Trusted Extensions 構成と管理

Part No: E53981
2014 年 7 月

ORACLE

目次

図目次

表目次

このドキュメントの使用

- **概要** – 1 つ以上のシステムで Oracle Solaris の Trusted Extensions 機能を有効化、構成、および保守する方法について説明します。
- **対象読者** – ラベル付きのシステムおよびネットワークのシステム管理者。
- **必要な知識** – セキュリティーラベルおよびサイトのセキュリティー要件。

製品ドキュメントライブラリ

この製品に関する最新情報および既知の問題については、ドキュメントライブラリ (http://www.oracle.com/pls/topic/lookup?ctx=E56342) に記載されています。

Oracle サポートへのアクセス

Oracle ユーザーは My Oracle Support から電子サポートにアクセスできます。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。

フィードバック

このドキュメントに関するフィードバックを http://www.oracle.com/goto/docfeedback からお聞かせください。

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 のインストールと有効化、および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 を構成する際に考慮す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 システム上のさまざまな Trusted Extensions 構成用のタスクマップを示します。

第3章「Oracle Solaris への Trusted Extensions 機能の追加」では、Trusted Extensions 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」では、モニターがあるシステムで Trusted Extensions を構成する手順を示します。

第5章「Trusted Extensions 用の LDAP の構成」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

1 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。

Oracle Solaris 11.2 での Trusted Extensions の新機能

このセクションでは、既存のお客様向けに、このリリースでの Trusted Extensions の重要な新機能について説明します。

- リブートせずに Trusted Extensions をインストールおよび構成できます。詳細は、`labeladm`(1M) のマニュアルページを参照してください。手順については、38 ページの「Trusted Extensions の有効化」を参照してください。
- Trusted Extensions をブートする前に、カスタマイズしたラベルエンコーディングファイルを簡単にインストールできます。詳細は、`labeladm`(1M) のマニュアルページを参照してください。例および手順については、44 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」を参照してください。
- Trusted Extensions は、`armor` パッケージから取得した、標準化された役割の ARMOR (Authorization Roles Managed on RBAC) セットを使用できます。ARMOR および Oracle Solaris のその他の新しいセキュリティー機能の詳細は、『Oracle Solaris 11.2 でのユーザーとプロセスのセキュリティー保護 』の「Oracle Solaris 11.2 での権利の新機能」を参照してください。
- `txzonemgr` コマンドは、ネットワークインタフェースの割り当てをより高速かつ確実に実行します。

Trusted Extensions でのセキュリティー計画

このセクションでは、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説明します。

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、20 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、19 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

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 `root` に割り当てられる機能は、いくつか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オーバーライド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、次の保護プロファイルについて、Common Criteria Recognition Agreement (CCRA) の保証レベル EAL4+ への準拠が認証されています。

- Advanced Management
- Extended Identification and Authentication
- Labeled Security
- Virtualization

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 を構成する担当者の計画

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構成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オーバーライドできるか
- 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。

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、管理者はユーザーとしてログインし、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 11.2 システムのインストール 』、および『*リリースノート*』の「インストール」のセクションで説明されている、Oracle Solaris 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 11.2 での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、4 種類のホストを認識します。どちらの種類のホストにも、表1-1「Trusted Extensions のデフォルトホストテンプレート」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 のデフォルトホストテンプレート

ホストタイプ	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します。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。

ホストタイプ	テンプレート名	目的
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します。CIPSO パケットはラベル付けされます。
netif	netif	adaptive ホストからのパケットを特定のネットワークインタフェース上で受信するホストを識別します。
adaptive	adapt	ラベルのないホストまたはネットワークを識別しますが、ラベルなしのパケットを netif ホスト上の特定のインタフェースに送信します。

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」を参照してください。リモート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 でのラベル付きゾーンの計画

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構成します。重複しないすべてのラベルに対してそれぞれ 1 つ以上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、ほかのシステムに到達することはできません。同じラベルで実行されるサービスをさらに分離するには、セカンダリゾーンを作成します。詳細は、176 ページの「プライマリおよびセカンダリラベル付きゾーン」を参照してください。

- 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リモートホストの具体的な 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、リモート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。詳細は、`txzonemgr`(1M) 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リモート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、リモート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。

ラベル付きゾーンに制限されているアプリケーション

デフォルトでは、ラベル付きゾーンは大域ゾーンのネームサービスを共有し、`/etc/passwd` ファイルと `/etc/shadow` ファイルも含め大域ゾーンの構成ファイルの読み取り専用コピーを持っています。ラベル付きゾーンからそのラベル付きゾーンにアプリケーションをインストールする予定があり、パッケージによってゾーンにユーザーが追加される場合は、ゾーン内にこれらのファイルの書き込み可能コピーが必要です。

`pkg:/service/network/ftp` などのパッケージはユーザーアカウントを作成します。ラベル付きゾーン内で `pkg` コマンドを実行してこのパッケージをインストールするには、ゾーン内で別個の `nscd` デーモンが実行されていることと、ゾーンに排他的 IP アドレスが割り当てられていることが必要です。詳細は、59 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。

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、このセクションは省略できます。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 用の LDAP の構成」を参照してください。

Trusted Extensions での監査の計画

デフォルトで監査は有効です。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。61 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。詳細は、『Oracle Solaris 11.2 での監査の管理 』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 と監査」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 ソフトウェアは、ユーザーに対して適切なセキュリティーデフォルトを提供します。このようなセキュリティーデフォルト設定を表1-2「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」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`	`15`
	`CRYPT_ALGORITHMS_ALLOW`	`1,2a,md5,5,6`
	`CRYPT_DEFAULT`	`5` (`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`

注記 - `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 のインストールチームの結成

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。構成プロセスの初期に、このチームは管理役割、およびそれらの役割になれる信頼できる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、管理役割になります。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「Trusted Extensions システムの管理: 役割によるタスク区分」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。

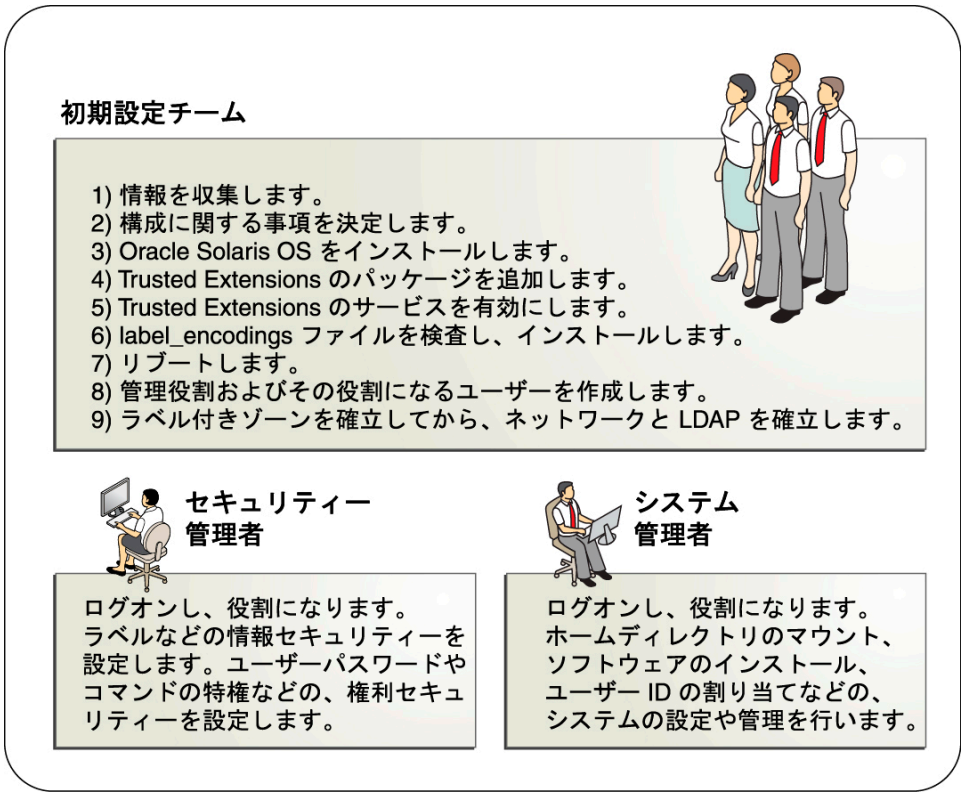
  このストラテジでは、構成プロセスは記録されません。
- 初期設定チームが root 役割をユーザーに変更します。

  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リモート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などのタスクを担当します。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などのタスクを担当します。

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、35 ページの「Trusted Extensions インストール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、およびオプションで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。

- label_encodings ファイルがインストールおよび構成されます。
- 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。
- デバイスを使用するためには、割り当てる必要があります。
- ウィンドウシステムをインストールする場合、このソフトウェアはトラステッドデスクトップ Solaris Trusted Extensions (GNOME) を作成します。このラベル付けされたウィンドウ環境により、管理ワークスペースが大域ゾーン内に提供されます。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。

  また、Trusted Extensions に、システムを管理するための GUI が表示されます。リストについては、第7章「Trusted Extensions 管理ツール」を参照してください。

♦ ♦ ♦ 第 2 章

2 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タスクについて概説します。

注意 - Trusted Extensions をリモートで有効化および構成する場合は、Trusted Extensions 環境にブートする前に第12章「Trusted Extensions でのリモート管理」をよく確認してください。

タスクマップ: 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、次のタスクを実行します。

タスク	手順
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。	35 ページの「Trusted Extensions インストール前のセキュリティー問題の解決」
Trusted Extensions を有効にします。	38 ページの「Trusted Extensions の有効化」

タスクマップ: Trusted Extensions の構成の選択

次のタスク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。

タスク	手順
デモ用の Trusted Extensions システムを作成します。	32 ページの「タスクマップ: 提供されたデフォルトを使用した Trusted Extensions の構成」

タスク	手順
企業用の Trusted Extensions システムを作成します。	32 ページの「タスクマップ: サイトの要件に応じた Trusted Extensions の構成」
リモートシステムで 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 でのリモート管理」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。
Oracle の Sun Ray サーバーの Trusted Extensions を構成します。	Sun Ray 製品ドキュメント (http://www.oracle.com/technetwork/server-storage/sunrayproducts/docs/index.html) Web サイトを参照してください。 初期クライアントサーバー通信を構成するには、229 ページの「ホストおよびネットワークへのラベル付け」を参照してください。

タスクマップ: 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、次のタスクを順番に実行します。

タスク	手順
Trusted Extensions のパッケージを読み込みます。	38 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。	38 ページの「Trusted Extensions の有効化」
ログインします。	40 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。	48 ページの「デフォルトの Trusted Extensions システムを作成する」 または 49 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。	52 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」

タスクマップ: 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。

タスクの順番は、次のタスクマップに示されています。

- 48 ページの「ラベル付きゾーンの作成」のタスクを行う必要があります。

■ サイトの要件に応じて、その他の構成タスクを実行します。

タスク	手順
大域ゾーンを構成します。	43 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。	48 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。	54 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。 **注記 -** LDAP を使用しない場合は省略してください。	第5章「Trusted Extensions 用の LDAP の構成」
システムの構成を完了します。	97 ページのTrusted Extensions の管理

♦ ♦ ♦ 第 3 章

3 Oracle Solaris への Trusted Extensions 機能の追加

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 機能は、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。インストールが終了するまで管理者の役割と追加のユーザーは作成されないので、Trusted Extensions の有効化および構成は、少なくとも 2 人で構成される初期設定チームで行うことをお勧めします。

Trusted Extensions インストール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 システムの場合は、BIOS と GRUB メニューを保護します。
   - 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。編集手順については、44 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」を参照してください。Trusted Extensions を有効にしたあとで、かつリブート前にエンコーディングファイルをインストールするには、38 ページの「Trusted Extensions の有効化」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

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

注記 - 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。その場合、構成プロセスの初期段階でこれらの役割を作成する必要があります。独自の役割を作成したり、7 つの役割を含む armor パッケージをインストールしたり、ARMOR 役割に加えて役割を作成したりできます。ARMOR の役割については、ARMOR 標準の説明を参照してください。

   役割を使用してシステムを構成する必要がない場合、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 のインストールおよび有効化

Oracle Solaris OS では、Trusted Extensions サービス svc:/system/labeld:default はデフォルトで無効にされています。

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
- すべてのネットワーク通信
- ウィンドウプロセスも含む、すべてのプロセス

▼ 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 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: xxxxxxxx
#
```

2. **Trusted Extensions パッケージをダウンロードおよびインストールします。**

   - **マルチレベルデスクトップを実行するシステムの場合、次のパッケージをインストールします。**

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

   - **マルチレベルデスクトップを必要としないヘッドレスシステムまたはサーバーの場合、次のパッケージをインストールします。**

     ```
     # pkg install system/trusted
     # pkg install system/trusted/trusted-global-zone
     ```

3. **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
   ```

▼ Trusted Extensions の有効化

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. **端末ウィンドウで、`labeld` サービスを有効化します。**

注記 - labeladm コマンドを使用して、labeld サービスを制御します。labeld サービスを直接操作しないでください。詳細は、labeladm(1M) のマニュアルページを参照してください。

```
# labeladm enable -r
```

サービスを有効化するとき、labeladm コマンドで複数のオプションを使用できます。

-i	確認プロンプトを抑制します。
-m	エラーメッセージを syslog およびコンソールに送信します。
-n	サービスを有効にせずにコマンドをテストします。
-r	サービスの有効化をシステムのリブート後まで遅らせます。これは、以前のリリースと同じ動作です。

2. **サービスが使用可能になっていることを確認します。**

```
# labeladm info
     Labeling status: pending enable on boot
          Latest log: "/var/user/root/trusted-extensions-install-log"
Label encodings file: /etc/security/tsol/label_encodings
```

注意 - Trusted Extensions の有効化や構成をリモートで行う場合には、第12章「Trusted Extensions でのリモート管理」をよく確認してください。リモート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 システムをリモート管理用に構成しなかった場合、そのシステムにはリモートシステムから到達できません。

3. **カスタマイズしたラベルエンコーディングファイルがある場合は、ここでインストールします。**

```
# labeladm encodings path-to-encodings-file
```

4. **システムをリブートします。**

-r オプションを使用した場合は、このコマンドを実行する必要があります。

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

次の手順 40 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 38 ページの「Trusted Extensions の有効化」を完了しました。

- **Oracle Solaris の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。

  注記 - 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、セキュア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 ではセキュア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。

  - **デスクトップパッケージをインストールしなかった場合は、端末を開いて、root 役割になります。**
  - **デスクトップパッケージをインストールした場合は、次の手順を実行します。**

    a. **マウスを使用して「ステータス」ウィンドウと「Clearance」ウィンドウを閉じます。**

    b. **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。

    c. **トラステッドストライプ内でログイン名をクリックして、root 役割になります。**

       プルダウンメニューから root 役割を選択します。

セキュリティー上の考慮点

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。

- 大域ゾーンを構成する場合は、43 ページの「Trusted Extensions での大域ゾーンの設定」に進みます。
- デフォルトのシステムを構成する場合は、48 ページの「ラベル付きゾーンの作成」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 でのリモート管理」に戻ります。

♦ ♦ ♦ 第 4 章

4 Trusted Extensions の構成

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、97 ページの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、次のタスク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、48 ページの「ラベル付きゾーンの作成」に進みます。

表 4-1 Trusted Extensions での大域ゾーンの設定

タスク	説明	手順
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 11.2 でのシステムおよび接続されたデバイスのセキュリティー保護 』の「システムハードウェアアクセスの制御」
ラベルを構成します。	ラベルはサイトに合わせて構成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。	44 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」

