刷の管理 (手順)

この章では、Trusted Extensions 印刷出力でラベルを印刷する方法について説明します。

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。

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 Oracle 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。デフォルトでは単一レベル印刷が構成されます。マルチレベル印刷は、大域ゾーンでのみ実装されます。大域ゾーンの印刷サーバーを使用するには、ラベル付きゾーンを IP インスタンス、VNIC のいずれかとして構成する必要があります。このアドレスは、大域ゾーンの IP アドレスとは別である必要があります。

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、Oracle Solaris 印刷サーバーに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 Oracle 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 Oracle 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ラベルを印刷します。この情報は、`label_encodings` ファイルから取得されます。

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できます。

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、Oracle Solaris 印刷からの機能に依存します。Oracle Solaris OS では、`job-sheets` オプションによってバナーページの作成が処理されます。ラベル付けを実施するため、印刷ジョブが PostScript ファイルに変換されます。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。

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。詳細は、『Oracle Solaris の管理: 一般的なタスク』の第 15 章「CUPS を使用したプリンタの設定と管理 (手順)」を参照してください。

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
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。	262 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」
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。	261 ページの「ゾーンをシングルレベル印刷サーバーとして構成する」
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。	264 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。	266 ページの「プリンタに制限付きのラベル範囲を構成する」

▼ ゾーンをシングルレベル印刷サーバーとして構成する

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、『Trusted Extensions ユーザーガイド』の「自分の最下位ラベルでワークスペースを追加する方法」を参照してください。
2. 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、『Trusted Extensions ユーザーガイド』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. 接続されているすべてのプリンタの特性を定義します。
   a. ゾーンのラベルで **CUPS** 印刷サーバーの構成ファイル **/etc/cups/cupsd.conf** を編集します。

4 印刷サーバーに接続されている各プリンタに適切なジョブシートを割り当てます。

たとえば次のように指定すると、適切なラベル付きシートが作成されます。

```
#CUPS-BANNER for INTERNAL print jobs
Show job-id job-name job-originating-user-name job-originating-host-name job-billing
Header CONFIDENTIAL : INTERNAL USE ONLY
Footer CONFIDENTIAL : INTERNAL USE ONLY
Image images/cups.png
```

次のコマンドを使用します。

```
$ lpadmin -p printer -o job-sheets-default=labeled,labeled
```

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。

5 プリンタをテストします。

注 – セキュリティー上の理由により、管理ラベルつまり ADMIN_HIGH、ADMIN_LOW のいずれかが付いたファイルでは、印刷時の本文ページに ADMIN_HIGH が印刷されます。label_encodings ファイル内のもっとも高い値のラベルとコンパートメントが、バナーページとトレーラページにラベル付けされます。

---

root として、および一般ユーザーとして、次の手順を実行します。

a. コマンド行からプレーンファイルを印刷します。

b. **Oracle Beehive**、ブラウザ、エディタなどのアプリケーションからファイルを印刷します。

c. ラベルが正しく印刷されることを確認します。

参照
- ラベル付き出力を禁止する – 267 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 – 264 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」

▼ 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. 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。

```
# tncfg -z global add mlp_shared=515/tcp
# tncfg -z global add mlp_private=515/tcp
```

2. 接続されているすべてのプリンタの特性を定義します。

```
# lpadmin -p printer-name -v /dev/null \
-o protocol=tcp -o dest=printer-IP-address:9100 -T PS -I postscript
# accept printer-name
# enable printer-name
```

3. 印刷サーバーに接続されている各プリンタを、ラベル付きジョブシートで構成します。

```
$ lpadmin -p printer -o job-sheets-default=labeled,labeled
```

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。

4. 印刷を可能にするすべての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。

   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-zone
```

   b. 各ラベル付きゾーンで **/etc/cups/client.conf** ファイルを作成します。

このファイルは、印刷サービスのために大域ゾーンの cupsd デーモンに接続します。このファイルを変更し、印刷サーバーの名前と IP アドレスを含めます。構成ファイルについては、client.conf(5) のマニュアルページを参照してください。

   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
```

5. 各ラベル付きゾーンで、プリンタをテストします。

root として、および一般ユーザーとして、次の手順を実行します。

   a. コマンド行からプレーンファイルを印刷します。

   b. **Oracle Beehive**、ブラウザ、エディタなどのアプリケーションからファイルを印刷します。

   c. ラベルが正しく印刷されることを確認します。

参照
- プリンタラベル範囲を制限する – 266 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 – 267 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 – 264 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」

▼ 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。

- 261 ページの「ゾーンをシングルレベル印刷サーバーとして構成する」
- 262 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」
- 268 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になっている必要があります。

1. 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。

   - 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、『Trusted Extensions ユーザーガイド』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、『Trusted Extensions ユーザーガイド』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
     ```

2 プリンタをテストします。

注 – セキュリティー上の理由により、管理ラベルつまり ADMIN_HIGH、ADMIN_LOW のいずれかが付いたファイルでは、印刷時の本文ページに ADMIN_HIGH が印刷されます。label_encodings ファイル内のもっとも高い値のラベルとコンパートメントが、バナーページとトレーラページにラベル付けされます。

大域ゾーンの root と役割、およびラベル付きゾーンの root、役割、および一般ユーザーに対して印刷が正しく機能することを、すべてのクライアント上でテストします。

a. コマンド行からプレーンファイルを印刷します。

b. **Oracle Beehive**、ブラウザ、エディタなどのアプリケーションからファイルを印刷します。

c. ラベルが正しく印刷されることを確認します。

▼ 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。
2. 「管理」ボタンをクリックして「デバイス管理」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、113 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。

タスク	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。	267 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 Oracle 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。	268 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。	269 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。	270 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。	269 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」
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。	270 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。	152 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」 146 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 **Oracle 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

Oracle 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。

- 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、228 ページの「セキュリティーテンプレートにホストを追加する」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 Oracle 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 19–1 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、Oracle 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 16–5 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。
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、152 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　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、152 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。

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。

  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。

  `solaris.print.ps` 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、152 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 19–2 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 20 章

Trusted Extensions のデバイス (概要)

この章では、Trusted Extensions で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

Oracle 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 機能が設定されたシステムは、Oracle 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、デバイスマネージャーを使用する必要があります。

Oracle Solaris でのデバイス保護については、『Oracle Solaris の管理: セキュリティーサービス』の第 5 章「デバイスアクセスの制御 (タスク)」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 Oracle Solaris 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、『Oracle Solaris の管理: セキュリティーサービス』の「デバイスポリシーの構成 (タスクマップ)」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。Oracle Solaris 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、『Oracle Solaris の管理: セキュリティーサービス』の「デバイスクリーンスクリプト」を参照してください。

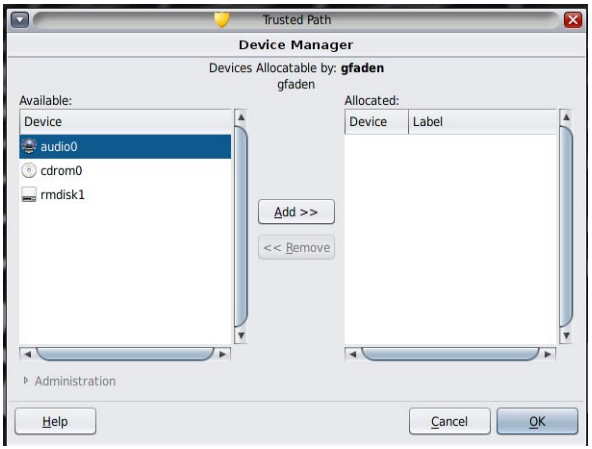
Trusted Extensions ソフトウェアの場合、デバイスクリーンスクリプトは一定の要件を満たさなくてはなりません。この要件については、`device_clean(5)` のマニュアルページを参照してください。

デバイスマネージャー GUI

デバイスマネージャーは、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。

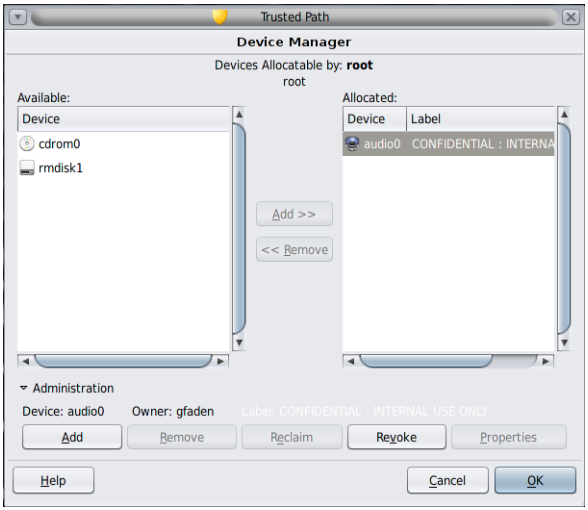
この GUI はデバイスマネージャーと呼ばれます。この GUI は、トラステッドパスメニューから「デバイスの割り当て」を選択することによって起動します。次の図は、`audio` デバイスを割り当てることのできるユーザーがデバイスマネージャーを開いたところです。

図 20–1　ユーザーが開いたデバイスマネージャー



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。



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、Oracle Solaris インタフェースと Trusted Extensions インタフェースを使用します。