タスク	説明	手順
IPv6 ネットワークを構成します。	Trusted Extensions IPv6 CIPSO ネットワークとの互換性を有効にします。	46 ページの「Trusted Extensions で IPv6 CIPSO ネットワークを構成する方法」
DOI を変更します。	1 でない解釈ドメイン (DOI) を指定します。	47 ページの「異なる解釈ドメインを構成する方法」
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 用の LDAP の構成」
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。	93 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。

注記 - 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、79 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」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。**

        `# labeladm encodings` *`full-pathname-of-label-encodings-file`*

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

---> VERSION = MYCOMPANY LABEL ENCODINGS  3.0 10/10/2013

---> 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、アーカイブの意味解析のコピーを出力してから、ファイルをインストールします。

```
# labeladm encodings /tmp/encodings/label_encodings2
```

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。

```
# labeladm
     Labeling status: disabled
          Latest log: ""
Label encodings file: /var/tsol/encodings/label-encodings-file
# /usr/sbin/chk_encodings -a /var/tsol/encodings/label-encodings-file | head -4
No errors found in /var/tsol/encodings/label-encodings-file

---> VERSION = MYCOMPANY LABEL ENCODINGS  3.0 10/10/2013
```

次の手順 LDAP を構成する前、または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 CIPSO ネットワークを構成する方法

IPv6 の場合、Trusted Extensions はセキュリティーラベル付けプロトコルとして CALIPSO (Common Architecture Label IPv6 Security Option) を使用します。構成は不要です。廃止された Trusted Extensions IPv6 CIPSO プロトコルを実行しているシステムと通信する必要がある場合は、この手順を実行します。ほかの CALIPSO システムと通信する場合は、この手順を実行しないでください。

注意 - IPv6 CALIPSO プロトコルを使用するシステムは、廃止された TX IPv6 CIPSO プロトコルを使用するシステムとは通信できません。これは、これらのプロトコルには互換性がないためです。

廃止された Trusted Extensions IPv6 CIPSO のオプションには、パケットの「IPv6 Option Type」フィールドに使用する IANA (Internet Assigned Numbers Authority) 番号がありません。この手順で設定するエントリは、ローカルネットワーク上で使用する番号を指定します。

始める前に 廃止された占有の Trusted Extensions IPv6 CIPSO セキュリティーラベル付けオプションを使用するシステムと通信する必要がある場合は、この手順を実行します。

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 ブート中に IPv6 CIPSO 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。たとえば、エントリのスペルが間違っている場合は、次のメッセージが表示されます:「sorry, variable 'ip6opt_1d' is not defined in the 'ip' module. Verify that the entry is spelled correctly」。

- エントリを修正します。
- /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。

次の手順 LDAP を構成する前、または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。

▼ 異なる解釈ドメインを構成する方法

サイトで 1 の解釈ドメイン (DOI) が使用されない場合は、すべての security templateで セキュリティーテンプレート 値を変更する必要があります。詳細は、216 ページの「セキュリティーテンプレートの解釈のドメイン」を参照してください。

始める前に 大域ゾーンで root 役割になっています。

- **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
```

注記 - 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
- 213 ページの「Trusted Extensions のネットワークセキュリティー属性」
- 233 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 用の LDAP の構成」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、48 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

このセクションの手順では、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。

注記 - LDAP を使用する予定の場合は、第5章「Trusted Extensions 用の LDAP の構成」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。

表 4-2 ラベル付きゾーンの作成

タスク	説明	手順
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。このコマンドは、デスクトップを持たないシステムで実行できます。	48 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。	49 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。	49 ページの「ラベル付きゾーンを対話形式で作成する」
ゾーンコマンドを使用して、ラベル付きゾーンを作成します。	ラベル付きゾーンを 1 つ作成します。この手順は、デスクトップを持たないシステムで実行できます。	53 ページの「`zonecfg` コマンドを使用してラベル付きゾーンを作成する方法」
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。この手順は、デスクトップシステムだけで動作します。	52 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.(オプション) 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。	54 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リモート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リモートホストとも通信できません。

始める前に デスクトップを持たないシステムの大域ゾーン内にいるか、40 ページの「Trusted Extensions にログインする」を完了してデスクトップにログインしています。root 役割になっています。

1. **端末ウィンドウを開きます。**

   デスクトップでは、4 番目のワークスペースを使用できます。

2. **(オプション) 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 ワークスペースから Trusted Extensions のラベル付きゾーンにアクセスする場合は、52 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 40 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 48 ページの「デフォルトの Trusted Extensions システムを作成する」、49 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、54 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。

▼ zonecfg コマンドを使用してラベル付きゾーンを作成する方法

デスクトップ上にいない場合は、通常のゾーンコマンドを使用してラベル付きゾーンを作成する必要があります。デスクトップ上にいる場合は、この方法も使用できます。-t オプションはゾーンのブランドを指定し、ラベルは明示的に設定する必要があります。詳細は、brands(5) のマニュアルページを参照してください。

1. **zonecfg コマンドを実行してラベル付きゾーンを作成します。**

詳細は、zonecfg(1M) のマニュアルページを参照してください。

この例では、public という名前のゾーンを作成します。

```
# zonecfg -t SYStsoldef -z public
```

2. **tncfg コマンドを使用してラベルを設定します。**

詳細は、tncfg(1M) のマニュアルページを参照してください。

この例では、public ゾーンにラベル public を付けます。

```
# tncfg -z public set label=PUBLIC
```

3. **zoneadm コマンドを使用して、ゾーンをインストールします。**

詳細は、zoneadm(1M) のマニュアルページを参照してください。

```
# zoneadm -z public install
```

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、23 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。次のタスクマップでは、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。

表 4-3 Trusted Extensions でネットワークインタフェースを構成するためのタスクマップ

タスク	説明	手順
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、リモートシステムとの通信に使用されます。	55 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。	55 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。	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。	56 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」

タスク	説明	手順
ゾーンは IP スタックを共有します。		
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、リモート攻撃から保護された特権付きサービスを提供できます。	56 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。	57 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」
ゾーンをリモート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リモートシステムに到達できるようにします。	58 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」
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。	59 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、49 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リモート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、58 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、49 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. **「Configure Network Interfaces」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. **「OK」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。

   注記 - 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、58 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、49 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. **「Configure Network Interfaces」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。

   注記 - 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、58 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リモート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、49 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」
- 229 ページの「ホストおよびネットワークへのラベル付け」

▼ 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。ラベル付きゾーンでは、インストールする予定のパッケージがそのラベルのユーザーアカウントを必要とする場合、ゾーンごとに個別のネームサービスを構成することができます。背景情報については、24 ページの「ラベル付きゾーンに制限されているアプリケーション」および139 ページの「Trusted Extensions でユーザーを作成する前に必要な決定事項」を参照してください。

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、49 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。

注記 - 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
   ```

   `root` 役割になってステップ 1 で Labeled Zone Manager を実行したユーザーのアカウントが、リブート後に各ゾーン内に構成されます。ラベル付きゾーンに固有のほかのアカウントは、ゾーンに手動で追加する必要があります。

注記 - LDAP リポジトリに格納されたアカウントは、引き続き大域ゾーンから管理されます。

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, 2012  10:10:12 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。

表 4-4 Trusted Extensions で役割とユーザーを作成するためのタスクマップ

タスク	説明	手順
ARMOR 役割をインストールします。	ARMOR 標準により定義される 7 つの役割を作成して、それらを割り当てます。	『Oracle Solaris 11.2 でのユーザーとプロセスのセキュリティー保護 』の「役割の作成」の最初の例
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。	62 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。	63 ページの「システム管理者役割を作成する」
管理役割になるユーザーを作成します。	役割になることができる 1 人または複数のユーザーを作成します。	64 ページの「Trusted Extensions で役割になれるユーザーを作成する」
役割が各自のタスクを実行できることを確認します。	役割をテストします。	66 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。	68 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。

   注記 - ARMOR 役割を使用する場合は、『Oracle Solaris 11.2 でのユーザーとプロセスのセキュリティー保護 』の「役割の作成」セクションの ARMOR の例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。

   注記 - 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、管理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 audit_flags=cusa:no secadmin
   ```

2. **役割の初期パスワードを提供します。**

   ```
   # passwd -r files secadmin
   New Password: xxxxxxxx
   Re-enter new Password: xxxxxxxx
   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=cusa:no 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: xxxxxxxx
Re-enter new Password: xxxxxxxx
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、64 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=cusa:no\
-K profiles="System Administrator" -K lock_after_retries=no sysadmin
```

2. **役割の初期パスワードを提供します。**

```
# passwd -r files sysadmin
```

```
New Password: xxxxxxxx
Re-enter new Password: xxxxxxxx
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。

   注記 - 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。root 役割だけが、ユーザーごとに監査フラグを設定できます。

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

   注記 - 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: xxxxxxxx
Re-enter new Password: xxxxxxxx
```

注記 - 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. **簡易認証を割り当てます。**

      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、ラベルなしの印刷、リモートからのログイン、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、153 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」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「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」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 audit_flags=lo,ex:no \
-K  idletime=8 -K idlecmd=lock -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: xxxxxxxx
Re-enter new Password: xxxxxxxx
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、62 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 またはルーティング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。**

■ **マルチレベルデスクトップを実行していないシステムで、端末ウィンドウを開きます。**

a. **その役割に切り替えます。**

```
% su - rolename
```

b. **PRIV_PFEXEC フラグが有効であることを確認します。**

```
# ppriv $$
...
flags = PRIV_PFEXEC
...
```

■ **マルチレベルデスクトップで、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ません。
- 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、204 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リモート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、70 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リモート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リモート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

注記 - デスクトップパネルを画面上部に移動した場合は、Trusted Extensions トラステッドストライプでそれらが覆われます。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

次のタスクは、Trusted Extensions システムを必要に応じて構成するのに役立ちます。最後のタスクでは、Trusted Extensions 機能を Oracle Solaris から削除できます。

表 4-5 追加の Trusted Extensions 構成のタスクマップ

タスク	説明	手順
サイトのセキュリティーについてユーザーに通知します。	ログイン時にセキュリティーメッセージを表示します。	『Oracle Solaris 11 セキュリティーガイドライン 』の「バナーファイルにセキュリティーメッセージを配置する方法」 『Oracle Solaris 11 セキュリティーガイドライン 』の「セキュリティーメッセージをデスクトップログイン画面に配置する方法」
既存のゾーンと同じラベルで動作するサービスを含めるために、ラベル付きゾーンを作成します。	プライマリゾーンと同じラベルでセカンダリゾーンを作成します。	74 ページの「セカンダリラベル付きゾーンを作成する方法」
すべてのラベルのディレクトリおよびファイルを保持するデータセットを作成します。	最小限のオーバーヘッドでファイルのラベルを変更できるデータセットを作成し、マウントします。	75 ページの「マルチレベルのデータセットを作成および共有する方法」
各ラベルでホームディレクトリサーバーを作成します。	ラベルごとに 1 つずつ、複数のホームディレクトリサーバーを作成します。または、マルチレベルのホームディレクトリサーバーを作成します。	68 ページの「Trusted Extensions でホームディレクトリサーバーを作成する」

タスク	説明	手順
役割になれる初期ユーザーを作成します。	役割になったときにシステムの管理を任せるユーザーを作成します。	64 ページの「Trusted Extensions で役割になれるユーザーを作成する」
Trusted Extensions を削除します。	Trusted Extensions およびすべての信頼できるデータをシステムから削除します。また、Trusted Extensions を実行するための Oracle Solaris システムの準備も行います。	80 ページの「 Trusted Extensions をシステムから削除する」

▼ セカンダリラベル付きゾーンを作成する方法

セカンダリラベル付きゾーンは、サービスを異なるゾーンに分離し、しかも同じラベルで実行できるようにする場合に役立ちます。詳細は、176 ページの「プライマリおよびセカンダリラベル付きゾーン」を参照してください。

始める前に プライマリゾーンが存在する必要があります。セカンダリゾーンは排他的 IP アドレスを持つ必要があり、デスクトップを要求することはできません。

大域ゾーンで `root` 役割になっている必要があります。

1. **セカンダリゾーンを作成します。**

   コマンド行またはラベル付きゾーン GUI `txzonemgr` を使用できます。

   - **コマンド行を使用します。**

     ```
     # tncfg -z secondary-label-service primary=no
     # tncfg -z secondary-label-service label=public
     ```

   - **`txzonemgr` を使用します。**

     ```
     # txzonemgr &
     ```

     新規ゾーンの作成に移動し、プロンプトに従います。

   注記 - ネットマスクは接頭辞形式で入力する必要があります。たとえば、`255.255.254.0` ネットマスクと同等の接頭辞は `/23` です。

2. **ゾーンがセカンダリゾーンであることを確認します。**

   ```
   # tncfg -z zone info primary
   primary=no
   ```

例 4-6 Public スクリプト用のゾーンの作成

この例では、管理者は、スクリプトとバッチジョブを実行するために設計された Public ゾーンを分離します。

```
# tncfg -z public-scripts primary=no
# tncfg -z public-scripts label=public
```

▼ マルチレベルのデータセットを作成および共有する方法

マルチレベルのデータセットは、情報をダウングレードまたはアップグレードするときに役立つコンテナです。詳細は、194 ページの「ファイルのラベル変更に使用されるマルチレベルのデータセット」を参照してください。また、マルチレベルの NFS ファイルサーバーが多数の NFS クライアントにさまざまなラベルでファイルを提供する場合にも、マルチレベルのデータセットが役立ちます。

始める前に マルチレベルのデータセットを作成するには、大域ゾーンで `root` 役割になる必要があります。

1. **マルチレベルのデータセットを作成します。**

   ```
   # zfs create -o mountpoint=/multi -o multilevel=on rpool/multi
   ```

   `rpool/multi` は大域ゾーンの `/multi` にマウントされたマルチレベルのデータセットです。

   データセットのラベル範囲の上限を制限するには、例4-7「`ADMIN_HIGH` より低い最上位のラベルでマルチレベルのデータセットを作成する」を参照してください。

2. **マルチレベルのデータセットがマウントされていることと、そのマウントポイントに `ADMIN_LOW` ラベルが付いていることを確認します。**

   ```
   # getlabel /multi
   /multi: ADMIN_LOW
   ```

3. **親ファイルシステムを保護します。**

   プール内のすべてのファイルシステムについて、次の ZFS プロパティーを `off` に設定します。

   ```
   # zfs set devices=off rpool/multi
   # zfs set exec=off rpool/multi
   # zfs set setuid=off rpool/multi
   ```

4. **(オプション) プールの圧縮プロパティーを設定します。**

ZFS では通常、圧縮はファイルシステムのレベルで設定されます。ただし、このプール内のファイルシステムはすべてデータファイルなので、圧縮はプールのトップレベルのデータセットで設定されます。

```
# zfs set compression=on rpool/multi
```

『Oracle Solaris 11.2 での ZFS ファイルシステムの管理 』の「ZFS の圧縮、複製解除、暗号化のプロパティー間の関連」も参照してください。

5. **マルチレベルのデータセットに含める各レベルの最上位ディレクトリを作成します。**

```
# cd /multi
# mkdir public internal
# chmod 777 public internal
# setlabel PUBLIC public
# setlabel "CNF : INTERNAL" internal
```

6. **アクセスを承認されている各ラベル付きゾーンに、マルチレベルのデータセットを LOFS でマウントします。**

たとえば、次の一連の `zonecfg` コマンドは、データセットを `public` ゾーンにマウントします。

```
# zonecfg -z public
zonecfg:public> add fs
zonecfg:public:fs> set dir=/multi
zonecfg:public:fs> set special=/multi
zonecfg:public:fs> set type=lofs
zonecfg:public:fs> end
zonecfg:public> exit
```

マルチレベルのデータセットでは、マウント先ゾーンと同じラベルのファイルの書き込みと、下位レベルのファイルの読み取りが許可されます。マウントされたファイルのラベルは、表示と設定が可能です。

7. **NFS を使用してマルチレベルのデータセットをほかのシステムと共有するには、次のようにします。**

   a. **大域ゾーンの NFS サービスをマルチレベルサービスにします。**