Oracle Solaris のコマンド行インタフェースについては、『Oracle Solaris の管理: セキュリティーサービス』の「デバイスの保護 (参照)」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、『Oracle Solaris の管理: セキュリティーサービス』の「デバイスの強制的な割り当て」と『Oracle Solaris の管理: セキュリティーサービス』の「デバイスの強制的な割り当て解除」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 21 章

Trusted Extensions でのデバイス管理 (手順)

この章では、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)

周辺デバイス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。	280 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。	280 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。	288 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、役割もデバイスマネージャーを使う必要があります。Oracle Solaris の `allocate` コマンドは、Trusted Extensions では機能しません。次の作業マップでは、Trusted Extensions でデバイスを使用するためのユーザー手順へのリンクを示します。

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。	『Trusted Extensions ユーザーガイド』の「Trusted Extensions でデバイスを割り当てる」
ポータブルメディアを使用してファイルを転送します。	80 ページの「Trusted Extensions でポータブルメディアからファイルをコピーする」 79 ページの「Trusted Extensions でファイルをポータブルメディアにコピーする」

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。	『Oracle Solaris の管理: セキュリティーサービス』の「デバイスポリシーの構成 (タスクマップ)」
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」承認のある権利プロファイルをユーザーに割り当てます。	『Oracle Solaris の管理: セキュリティーサービス』の「ユーザーによるデバイス割り当てを承認する方法」
	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。	288 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。	281 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。	285 ページの「Trusted Extensions でデバイスを解除または再利用する」
	Oracle 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。	『Oracle Solaris の管理: セキュリティーサービス』の「デバイスの強制的な割り当て」 『Oracle Solaris の管理: セキュリティーサービス』の「デバイスの強制的な割り当て解除」
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 21–2
	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 21–1
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。	286 ページの「Trusted Extensions で割り当て不可のデバイスを保護する」
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。	287 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

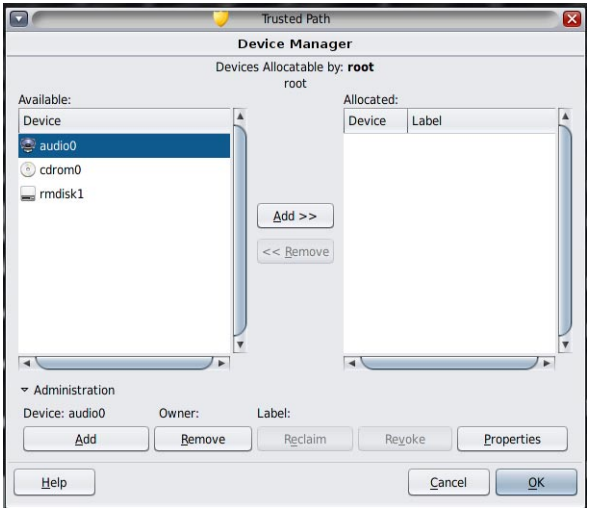
デフォルトで割り当て可能なデバイスは、ラベル範囲が `ADMIN_LOW` から `ADMIN_HIGH` であり、使用するには割り当てられる必要があります。また、ユーザーはデバイス割り当てを承認されている必要があります。これらのデフォルトは変更可能です。

使用するために割り当て可能なデバイスは次のとおりです。

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

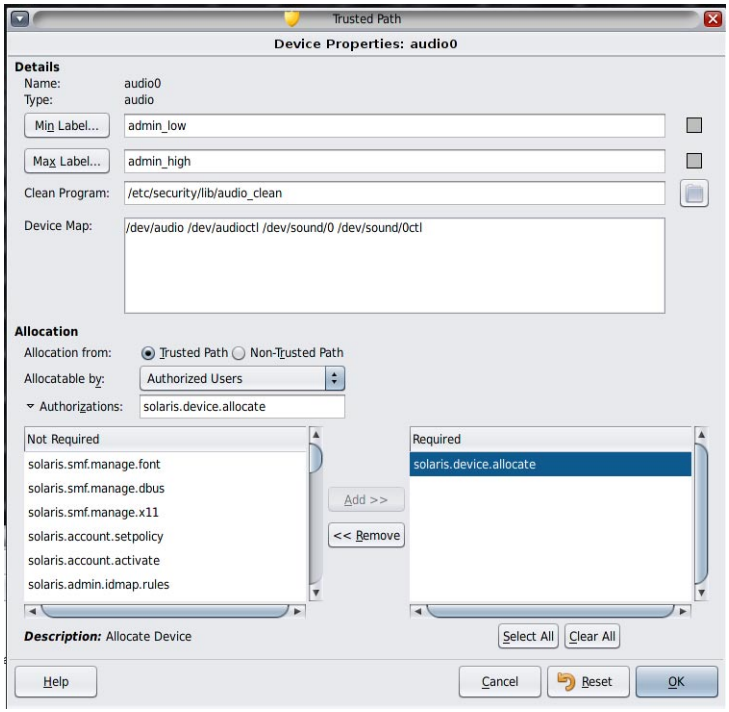
始める前に　大域ゾーンでセキュリティー管理者役割になります。

1 「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。

「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、root 役割が表示しているオーディオデバイスを示したものです。



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、113 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」の下の「Device Configuration」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。

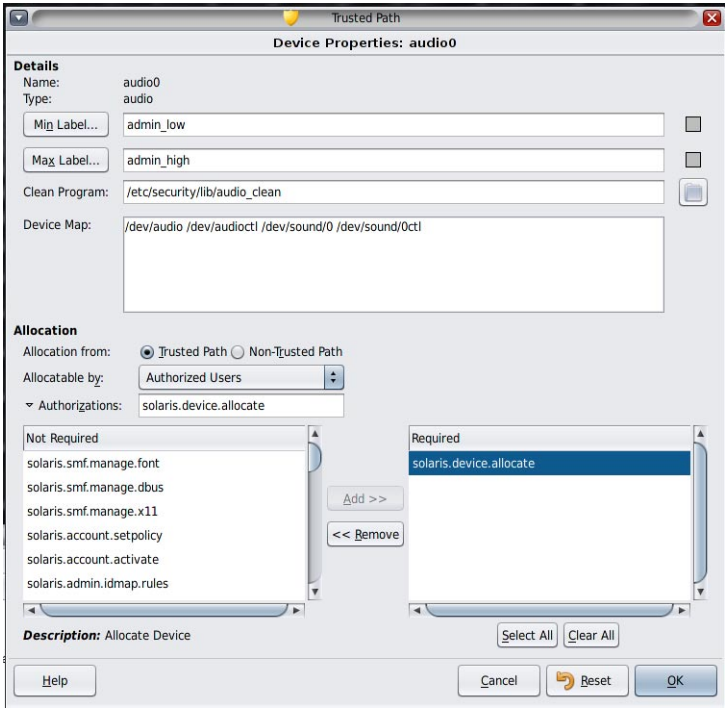
5 デバイスが遠隔で割り当て可能かどうかを指定します。

「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、288 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。

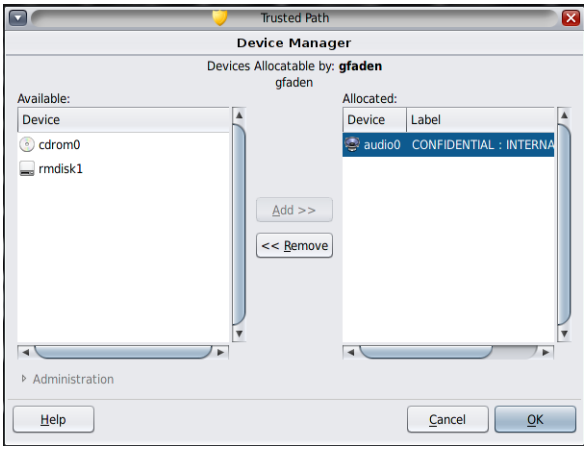
7 「了解」をクリックして変更を保存します。

▼ 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 「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. デバイスマネージャーで「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、113 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 21–1 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
```

▼ 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 `root` 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. 「**Device Properties**」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. デバイスマネージャーを開きます。
   b. 「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。	289 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。	292 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。	292 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 21–1 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。
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、**Oracle Directory Server Enterprise Edition (Directory Server)** 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。
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、292 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 21–2 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 21–3 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、289 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. 281 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. 「管理」ボタンをクリックします。
   c. 「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、152 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。
  詳細な手順については、『Oracle Solaris の管理: セキュリティーサービス』の「ユーザーの RBAC プロパティーを変更する方法」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

次の権利プロファイルでは、役割がデバイスを解除または再利用できます。

- All Authorizations
- Device Management

次の権利プロファイルでは、役割がデバイスを作成または構成できます。

- All Authorizations
- Device Security

例 21–4 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を行います。

1. 289 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 22 章

22 Trusted Extensions での監査 (概要)

この章では、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 Oracle 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。
- ゾーンごとの監査は、ラベル付きゾーンの `root` アカウントが必要となるため、推奨されません。
- 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。システム管理者は、監査ファイル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、監査ログを確認します。

Trusted Extensions の役割による監査の管理

Trusted Extensions での監査には、Oracle Solaris OS の場合と同様の計画が必要です。計画については、『Oracle Solaris の管理: セキュリティーサービス』の第 27 章「監査の計画」を参照してください。

監査管理のための役割の担当

Trusted Extensions では、監査を担当する役割が個別に分かれています。

- root 役割は、監査フラグをユーザーや権利プロファイルに割り当てたり、audit_warn スクリプトなどのシステムファイルを編集したりします。
- 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。この役割は監査レコードの確認も行います。
- セキュリティー管理者役割は監査対象を決定し、監査を構成します。この役割は、初期設定チームが68 ページの「Trusted Extensions でセキュリティー管理者役割を作成する」を実行すると作成されます。

注 – システムでは、セキュリティー管理者が事前に選択した監査クラスのイベントのみが記録されます。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

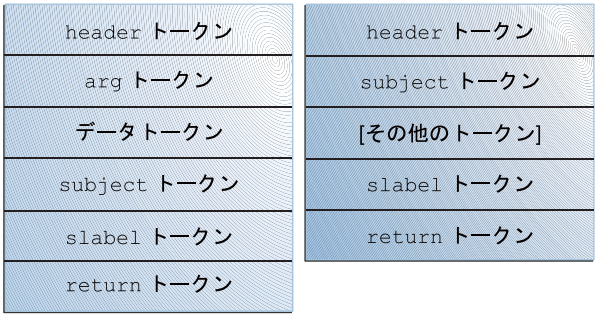
Trusted Extensions で監査を構成し管理する手順は、Oracle Solaris での手順とわずかに異なるだけです。Trusted Extensions では、監査の構成は大域ゾーンで実行されます。ゾーンごとの監査は構成されないため、ユーザーアクションの監査は、大域ゾーンでもラベル付きゾーンでもまったく同様に行われます。監査レコードにはすべての監査イベントのラベルが含められます。

- セキュリティー管理者は、Trusted Extensions に固有の監査ポリシーである windata_down や windata_up を選択できます。
- システム管理者は、監査レコードの確認時に監査レコードをラベル別に選択できます。詳細は、auditreduce(1M) のマニュアルページを参照してください。

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 Oracle Solaris 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。次の図は、Trusted Extensions の典型的なカーネル監査レコードとユーザーレベル監査レコードを示したものです。

図 22–1 ラベル付きシステムでの一般的な監査レコード構造



Trusted Extensions の監査クラス

Trusted Extensions は、X ウィンドウ監査クラスを Oracle Solaris に追加します。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。

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。

- **xa –** このクラスは、X サーバーへのアクセス、つまり X クライアント接続と X クライアント接続解除を監査します。
- **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 Oracle Solaris 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。トークンの定義は、`audit.log(4)` のマニュアルページに一覧されています。

表 22–1 Trusted Extensions の監査トークン

トークン名	説明
298 ページの「`label` トークン」	機密ラベル
299 ページの「`xatom` トークン」	X ウィンドウのアトム ID
299 ページの「`xcolormap` トークン」	X ウィンドウのカラー情報
299 ページの「`xcursor` トークン」	X ウィンドウのカーソル情報
299 ページの「`xfont` トークン」	X ウィンドウのフォント情報
299 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
300 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
300 ページの「`xproperty` トークン」	X ウィンドウのプロパティー情報
300 ページの「`xselect` トークン」	X ウィンドウのデータ情報
300 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。

`label` トークンは、`praudit -x` コマンドによって次のように表示されます。

```
<sensitivity_label>ADMIN_LOW</sensitivity_label>
```

xatom トークン

xatom トークンは、X アトムを識別します。

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
```

xcolormap トークン

xcolormap トークンには、X サーバー識別子や作成者のユーザー ID など、カラーマップの使用に関する情報が含まれます。

xcolormap トークンは、praudit によって次のように表示されます。

```
<X_colormap xid="0x08c00005" xcreator-uid="srv"/>
```

xcursor トークン

xcursor トークンには、X サーバー識別子や作成者のユーザー ID など、カーソルの使用に関する情報が含まれます。

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 トークンには、X サーバー識別子や作成者のユーザー ID など、フォントの使用に関する情報が含まれます。

xfont トークンは、praudit によって次のように表示されます。

```
<X_font xid="0x08c00001" xcreator-uid="srv"/>
```

xgc トークン

xgc トークンには、X ウィンドウのグラフィックコンテキストに関する情報が含まれます。

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

<X_graphic_context xid="0x30002804" xcreator-uid="srv"/>
```

xpixmap トークン

xpixmap トークンには、X サーバー識別子や作成者のユーザー ID など、ピクセルマッピングの使用に関する情報が含まれます。

xpixmap トークンは、praudit -x によって次のように表示されます。

```
<X_pixmap xid="0x2f002004" xcreator-uid="srv"/>
```

xproperty トークン

xproperty トークンには、X サーバー識別子や作成者のユーザー ID、アトム識別子など、ウィンドウの各種プロパティーに関する情報が含まれます。

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。

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、X サーバーおよび作成者のユーザー ID を識別します。

xwindow トークンは、praudit によって次のように表示されます。

```
<X_window xid="0x07400001" xcreator-uid="srv"/>
```

Trusted Extensions での監査ポリシーオプション

Trusted Extensions は、既存の監査ポリシーオプションに 2 つのウィンドウ監査ポリシーオプションを追加します。

```
$ 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 auditrecord 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。
- auditrecord コマンドには、Trusted Extensions の監査イベントが含まれます。

◆ ◆ ◆ 第 23 章

Trusted Extensions のソフトウェア管理 (リファレンス)

この章では、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

Oracle 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 Oracle Solaris システムにソフトウェアを追加する場合と同様です。

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。パッケージとゾーンの詳細については、『Oracle Solaris のシステム管理 (Oracle Solaris ゾーン、Oracle Solaris 10 ゾーン、およびリソース管理)』の第 24 章「ゾーンがインストールされている Oracle Solaris 11 システムでの自動インストールおよびパッケージ」を参照してください。

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。

Oracle Solaris ソフトウェアのセキュリティーメカニズム

Trusted Extensions は、Oracle Solaris と同じセキュリティーメカニズムを使用します。セキュリティーメカニズムには、次の機能が含まれます。

- 承認 – プログラムのユーザーに、特定の承認を要求できます。承認については、『Oracle Solaris の管理: セキュリティーサービス』の「RBAC の要素と基本概念」を参照してください。`auth_attr(4)` 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、『Oracle Solaris の管理: セキュリティーサービス』の第 8 章「役割と特権の使用 (概要)」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、『Oracle Solaris のシステム管理 (Oracle Solaris ゾーン、Oracle Solaris 10 ゾーン、およびリソース管理)』の「ppriv ユーティリティーの使用」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、『Oracle Solaris の管理: セキュリティーサービス』の「RBAC の権利プロファイル」を参照してください。
- 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。Oracle Solaris 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。

   追加情報については、『Oracle Solaris 11 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、『Trusted Extensions Developer's Guide』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。

◆ ◆ ◆ 付 録 A

サイトのセキュリティーポリシー

この付録では、サイトのセキュリティーポリシーについて解説し、詳細についての参考文書や Web サイトを紹介します。

セキュリティーポリシーの作成と管理

各 Solaris Trusted Extensions サイトは固有であるので、それぞれ独自のセキュリティーポリシーを作成します。セキュリティーポリシーを作成および管理する場合は、次のタスクを実行してください。

- セキュリティーチームの設置。セキュリティーチームは、トップレベルの経営、人事管理、コンピュータシステム管理と管理者、および設備管理からの代表者で構成する必要があります。チームは、Trusted Extensions 管理者のポリシーと手順を検討し、すべてのシステムユーザーに適用される一般セキュリティーポリシーを勧告する必要があります。
- 経営管理担当者に対するサイトセキュリティーポリシーについての教育。サイトの経営管理に携わる担当者は全員、セキュリティーポリシーに関する教育を受ける必要があります。ポリシーの情報はコンピュータシステムのセキュリティーに直接関係するので、一般ユーザーがセキュリティーポリシーに触れることができないようにする必要があります。
- ユーザーに対する Trusted Extensions ソフトウェアおよびセキュリティーポリシーについての教育。すべてのユーザーは『Trusted Extensions ユーザーガイド』を読む必要があります。システムが正常に動作していない場合、通常、これを最初に知るのはユーザーであるため、ユーザーはシステムに関する知識を持

ち、発生した問題をシステム管理者に報告する必要があります。セキュリティー保護された環境では、次のような異常に気が付いたら、ただちにシステム管理者に報告する必要があります。

- 各セッションの初めに報告される前回のログイン時間が間違っている
- ファイルデータに異常な変更がある
- 人間が理解できる形式の印刷出力をなくしたり盗まれたりした
- ユーザー機能が実行できない

- セキュリティーポリシーの施行。セキュリティーポリシーが施行されていなかったり遵守されていない場合、Trusted Extensions が設定されたシステムに格納されるデータは保護されません。問題を記録する手順、および問題解決のために行なった措置を記録する手順を決定しなければなりません。
- セキュリティーポリシーの定期的な検討。セキュリティーチームは、セキュリティーポリシーの評価と、前回のポリシー評価のあとに発生したすべてのできごとの評価を定期的に行わなければなりません。これによってポリシーを修正することによって、セキュリティーを向上させることができます。