```
# tncfg -z global add mlp_private=2049/tcp
# tncfg -z global add mlp_private=111/udp
# tncfg -z global add mlp_private=111/tcp
```

   b. **NFS サービスを再起動します。**

```
# svcadm restart nfs/server
```

c. **マルチレベルのデータセットを共有します。**

```
# share /multi
```

NFS でマウントされたマルチレベルのデータセットでは、マウント先ゾーンと同じラベルのファイルの書き込みと、下位レベルのファイルの読み取りが許可されます。マウントされたファイルのラベルは、確実に表示することや設定することはできません。詳細は、195 ページの「別のシステムのマルチレベルデータセットのマウント」を参照してください。

例 4-7 ADMIN_HIGH より低い最上位のラベルでマルチレベルのデータセットを作成する

この例では、管理者はデフォルトの ADMIN_HIGH より低い上限 (最上位ラベル) で、マルチレベルのデータセットを作成します。データセットの作成時に、管理者はこのラベル上限を mslabel プロパティーで指定します。この上限により、大域ゾーンのプロセスはマルチレベルのデータセット内にファイルやディレクトリを作成できなくなります。ラベル付きゾーンだけが、データセット内にディレクトリやファイルを作成できます。multilevel プロパティーが on なので、mslabel プロパティーで設定されるのは上限であり、シングルラベルデータセットのラベルではありません。

```
# zfs create -o mountpoint=/multiIUO -o multilevel=on \
   -o mlslabel="CNF : INTERNAL" rpool/multiIUO
```

次に、管理者は各ラベル付きゾーンにログインし、マウントされたデータセット内にゾーンのラベルでディレクトリを作成します。

```
# zlogin public
# mkdir /multiIUO
# chmod 777 /multiIUO
# zlogin internal
# mkdir /multiIUO
# chmod 777 /multiIUO
```

マルチレベルのデータセットは、マウント先ゾーンのリブート後、承認されたユーザーにそのゾーンのラベルで表示されます。

次の手順 ユーザーがファイルのラベルを変更できるようにするには、184 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。

ファイルのラベルを変更する手順については、『Trusted Extensions ユーザーズガイド 』の「マルチレベルデータセットのデータをアップグレードする方法」および『Trusted Extensions ユーザーズガイド 』の「マルチレベルデータセットのデータをダウングレードする方法」を参照してください。

▼ 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。

注記 - 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。**
   たとえば、次のコマンドは JAZ 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割り当てます。

   ```
   # allocate rmdisk0
   ```

   ウィンドウシステムで、デバイスマネージャーを使用できます。ファイルブラウザを 2 つ開いて、デバイスからディスクにファイルをドラッグします。詳細は、『Trusted Extensions ユーザーズガイド 』の「Trusted Extensions でデバイスを割り当てる」を参照してください。

2. **デバイスの割り当てを解除します。**

   ```
   # deallocate rmdisk0
   ```

   デバイスマネージャーを使用してデバイスの割り当てを解除する場合は、『Trusted Extensions ユーザーズガイド 』の「Trusted Extensions でデバイスの割り当てを解除する」を参照してください。

注記 - 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 4-8 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 \
/export/commonfiles
```

管理者は、CD を CD-ROM ドライブに挿入して割り当てます。

```
# allocate cdrom0
```

ファイルを CD に転送したあとで、管理者は Trusted Path 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。**

   ```
   # allocate cdrom0
   ```

   ウィンドウシステムで、デバイスマネージャーを使用できます。詳細は、『Trusted Extensions ユーザーズガイド 』の「Trusted Extensions でデバイスを割り当てる」を参照してください。

2. **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/policy.conf /etc/security/policy.conf.orig
   ```

3. **ファイルを割り当てられたメディアからディスク上の場所にコピーしてから、転送します。**

   たとえば、policy.conf ファイルを転送します。

   ```
   # cp /dev/rdsk/cdrom0/trusted/* /tmp
   # cp /tmp/policy.conf /etc/security/policy.conf
   ```

4. **デバイスの割り当てを解除します。**

   ```
   # deallocate cdrom0
   ```

デバイスマネージャーから割り当てを解除する場合は、『Trusted Extensions ユーザーズガイド 』の「Trusted Extensions でデバイスの割り当てを解除する」を参照してください。

5. **メディアを取り出します。**

```
# eject cdrom0
```

▼ 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 ゾーンの作成と使用 』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。**

```
# labeladm disable -r
```

   詳細は、`labeladm`(1M) のマニュアルページを参照してください。

4. **(オプション) システムをリブートします。**

5. **システムを構成します。**

   基本的なネットワーク処理、ネームサービス、ファイルシステムマウントなどのさまざまなサービスを、Oracle Solaris システム用に構成することが必要な場合があります。

♦ ♦ ♦ 第 5 章

5 Trusted Extensions 用の LDAP の構成

この章では、Trusted Extensions で使用するために Oracle Directory Server Enterprise Edition (LDAP サーバー) を構成する方法について説明します。LDAP サーバーは、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。末尾のセクション、92 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。

LDAP サーバーの構成には、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*のタスクマップの手順に従います。

- 81 ページの「Trusted Extensions ネットワークでの LDAP の構成」
- 82 ページの「Trusted Extensions システムでの LDAP プロキシサーバーの構成」

Trusted Extensions ネットワークでの LDAP の構成

表 5-1 Trusted Extensions ネットワークで LDAP を構成するためのタスクマップ

タスク	説明	手順
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 LDAP サーバーにします。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。	83 ページの「LDAP サーバーの情報を収集する」 84 ページの「Oracle Directory Server Enterprise Edition をインストールする」 87 ページの「Oracle Directory Server Enterprise Edition のログを構成する」
Trusted Extensions データベースをサーバーに追加します。	Trusted Extensions システムファイルのデータを LDAP サーバーに入力します。	89 ページの「Oracle Directory Server Enterprise Edition にデータを入力する」

タスク	説明	手順
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。	93 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

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、このタスクマップを使用します。

表 5-2 Trusted Extensions システムで LDAP プロキシサーバーを構成するためのタスクマップ

タスク	説明	手順
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。	89 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。	91 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。	89 ページの「Oracle Directory Server Enterprise Edition のマルチレベルポートを構成する」
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。	93 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 LDAP サーバー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。

注記 - この LDAP サーバーを NFS サーバーまたは Sun Ray クライアント用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 サーバーの情報を収集する

- **次の項目の値を決定します。**

  各項目は、システム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	アクションまたは情報
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ー DN	デフォルト値は「`cn=Directory Manager`」です。
ディレクトリマネージャーパスワード	「`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。
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。
接尾辞	「`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「このサーバーに構成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。
管理ポート	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 パッケージは、Oracle Web サイト (http://www.oracle.com/technetwork/middleware/id-mgmt/overview/index-085178.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、パスワード操作およびパスワードポリシーを決定するクライアント用に構成されます。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 11.2 でのシステムおよび接続されたデバイスのセキュリティー保護 』の「パスワード情報の管理」を参照してください。`pam.conf`(4) のマニュアルページも参照してください。

注記 - 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。

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

2. **Oracle Directory Server Enterprise Edition パッケージを Oracle Web サイト (http://www.oracle.com/technetwork/middleware/id-mgmt/overview/index-085178.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。**

   83 ページの「LDAP サーバーの情報を収集する」からの情報を使って質問に答えます。質問の完全なリスト、デフォルト、および推奨される回答については、『Oracle Solaris 11.2 ディレクトリサービスとネームサービスでの作業: LDAP 』の第 4 章「Oracle Directory Server Enterprise Edition への LDAP クライアントの設定」および『Oracle Solaris 11.2 ディレ

クトリサービスとネームサービスでの作業: LDAP 』の第 5 章「LDAP クライアントの設定」を参照してください。

4. **(オプション) 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. **(オプション) `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. **ブートするたびに 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. **インストールを検証します。**

```
# 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 11.2 ディレクトリサービスとネームサービスでの作業: LDAP 』の第 6 章「LDAP のトラブルシューティング」を参照してください。

▼ LDAP サーバー用 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 LDAP サーバーにデータを入力します。このタスクは、LDAP サーバー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 LDAP サーバーを使用することも、別個のシステムに Trusted Extensions を追加することもできます。手順については、第3章「Oracle Solaris への Trusted Extensions 機能の追加」を参照してください。

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 11.2 ディレクトリサービスとネームサービスでの作業: LDAP 』の「enableShadowUpdate スイッチ」および 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. **(オプション) さらにログを構成します。**

   ログごとに次の構成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構成する

Trusted Extensions で作業するには、LDAP サーバー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) として構成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. **端末ウィンドウで、`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、およびリモートシステムに関する 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、LDAP サーバーデータベースに 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、86 ページの「LDAP サーバー用 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 LDAP サーバー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、229 ページの「ホストおよびネットワークへのラベル付け」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 LDAP サーバーに 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 LDAP サーバー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、86 ページの「LDAP サーバー用 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、89 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 が構成されているシステムで、プロキシサーバーを作成します。**

   注記 - 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 11.2 ディレクトリサービスとネームサービスでの作業: LDAP 』の第 5 章「LDAP クライアントの設定」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 11.2 ディレクトリサービスとネームサービスでの作業: LDAP 』の第 6 章「LDAP のトラブルシューティング」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。

注記 - 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 LDAP サーバーが存在しなければなりません。Trusted Extensions データベースのデータがサーバーに入力されていて、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、LDAP サーバー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、サービスをリフレッシュします。**

   ```
   # 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、ステップ 2 からステップ 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について」では、Trusted Extensions の固定の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」では、Trusted Extensions 管理の概要を説明します。

第10章「Trusted Extensions のユーザー、権利、および役割について」では、Trusted Extensions での役割ベースのアクセス制御 (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」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 でのリモート管理」では、Trusted Extensions のリモート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」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」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」では、Trusted Extensions でのネットワークデータベースやルーティング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」では、Trusted Extensions でネットワークデータベースやルーティングを管理する手順を示します。

第17章「Trusted Extensions および LDAP について」では、Trusted Extensions でのメール固有の問題について説明します。

第18章「Trusted Extensions のマルチレベルメールについて」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」では、Trusted Extensions で印刷を処理する手順を示します。

第20章「Trusted Extensions のデバイスについて」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機能について説明します。

第21章「Trusted Extensions のデバイスの管理」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 と監査」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」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

6 Trusted Extensions の管理の概念

この章では、Trusted Extensions 機能が構成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、暗号化、およびストレージも含め、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 をオーバーライドできません。

  Oracle Solaris OS と同様に、MAC のオーバーライドを許可する場合は、セキュリティーポリシーをオーバーライド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 が構成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、マルチレベルバージョンの Oracle Solaris デスクトップである Solaris Trusted Extensions (GNOME) を提供します。この名前は Trusted GNOME に短縮できます。
- 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 CLI 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。

- ウィンドウ環境では、Trusted Extensions は管理用 GUI を提供します。たとえば、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、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構成されている場合、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。モニターを垂直に構成すると、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。

ただし、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

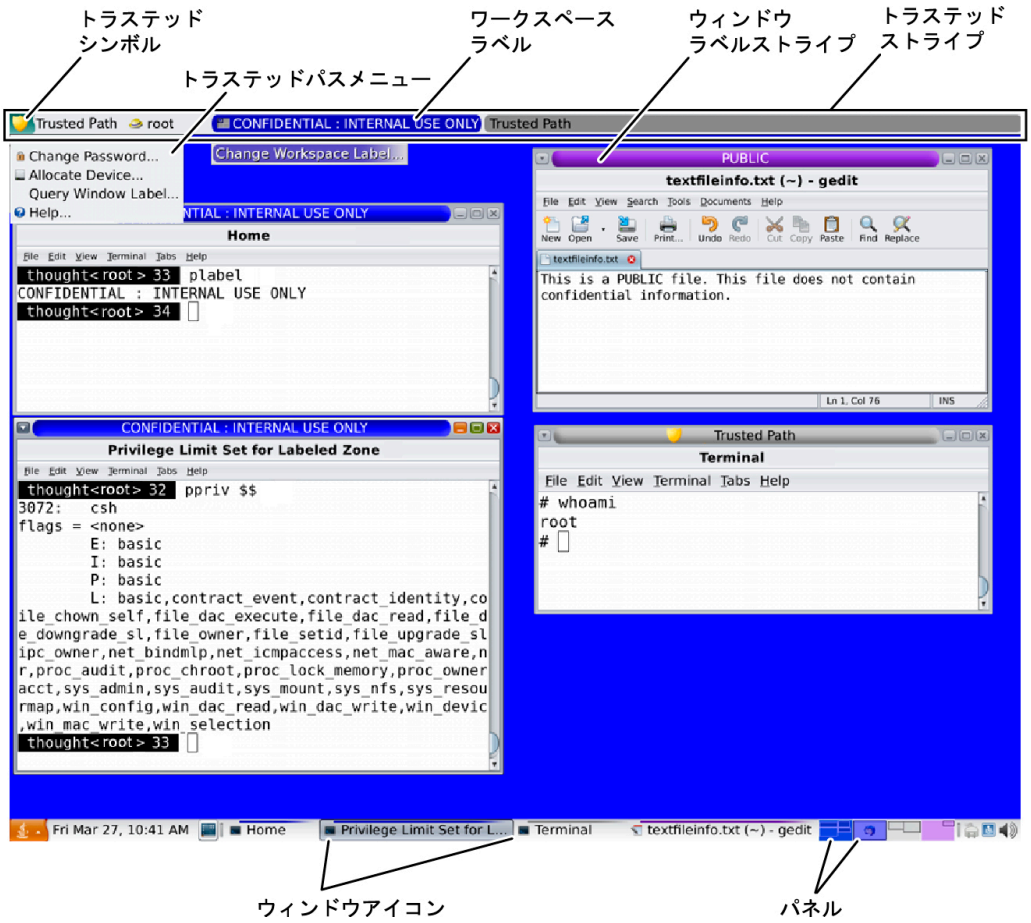
Trusted Extensions ソフトウェアにより、Oracle Solaris システムにラベルが追加されます。また、ラベル付きワークスペースと、ラベルビルダーやデバイスマネージャーなどのトラステッドアプリケーションも追加されます。このセクションで説明する概念は、ユーザーと管理者の両方にとって、Trusted Extensions を理解するために必要な知識です。『Trusted Extensions ユーザーズガイド 』でも、これらの概念をユーザーを対象として説明しています。

Trusted Extensions の保護

Trusted Extensions ソフトウェアは Oracle Solaris OS の保護を強化します。Trusted Extensions は、ユーザーと役割を承認されたラベル範囲に限定します。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 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「Trusted Extensions マルチレベルデスクトップ」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 ソフトウェアを必要とします。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、随意アクセス制御 (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` および `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。Oracle Solaris の提供する特殊なアクセス権 *privileges* および *authorizations* により、MAC と DAC の両方をオーバーライドできます。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

ラベルおよび認可上限は、Trusted Extensions の必須アクセス制御 (MAC) の中心にあります。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	関係	ラベル 2
NEED_TO_KNOW Eng Mkt	(完全に) 優位	INTERNAL Eng Mkt

ラベル 1	関係	ラベル 2
NEED_TO_KNOW Eng Mkt	(完全に) 優位	NEED_TO_KNOW Eng
NEED_TO_KNOW Eng Mkt	(完全に) 優位	INTERNAL Eng
NEED_TO_KNOW Eng Mkt	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。元のファイルは、/etc/security/tsol ディレクトリにあります。Trusted Extensions が有効になると、このファイルの場所は labeld サービスのプロパティーとして格納されます。セキュリティー管理者は、サイトの label_encodings ファイルを構成します。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** – 印刷出力の印刷バナー、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。

minimum-label ≤ *permitted-label* ≤ *clearance*

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、印刷出力など、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」および『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「Trusted Extensions マルチレベルデスクトップ」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 を使用して構成されたシステムでは、`root` 以外のいくつかの役割によりシステムが管理されます。通常は、システム管理者役割とセキュリティー管理者役割が管理機能を実行します。場合によっては、初期設定後に `root` 役割が管理できます。デスクトップシステムでは、ユーザーが役割を引き受けるとワークスペースが役割ワークスペースに変化します。

Trusted Extensions で役割が使用可能なプログラムは、特殊なプロパティーである*トラステッドパス属性*を保持します。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。権利プロファイルと役割については、『Oracle Solaris 11.2 でのユーザーとプロセスのセキュリティー保護 』の第 1 章「権利を使用したユーザーとプロセスの制御について」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 が構成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、役割だけが使用できます。

役割ワークスペース内のデスクトップシステムで、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。コマンド行ツールは、デスクトップを実行していないシステムで使用できます。

表 7-1 Trusted Extensions 管理ツール

ツール	説明	参照先
`/usr/sbin/labeladm`	Trusted Extensions を有効および無効にします。 ラベルエンコーディングファイルのインストールにも使用されます。	37 ページの「Trusted Extensions のインストールおよび有効化」、44 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」、および `labeladm`(1M) のマニュアルページを参照してください。

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。	48 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。
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303 ページの「Trusted Extensions でのデバイスの扱い」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、155 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 ユーザーズガイド 』の「ラベルの異なるウィンドウ間でデータを移動する方法」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、ゾーンおよびネットワークの構成ツールであり、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、すべてのゾーンを 1 つずつ削除するよう求められます。
- 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。このスクリプトは IPv4 および IPv6 アドレスを処理します。

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、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 のデバイスの管理」を参照してください。

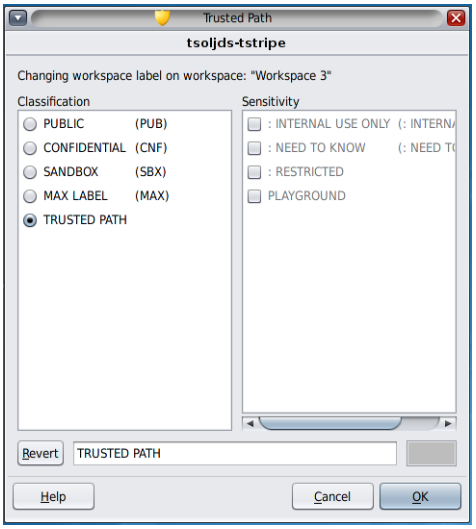
Trusted Extensions の選択マネージャー

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、ラベルビルダーはデスクトップログイン時に表示されます (『Trusted Extensions ユーザーズガイド 』の第 2 章「Trusted Extensions へのログイン」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 `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。

注記 - 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について

この章では、Trusted Extensions が構成されたシステムの、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、通常ある制限された役割になることでシステムを管理するという点です。

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。

- 役割作成の概要については、『Oracle Solaris 11.2 でのユーザーとプロセスのセキュリティー保護 』の「ユーザーへの権利の割り当て」を参照してください。
- 役割を作成するには、61 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 11.2 での監査の管理 』の第 3 章「監査サービスの管理」で説明しています。

注記 - *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** – 役割と権利プロファイルの追加については、『Oracle Solaris 11.2 でのユーザーとプロセスのセキュリティー保護 』の第 3 章「Oracle Solaris での権利の割り当て」で説明しています。
- **承認** – 新しい承認の追加例については、312 ページの「Trusted Extensions でのデバイス承認のカスタマイズ」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。
- **「選択マネージャー」ダイアログボックス** – マルチレベルセッションの承認されたユーザーは、情報を別のラベルにアップグレードまたはダウングレードできます。

- **TrustedExtensionsPolicy ファイル** – 管理者は Trusted Extensions に固有の X サーバー拡張のポリシーを変更できます。詳細は、TrustedExtensionsPolicy(4) のマニュアルページを参照してください。

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。各役割を果たすようにユーザーにトレーニングを実施する必要があります。評価された構成の要件に矛盾しないように、このセクション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。

電子メールの使用のガイドライン

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、このファイルを読み取ることができるのは `root` 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。

グループの管理について

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プライマリグループとして所有するユーザーはすべて、別のプライマリ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。詳細は、125 ページの「`sel_config` ファイル」および `sel_config`(4) のマニュアルページを参照してください。
- `/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`

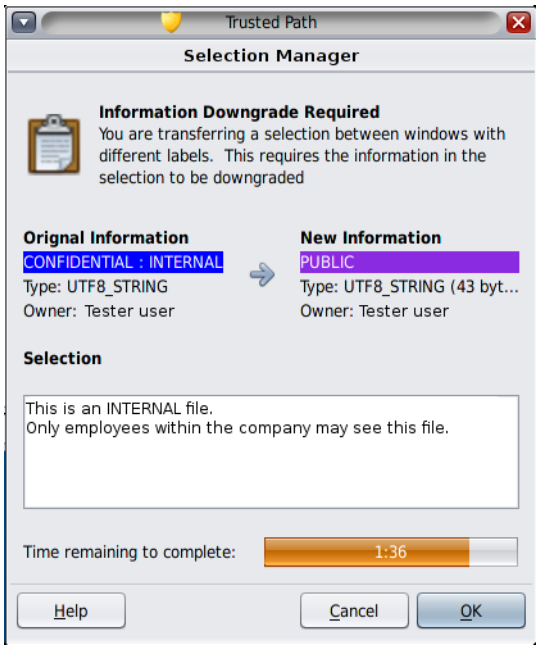
ウィンドウ内やファイル内の選択範囲には、異なる規則が適用されます。「選択範囲」のドラッグ & ドロップでは、常にラベルと所有者が同じである必要があります。ウィンドウ間のドラッグ & ドロップは、`sel_config` ファイルではなく、選択マネージャーアプリケーションを介して行われます。

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

ウィンドウシステムでは、Trusted Extensions にラベル変更を仲介するための選択マネージャーが用意されています。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マネージャーが表示されます。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セクション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、選択マネージャー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
- 「選択マネージャー」ダイアログボックスを表示するかどうか

♦ ♦ ♦ 第 9 章

9 Trusted Extensions での一般的なタスク

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。

デスクトップシステムで Trusted Extensions 管理者として作業を開始する

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。

表 9-1 Trusted Extensions デスクトップへのログインおよび使用

タスク	説明	手順
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 ユーザーズガイド 』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 ユーザーズガイド 』の「ラベル付きシステムでの作業」
トラステッドパスを必要とするタスクを実行します。	次のタスクが含まれます。 ■ デバイスの割り当て ■ パスワードの変更 ■ ワークスペースのラベルの変更	『Trusted Extensions ユーザーズガイド 』の「トラステッドアクションの実行」
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」

タスク	説明	手順
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 で大域ゾーンを終了する方法」

▼ 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、151 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「Trusted Extensions マルチレベルデスクトップ」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 ユーザーズガイド 』の第 4 章「Trusted Extensions の要素」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 で大域ゾーンを終了する方法

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 ユーザーズガイド 』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 での一般的なタスクの実行

次のタスクマップでは、Trusted Extensions での一般的な管理手順について説明します。

表 9-2 Trusted Extensions で一般的な管理タスクを実行するためのタスクマップ

タスク	説明	手順
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「デスクトップシステムで root のパスワードを変更する方法」
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。	134 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 11.2 でのシステムおよび接続されたデバイスのセキュリティー保護 』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 ユーザーズガイド 』の「Trusted Extensions でデバイスを割り当てる」
システム構成ファイルを変更します。	Trusted Extensions および Oracle Solaris のデフォルトのセキュリティー値を変更します。	134 ページの「システムファイルでセキュリティーデフォルトを変更する」
システムをリモートで管理します。	リモートシステムから Trusted Extensions システムを管理します。	第12章「Trusted Extensions でのリモート管理」

▼ デスクトップシステムで root のパスワードを変更する方法

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 を構成する場合は、第5章「Trusted Extensions 用の LDAP の構成」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、59 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、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
```

注記 - 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 エラーメッセージ `atohexlabel parsing error found in <string> at position 0` 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示します。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

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 11.2 でのシステムおよび接続されたデバイスのセキュリティー保護 』の第 3 章「システムアクセスの制御」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 大域ゾーンにいて、`solaris.admin.edit/`*filename* 承認が割り当てられています。デフォルトでは、`root` 役割がこの承認を持っています。

- **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。最初の 2 つのファイルは、Trusted Extensions に固有のものです。

ファイル	タスク	参照先
/usr/share/gnome/ 内の sel_config	情報が別のラベルに移動されるときにシステムがどのように動作するかを指定します。	sel_config(4) のマニュアルページ
/usr/lib/xorg/ 内の TrustedExtensionsPolicy	X サーバーのラベル分離の SUN_TSOL セキュリティーポリシーの実施を変更します。	TrustedExtensionsPolicy(4) のマニュアルページ
/etc/default/login	パスワード試行の許容回数を減らします。	passwd(1) のマニュアルページ
/etc/default/kbd	キーボードでの停止を無効にします。	『Oracle Solaris 11.2 でのシステムおよび接続されたデバイスのセキュリティー保護 』の「システムのアボートシーケンスを無効にする方法」 **注記 -** 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

10 Trusted Extensions のユーザー、権利、および役割について

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、61 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 11.2 のユーザーアカウントとユーザー環境の管理 』の「CLI を使用したユーザーアカウントの設定と管理のタスクマップ」
- 『Oracle Solaris 11.2 でのユーザーとプロセスのセキュリティー保護 』

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構成されています。デフォルトの説明については、140 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、317 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、312 ページの「Trusted Extensions でのデバイス承認のカスタマイズ」を参照してください。
- ラベル付きゾーンで個別にユーザーアカウントを作成する必要があるかどうかを決定します。

  デフォルトでは、ラベル付きゾーンは大域ゾーンのネームサービス構成を共有します。したがって、ユーザーアカウントは大域ゾーンで作成され、すべてのゾーンに使用されます。ラベル付きゾーンの `/etc/passwd` ファイルと `/etc/shadow` ファイルは、大域ゾーンのファイルの読み取り専用表示です。同様に、ラベル付きゾーンでは LDAP データベースは読み取り専用です。

  ゾーン内からゾーンにアプリケーションをインストールする場合は、`pkg:/service/network/ftp` などのユーザーアカウントの作成が必要になることがあります。ゾーン固有のアプリケーションがユーザーアカウントを作成できるようにするには、59 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」の説明に従って、ゾーンごとのネームサービスデーモンを構成する必要があります。そのようなアプリケーションによってラベル付きゾーンに追加されたユーザーアカウントは、ゾーン管理者が手動で管理する必要があります。

注記 - LDAP に格納されたアカウントは、引き続き大域ゾーンから管理されます。

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をオーバーライドします。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、141 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、20 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` ファイルの値をオーバーライドします。

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	使用可能な値	注意事項
IDLECMD	LOCK	LOCK | LOGOUT	ログインユーザーに適用されます。
IDLETIME	15	0 - 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をオーバーライドします。

26 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、140 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	アクションの要/不要	割り当ての効果
パスワード	なし	必須	ユーザーにパスワードが設定されます
役割	なし	オプション	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	オプション	ユーザーに追加承認が割り当てられます

ユーザー属性	デフォルト値の設定場所	アクションの要/不要	割り当ての効果
権利プロファイル	policy.conf ファイル	オプション	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	オプション	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	オプション	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	オプション	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	オプション	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。

注記 - 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。スケーラビリティーを確保するため、承認を権利プロファイルに追加し、プロファイルをユーザーに割り当てます。

権利プロファイルの割り当て

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 11.2 でのユーザーとプロセスのセキュリティー保護 』の「割り当てられた権利の検索順序」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。

注記 - 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、154 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。監査の詳細は、『Oracle Solaris 11.2 での監査の管理 』および第22章「Trusted Extensions と監査」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                 .cshrc                  .mime_types
.aliases                .emacs                  .newsrc
.bashrc                 .login                  .signature
.bashrc.user            .mailrc                 .soffice
```

♦ ♦ ♦ 第 11 章

11 Trusted Extensions でのユーザー、権利、役割の管理

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

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、次のタスク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。

表 11-1 セキュリティーのためにユーザー環境をカスタマイズするためのタスクマップ

タスク	説明	手順
ラベル属性を変更します。	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。	147 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「システムのアイドル設定の変更」
	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「各ユーザーの基本的な特権セットの修正」
	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「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」

タスク	説明	手順
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。	151 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。追加の Trusted Extensions システムのインストール時に、変更されたエンコーディングファイルを使用します。

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「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」の26 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. **アクティブなエンコーディングファイルのコピーを編集します。**

   a. **アクティブなファイルを検出します。**

   ```
   # labeladm encodings
   Label encodings file: /var/tsol/encodings/label_encodings.fSaG.L
   ```

   b. **アクティブなファイルのコピーを編集します。**

   ```
   # cp /var/tsol/encodings/label_encodings.fSaG.L /tmp/tmp-encodings
   # pfedit /tmp/tmp-encodings
   ```

3. **システムのラベルエンコーディングファイルを置き換えて、システムをリブートします。**

   ```
   # labeladm encodings /tmp/tmp-encodings
   # /usr/sbin/reboot
   ```

4. **Trusted Extensions システムごとに、この手順を繰り返します。**

注意 - アクティブなラベルエンコーディングファイルの内容は、すべてのシステムで同一である必要があります。

▼ policy.conf のデフォルトを修正する

Trusted Extensions で policy.conf のデフォルトを変更する方法は、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「policy.conf ファイル内の Trusted Extensions セキュリティーのデフォルト」を参照してください。

2. **設定を変更します。**

```
# pfedit /etc/security/policy.conf
```

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 Sun Ray インストールのセキュリティー管理者が、一般ユーザーにほかの Sun Ray ユーザーのプロセスを表示できないようにします。そこで、Trusted Extensions によって構成されている各システムで、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。次のブート以降、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することができます。また、ユーザーの最小ラベルで既存の .copy_files および .link_files ファイルを修正することもできます。この手順は、管理者役割がサイトの設定を自動化するためのものです。

始める前に 大域ゾーンで、システム管理者役割になっている必要があります。詳細は、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。**

      ```
      # pfedit /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「ユーザーの起動ファイルのカスタマイズ」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。**

      ```
      # pfedit /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 11.2 のユーザーアカウントとユーザー環境の管理 』の「ユーザーの作業環境について」を参照してください。
   - 詳細は、『Oracle Solaris 11.2 のユーザーアカウントとユーザー環境の管理 』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. **(オプション) 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内で、管理者はカスタマイズを追加します。

```
## .cshrc file
setenv EDITOR emacs
setenv ETOOLS /net/tools/etools

## .ksh file
export EDITOR emacs
export ETOOLS /net/tools/etools
```

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

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。次のタスクマップでは、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タスクについて説明します。

表 11-2 ユーザーと権利を管理するためのタスクマップ

タスク	説明	手順
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。	153 ページの「便利な承認のための権利プロファイルを作成する」
ユーザーのデフォルト特権セットを修正します。	ユーザーのデフォルトの特権セットから特権を削除します。	154 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、アカウントロックをオフにします。	155 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。	155 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。	156 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、147 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 11.2 でのユーザーとプロセスのセキュリティー保護 』の「権利プロファイルを作成する方法」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` – リモートログイン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 11.2 でのユーザーとプロセスのセキュリティー保護 』の「ユーザーへの権利の割り当て」を参照してください。

▼ ユーザーの特権セットを制限する

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

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。

- **`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 11.2 でのユーザーとプロセスのセキュリティー保護 』の「権利プロファイルを作成する方法」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「各ユーザーの基本的な特権セットの修正」 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、184 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。

- **適切なユーザーと役割に Object Label Management 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 11.2 でのユーザーとプロセスのセキュリティー保護 』の「ユーザーへの権利の割り当て」を参照してください。

例 11-5 ユーザーがファイルのラベルのアップグレードはできるがダウングレードはできないようにする

Object Label Management 権利プロファイルにより、ユーザーはラベルのアップグレードとダウングレードを行うことができます。この例では、管理者は信頼できるユーザーにデータのアップグレードを許可しますが、ダウングレードは禁止します。

管理者は Object Label Management プロファイルに基づいて権利プロファイルを作成し、この新しいプロファイルの「ファイルラベルのダウングレード」承認と「DragNDrop または CutPaste 情報のダウングレード」承認を削除します。