サイトのセキュリティーポリシーと Trusted Extensions

セキュリティー管理者は、サイトのセキュリティーポリシーに基づいて Trusted Extensions ネットワークを設計しなければなりません。セキュリティーポリシーが次のような構成上の決定の基準になります。

- すべてのユーザーについてどの程度の監査が行われるか、また、どのイベントクラスについて行われるか
- 役割を持つユーザーについてどの程度の監査が行われるか、また、どのイベントクラスについて行われるか
- 監査データをどのように管理、保管、および評価するか
- システムでどのラベルを使用するか、また、一般ユーザーが `ADMIN_LOW` ラベルおよび `ADMIN_HIGH` ラベルを表示できるか
- 各ユーザーにどのユーザー認可上限が割り当てられるか
- デバイスがある場合、どの一般ユーザーによってどのデバイスを割り当てることができるか
- システム、プリンタ、その他のデバイスにどのラベル範囲が定義されるか
- 評価された構成で Trusted Extensions が使用されるかどうか

コンピュータのセキュリティーに関する推奨事項

サイトのセキュリティーポリシーを構築するときには、次のガイドラインのリストを検討してください。

- Trusted Extensions が設定されたシステムの最上位ラベルは、サイトで実行される作業のセキュリティーレベルの上限を超えないように割り当ててください。
- システムのリブート、停電、およびシャットダウンは、手動でサイトログに記録します。
- ファイルシステムの損傷を文書化して、影響を受けたすべてのファイルについて、潜在的なセキュリティーポリシー違反がないか分析します。
- 操作マニュアルと管理者マニュアルは、その情報を使用する正当な理由のある人員以外が読めないようにします。
- Trusted Extensions ソフトウェアの異常な動作または予期しない動作は、報告および文書化して、原因を突き止めます。
- Trusted Extensions が設定されたシステムは、可能であれば 2 人以上で管理します。セキュリティー関連の決定に関するセキュリティー管理権限を、1 人に割り当てます。システム管理タスクに関するシステム管理権限を、それとは別の人に割り当てます。
- 定期的なバックアップルーチンを定めます。
- 承認は、それを必要とし、適切に使用すると信頼できるユーザーのみに割り当てます。
- プログラムに特権を割り当てるのは、作業を行うために特権が必要な場合、また、プログラムを精査して特権の使用についての信頼性が証明された場合のみです。新しいプログラムに特権を設定する際は、その基準として、既存の Trusted Extensions プログラムの特権を確認します。
- 監査情報は定期的に確認および分析を行います。異常なイベントがないか調査して、そのイベントの原因を判別します。
- 管理 ID の数は最小限にします。
- setuid および setgid プログラムの数を最小限にします。承認、特権、役割を使用して、プログラムを実行し、誤使用を回避します。
- 管理者は、一般ユーザーが妥当なログインシェルを持っていることを、定期的に確認します。
- 管理者は、一般ユーザーがシステム管理の ID の値ではなく、妥当なユーザー ID の値を持っていることを定期的に確認してください。

物理的セキュリティーに関する推奨事項

サイトのセキュリティーポリシーを構築するときには、次のガイドラインのリストを検討してください。

- Trusted Extensions が設定されたシステムへのアクセスを制限します。もっとも安全な場所は、通常、1 階以外の屋内です。
- Trusted Extensions が設定されたシステムへのアクセスを監視および文書化します。
- コンピュータ装置は、盗難を防ぐために、テーブルや机などの大きな室内用具に固定します。木製用具に固定する場合は、金属プレートを付けて強度を上げます。
- 機密度の高い情報にはリムーバブルストレージメディアの使用を検討します。使用していないメディアは適切に保管します。
- システムのバックアップおよびアーカイブは、システムとは別の安全な場所に保管します。
- バックアップメディアおよびアーカイブメディアへの物理的なアクセスは、システムへのアクセスと同じ方法で制限します。
- コンピュータ施設に高温アラームを設置し、温度が製造元の仕様の範囲外になったらわかるようにします。推奨範囲は 10 ～ 32°C です。
- コンピュータ施設は水検知器を設置し、床、下張り床の隙間、天井の水漏れなどがわかるようにします。
- 火災を知らせる煙探知機、および防火システムを設置します。
- 湿度アラームを設置し、湿度が高すぎたり低すぎたりするとわかるようにします。
- コンピュータに TEMPEST シールドがない場合は、使用を検討します。TEMPEST シールドは、施設の壁、床、天井などに使用できます。
- TEMPEST を使用した装置の開閉は認定された技術者のみに許可し、電磁放射を確実に防護します。
- コンピュータ装置が置かれている施設や部屋に侵入できる物理的な不備がないか確認します。上げ床、吊り天井、通風口、元の壁と対隣壁の間などを調べます。
- コンピュータ施設内またはコンピュータ装置の近くでの飲食および喫煙を禁止します。コンピュータ装置に影響を与えずにこれらの行為が可能な区域を設けます。
- コンピュータ施設の設計図を保護します。
- コンピュータ施設の建物の設計図、間取り図、写真などの使用を制限します。

個人のセキュリティーに関する推奨事項

サイトのセキュリティーポリシーを構築するときには、次のガイドラインのリストを検討してください。

- パッケージ、文書、およびストレージメディアは、入手した時点およびセキュリティー保護されたサイトから外部へ持ち出す前に検査します。
- 訪問者を含むすべての人に ID カードを常時身に着けるように求めます。
- 複製や偽造が困難な ID カードを使用します。
- 訪問者の立ち入りを禁止する領域を決め、標識によって明らかにわかるようにします。
- 訪問者には常にだれかが付き添います。

よくあるセキュリティー違反

コンピュータを完全にセキュリティー保護することはできません。コンピュータ施設のセキュリティーの限界は、その施設の使用者しだいです。セキュリティー違反のほとんどのアクションは、ユーザーの注意や装置の追加によって簡単に解決できます。次に、発生する可能性のある問題の例を示します。

- ユーザーが、システムへのアクセスを許可されていない人にパスワードを教える。
- ユーザーがパスワードを書き留め、それを失くしたり、安全でない場所に放置したりする。
- ユーザーが、簡単に推測できる語や名前をパスワードに設定する。
- パスワードを入力しているのをほかのユーザーに見られ、パスワードを知られる。
- 承認されていないユーザーがハードウェアの取り外しや交換を行なったり、ハードウェアに不正な変更を加える。
- ユーザーが画面をロックしないでシステムを放置する。
- ユーザーがファイルのアクセス権を変更し、ほかのユーザーがそのファイルを読み取れるようにする。
- ユーザーがファイルのラベルを変更し、ほかのユーザーがそのファイルを読み取れるようにする。
- 機密の印刷文書をシュレッダーにかけないで処分したり、安全でない場所に放置したりする。
- 施設のドアに施錠をしない。
- 鍵を紛失する。
- リムーバブルストレージメディアを適切に保管しない。

- 外部に面した窓からコンピュータ画面が見える。
- ネットワークケーブルが盗聴される。
- 電子的な傍受によって、コンピュータ装置から放射される信号が捕捉される。
- 停電、過電流、スパイクによってデータが破壊される。
- 地震、洪水、竜巻、台風、落雷によってデータが破壊される。
- 太陽の黒点の活動など、外部の電磁放射の干渉によってファイルが解読できなくなる。

その他のセキュリティー関連資料

米国政府発行の出版物では、コンピュータセキュリティーに関する標準、ポリシー、方法、および用語が詳細に説明されています。さらに、UNIX システムのシステム管理者向けのガイドもここに示されています。UNIX のセキュリティー上の問題と解決策を十分に理解するのに役立ちます。

インターネットを通じても資料を入手できます。特に、CERT (`http://www.cert.org`) の Web サイトには、企業やユーザー向けにソフトウェアのセキュリティーホールに関する警告が掲載されています。SANS 協会 (`http://www.sans.org/`)では、トレーニング、詳細な用語集、インターネットからの主な脅威の最新リストが提供されています。

米国政府出版物

米国政府は、多数の出版物を Web 上で提供しています。米国国立標準技術研究所 (NIST) の コンピュータセキュリティーリソースセンター (CSRC) が、コンピュータセキュリティーに関する情報を発表しています。NIST のサイト (`http://csrc.nist.gov/index.html`)からダウンロードできる出版物の一部を次に示します。

- An Introduction to Computer Security: The NIST Handbook.SP 800-12, October 1995.
- Standard Security Label for Information Transfer.FIPS-188, September 1994.
- Swanson, Marianne and Barbara Guttman.Generally Accepted Principles and Practices for Securing Information Technology Systems.SP 800-14, September 1996.
- Tracy, Miles, Wayne Jensen, and Scott Bisker.Guidelines on Electronic Mail Security.SP 800-45, September 2002. セクション E.7 では、メール用の LDAP の安全な設定について解説。
- Wilson, Mark and Joan Hash.Building an Information Technology Security Awareness and Training Program.SP 800-61, January 2004.便利な用語集を収録。
- Grace, Tim, Karen Kent, and Brian Kim.Computer Security Incident Handling Guidelines.SP 800-50, September 2002. セクション E.7 では、メール用の LDAP の安全な設定について解説。

- Scarfone, Karen,Wayne Jansen, and Miles Tracy. Guide to General Server Security SP 800-123, July 2008.
- Souppaya, Murugiah, John Wack, and Karen Kent.Security Configuration Checklists Program for IT Products. SP 800-70, May 2005.

UNIXのセキュリティーに関する出版物

Sun Microsystems Security Engineers. Solaris 10 Security Essentials. Prentice Hall, 2009.

Chirillo, John and Edgar Danielyan.Sun Certified Security Administration for Solaris 9 & 10 Study Guide.McGraw-Hill/Osborne, 2005.

Garfinkel, Simson, Gene Spafford, and Alan Schwartz.Practical UNIX and Internet Security, 3rd Edition.O'Reilly & Associates, Inc, Sebastopol, CA, 2006.

一般的なコンピュータセキュリティーに関する出版物

Brunette, Glenn M. and Christoph L. Toward Systemically Secure IT Architectures. Sun Microsystems, Inc, June 2005.

Kaufman, Charlie, Radia Perlman, and Mike Speciner.Network Security: Private Communication in a Public World, 2nd Edition.Prentice-Hall, 2002.

Pfleeger, Charles P. and Shari Lawrence Pfleeger. Security in Computing.Prentice Hall PTR, 2006.

Privacy for Pragmatists: A Privacy Practitioner's Guide to Sustainable Compliance.Sun Microsystems, Inc, August 2005.

Rhodes-Ousley, Mark, Roberta Bragg, and Keith Strassberg.Network Security: The Complete Reference.McGraw-Hill/Osborne, 2004.

Stoll, Cliff. The Cuckoo's Egg.Doubleday, 1989. (『カッコウはコンピュータに卵を産む(上・下)』、草思社発行、1991)

UNIX全般に関する出版物

Bach, Maurice J. The Design of the UNIX Operating System. Prentice Hall, Englewood Cliffs, NJ, 1986. (『UNIXカーネルの設計』、共立出版発行、1991)

Nemeth, Evi, Garth Snyder, and Scott Seebas.UNIX System Administration Handbook.Prentice Hall, Englewood Cliffs, NJ, 1989. (『UNIXシステム管理入門』、ソフトバンククリエイティブ発行、1992)

◆ ◆ ◆ 付 録 B

Trusted Extensions の構成チェックリスト

このチェックリストでは、Trusted Extensions. の主な構成タスクの概要を示します。これらの主なタスクに、細かいタスクの概略が含まれています。このチェックリストだけでは、このマニュアルに記述されている各手順を実行することはできません。

Trusted Extensions を構成するためのチェックリスト

次のリストは、サイトで Trusted Extensions を有効化および構成するために必要な事項を示します。ほかの場所に記載されているタスクは、相互参照されます。

1. 次を参照します。
   - パート II「Trusted Extensions の管理」の初めの 5 つの章を読みます。
   - サイトのセキュリティー要件を把握します。
   - 308 ページの「サイトのセキュリティーポリシーと Trusted Extensions」を読みます。
2. 次の準備をします。
   - `root` パスワードを決定します。
   - PROM または BIOS のセキュリティーレベルを決定します。
   - PROM または BIOS のパスワードを決定します。
   - 周辺機器の接続を許可するかを決定します。
   - 遠隔プリンタへのアクセスを許可するかを決定します。
   - ラベルなしネットワークへのアクセスを許可するかを決定します。
3. Trusted Extensions を有効にします。48 ページの「Trusted Extensions サービスの有効化とログイン」を参照してください。
   a. Oracle Solaris OS をインストールします。
   b. Trusted Extensions のパッケージを読み込みます。
   c. Trusted Extensions サービス `svc:/system/labeld` を有効にします。
   d. リブートします。

4. (省略可能) 大域ゾーンをカスタマイズします。51 ページの「Trusted Extensions での大域ゾーンの設定」を参照してください。
   a. Trusted Extensions の IPv6 を有効化します (IPv6 を使用する場合)。
   b. 1 以外の DOI を使用する場合には、`/etc/system` ファイル内およびすべてのセキュリティーテンプレート内にその DOI を設定します。
   c. サイトの `label_encodings` ファイルを確認してインストールします。
   d. リブートします。
5. ラベル付きゾーンを追加します。56 ページの「ラベル付きゾーンの作成」を参照してください。
   a. 2 つのラベル付きゾーンを自動的に構成します。
   b. ラベル付きゾーンを手動で構成します。
   c. ラベル付きワークスペースを作成します。
6. LDAP ネームサービスを構成します。第 5 章「Trusted Extensions のための LDAP の構成 (手順)」を参照してください。

   Trusted Extensions プロキシサーバーまたは Trusted Extensions LDAP サーバーを作成します。ファイルネームサービスで必要な設定はありません。
7. 大域ゾーン用およびラベル付きゾーン用のインタフェースと経路指定を設定します。61 ページの「Trusted Extensions でのネットワークインタフェースの構成」を参照してください。
8. ネットワークを設定します。220 ページの「ホストおよびネットワークへのラベル付け (作業マップ)」を参照してください。
   - 単一ラベルのホストおよび制限範囲のホストを特定します。
   - ラベルなしホストからの受信データに適用するラベルを決定します。
   - セキュリティーテンプレートをカスタマイズします。
   - 各ホストをセキュリティーテンプレートに割り当てます。
   - サブネットをセキュリティーテンプレートに割り当てます。
9. その他の構成を実行します。
   a. LDAP 用のネットワーク接続を設定します。
      - すべてのセキュリティーテンプレートの `cipso` ホストタイプに、LDAP サーバーまたはプロキシサーバーを割り当てます。
      - すべてのセキュリティーテンプレートの `cipso` ホストタイプに、LDAP クライアントを割り当てます。
      - ローカルシステムを LDAP サーバーのクライアントにします。
   b. ローカルユーザーおよびローカル管理役割を設定します。67 ページの「Trusted Extensions での役割とユーザーの作成」を参照してください。
      - セキュリティー管理者役割を作成します。
      - セキュリティー管理者役割になれるローカルユーザーを作成します。

- その他の役割を作成し、場合によって、その役割になるローカルユーザーを作成します。

c. ユーザーがアクセスできるすべてのラベルでホームディレクトリを作成します。74 ページの「Trusted Extensions での集中管理ホームディレクトリの作成」を参照してください。

- NFS サーバーにホームディレクトリを作成します。
- 暗号化可能なローカルの ZFS ホームディレクトリを作成します。
- (省略可能) 下位レベルのホームディレクトリをユーザーが読み取れないようにします。

d. 印刷を設定します。261 ページの「ラベル付き印刷の構成 (作業マップ)」を参照してください。

e. デバイスを設定します。279 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。

i. デバイス管理プロファイルまたはシステム管理者プロファイルを役割に割り当てます。

ii. デバイスを使用可能にするには、次のいずれかを行います。

- システムごとに、デバイスを割り当て可能にします。
- 選択したユーザーおよび役割にデバイスの割り当て承認を割り当てます。

f. Oracle Solaris の機能を構成します。

- 監査を設定します。
- システムセキュリティー値を構成します。
- 特定の LDAP クライアントから LDAP を管理できるようにします。
- LDAP でユーザーを設定します。
- LDAP でネットワークの役割を設定します。

g. ファイルシステムをマウントおよび共有します。第 14 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。

◆ ◆ ◆ 付録 C

Trusted Extensions 管理の手引き

Trusted Extensions のインタフェースは Oracle 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 D 「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。Oracle Solaris 11 リリースでは、`txzonemgr -c` コマンドは、最初の 2 つのラベル付きゾーンを作成するメニューをバイパスします。
デバイスマネージャー	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。 `tgnome-selectlabel` ユーティリティーを使用すると、ラベルビルダーをカスタマイズできます。『Trusted Extensions Developer's Guide』の「tgnome-selectlabel Utility」を参照してください。
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「(ログイン/ワークスペース) パスワードを変更」メニュー項目が表示されます。Trusted GNOME 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、114 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 Oracle Solaris インタフェースの拡張

Trusted Extensions は、既存の Oracle 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 Oracle Solaris コマンドにオプションを追加します。Trusted Extensions のすべてのインタフェースの一覧については、付録 D「Trusted Extensions マニュアルページのリスト」を参照してください。
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、186 ページの「Trusted Extensions での NFS マウントされたファイルシステムへのアクセス」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。

Trusted Extensions は、exec_attr データベースに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、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、140 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、297 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。

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、Oracle 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。

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。

役割
: Oracle 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。

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 Oracle Solaris よりも制限されています。

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、Oracle 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。

  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。

◆ ◆ ◆ 付 録 D

Trusted Extensions マニュアルページのリスト

Trusted Extensions は Oracle Solaris OS の構成の 1 つです。この付録では、Trusted Extensions に関する情報が含まれているマニュアルページについて説明します。

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は、Trusted Extensions が構成されているシステムにのみ該当します。説明文には、Trusted Extensions ドキュメントセット内でのこれらの機能に関する例や説明へのリンクが含まれています。