```
# profiles -p "Object Label Management"
profiles:Object Label Management> set name="Object Upgrade"
profiles:Object Upgrade> info auths
...
profiles:Object Upgrade> remove auths="solaris.label.file.downgrade,
solaris.label.win.downgrade"
profiles:Object Upgrade> commit
profiles:Object Upgrade> end
```

次に、管理者は信頼できるユーザーにこのプロファイルを割り当てます。

```
# usermod -P +"Object Upgrade" jdoe
```

▼ 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。**

   注記 - 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、123 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

12 Trusted Extensions でのリモート管理

この章では、Trusted Extensions システムをリモート管理可能用に設定する方法と、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。

注記 - ヘッドレスシステムやその他のリモート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、19 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 でのリモート管理

リモート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リモート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リモート管理は行えません。

ネットワークが構成されるまでは、すべてのリモートホストに `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リモート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 以外のリモート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リモート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リモート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 ユーザーによるリモートログインは禁止されます。
- 2 つのデフォルトの PAM 値によってリモート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リモート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、大域ゾーンへのリモート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リモート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、リモート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 でのリモートシステムの管理方式

Trusted Extensions では、Secure Shell プロトコルとホストベースの認証を使用してリモートシステムに到達し、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リモート 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、Secure Shell クライアントは、元のユーザー名と役割名の両方をリモート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、次のリモート管理方式が可能です。

- **Trusted Extensions システムからの管理** – もっともセキュアなリモート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「リモート管理のための CIPSO ホストタイプの割り当て」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 スタックで `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、245 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` 役割を使用してリモート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、コマンド行からリモート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 サーバーでリモート 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、リモート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「リモートアクセス用に Xvnc で Trusted Extensions システムを構成する」を参照してください。

Trusted Extensions でのリモートシステムの構成および管理

リモート管理を有効にしたあと、かつリモート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。

表 12-1 Trusted Extensions でリモートシステムを構成および管理するためのタスクマップ

タスク	説明	手順
Trusted Extensions システムのリモート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「リモート Trusted Extensions システムのリモート管理を有効にする」
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、リモート 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「リモートアクセス用に Xvnc で Trusted Extensions システムを構成する」

タスク	説明	手順
Trusted Extensions システムにリモートでログインします。	リモートシステム上の役割になってそのシステムを管理します。	167 ページの「リモート Trusted Extensions システムにログインして管理する」

注記 - 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リモート管理の方法を判定します。

▼ リモート Trusted Extensions システムのリモート管理を有効にする

この手順では、ある Oracle Solaris リモート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。リモートシステムは Secure Shell サーバーです。

始める前に リモートシステムに 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。`root` 役割になっている必要があります。

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 11.2 での Secure Shell アクセスの管理 』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。

   注記 - `cat` コマンドは使用しないでください。Secure Shell 接続経由で公開鍵をコピー&ペーストします。Secure Shell 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 Secure Shell 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. **Secure Shell サーバーで、`ssh` ポリシーを引き下げて `root` がリモートログインを行えるようにします。**

   ```
   # pfedit /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。

注記 - 管理者は root 役割になるので、リモート 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. **Secure Shell サーバーで ssh サービスを再起動します。**

```
# svcadm restart ssh
```

4. **Secure Shell 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
# pfedit .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. **Secure Shell サーバーで 2 つの PAM ポリシーを引き下げます。**

   a. **/etc/pam.d/other を /etc/pam.d/other.orig にコピーします。**

```
# cp /etc/pam.d/other /etc/pam.d/other.orig
```

   b. **pam_roles エントリを変更して、役割によるリモートログインを許可します。**

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

   c. **pam_tsol_account エントリを変更して、ラベルなしホストから Trusted Extensions リモートシステムへの接続を許可します。**

```
# pfedit /etc/pam.d/other
# Default definition for Account management
# Used when service name is not explicitly mentioned for account management
# ...
#account requisite    pam_roles.so.1
```

```
# Enable remote role assumption
account requisite    pam_roles.so.1   allow_remote
#
account required     pam_unix_account.so.1
#account required     pam_tsol_account.so.1
# Enable unlabeled access to TX system
account required     pam_tsol_account.so.1  allow_unlabeled
```

6. **この構成をテストします。**

   a. **リモート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、リモートシステム上の** `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、リモートシステムで Trusted Extensions を有効にし、リブートします。**

```
# svcadm enable -s labeld
# /usr/sbin/reboot
```

例 12-1 リモート管理のための 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リモート 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*

管理者がラベルなしシステムからリモート Trusted Extensions ホストを構成できるようにするため、管理者はリモートホストの `pam.d/other` ファイル内に `allow_unlabeled` オプションを残します。

▼ リモートアクセス用に 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、クライアントをリモートサーバーに接続し、クライアントのウィンドウにリモートサーバーのデスク

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、245 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。**

```
# pkg search vnc
... set    VNC client based on the TigerVNC open source release that
           displays a session over RFB protocol from a VNC server
           pkg:/desktop/remote-desktop/tigervnc@version
... set    X Window System server based on X.Org Foundation open source
           release and TigerVNC open source release that displays over
           RFB protocol to a VNC client
           pkg:/x11/server/xvnc@version
...
```

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。

```
# pkg install server/xvnc
# pkg install remote-desktop/tigervnc
```

注記 - GUI を開くことができない場合は、ローカルの root アカウントを X サーバーのアクセス制御リストに追加します。X サーバーにログインしたユーザーでこのコマンドを実行します。

```
% xhost +si:localuser:root
```

詳細は、xhost(1) および Xsecurity(5) のマニュアルページを参照してください。

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。**

   ヒント - Xsession ファイルの変更を行う前に元のコピーを保存します。

   ```
   DISPLAY=unix:$(echo $DISPLAY|sed -e s/::ffff://|cut -d: -f2)
   ```

   ステップ 2 およびステップ 3 のファイルには、パッケージ属性 preserve=true が付いています。パッケージのアップグレードおよびパッケージの修正の際に、変更したファイルがこの属性によって受ける影響については、pkg(5) のマニュアルページを参照してください。

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. **(オプション) VNC 接続を監査します。**

   システム別およびユーザー別の監査イベントの事前選択については、『Oracle Solaris 11.2 での監査の管理 』の「監査サービスの構成」を参照してください。

9. **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 ユーザーズガイド 』の「Trusted Extensions へのログイン」を参照してください。

例 12-2 テスト環境で Vino を使用してデスクトップを共有する

この例では、2 人の開発者が GNOME Vino サービスを使用して「起動」->「システム」->「設定」->「デスクトップの共有」メニューからディスプレイを共有しています。前述の手順に加えて、XTEST 拡張を有効することによって Trusted Extensions ポリシーを引き下げます。

```
# pfedit /usr/X11/lib/X11/xserver/TrustedExtensionsPolicy
## /usr/X11/lib/X11/xserver/TrustedExtensionsPolicy file
...
#extension XTEST
extension XTEST
...
```

▼ リモート 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 を使用してリモート Trusted Extensions システムを管理できます。

始める前に 162 ページの「リモート Trusted Extensions システムのリモート管理を有効にする」の説明に従って、ローカルシステム上とリモート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、リモート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リモート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: xxxxxxxx
   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: xxxxxxxx
   ```

   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リモート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12-3「リモートシステムでのラベル付きゾーンの構成」を参照してください。

例 12-3 リモートシステムでのラベル付きゾーンの構成

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リモートシステム上のラベル付きゾーンを構成します。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: xxxxxxxx
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: xxxxxxxx
```

同じ端末で、管理者は remoterole 役割として txzonemgr GUI を起動します。

```
TXnohead4 # /usr/sbin/txzonemgr &
```

Labeled Zone Manager はリモート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 12-4 リモートラベル付きゾーンへのログイン

管理者は、リモートシステム上の 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。

- 大域ゾーンにリモートログインしてリモート大域ゾーンのワークスペースを表示したあと、ワークスペースを 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 ゾーンにリモートログインしたあと、ファイルを編集します。

リモート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*そのリモート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、リモート PUBLIC 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。リモート 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

13 Trusted Extensions でのゾーンの管理

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。各ラベルに 1 つ以上の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。

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 システムでは、すべてのゾーンが *labeled* というブランドを持ち、ラベル付きゾーン内の書き込み可能なファイルおよびディレクトリはすべてゾーンと同じラベルになります。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、別個の 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リモート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」および193 ページの「`mlslabel` プロパティーとシングルレベルのファイルシステムのマウント」を参照してください。

Trusted Extensions 内のゾーンは、Oracle Solaris ゾーン製品上に構築されています。参照情報については、『Oracle Solaris ゾーンの紹介 』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23 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。説明については、『Oracle Solaris ゾーンの紹介 』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。このガイドでは、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、サイト固有のドキュメント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リモート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、250 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は、次の条件下でリモートファイルシステムを読み取り/書き込み権付きでマウントできます。

- マウントする側のシステムには、リモート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リモートファイルシステムをマウントする必要があります。

  システムはリモート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、202 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。

プライマリおよびセカンダリラベル付きゾーン

特定のラベルで最初に作成するゾーンはプライマリラベル付きゾーンです。そのラベルは一意です。そのラベルでほかのプライマリゾーンを作成することはできません。

セカンダリゾーンは、プライマリゾーンと同じラベルのゾーンです。セカンダリゾーンを使用すると、同じラベルの別個のゾーンにサービスを分離することができます。そのようなサービスでは、ネームサーバー、プリンタ、データベースなどのネットワークリソースを、特権を使用せずに共有できます。同じラベルで複数のセカンダリゾーンを作成できます。

具体的には、セカンダリゾーンはプライマリゾーンとは次のように異なっています。

- セカンダリゾーンのラベル割り当ては一意でなくてもかまいません。
- セカンダリゾーンでは排他的 IP ネットワークを使用する必要があります。

  この制限により、ラベル付きパケットが確実に正しいゾーンに到達します。
- セカンダリゾーンに GNOME パッケージはインストールされません。

  セカンダリゾーンは GNOME トラステッドデスクトップには表示されません。
- セカンダリゾーンを `setlabel` コマンドの宛先ゾーンに指定することはできません。

  同じラベルのゾーンが複数存在する場合、このコマンドは宛先ゾーンを解決できません。

どのラベルでも、プライマリラベル付きゾーンは最大で 1 つ、セカンダリラベル付きゾーンは任意の数だけ作成できます。ただし、大域ゾーンは例外です。`ADMIN_LOW` ラベルを割り当てることができるゾーンは 1 つだけなので、セカンダリゾーンは作成できません。セカンダリゾーンの作成については、74 ページの「セカンダリラベル付きゾーンを作成する方法」および `zenity`(1) 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。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

次のタスクマップでは、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。

表 13-1 ゾーンを管理するためのタスクマップ

タスク	説明	手順
すべてのゾーンを表示します。	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。	178 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を表示します。	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。	178 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。	180 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。	181 ページの「下位ファイルのマウントを無効にする」
ファイルのラベルを変更するためにマルチレベルのデータセットを作成します。	1 つの ZFS データセットのファイルのラベルを変更できるようにします。特権は必要ありません。	75 ページの「マルチレベルのデータセットを作成および共有する方法」
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。	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。	184 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。	182 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」。
新しいプライマリ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。	49 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。
セカンダリゾーンを構成します。	デスクトップを必要としないサービスを分離するためにゾーンを作成します。	74 ページの「セカンダリラベル付きゾーンを作成する方法」。

タスク	説明	手順
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。	250 ページの「ゾーンにマルチレベルポートを作成する」 例16-22「udp 経由 NFSv3 用のプライベートマルチレベルポートの構成」
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。	205 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 ゾーンの作成と使用 』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. **ウィンドウシステム上で、`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. **`zoneadm list -v` コマンドも使用できます。**

```
# 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。ゾーンが再起動したら、一般ユーザーは passwd ファイル内のエントリを表示できます。

```
# 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。特定ゾーンのすべての下位レベルファイルの表示を禁止するには、そのゾーンから 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

この例では、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、ゾーンがブート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ブートします。**

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

ゾーンがブートすると、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、155 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み許可する

この例では、セキュリティー管理者は `zonecfg` コマンドを使用して、`CNF: INTERNAL USE ONLY` ゾーンの情報のダウングレードを許可しますが、アップグレードは禁止します。

```
# zonecfg -z internal set limitpriv=default,file_downgrade_sl
```

例 13-6 `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

14 Trusted Extensions でのファイルの管理とマウント

この章では、ファイルの共有およびマウントの際の Trusted Extensions ポリシーと、このポリシーがマルチレベルのデータセットの ZFS マウントおよびシングルレベルの ZFS データセットの LOFS マウントと NFS マウントに与える影響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 で可能なマウント

Trusted Extensions は、2 種類の ZFS データセットをマウントできます。

- *シングルレベルのラベル付きデータセット*は、そのデータが配置またはマウントされているゾーンと同じラベルを持ちます。シングルレベルのデータセット内のファイルとディレクトリは、すべて同じラベルになります。このようなデータセットは、Trusted Extensions の典型的なデータセットです。
- *マルチレベルのデータセット*は、異なるラベルのファイルとディレクトリを含むことができます。このようなデータセットは、多くの異なるラベルで NFS クライアントにサービスを効率よく提供し、ファイルのラベル変更処理の効率を高めることができます。

Trusted Extensions では、次のマウントが可能です。

- **ZFS マウント** – 管理者が作成するマルチレベルのデータセットは、大域ゾーンに ZFS でマウントできます。ZFS でマウントされたマルチレベルのデータセットは、同じシステムのラベル付きゾーンに LOFS でマウントできます。

  シングルレベルのデータセットも、管理者が作成してラベル付きゾーンに ZFS でマウントすることができます。

- **LOFS マウント** – 前の段落で説明したとおり、大域ゾーンはシングルレベルのデータセットをラベル付きゾーンに LOFS でマウントすることができます。マウントのラベルは `ADMIN_LOW` なので、ラベル付きゾーンにマウントされたファイルはすべて読み取り専用になります。

  大域ゾーンは、マルチレベルのデータセットをラベル付きゾーンに LOFS でマウントすることもできます。ゾーンと同じラベルでマウントされたファイルは変更可能です。適切なアクセス権があれば、ファイルはラベル変更可能です。ゾーンのラベルより低いレベルにマウントされたファイルは表示可能です。

- **NFS マウント** – ラベル付きゾーンは、シングルレベルのデータセットをそのゾーンのラベルでマウントすることができます。このようなファイルは、別のラベル付きゾーンからのもの、あるいは、ラベル付きゾーンと同じラベルが割り当てられた信頼できないシステムからのものである可能性があります。

  大域ゾーンは、別の Trusted Extensions システムからマルチレベルのデータセットを NFS でマウントすることができます。マウントされたファイルは、表示と変更が可能ですが、ラベル変更はできません。また、マウント先ゾーンと同じラベルのファイルおよびディレクトリだけが、正しいラベルを返します。