Trusted Extensions マニュアルページ	目的および追加情報へのリンク
`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。 281 ページの「Trusted Extensions でデバイスを構成する」を参照してください。
`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。 例については、132 ページの「ラベルの 16 進値を求める」を参照してください。
`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。 例については、『Trusted Extensions Label Administration』の「How to Debug a label_encodings File」と例 4–1 を参照してください。
fgetlabel(2)	ファイルのラベルの取得
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。 例については、176 ページの「マウントされたファイルのラベルを表示する」を参照してください。
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。 『Trusted Extensions Developer's Guide』の「Acquiring a Sensitivity Label」
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

	例については、133 ページの「可読のラベルを 16 進形式から取得する」を参照してください。
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)	Trusted Extensions ラベル属性の説明
libtsnet(3LIB)	Trusted Extensions ネットワークライブラリ
libtsol(3LIB)	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
	その使用例については、166 ページの「遠隔 Trusted Extensions システムにログインして管理する」を参照してください。
plabel(1)	プロセスラベルの取得
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することによるデバイスの割り当ての防止
	例については、281 ページの「Trusted Extensions でデバイスを構成する」を参照してください。
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
	123 ページの「データのセキュリティーレベルを変更する際の規則」を参照してください。
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
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。

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
tncfg(1M)	トラステッドネットワークデータベースの管理。トラステッドネットワークを管理するための txzonmgr GUI の代替です。list サブコマンドは、ネットワークインタフェースのセキュリティー特性を表示します。tncfg は、tninfo コマンドよりも詳しい情報を提供します。 さまざまな例については、第 16 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。
tnctl(1M)	Trusted Extensions ネットワークパラメータの設定。tncfg コマンドを使用することもできます。 例については、例 12–1 を参照してください。
tnd(1M)	LDAP ネームサービスが有効化された場合のトラステッドネットワークデーモンの実行。
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。 246 ページの「Trusted Extensions ネットワークをデバッグする」。tncfg コマンドや txzonemgr GUI を使用することもできます。 tncfg コマンドとの比較については、195 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。
trusted_extensions(5)	Trusted Extensions の概要
txzonemgr(1M)	ラベル付きゾーンとネットワークインタフェースの管理。コマンド行オプションを使用すると、2 つのゾーンを自動作成できます。このコマンドは、構成ファイルを入力として受け入れ、ゾーンの削除を可能にします。txzonemgr は zenity (1) スクリプトです。

	56 ページの「ラベル付きゾーンの作成」と 245 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)」を参照してください。
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
tgnome-selectlabel ユーティリティー	ラベルビルダー GUI を作成できるようにする 詳細は、『Trusted Extensions Developer's Guide』の「tgnome-selectlabel Utility」を参照してください。
updatehome(1)	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 148 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。
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 Oracle Solaris マニュアルページ

Trusted Extensions では、Oracle Solaris の次のマニュアルページに情報が追加されます。

Oracle Solaris のマニュアルページ	**Trusted Extensions** での変更内容と追加情報へのリンク
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。Trusted Extensions では、一般ユーザーはこのコマンドを使用しません。 ユーザー手順については、『Trusted Extensions ユーザーガイド』の「Trusted Extensions でデバイスを割り当てる」を参照してください。
auditconfig(1M)	ラベル付き情報のウィンドウポリシー、監査クラス、監査イベント、および監査トークンの追加。

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。 例については、『Oracle Solaris の管理: セキュリティーサービス』の「監査トレールから監査イベントを選択する方法」を参照してください。
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。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。 詳細は、187 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。
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。Trusted Extensions では、一般ユーザーはこのコマンドを使用しません。 ユーザー手順については、『Trusted Extensions ユーザーガイド』の「Trusted Extensions でデバイスを割り当てる」を参照してください。
device_clean(5)	Trusted Extensions でデフォルトで呼び出される
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
ikeadm(1M)	ラベル付き IKE プロセス用のデバッグフラグ 0x0400 の追加。
ike.config(4)	label_aware グローバルパラメータと 3 つのフェーズ 1 変換キーワード single_label、multi_label、および wire_label の追加

in.iked(1M)	大域ゾーンでのマルチレベル UDP ポート 500 および 4500 経由のラベル付きセキュリティーアソシエーションのネゴシエーションのサポート。 また、ike.config(4) のマニュアルページも参照してください。
ipadm(1M)	all-zones インタフェースを永続プロパティー値として追加。 例については、245 ページの「システムのインタフェースが稼働していることを確認する」を参照してください。
ipseckey(1M)	label、outer-label、および implicit-label 拡張の追加。これらの拡張は、セキュリティーアソシエーションの内側で伝送されるトラフィックに Trusted Extensions ラベルを関連付けます。
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)	LDAP での 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。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。
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。 例については、195 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。
pf_key(7P)	IPsec セキュリティーアソシエーション (SA) へのラベルの追加
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。-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。 例については、195 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。
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
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)	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。 190 ページの「Trusted Extensions でファイルをバックアップする」と 191 ページの「Trusted Extensions でファイルを復元する」を参照してください。
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 に固有の idletime、idlecmd、clearance、および min_label ユーザーセキュリティー属性の追加 34 ページの「Trusted Extensions でのユーザーセキュリティーの計画」を参照してください。

用語集

CIPSO ラベル
共通 IP セキュリティーオプション (Common IP Security Option)。CIPSO は、Trusted Extensions が実装するラベル標準です。

.copy_files ファイル
マルチラベルシステムに関する任意の設定ファイル。このファイルには、システムまたはアプリケーションが正常に動作するためにユーザー環境またはユーザーアプリケーションで必要とされる `.cshrc`、`.mozilla` などの起動ファイルのリストが含まれます。ユーザーのホームディレクトリが高いラベルで作成されると、`.copy_files` に含まれるファイルがそのディレクトリにコピーされます。.link_files ファイルも参照。

DAC
任意アクセス制御を参照。

domain
インターネットのネーミング階層の一部。ローカルネットワーク上のシステムのグループであり、管理ファイルを共有します。

GFI
政府提供情報 (Government Furnished Information の略)。このマニュアルでは、米国政府提供の label_encodings ファイルを指します。Trusted Extensions ソフトウェアで GFI を使用するには、Oracle 固有の `LOCAL DEFINITIONS` セクションを GFI の末尾に追加します。詳細は、『Trusted Extensions Label Administration』の第 5 章「Customizing the LOCAL DEFINITIONS Section (Tasks)」を参照。

IP アドレス
インターネットプロトコル (Internet Protocol、IP) アドレス。インターネットプロトコルによって通信が可能になるための、ネットワークに接続されたシステムを識別する一意の数字。IPv4 のアドレスは、ピリオドで区切られた 4 つの数字です。通常、IP アドレスの各部は 0 から 225 です。ただし、最初の数字は 224 未満とし、最後の数字は 0 以外にしてください。

IP アドレスは、論理的に、ネットワークの部分と ネットワーク上のsystemの部分に分けられます。ネットワーク番号は電話番号の市外局番、システム番号はそれ以外の電話番号に相当します。

label
オブジェクトに割り当てられるセキュリティー識別子。ラベルは、オブジェクトの情報を保護するレベルを基準にします。セキュリティー管理者がどのようにユーザーを設定したかによって、ユーザーは機密ラベルを参照できたりできなかったりします。ラベルはlabel_encodings ファイルで定義されます。

label_encodings ファイル
認可範囲、ラベルビュー、デフォルトのラベル表示/非表示、デフォルトのユーザー認可上限、およびその他のラベルに関する事項を含む完全な機密ラベルを定義するファイル。

.link_files ファイル　マルチラベルシステムに関する任意の設定ファイル。このファイルには、システムまたはアプリケーションが正常に動作するためにユーザー環境またはユーザーアプリケーションで必要とされる `.cshrc`、`.mozilla` などの起動ファイルのリストが含まれます。ユーザーのホームディレクトリが高いラベルで作成されると、`.link_files` に含まれるファイルがそのディレクトリにリンクされます。.copy_files ファイルも参照。

MAC　必須アクセス制御を参照。

process　コマンドを呼び出したユーザーに代わってコマンドを実行するアクション。プロセスは、ユーザー ID (UID)、グループ ID (GID)、補助グループリスト、ユーザーの監査 ID (AUID) などの多数のセキュリティー属性をユーザーから受け取ります。プロセスが受け取るセキュリティー属性には、実行されるコマンドが使用可能な特権、および現在のワークスペースの機密ラベルも含まれます。

system　コンピュータの総称。インストール後、ネットワーク上のシステムはホストとも呼ばれます。

tnrhdb データベース　トラステッドネットワークの遠隔ホストデータベース。このデータベースは、ラベル特性のセットを遠隔ホストに割り当てます。このデータベースは、`/etc/security/tsol/tnrhdb` のファイルとしてアクセス可能となっています。

tnrhtp データベース　トラステッドネットワークの遠隔ホストテンプレート。このデータベースは、遠隔ホストに割り当てることができるラベル特性のセットを定義します。このデータベースは、`/etc/security/tsol/tnrhtp` のファイルとしてアクセス可能となっています。

txzonemgr スクリプト　`/usr/sbin/txzonemgr` スクリプトは、ラベル付きゾーンを管理するための簡単な GUI を提供します。このスクリプトは、ネットワーキングオプションのメニュー項目も提供します。`txzonemgr` は、root ユーザーによって大域ゾーンで実行されます。