  ラベル付きゾーンは、別の Trusted Extensions システムからマルチレベルのデータセットを NFS でマウントすることができます。NFS でマウントされたファイルはラベル変更できず、ファイルのラベルを `getlabel` コマンドで判定できません。ただし、MAC ポリシーは正しく動作します。ゾーンと同じラベルでマウントされたファイルは、表示と変更が可能です。下位レベルのファイルは表示可能です。

マウントされたファイルシステムに対する Trusted Extensions ポリシー

Trusted Extensions は Oracle Solaris と同じファイルシステムおよびファイルシステム管理コマンドをサポートしていますが、Trusted Extensions にマウントされるファイルシステムは、ラベル付きデータの表示と変更に関する必須アクセス制御 (MAC) ポリシーに従います。マウントポリシーおよび読み取りと書き込みのポリシーにより、ラベル付けに関する MAC ポリシーが適用されます。

シングルレベルのデータセットに対する Trusted Extensions ポリシー

シングルレベルのデータセットの場合、マウントポリシーにより、MAC に違反する NFS マウントや LOFS マウントが回避されます。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。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、その所有者のラベルでマウントされます。

NFS でマウントされたシングルレベルのデータセットの動作は、次のようにまとめられます。

- 大域ゾーンでは、マウントされたすべてのファイルが表示可能ですが、変更可能なのはラベル `ADMIN_HIGH` の付いたファイルだけです。
- ラベル付きゾーンでは、そのゾーンのラベル以下でマウントされたすべてのファイルが表示可能ですが、変更可能なのはゾーンのラベルのファイルだけです。
- 信頼できないシステムでは、その信頼できないシステムに割り当てられたラベルと同じラベルを持つラベル付きゾーンからのファイルシステムのみ、表示と変更が可能です。

LOFS でマウントされたシングルレベルのデータセットの場合、マウントされたファイルは表示可能です。それらはラベル `ADMIN_LOW` なので変更できません。

マルチレベルのデータセットに対する Trusted Extensions ポリシー

マルチレベルのデータセットの場合、MAC 読み取りおよび書き込みポリシーが、ファイルシステム単位ではなく、ファイルおよびディレクトリ単位で適用されます。

マルチレベルのデータセットは大域ゾーンにのみマウントできます。ラベル付きゾーンは、`zonecfg` コマンドで指定された LOFS マウントポイントを使用して、マルチレベルのデータセットにアクセスできます。手順については、75 ページの「マルチレベルのデータセットを作成および共有する方法」を参照してください。大域ゾーンまたはラベル付きゾーンのプロセスは、適切な権限が付与されていれば、ファイルとディレクトリのラベルを変更できます。ラベル変更の例については、『Trusted Extensions ユーザーズガイド 』を参照してください。

- 大域ゾーンでは、マルチレベルのデータセット内のすべてのファイルが表示可能です。ラベル `ADMIN_HIGH` の付いたマウントされたファイルは変更可能です。

- ラベル付きゾーンでは、マルチレベルのデータセットは LOFS 経由でマウントされます。ゾーンと同じラベルまたはより低いレベルでマウントされたファイルは、表示可能です。ゾーンと同じラベルでマウントされたファイルは変更可能です。
- マルチレベルのデータセットは、大域ゾーンから NFS 経由で共有することもできます。リモートクライアントは、そのネットワークラベルのほうが優位であるファイルを表示でき、等しいラベルの付いたファイルを変更できます。ただし、NFS でマウントされたマルチレベルのデータセットのラベルを変更することはできません。NFS マウントについては、195 ページの「別のシステムのマルチレベルデータセットのマウント」を参照してください。

詳細は、194 ページの「ファイルのラベル変更に使用されるマルチレベルのデータセット」を参照してください。

MAC 読み取り/書き込みポリシーには特権のオーバーライドなし

ファイルの読み取りと書き込みに関する MAC ポリシーには、特権のオーバーライドがありません。シングルレベルのデータセットを読み取り/書き込み権付きでマウントできるのは、ゾーンのラベルがデータセットのラベルと等しい場合だけです。読み取り専用マウントの場合、ゾーンのラベルがデータセットのラベルより優位であることが必要です。マルチレベルのデータセットの場合、すべてのファイルとディレクトリよりも `mlslabel` プロパティーのほうが優位でなければなりません。このプロパティーのデフォルト値は `ADMIN_HIGH` です。マルチレベルのデータセットの場合、MAC ポリシーはファイルおよびディレクトリのレベルで適用されます。MAC ポリシーの適用はどのユーザーにも表示されません。ユーザーは、オブジェクトに対する MAC アクセスを持っていないかぎり、そのオブジェクトを表示できません。

シングルレベルのデータセットに対する Trusted Extensions の共有ポリシーとマウントポリシーは、次のようにまとめられます。

- 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` タイプのリモートホストテンプレートを持っている必要があります。
- Trusted Extensions システムが信頼できないシステムのファイルシステムをマウントできるようにするためには、Trusted Extensions システムによって信頼できないシステムに割り当てられたシングルラベルが、大域ゾーン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信頼できない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 システムによって信頼できないシステムに割り当てられたシングルラベルが、マウント先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が LOFS でマウントされた場合、そのファイルは表示はできますが、変更はできません。NFS マウントの詳細については、196 ページの「Trusted Extensions での NFS サーバーとクライアントの構成」を参照してください。

マルチレベルのデータセットに対する Trusted Extensions の共有ポリシーとマウントポリシーは、次のようにまとめられます。

- Trusted Extensions システムがマルチレベルのデータセットを別のシステムと共有できるためには、NFS サーバーがマルチレベルサービスとして構成されている必要があります。
- Trusted Extensions システムがマルチレベルのデータセットをラベル付きゾーンと共有できるためには、大域ゾーンがゾーン内でデータセットを LOFS でマウントする必要があります。

  ラベル付きゾーンは、LOFS でマウントされたこれらのファイルとディレクトリのうち、ラベルがゾーンのラベルと一致するものに対しては書き込みアクセス、ゾーンのラベルのほうが優位であるファイルとディレクトリに対しては読み取りアクセスを行うことができます。MAC ポリシーはファイルおよびディレクトリのレベルで適用されます。

Trusted Extensions でのファイルシステムの共有とマウントの結果

Trusted Extensions では、共有ファイルによって管理が簡単になり、効率と速度を向上させることができます。MAC は常に適用されます。

- ラベル付きゾーンのシングルレベルのデータセットを NFS 経由で共有する– Oracle Solaris と同様に、共有ディレクトリによって管理が簡単になります。たとえば、Oracle Solaris のマニュアルページを 1 つのシステムにインストールし、マニュアルページのディレクトリをほかのシステムと共有することができます。
- 大域ゾーンのマルチレベルのデータセットを LOFS 経由で共有する – LOFS でマウントされたデータセットにより、あるラベルから別のラベルにファイルを移動する際の効率と速度が向上します。ファイルはデータセット内で移動されるため、入出力操作は使用されません。
- 大域ゾーンのマルチレベルのデータセットを NFS 経由で共有する – NFS サーバーは、多くのラベルのファイルを含むマルチレベルのデータセットを多くのクライアントに対して共有することができます。このような構成では、管理が簡単になり、単一の場所でファイルを配布で

きます。特定のラベルのクライアントにサービスを提供するために、そのラベルのサーバーが必要になるわけではありません。

大域ゾーンでのファイルの共有とマウント

大域ゾーンでのファイルのマウントは、MAC ポリシーに従う Oracle Solaris でのファイルのマウントと同じです。大域ゾーンから共有されたファイルは、そのファイルのラベルで共有されます。したがって、すべてのファイルがラベル ADMIN_LOW で共有されるため、大域ゾーンのファイルシステムをほかの Trusted Extensions システムの大域ゾーンと共有することは有用ではありません。大域ゾーンがほかのシステムと共有することで役立つファイルは、マルチレベルのデータセットです。

大域ゾーンから LOFS 経由で共有されたシングルレベルのデータセットのファイルとディレクトリは、ADMIN_LOW で共有されます。たとえば、大域ゾーンの /etc/passwd ファイルと /etc/shadow ファイルを、システム上のラベル付きゾーン内に LOFS でマウントできます。ファイルは ADMIN_LOW なので、ラベル付きゾーンで表示され、読み取り専用です。マルチレベルのデータセットのファイルとディレクトリは、そのオブジェクトのラベルで共有されます。

大域ゾーンは、マルチレベルのデータセットを NFS 経由で共有することもできます。NFS サービスがマルチレベルポートを使用するように構成されている場合、クライアントはこのデータセットのマウントをリクエストすることができます。クライアントのラベルが、クライアントの NFS マウントリクエストを処理するネットワークインタフェースの cipso テンプレートに指定されているラベル範囲内にある場合、このリクエストは成功します。

具体的には、大域ゾーンおよびマウントされたファイルの動作は、次のようになります。

- Trusted Extensions クライアント上の大域ゾーンでは、共有に含まれるものはすべて読み取り可能で、ローカルの大域ゾーンのプロセスと同様に、クライアントは ADMIN_HIGH で書き込むことができます。
- クライアントがラベル付きゾーンの場合、そのゾーンのラベルが共有ファイルのラベルと一致していれば、マウントされたファイルは読み取り/書き込み可能です。
- クライアントがラベルなしシステムの場合、そのクライアントに割り当てられたラベルが共有ファイルのラベルと一致していれば、マウントされたファイルは読み取り/書き込み可能です。
- ラベル ADMIN_LOW のクライアントはデータセットをマウントできません。
- マルチレベルのデータセットを同じシステム上のラベル付きゾーンと共有するには、大域ゾーンで LOFS を使用します。

NFS マウント上のファイルの表示とラベル変更の詳細は、195 ページの「別のシステムのマルチレベルデータセットのマウント」を参照してください。

非大域ゾーンでのファイルの共有とマウント

ラベル付きゾーンのファイルは、ほかのシステムとそのゾーンのラベルで共有することができます。したがって、ラベル付きゾーンのファイルシステムは、ほかの Trusted Extensions システム上にある同じラベルのゾーン、および同じラベルが割り当てられている信頼できないシステムと共有することができます。これらのマウントを仲介する ZFS プロパティーについては、193 ページの「mslabel プロパティーとシングルレベルのファイルシステムのマウント」を参照してください。

大域ゾーンからラベル付きゾーンへの LOFS マウントは、シングルレベルのデータセットの場合は読み取り専用になります。190 ページの「MAC 読み取り/書き込みポリシーには特権のオーバーライドなし」で説明されているとおり、マルチレベルのデータセットの場合、MAC ポリシーはファイルおよびディレクトリのラベルごとに適用されます。

mslabel プロパティーとシングルレベルのファイルシステムのマウント

ZFS で提供されるセキュリティーラベルプロパティー mslabel には、データセット内のデータのラベルが含まれます。mslabel 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。

mslabel 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 mslabel プロパティーが未定義の場合は、mslabel 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、mslabel 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、次のような構文を使用します。

```
# 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。

ファイルのラベル変更に使用されるマルチレベルのデータセット

マルチレベルの ZFS データセットには、異なるラベルのファイルとディレクトリが含まれます。ファイルとディレクトリにはそれぞれ個別にラベルが付けられ、ファイルの移動やコピーを行うことなくラベルを変更することができます。ファイルのラベルは、データセットのラベル範囲内で変更できます。マルチレベルのデータセットの作成と共有については、75 ページの「マルチレベルのデータセットを作成および共有する方法」を参照してください。

通常は、データセット内のすべてのファイルとディレクトリに、データセットがマウントされているゾーンと同じラベルが付けられます。このラベルは、データセットがゾーン内で最初にマウントされたときに、`mlslabel` という ZFS プロパティーに自動的に記録されます。このようなデータセットは*シングルレベルのラベル付きデータセット*です。データセットがマウントされている間は `mlslabel` プロパティーを変更することはできないため、マウント先ゾーンは `mlslabel` プロパティーを変更できません。

`mlslabel` プロパティーが設定されたあとは、ゾーンのラベルがデータセットの `mlslabel` プロパティーと一致しないかぎり、ゾーン内でデータセットを読み取り/書き込み権付きでマウントすることはできません。さらに、大域ゾーンも含めいずれかのゾーンに現在 ZFS マウントされているデータセットは、ほかのゾーンに ZFS マウントできません。シングルレベルのラベル付きデータセットに含まれるファイルのラベルは固定なので、`setlabel` コマンドでファイルのラベルを変更すると、ファイルはターゲットラベルに対応するプライマリゾーン内の同等のパス名に実際に移

動されます。このようなゾーン間の移動は、効率の低下や混乱を招くことがあります。マルチレベルのデータセットは、データのラベルを変更するための効率のよいコンテナになります。

大域ゾーンにマウントされたマルチレベルのデータセットの場合、`mslabel` プロパティーのデフォルト値は `ADMIN_HIGH` です。この値は、データセットのラベル範囲の上限を指定します。より低いラベルを指定した場合、ゾーンからデータセットに書き込むことができるのは、そのゾーンのラベルよりも `mslabel` プロパティーのほうが優位である場合だけです。

Object Label Management 権利プロファイルが割り当てられたユーザーまたは役割には、自分が DAC アクセス権を持っているファイルやディレクトリを、アップグレードまたはダウングレードする適切な特権があります。手順については、155 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。

ユーザープロセスに対しては、追加のポリシー制約が適用されます。

- デフォルトでは、ラベル付きゾーンのプロセスはファイルやディレクトリのラベルを変更できません。ラベル変更を有効にするには、184 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。ファイルのダウングレードは許可するがアップグレードは許可しないなど、より詳細な制御を指定するには、例13-5「`internal` ゾーンからのダウングレードのみ許可する」 を参照してください。
- ディレクトリが空でない場合、そのラベルを変更することはできません。
- ファイルおよびディレクトリは、それを含んでいるディレクトリのラベルより下にダウングレードすることはできません。

  ラベルを変更するには、下位レベルのディレクトリにファイルを移動してから、ラベルを変更します。
- データセットをマウントしているゾーンは、ファイルやディレクトリをゾーンのラベルより上にアップグレードすることはできません。
- ファイルがいずれかのゾーンでプロセスによって現在開かれている場合、そのラベルを変更することはできません。
- ファイルおよびディレクトリは、データセットの `mslabel` 値より上にアップグレードできません。

別のシステムのマルチレベルデータセットのマウント

大域ゾーンは、マルチレベルのデータセットを NFS 経由で Trusted Extensions システムおよびラベルなしシステムと共有できます。データセットは、大域ゾーンとラベル付きゾーン、およびラ

ベルなしシステムにその割り当てられているラベルでマウントできます。ADMIN_LOW ラベルなしシステムは例外です。これはマルチレベルのデータセットをマウントできません。

マルチレベルのデータセットが ADMIN_HIGH より低いラベルで作成されている場合、そのデータセットを別の Trusted Extensions システムの大域ゾーンにマウントできます。ただし、ファイルは大域ゾーン内で表示できますが、変更はできません。ラベル付きゾーンが別のシステムの大域ゾーンからマルチレベルのデータセットを NFS でマウントする場合は、いくつかの制限が適用されます。

- NFS でマウントされたマルチレベルのデータセットには、いくつかの制限が適用されます。
- Trusted Extensions の NFS クライアントは、書き込み可能なファイルに関してのみ、正しいラベルを表示できます。getlabel コマンドでは、下位レベルのファイルのラベルが、クライアントと同じラベルとして誤って報告されます。MAC ポリシーが有効になっているため、これらのファイルは読み取り専用のままになり、上位レベルのファイルは表示されません。
- クライアントが持っている特権は、NFS サーバーではすべて無視されます。

これらの制限のため、自分の大域ゾーンからサービスを提供されているラベル付きゾーンのクライアントには、LOFS を使用することをお勧めします。このようなクライアントに対して NFS は機能しますが、クライアントは制限を受けます。LOFS マウントの手順については、75 ページの「マルチレベルのデータセットを作成および共有する方法」を参照してください。

Trusted Extensions での NFS サーバーとクライアントの構成

上位レベルのゾーンのユーザーが下位レベルのディレクトリを表示できるようにすることができます。下位レベルのディレクトリの NFS サーバーは、Trusted Extensions システムか信頼できないシステムです。

トラステッドシステムにはサーバー構成が必要です。信頼できないシステムにはクライアント構成が必要です。

- **トラステッドシステムの NFS サーバー構成** – トラステッドシステムの下位レベルのディレクトリをラベル付きゾーンで表示できるようにするには、サーバーを構成する必要があります。
  - NFS サーバーの大域ゾーンで、NFS サービスをマルチレベルサービスとして構成する必要があります。
  - 大域ゾーンから、net_bindmlp 特権をラベル付きゾーンの limitpriv 特権セットに追加する必要があります。

- ラベル付きゾーンで、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。ラベル付きゾーンのステータスが `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、202 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。

- **信頼できない NFS サーバーの NFS クライアント構成** – サーバーは信頼されていないため、NFS クライアントは信頼できるクライアントでなければなりません。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、204 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。

注記 - `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 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、198 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。

注記 - 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、156 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、リモート 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、69 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リモート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ブートすると、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。

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16-22「udp 経由 NFSv3 用のプライベートマルチレベルポートの構成」を参照してください。

Trusted Extensions システムはそのシングルレベルのデータセットをラベルなしホストと共有することもできます。ラベルなしホストにエクスポートされたファイルシステムは、そのラベルが、エクスポート元のシステムによってそのリモートホスト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リモート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。

大域ゾーンがマルチレベルのデータセットを NFSv4 サービスを実行しているクライアントと共有している場合、MAC ポリシーはデータセット全体のラベルではなく、個々のファイルおよびディレクトリ単位で適用されます。

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 Solaris システムがシングルレベルおよびマルチレベルのデータセットにアクセスできるかどうかは、そのシステムに割り当てられたラベルによって決まります。

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。リモート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。

ラベル付きファイルのバックアップ、共有、マウント

次のタスクマップでは、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。

表 14-1 ラベル付きファイルをバックアップ、共有、およびマウントするためのタスクマップ

タスク	説明	手順
ファイルをバックアップします。	ラベルを維持してデータをアーカイブします。	201 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。	バックアップからラベル付きデータを復元します。	201 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。	202 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。	204 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。このタスクによって、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。	69 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リモートホームディレクトリにアクセスできるようにする」

タスク	説明	手順
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。	181 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。	205 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。

- **次のコマンドのいずれかを実行して、ラベルを保存するバックアップを実行します。**
  - 大規模なバックアップの場合は、`zfs send -r | -R` *filesystem*`@snap`

    リモートサーバーへのバックアップの送信など、使用できる方法については、『Oracle Solaris 11.2 での ZFS ファイルシステムの管理 』の「ZFS データを送信および受信する」を参照してください。
  - 小規模バックアップの場合は、`/usr/sbin/tar cT`

    `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。
  - `zfs` または `tar` バックアップコマンドを呼び出すスクリプト

▼ 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。

- **次のコマンドのいずれかを使用して、ラベル付きバックアップを復元します。**
  - 大規模な復元の場合は、`zfs receive -vF` *filesystem*`@snap`

    リモートサーバーからのバックアップの復元など、使用できる方法については、『Oracle Solaris 11.2 での ZFS ファイルシステムの管理 』の「ZFS データを送信および受信する」を参照してください。
  - 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。

- zfs または tar 復元コマンドを呼び出すスクリプト

▼ 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ます。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 ユーザーズガイド 』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、ライター向けのドキュメント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、ゾーンをブートします。**

```
# 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 11.2 での ZFS ファイルシステムの管理 』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、204 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ドキュメント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、そのリモート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 つのリモート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信頼できないリモートホストに割り当てられています。
  - 信頼できるリモート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ます。
- 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ブート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 ユーザーズガイド 』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。
- **ゾーンのブート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. **`Step 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ステップ 1.3.a 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、リモート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

15 トラステッドネットワーク

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について

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、ラベルを付けることができます。パケットのラベルは、IP パケットの分類、分離、および経路指定を行います。ルーティングの決定では、データの機密ラベルが宛先のラベルと比較されます。

Trusted Extensions は IPv4 および IPv6 パケットのラベルをサポートします。

- IPv4 パケットの場合、Trusted Extensions は CIPSO (Commercial IP Security Option) ラベルをサポートします。
- IPv6 パケットの場合、Trusted Extensions は CALIPSO (Common Architecture Label IPv6 Security Option) ラベルをサポートします。

  IPv6 CIPSO ネットワーク上のシステムと相互運用する必要がある場合は、46 ページの「Trusted Extensions で IPv6 CIPSO ネットワークを構成する方法」を参照してください。

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 CALIPSO または CIPSO ラベルにマップされます。このラベルは IP パケットに埋め込まれ、それによってパケットは*ラベル付き*パケットになります。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、ラベルオプションが含まれます。CIPSO データパケットは IPv4 ネットワークで送信されます。CALIPSO パケットは IPv6 ネットワークで送信されます。

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。

CIPSO オプション付き IPv4 ヘッダー	TCP、UDP、または SCTP	データ

標準の IPv6 形式では、オプションを指定した 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 パケットは、セキュリティー属性として IP ヘッダーに CALIPSO オプションを使用します。

CALIPSO オプション付き IPv6 ヘッダー	TCP、UDP、または SCTP	データ

Trusted Extensions のマルチキャストパケット

Trusted Extensions は LAN 内のマルチキャストパケットにラベルを追加できます。この機能を使用すると、ラベル付きマルチキャストパケットを、そのマルチキャストパケットと同じラベルまたはラベル範囲内で動作する CIPSO または CALIPSO システムに送信できます。異機種システム混在 LAN、つまり、ラベル付きホストとラベルなしホストの両方が存在する LAN では、マルチキャストはマルチキャストグループのメンバーシップを確認できません。

注意 - 異機種システム混在 LAN ではラベル付きマルチキャストパケットを送信しないでください。ラベル付き情報の漏洩が発生する可能性があります。

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)
- IPv4 パケットの CIPSO ラベルおよび IPv6 パケットの CALIPSO 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、210 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、212 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。
- 15 ページの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」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、224 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リフレッシュします。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ルーティング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、経路のセキュリティー属性を表示するために、Oracle Solaris の `route` の使用法を拡張します。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` キーワードはオプションで、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、173 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。ただし、送信側が*適応型*ホストの場合は、受信側のネットワークインタフェースがそのデフォルトラベルを着信パケットに割り当てます。セキュリティー属性の詳細については、213 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。
- `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、リモートシステム (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、これらをリモートシステ

ムに割り当てます。リモート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、次が含まれます。

- 4 つのホストタイプ: `unlabeled`、`cipso`、`adaptive`、`netif` のいずれか。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。214 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、213 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、リモート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 が構成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、217 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 CALIPSO または 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、215 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** – オプションです。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 4 種類のホストタイプをサポートし、4 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** – ラベル付き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。このホストタイプは CALIPSO および CIPSO ラベルをサポートします。

  IPv6 の場合は、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 CALIPSO プロトコルが使用されます。IPv4 の場合は、CIPSO プロトコルが使用されます。CALIPSO および CIPSO ヘッダー内のラベルは、データのラベルから自動的に派生します。派生したラベルは、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にラベルを付けるために使用されます。

- **unlabeled ホストタイプ** – 標準ネットワークプロトコルを使用し、ラベル付き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。

- **adaptive ホストタイプ -** ラベルは付いていないが、ラベル付きシステムの特定のネットワークインタフェースにパケットを送信するホストのサブネットに使用します。ラベル付きシステムは、そのネットワークインタフェースのデフォルトラベルを着信パケットに適用します。

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、あるいは、ラベル付きシステムにデータを送信すると想定されるホストに割り当てられます。このホストタイプはデフォルトラベルを提供しません。通信のラベルは、受信側システムのラベル付きネットワークインタフェースから派生します。このホストタイプは、ゲートウェイにではなく、エンドノードのシステムに割り当てられます。

`adaptive` ホストタイプは、トラステッドネットワークの計画と拡大/縮小に柔軟性を提供します。管理者は、新しいシステムのデフォルトラベルが前もってわからなくても、新しいラベルなしシステムを使用してネットワークを拡大できます。`netif` ホストのラベル付きネットワークインタフェースにパケットを送信するように `adaptive` ホストが構成されている場合は、その `netif` ホストのインタフェースのデフォルトラベルによって、該当するラベルが着信パケットに割り当てられます。

- **`netif` ホストタイプ** – `adaptive` ホストからのパケットを特定のネットワークインタフェース上で受信するインタフェースのホスト名に使用します。このホストタイプは、Trusted Extensions システム上のインタフェースに割り当てられます。`netif` インタフェースのデフォルトラベルは、着信パケットに適用されます。

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

`unlabeled` および `netif` 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、47 ページの「異なる解釈ドメインを構成する方法」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。

- ホストがラベル付きリモート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には

  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。
- ラベル付き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には

  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、リモート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。この属性はオプションです。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「Trusted Extensions ホストアドレスと代替メカニズムのエントリ」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	192.168.118.57 192.168.118.57/32	192.168.118.57 /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
	192.168.118.0 192.168.118.0/24	192.168.118. サブネット上のすべてのアドレス。
	192.168.0.0/24	192.168.0. サブネット上のすべてのアドレス。
	192.168.0.0 192.168.0.0/16	192.168. サブネット上のすべてのアドレス。
	192.0.0.0 192.0.0.0/8	192. サブネット上のすべてのアドレス。
	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。

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
	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 Sun Ray サーバーの tnrhdb エントリを作成するには、例16-19「ラベル付き Sun Ray サーバーの有効な初期アドレスの構成」を参照してください。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16-18「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」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、245 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は、『Oracle Solaris 11.2 でのネットワーク配備の計画 』の「ネットワークの IP アドレス指定形式の決定」を参照してください。

Trusted Extensions のルーティングについて

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、動的ルーティングをサポートしません。静的なルーティングの詳細は、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。

注記 - `adaptive` ホストからのパケットを転送すると想定されるラベル付きゲートウェイは、そのインバウンドインタフェースを `netif` ホストタイプのテンプレートで構成する必要があります。`adaptive` および `netif` ホストタイプの定義については、214 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。

ルーティングに関する背景

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ルーティングしている場合、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 のルーティングでは、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 のルーティングテーブルエントリ

Trusted Extensions のルーティング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。

注記 - 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 CALIPSO または 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、ルーティング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。

注記 - 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 CALIPSO または CIPSO オプションに指定されている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次のように処理されます。
  - 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。
  - ラベル付き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。
  - `adaptive` ホストからのパケットを転送すると想定されるラベル付きゲートウェイは、そのインバウンドインタフェースを `netif` ホストタイプのテンプレートで構成する必要があります。`adaptive` および `netif` ホストタイプの定義については、214 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。

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、パケットはラベル付きオプションに指定されている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 でのルーティングの管理

Trusted Extensions は、ネットワーク間通信のルーティングを、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 とルーティングの詳細は、次のマニュアルを参照してください。

- 『Oracle Solaris 11.2 でのネットワークコンポーネントの構成と管理 』の「Oracle Solaris のネットワーク管理に関する詳細情報の参照先」
- `netcfg`(1M) のマニュアルページ

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。

- ラベル付きルーターは、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、ラベル付きルーターは、必要なラベル付きオプションが 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、ラベル付き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、ラベルを認識するゲートウェイのみが、CALIPSO または CIPSO IP オプションの内容を使用して、MAC を実施できます。

トラステッドルーティング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ルーティングテーブルが拡張されます。属性については、219 ページの「Trusted

Extensions のルーティングテーブルエントリ」を参照してください。Trusted Extensions では、ルーティングテーブルのエントリを管理者が手動で作成する、静的ルーティング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。

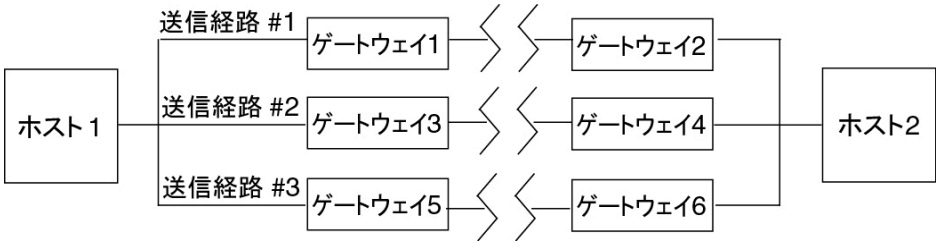
ルーティングソフトウェアは、ルーティングテーブルで宛先ホストへの送信経路を探します。ホストが明示的に定義されていない場合、ルーティングソフトウェアは、ホストが配置されているサブネットのエントリを探します。ホストとサブネットのどちらも定義されていない場合、デフォルトゲートウェイが定義されていれば、ホストはデフォルトゲートウェイにパケットを送信します。複数のデフォルトゲートウェイを定義可能で、それぞれが同等に扱われます。

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ルーティング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 のルーティング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 経路とルーティング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、ルーティング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 のルーティングコマンド

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、ルーティング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、ルーティング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、ルーティング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、ルーティング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、250 ページの「デフォルトルートを追加する」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には、CALIPSO または CIPSO IP オプションを使用します。ラベルを暗黙的に送信するには、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 11.2 でのネットワークのセキュリティー保護 』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、253 ページの「ラベル付き IPsec の構成」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、220 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 CALIPSO または 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、ラベルを認識しないネットワークやラベル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、226 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。伝送パケットにラベル付き 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。伝送パケットにラベル付き 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ラベル付き 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。

外部 IP ヘッダー	ESP または AH	内部 IP ヘッダー	TCP ヘッダー	データ

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。

外部 IP ヘッダー	UDP ヘッダー	IKE 鍵管理プロトコル

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、220 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	ラベルはラベル付き IP オプション内で可視となります。	ラベル付き 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	ラベル付き 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。 ワイヤー上のラベル付き 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、ラベル付き 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。

注記 - メッセージがネットワーク内を移動するときに、ラベルを認識するルーターがラベル付き 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ラベル付き IPオプションを保護することはできません。ラベル付き 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

16 Trusted Extensions でのネットワークの管理

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。

ホストおよびネットワークへのラベル付け

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。リモート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。

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

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、サイト固有のセキュリティーテンプレートを作成できます。

- 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。
- AD MIN_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。

- 限定された一連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。
- 指定されたラベルなしホストから、構成する信頼できるネットワークインタフェースに情報を送信して、ラベルなしホストからのパケットに正しいラベルを割り当てます。

既存のセキュリティーテンプレートの表示

リモートホストとネットワークにラベルを付ける前に、提供されているセキュリティーテンプレートを調べて、リモートホストとネットワークに到達できることを確認します。手順については、次を参照してください。

- セキュリティーテンプレートを表示します。230 ページの「セキュリティーテンプレートを表示する」を参照してください。
- 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。229 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」を参照してください。
- 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。232 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。

▼ 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。この手順で示す例では、デフォルトのセキュリティーテンプレートを使用します。

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
adapt
netif
```

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 のリモート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。

- 0.0.0.0/0 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。
- 0.0.0.0/0 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、245 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。

```
# tncfg -t adapt info
name=adapt
host_type=adapt
doi=1
min_label=ADMIN_LOW
max_label=ADMIN_HIGH
host=0.0.0.0/0
```

adapt テンプレートは adaptive ホストを示します。これはデフォルトのラベルを持つことができない信頼できないシステムです。代わりに、そのラベルは受信側のトラステッドシステムによって割り当てられます。ラベルは、ラベル付きシステムの netif テンプレートで指定されている、パケットを受信する IP インタフェースのデフォルトラベルから派生します。