アクセス権ビット　ファイルやディレクトリをだれが読み取り、書き込み、または実行できるかを表すために、所有者が一連のビットを指定する任意アクセス制御の一種。各ファイルまたはディレクトリに割り当てられるアクセス権には、所有者に設定されるセット、所有者のグループに設定されるセット、その他のすべてに設定されるセットの 3 つがあります。

遠隔ホスト　ローカルシステムとは異なるシステム。遠隔ホストは、ラベルなしホストまたはラベル付きホストになります。

オープンネットワーク　ほかのネットワークと物理的に接続され、Trusted Extensions ソフトウェアを使用して Trusted Extensions 以外のホストと通信する Trusted Extensions ホストのネットワーク。閉じたネットワークと比較。

解釈ドメイン **(DOI)**　Trusted Extensions が構成された Oracle Solaris システム上で、解釈ドメインは、類似のラベルが定義される可能性のある `label_encodings` ファイル同士を区別するために使用されます。DOI は、ネットワークパケット上のセキュリティー属性をローカルの `label_encodings` ファイルによる表現に変換するための規則セットです。同一の DOI を持つシステムはその規則セットを共有しており、ラベル付きのネットワークパケットを変換できます。

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

管理役割　役割が管理タスクを実行できるように、必要な承認、特権コマンド、およびトラステッドパスの役割を付与するセキュリティー属性。役割は、バックアップ、監査など、Oracle Solaris スーパーユーザーの権限のサブセットを実行します。

機密ラベル　オブジェクトまたはプロセスに割り当てられるセキュリティーlabel。このラベルは、含まれるデータのセキュリティーレベルに従ってアクセスを制限するために使用します。

クライアント　ネットワークに接続されているシステム。

権利プロファイル　コマンドのバンドル、および実行可能ファイルに割り当てられているセキュリティー属性のバンドルのためのメカニズム。権利プロファイルによって、Oracle Solaris 管理者は、だれがどのコマンドを実行できるかを制御でき、また、コマンドが実行されるときのコマンドの属性を制御できます。ユーザーはログインすると、ユーザーに割り当てられているすべての権利が有効になり、ユーザーのすべての権利プロファイルで割り当てられているすべてのコマンドおよび承認にアクセスできます。

コンパートメント　labelを構成する階層的ではない要素で、格付けとともに使用して認可上限やlabelを形成します。コンパートメントは、技術部署や学際的プロジェクトチームなどに使用される、情報の集合を表すために使われます。

最下位ラベル　ユーザーの機密ラベルの下限とシステムの機密ラベルの下限。ユーザーのセキュリティー属性を指定する際にセキュリティー管理者によって設定される最下位ラベルは、ユーザーが最初にログインするときの最初のワークスペースの機密ラベルです。`label_encodings` ファイルの最下位ラベルのフィールドでセキュリティー管理者によって指定される機密ラベルがシステムの下限を設定します。

システム管理者　Trusted Extensions において、ユーザーアカウントの設定のうちセキュリティーに関連しない部分など、標準的なシステム管理タスクの実行を担当するユーザーに割り当てられるトラステッド役割。セキュリティー管理者と比較。

システム認可範囲　セキュリティー管理者が label_encodings ファイルで定義する規則に従って作成されるすべての有効なラベルのセットと、Trusted Extensions が設定されたすべてのシステムで使用される 2 つの管理ラベルを含ませたもの。その 2 つの管理ラベルは `ADMIN_LOW` と `ADMIN_HIGH` です。

承認　セキュリティーポリシーによって許可されないアクションを実行できるように、ユーザーまたは役割に付与する権利。承認は権利プロファイルで付与されます。特定のコマンドが成功するには、ユーザーに特定の承認が必要です。たとえば、PostScript ファイルを印刷するには、Postscript 印刷の承認が必要です。

初期設定チーム　Trusted Extensions ソフトウェアの有効化および構成を監督する、最低 2 人のチーム。セキュリティーに関する決定とシステム管理に関する決定を別々のチームメンバーが担当します。

初期ラベル　ユーザーまたは役割に割り当てられる最下位ラベルであり、ユーザーの初期ワークスペースのラベル。 初期ラベルは、ユーザーまたは役割が作業できる最下位ラベルです。

責務分離	ユーザーの作成および認証に 2 人の管理者または 2 つの役割を必要とするセキュリティーポリシー。一方の管理者または役割には、ユーザー、ユーザーのホームディレクトリ、およびその他の基本的な管理を作成する責任があります。もう一方の管理者または役割には、パスワードおよびラベル範囲など、ユーザーのセキュリティー属性に対して責任があります。
セキュリティー管理者	機密情報を保護しなければならない組織において、サイトのセキュリティーポリシーを定義および実施する人員。この人物は、サイトで処理されているすべての情報へのアクセスが認められています。ソフトウェアで、適切な認可上限を持つ 1 人以上に対してセキュリティー管理者の管理役割が割り当てられます。この管理者は、ソフトウェアによってサイトのセキュリティーポリシーが実施されるように、すべてのユーザーおよびホストのセキュリティー属性を設定します。システム管理者と比較。
セキュリティー属性	Trusted Extensions セキュリティーポリシーを実施するために使用される属性。さまざまなセットのセキュリティー属性が、process、ユーザー、ゾーン、ホスト、割り当て可能なデバイス、およびその他のオブジェクトに割り当てられます。
セキュリティーテンプレート	`tnrhtp` データベースのレコードの 1 つで、Trusted Extensions ネットワークにアクセスできるホストのクラスのセキュリティー属性の定義に使用されます。
セキュリティーポリシー	Trusted Extensions ホスト上の、DAC、MAC、および情報へのアクセス方法を定義するラベル付け規則のセット。また、顧客サイトについて、そのサイトで処理される情報の機密度と、承認されていないアクセスから情報を保護する手段を定義する規則のセット。
セキュリティーラベルセット	tnrhtp データベースエントリに対して個別セットのセキュリティーラベルを指定します。セキュリティーラベルセットとともにテンプレートに割り当てられているホストは、そのラベルセットのいずれかのラベルに一致するパケットを送受信できます。
デバイス	デバイスには、プリンタ、コンピュータ、テープドライブ、フロッピードライブ、CD-ROM ドライブ、DVD ドライブ、オーディオデバイス、および内蔵擬似端末デバイスがあります。デバイスは、「同位読み取り、同位書き込み」の MAC ポリシーに従います。DVD ドライブなどのリムーバブルデバイスへのアクセスはデバイスの割り当てによって制御されます。
デバイスの割り当て	割り当て可能なデバイスの情報を、そのデバイスを割り当てたユーザー以外の者がアクセスできないように保護するメカニズム。デバイスが割り当て解除されるまで、デバイスを割り当てたユーザー以外の者がデバイスに関連付けられている情報にアクセスすることはできません。ユーザーがデバイスを割り当てるには、セキュリティー管理者によってデバイス割り当ての承認がユーザーに付与されている必要があります。
閉じたネットワーク	Trusted Extensions が設定されているシステムのネットワーク。このネットワークは Trusted Extensions 以外のホストから切り離されています。Trusted Extensions ネットワークの外へ配線せずに物理的に切り離すことができます。あるいは、Trusted Extensions ホストが Trusted Extensions ホストのみを認識するようにソフトウェアで切り離すことができます。ネットワークの外側からのデータ入力は、Trusted Extensions ホストに接続された周辺機器に制限されます。オープンネットワークと比較。

特権
: コマンドを実行中のプロセスに付与される権限。完全セットの特権は、基本機能から管理機能に至るまでのシステムの完全機能です。システムクロックの設定などのセキュリティーポリシーをバイパスする特権は、サイトのセキュリティー管理者が付与できます。

ドメイン名
: システムのグループの識別。ドメイン名は、ピリオドで区切られた一連のコンポーネント名から構成されます (たとえば、`example1.town.state.country.org`)。ドメイン名内で右側にあるコンポーネント名ほど、より大きな管理権限領域 (通常は遠隔) を表します。

トラステッドストライプ
: なりすましができない領域。Trusted GNOME では、このストライプは最上部にあります。このストライプには、トラステッドパスインジケータとウィンドウ機密ラベルによって、ウィンドウシステムの状態に関するフィードバックが視覚的に表示されます。機密ラベルがユーザーに表示されないように設定されている場合、トラステッドストライプはアイコンになって、トラステッドパスインジケータのみが表示されます。

トラステッドネットワークデータベース
: `tnrhtp` (トラステッドネットワークの遠隔ホストテンプレート) および `tnrhdb` (トラステッドネットワークの遠隔ホストデータベース) によって、Trusted Extensions システムが通信できる遠隔ホストが定義されます。

トラステッドパス
: Trusted Extensions が構成された Oracle Solaris システム上のトラステッドパスは、システムと対話するための、改ざん耐性を備えた信頼できる方法です。トラステッドパスを使えば、管理機能が損なわれることがなくなります。パスワードの変更など、保護する必要のあるユーザー機能でもトラステッドパスが使用されます。トラステッドパスがアクティブになっていると、改ざん耐性インジケータがデスクトップに表示されます。

トラステッド役割
: 管理役割を参照。

任意アクセス制御
: ファイルまたはディレクトリの所有者の判断によって付与または拒否されるアクセスのタイプ。Trusted Extensions には、UNIX アクセス権ビット と ACL の 2 種類の任意アクセス制御 (discretionary access control、DAC) があります。

認可上限
: ユーザーが作業可能なラベルのセットの上限。下限はセキュリティー管理者が割り当てる最下位ラベルです。認可上限は、セッション認可上限とユーザー認可上限の 2 種類があります。

認可範囲
: ユーザーまたはリソースのクラスに認可された機密ラベルのセット。有効なラベルのセット。システム認可範囲およびユーザー認可範囲も参照。

ネームサービス
: ネットワーク上の全システムに関する重要なシステム情報が収められている分散型ネットワークデータベース。ネットワーク上のシステムは、これを利用して相互通信を行います。ネームサービスを使用しないと、各systemはローカルの `/etc` ファイルにシステム情報のコピーを保持しなければなりません。

ネットワークに接続されたシステム
: ハードウェアとソフトウェアによって接続され、ローカルエリアネットワーク (LAN) とも呼ばれるシステムのグループ。システムをネットワークに接続するには、通常、1 台以上のサーバーが必要です。

ネットワークに接続されていないシステム
: ネットワークに接続されていない、またはほかのホストに依存しないコンピュータ。

必須アクセス制御
: ファイル、ディレクトリ、またはデバイスの機密ラベルとそれにアクセスしようとするプロセスの機密ラベルとの比較に基づくアクセス制御。あるラベルのプロセスが下位のラベルのファイルを読み取ろうとする場合、MAC 規則の「同位読み取り、下位読み取り」が適用されます。あるラベルのプロセスが別のラベルのディレクトリに書き込もうとする場合、MAC 規則の「同位書き込み、下位読み取り」が適用されます。

評価外の構成
: 評価された構成の基準を満たすと認められているソフトウェアがセキュリティーの基準を満たさない設定で構成される場合、そのソフトウェアは「評価外の構成」と呼ばれます。

評価された構成
: 認証局によって特定の基準に適合すると認定された構成で実行されている 1 つ以上の Trusted Extensions ホスト。米国での基準は TCSEC です。評価と認定を行うのは NSA です。

  - Solaris 10 11/06 リリースで設定されている Trusted Extensions ソフトウェアでは、多数の保護プロファイルが、ISO 標準である共通基準 v2.3 (2005 年 8 月) の評価保証レベル (EAL) 4 に認定されます。
  - NSA に認定された Trusted Extensions ソフトウェアは保証継続 (Assurance Continuity) を通して Solaris 10 5/09 リリースに設定されます。

  共通基準 v2 (CCv2) と保護プロファイルによって、以前の TCSEC U.S. 標準はレベル B1+ まで廃止されます。CCv2 に関する相互認証協定が米国、英国、カナダ、デンマーク、オランダ、ドイツ、およびフランスで調印されています。

  Trusted Extensions 構成ターゲットは、TCSEC C2 レベルと B1 レベルと同様の機能および一部の追加機能を示します。

ファイルシステム
: 論理的階層に編成および構成した情報のセットをなすファイルおよびディレクトリの集まり。ファイルシステムはローカル system または遠隔システムからマウントできます。

ブランドゾーン
: Trusted Extensions ではラベル付きの非大域ゾーン。より一般的には、ネイティブでないオペレーティング環境を含む非大域ゾーン。`brands(5)` のマニュアルページを参照。

プロファイルシェル
: 特権、承認、特殊な UID や GID などのセキュリティー属性を認識する特別なシェル。通常、プロファイルシェルは、ユーザーが使用できるコマンドを制限しますが、より多くの権限がある場合にはそれらのコマンドを実行できるようにすることも可能です。プロファイルシェルは、トラステッド役割のデフォルトのシェルです。

ホスト名
: ネットワーク上のその他の system によって認識される、システムの名前。この名前は、ドメイン内のすべてのシステムで一意です。通常、ドメインは単一の組織を表します。ホスト名は、文字、数字、マイナス符号 (–) を任意に組み合わせて作成できますが、先頭と末尾にマイナス符号は使用できません。

マルチレベルデスクトップ
: Trusted Extensions が構成された Oracle Solaris システムでは、ユーザーはある特定のラベルでデスクトップを実行できます。複数ラベルでの作業を承認されたユーザーは、各ラベルで作業するためのワークスペースを、ラベルごとに 1 つずつ作成できます。このマルチレベルデスクトップでは、承認済みユーザーは、異なるラベルのウィンドウ間でカット&ペーストを行なったり、さまざまなラベルでメールを受信したり、異なるラベルのワークスペース内でラベル付きウィンドウを表示して使用したりできます。

マルチレベルポート (MLP)
: Trusted Extensions が構成された Oracle Solaris システムでは、MLP は、あるゾーン内でマルチレベルサービスを提供するために使用されます。デフォルトでは、X サーバーは大域ゾーン内で定義されたマルチレベルサービスです。MLP はポート番号とプロトコルで指定されます。たとえば、マルチレベルデスクトップ用の X サーバーの MLP は、6000-6003 と TCP によって指定されます。

役割
: 役割は、ログインできないことを除いて、ユーザーと同じです。通常、管理機能を割り当てるために役割が使用されます。役割は、コマンドと承認の特定セットに制限されます。管理役割を参照。

ユーザー認可上限
: セキュリティー管理者によって割り当てられる認可上限で、ユーザーが常に作業可能なラベルのセットの上限を設定します。ユーザーは、ログインセッション時にデフォルトを受け入れたり、認可上限をさらに制限したりできます。

ユーザー認可範囲
: 一般ユーザーが system で作業できるすべての可能なラベルのセット。サイトのセキュリティー管理者が label_encodings ファイルで範囲を指定します。システム認可範囲を定義する適格な形式のラベルに関する規則は、このファイルの `ACCREDITATION RANGE` セクションの値 (上限、下限、組み合わせ制約など) によってさらに制限されます。

ラベル間の関係
: Trusted Extensions が構成された Oracle Solaris システムでは、あるラベルは、別のラベルよりも上位である、別のラベルと等しい、別のラベルから切り離されている、のいずれかになります。たとえば、ラベル `Top Secret` はラベル `Secret` よりも上位です。2 つのシステムが同じ解釈ドメイン (DOI) を持つ場合、一方のラベル `Top Secret` は他方のラベル `Top Secret` と等しくなります。

ラベル構成
: 単一ラベルまたはマルチラベルの機密ラベルに関する Trusted Extensions インストール時の選択。ほとんどの環境では、サイトのすべてのシステムでラベル構成は同一です。

ラベルセット
: セキュリティーラベルセットを参照。

ラベル付きシステム
: ラベル付きシステムとは、Trusted Extensions や MLS が有効化された SELinux など、マルチレベルオペレーティングシステムが実行されているシステムのことです。このシステムは、共通 IP セキュリティーオプション (CIPSO) でラベル付けされたヘッダーを含むネットワークパケットを送受信できます。

ラベル付きゾーン
: Trusted Extensions が構成された Oracle Solaris システムでは、すべてのゾーンに一意のラベルが割り当てられます。大域ゾーンもラベル付けされますが、ラベル付きゾーンは通常、 ラベルが割り当てられた非大域ゾーンを指します。ラベル付きゾーンは、ラベルが構成されていない Oracle Solaris システム上の非大域ゾーンとは異なる特性を 2 つ備えています。第 1 に、ラベル付きゾーンは同じプールのユーザー ID とグループ ID を使用する必要があります。第 2 に、ラベル付きゾーンは IP アドレスを共有できます。

ラベル付きホスト
: 複数のラベル付きシステムから成るトラステッドネットワークの一部をなすラベル付きシステム。

ラベルなしシステム　Trusted Extensions が構成された Oracle Solaris システムにとって、ラベルなしシステムとは、Trusted Extensions や MLS が有効化された SELinux などのマルチレベルオペレーティングシステムが実行されていないシステムのことです。ラベルなしシステムはラベル付きパケットを送信しません。通信中の Trusted Extensions システムがある単一のラベルをラベルなしシステムに割り当てた場合、その Trusted Extensions システムとラベルなしシステムとの間のネットワーク通信は、そのラベルで行われます。ラベルなしシステムは「シングルレベルシステム」とも呼ばれます。

ラベルなしホスト　Oracle Solaris OS を実行するシステムなど、ラベルなしネットワークパケットを送信する、ネットワークに接続されたシステム。

ラベル範囲　コマンド、ゾーン、および割り当て可能デバイスに割り当てられている機密ラベルのセット。最上位ラベルと最下位ラベルを指定することによってこの範囲を指定します。コマンドの場合、最上位ラベルと最下位ラベルは、コマンドが実行されるラベルを制限します。ラベルを認識しない遠隔ホストには、セキュリティー管理者が 1 つのラベルに制限するその他のホストと同様に、1 つの機密ラベルが割り当てられます。ラベル範囲は、デバイスが割り当てられるラベルを制限し、そのデバイスを使用する場合に情報が格納または処理されるラベルを制限します。

割り当て　デバイスへのアクセスを制御するメカニズム。デバイスの割り当てを参照。

索引

O

P

U

X

Z

あ

こ

さ

し

す

せ

そ

た

ち

つ

て

と

ひ

ふ

へ

わ