```
# tncfg -t netif info
name=netif
host_type=netif
doi=1
def_label=ADMIN_LOW
min_label=ADMIN_LOW
max_label=ADMIN_HIGH
host=127.0.0.1/32
```

netif テンプレートは、リモートホストではなく、信頼できるローカルネットワークインタフェースを指定します。netif テンプレートのデフォルトラベルは、そのテンプレート内のホストアドレスと一致する IP アドレスを持つ専用ネットワークインタフェースを備えているすべてのゾーンのラベルと等しくなければなりません。また、一致するゾーンインタフェースに対応する下位リンクは、同じラベルを共有するほかのゾーンにのみ割り当てることができます。

▼ システムの既知のネットワークにホストを追加する

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。**

```
# pfedit /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。**

```
# pfedit /etc/hosts

...
192.168.111.0   111-network
```

セキュリティーテンプレートの作成

このセクションでは、次のネットワーク構成のセキュリティーテンプレートを作成するためのアドバイスや例を示します。

- DOI は 1 とは異なる値です。47 ページの「異なる解釈ドメインを構成する方法」を参照してください。
- 信頼できるリモートホストに特定のラベルが割り当てられます。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」を参照してください。
- 信頼できないリモートホストに特定のラベルが割り当てられます。例16-2「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」を参照してください。

特定の要件に対応するセキュリティーテンプレートの例については、235 ページの「セキュリティーテンプレートへのホストの追加」を参照してください。

▼ 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。

注記 - 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変更したり削除したりしないでください。

- 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、245 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。

---

1. **(オプション) `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。**

   `CONFIDENTIAL` などのラベルでは、ラベル文字列または 16 進値のいずれかを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. **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 キーを押すと、部分的なプロパティーや値が補完されます。`exit` と入力してテンプレートを完成します。

     ```
     # tncfg -t newunlabeled
     tncfg:newunlabeled> info
     name=newunlabeled
     host_type=unlabeled
     ```

```
doi=1
def_label=ADMIN_LOW
min_label=ADMIN_LOW
max_label=ADMIN_HIGH
tncfg:newunlabeled> set mTab
set max_label=" set min_label="      Auto-complete shows two possible completions
tncfg:newunlabeled> set maTab      User types the letter a
tncfg:newunlabeled> set max_label=ADMIN_LOW
...
tncfg:newunlabeled> commit
tncfg:newunlabeled> exit
```

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。省略された属性ではデフォルト値が使用されます。ネットワークセキュリティー属性については、213 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。

```
# 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: unlab_1> 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16-4「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」を参照してください。

例 16-2 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 ラベルでのみパケットを送受信できる信頼できないホストのためのラベルなし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16-15「ラベル PUBLIC でのラベルなしサブネットワークの作成」を参照してください。

セキュリティーテンプレートへのホストの追加

このセクションでは、セキュリティーテンプレートにホストを追加するためのアドバイスや例を示します。不連続な IP アドレスの場合は、236 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。ホストの範囲の場合は、242 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。

このセクションの例では、次のようなリモートホストのラベルの割り当てを示しています。

- 信頼できるリモートゲートウェイは、PUBLIC トラフィックを処理します。例16-4「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」を参照してください。
- 信頼できないリモートホストがシングルラベルのルーターとして動作します – 例16-5「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」
- 信頼できるリモートホストは、トラフィックを狭いラベル範囲内に制限します。例16-6「制限されたラベル範囲を持つゲートウェイの作成」を参照してください。
- 信頼できるリモートホストに限定されたラベルセットが割り当てられます。例16-7「不連続なラベルのホストの作成」を参照してください。
- 信頼できるリモートホストに、ネットワークの残りから切り離されたラベルが割り当てられます。例16-8「開発者用のラベル付きホストの作成」を参照してください。
- 信頼できる netif ホストは、adaptive システムからのパケットにラベルを付けます。例16-9「netif ホスト用のセキュリティーテンプレートの作成」を参照してください。
- 信頼できない adaptive ホストは、パケットを netif ホストに送信します。例16-10「適応型ホスト用のセキュリティーテンプレートの作成」を参照してください。
- 信頼できる同機種ネットワークは、特定のラベルでマルチキャストアドレスを追加します。例16-11「ラベル付きマルチキャストメッセージの送信」を参照してください。
- ホストがセキュリティーテンプレートから削除されます。例16-12「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」を参照してください。
- 信頼できないリモートホストおよびネットワークにラベルが割り当てられます。例16-15「ラベル PUBLIC でのラベルなしサブネットワークの作成」を参照してください。

▼ 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。

- 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、232 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 11.2 ディレクトリサービスとネームサービスでの作業: DNS と NIS 』の第 3 章「ドメインネームシステムの管理」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、218 ページの「Trusted Extensions のルーティングについて」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. **(オプション) 追加しようとしているホスト名または IP アドレスに到達できることを確認します。**

   この例では、192.168.1.2 に到達できることを確認します。

   ```
   # arp 192.168.1.2
   gateway-2.example.com (192.168.1.2) at 0:0:0:1:ad: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。

2. **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。**

   この例では、192.168.1.2 IP アドレスを追加します。

   ```
   # 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。情報メッセージについては、例16-3「ホストのセキュリティーテンプレート割り当ての置換」を参照してください。

3. **変更後のセキュリティーテンプレートを表示します。**

   次の例は、cipso テンプレートに追加されたアドレス 192.168.1.2 を示します。

   ```
   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。

4. **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16-12「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」を参照してください。

例 16-3 ホストのセキュリティーテンプレート割り当ての置換

この例では、すでにテンプレートが割り当てられているホストにセキュリティーテンプレートを割り当てるときに表示される情報メッセージを示します。

```
# tncfg -t cipso
```

```
tncfg:cipso> add host=192.168.1.2
192.168.1.2 previously matched the admin_low template
tncfg:cipso> info
...
host=192.168.1.2/32
tncfg:cipso> exit
```

例 16-4　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「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」では、セキュリティー管理者が、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 16-5　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

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、CALIPSO または 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。

最初に、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_router
tncfg:unl_public_router> set host_type=unlabeled
tncfg:unl_public_router> set doi=1
tncfg:unl_public_router> set def_label="PUBLIC"
tncfg:unl_public_router> set min_label=ADMIN_LOW
tncfg:unl_public_router> set max_label=ADMIN_HIGH
tncfg:unl_public_router> exit
```

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_router
tncfg:unl_public_router> add host=192.168.131.82
tncfg:unl_public_router> exit
```

システムはすぐに、router-1 (192.168.131.82 アドレスのホスト名) 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 16-6 制限されたラベル範囲を持つゲートウェイの作成

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テンプレートを作成し、ゲートウェイをそのテンプレートに追加します。

```
# arp 192.168.131.78
gateway-ir.example.com (192.168.131.78) at 0:0:0:3:ab:cd

# 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
```

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 16-7 不連続なラベルのホストの作成

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、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
```

次に、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 cnf :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
```

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 16-8 開発者用のラベル付きホストの作成

この例では、セキュリティー管理者は 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> 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 16-9 netif ホスト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 netif セキュリティーテンプレートを作成します。このテンプレートは、IP アドレス 10.121.10.3 を含んでいるラベル付きネットワークインタフェースに割り当てられます。この割り当てにより、Trusted Extensions IP モジュールは、adaptive ホストから届くすべての着信パケットにデフォルトラベル PUBLIC を追加します。

```
# tncfg -t netif_public
tncfg:netif_public> set host_type=netif
tncfg:netif_public> set doi=1
tncfg:netif_public> set def_label="PUBLIC"
tncfg:netif_public> add host=10.121.10.3
tncfg:netif_public> commit
tncfg:netif_public> exit
```

例 16-10 適応型ホスト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が前もって計画を立てます。管理者は、公開情報を保持するネットワークおよび内部情報を保持するネットワークとして、異なるサブネットを作成します。次に、管理者は 2 つの adaptive ホストを定義します。公開サブネット内のシステムには PUBLIC ラベルが割り当てられます。内部ネットワーク内のシステムには IUO ラベルが割り当てられます。このネットワークは前もって計画されたため、各ネットワークが特定のラベルで情報を保持および送信します。もう 1 つの利点は、想定したインタフェースにパケットが配信されない場合に、ネットワークを簡単にデバッグできることです。

```
# tncfg -t adpub_192_168_10
tncfg:adapt_public> set host_type=adapt
tncfg:adapt_public> set doi=1
tncfg:adapt_public> set min_label="public"
tncfg:adapt_public> set max_label="public"
tncfg:adapt_public> add host=192.168.10.0
tncfg:adapt_public> commit
tncfg:adapt_public> exit

# tncfg -t adiuo_192_168_20
tncfg:adapt_public> set host_type=adapt
tncfg:adapt_public> set doi=1
tncfg:adapt_public> set min_label="iuo"
tncfg:adapt_public> set max_label="iuo"
tncfg:adapt_public> add host=192.168.20.0
tncfg:adapt_public> commit
tncfg:adapt_public> exit
```

例 16-11 ラベル付きマルチキャストメッセージの送信

この例では、ラベル付きの同機種 LAN で、セキュリティー管理者はラベル PUBLIC でパケットを送信するために使用できるマルチキャストアドレスを選択します。

```
# tncfg -t cipso_public
tncfg:cipso_public> add host=224.4.4.4
tncfg:cipso_public> exit
```

例 16-12 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、236 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。**

   この例では、2 つの IPv4 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。

   ```
   # tncfg -t cipso
   tncfg:cipso> add host=192.168.113.100/25
   192.168.113.100/25 previously matched the admin_low template
   ```

2. **アドレス範囲にセキュリティーテンプレートを割り当てるには、IP アドレスと接頭辞長を指定します。**

   次の例の接頭辞長 /25 は、192.168.113.0 から 192.168.113.127 までの連続する IPv4 アドレス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 /56 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
```

   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。情報メッセージについては、例16-13「ホストの範囲に対するセキュリティーテンプレートを置換する」を参照してください。

   例16-14「セキュリティーテンプレート内に誤って入力された IP アドレスの処理」に示すように、入力が誤っている場合も情報メッセージが表示されます。

例 16-13 ホストの範囲に対するセキュリティーテンプレートを置換する

この例では、すでにテンプレートが割り当てられているホストの範囲にセキュリティーテンプレートを割り当てるときに表示される情報メッセージを示します。

```
# 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
```

217 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オーバーライドされることが、Trusted Extensions の代替メカニズムによって保証されます。

例 16-14 セキュリティーテンプレート内に誤って入力された IP アドレスの処理

エントリが誤って入力されると、情報メッセージが表示されます。次のホスト追加により、アドレスから :200 が削除されます。

```
# tncfg -t cipso
tncfg:cipso> add host=2001:a08:3903::0/56
Invalid host: 2001:a08:3903::0/56
```

例 16-15 ラベル PUBLIC でのラベルなしサブネットワークの作成

例16-2「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」では、セキュリティー管理者は信頼できないホストにラベル PUBLIC を割り当て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を PUBLIC ラベルに割り当てます。割り当て側のシステム上のユーザーは、このサブネット内のホストのファイルシステムを PUBLIC ゾーンにマウントできます。

```
# 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に到達できるホストの制限

このセクションでは、ネットワークに到達できるホストを制限することにより、ネットワークを保護します。

- 245 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」.
- ブート時に接続するシステムを指定することにより、セキュリティーを向上させます。例16-16「IP アドレス 0.0.0.0/0 のラベルの変更」を参照してください。
- アプリケーションサーバーを構成して、リモートクライアントからの初期接続を受け入れます。例16-18「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」を参照してください。
- ラベル付きの Sun Ray サーバーを構成して、リモートクライアントからの初期接続を受け入れます。例16-19「ラベル付き Sun Ray サーバーの有効な初期アドレスの構成」を参照してください。

▼ 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リモートホスト (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。たとえば、潜在的な Sun Ray クライアントからの初期接続リクエストを受信するには、Sun Ray サーバーにこのエントリが含まれている必要があります。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、クライアントをラベル付き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。**

   ブート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16-17「Trusted Extensions システムがブート時に接続するシステムの列挙」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ブートが許可されていることを確認します。**

例 16-16 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 16-17 Trusted Extensions システムがブート時に接続するシステムの列挙

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。リモートホストは、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 16-18 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アプリケーションサーバーを構成して、潜在的なクライアントからの初期接続要求を受け入れます。

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。

例 16-19 ラベル付き Sun Ray サーバーの有効な初期アドレスの構成

この例では、セキュリティー管理者は Sun Ray サーバーを構成して、潜在的なクライアントからの初期接続要求を受け入れます。サーバーは非公開トポロジと Sun Ray サーバーのデフォルトを使用しています。

```
# utadm -a net0
```

次に、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       Sun Ray server address
host=192.168.128.0/24       Sun Ray 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       Sun Ray 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       Sun Ray 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、Sun Ray クライアントのみがサーバーに到達できるようにします。

ルートおよびマルチレベルポートの構成

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。

▼ デフォルトルートを追加する

この手順では、GUI を使用してデフォルトルートを追加します。この例では、コマンド行を使用してデフォルトルートを追加する方法を示します。

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。

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、236 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」および242 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ルートを作成します。**

```
# txzonemgr &
```

2. **デフォルトルート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。**

注記 - 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 16-20 route コマンドを使用した大域ゾーンのデフォルトルートの設定

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ルートを作成します。

```
# 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、250 ページの「デフォルトルートを追加する」を実行します。

例 16-21 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に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 16-22 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に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 16-23 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構成されています。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

このタスクマップでは、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。

表 16-1 ラベル付き IPsec を構成するためのタスクマップ

タスク	説明	手順
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。	253 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。	256 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 CALIPSO または 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。**

   229 ページの「ホストおよびネットワークへのラベル付け」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 11.2 でのネットワークのセキュリティー保護 』の「IPsec によって 2 つのサーバー間でネットワークトラフィックをセキュリティー保護する方法」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 11.2 でのネットワークのセキュリティー保護 』の「事前共有鍵で IKEv2 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. **CALIPSO または 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}
```

注記 - 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 11.2 でのネットワークのセキュリティー保護 』の「公開鍵証明書による IKEv2 の構成」の手順を完了するとき、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 11.2 でのネットワークのセキュリティー保護 』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。CALIPSO または 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 CALIPSO または 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. **229 ページの「ホストおよびネットワークへのラベル付け」の手順に従って次を定義します。**

   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 11.2 でのネットワークのセキュリティー保護 』の「IPsec のトンネルモードで 2 つの LAN 間の接続を保護する方法」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 11.2 でのネットワークのセキュリティー保護 』の「事前共有鍵で IKEv2 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
}
```

注記 - 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 11.2 でのネットワークのセキュリティー保護 』の「公開鍵証明書による IKEv2 の構成」の手順を完了するとき、`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

次のタスクマップでは、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。

表 16-2 トラステッドネットワークのトラブルシューティングに関するタスクマップ

タスク	説明	手順
システムとリモート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。	258 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」
	システムとリモート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。	259 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。	263 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、177 ページの「ゾーンの管理」を参照してください。
- NFS マウントのデバッグについては、205 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。**

   ブート時に、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. **ルーティング構成を確認します。**

```
# route get [ip] -secattr sl=label,doi=integer
```

詳しくは、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. **ルーティング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、ルーティングテーブルのエントリが表示されます。詳しくは、netstat(1M) のマニュアルページを参照してください。

▼ 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リモート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、93 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

17 Trusted Extensions および LDAP について

この章では、Trusted Extensions が構成されたシステムでの Oracle Directory Server Enterprise Edition (LDAP サーバー) の使用法について説明します。

Trusted Extensions での LDAP 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。

LDAP 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。

通常、このマルチレベルポートは、大域ゾーンで大域ゾーン向けに構成されます。したがって、ラベル付きゾーンには LDAP ディレクトリへの書き込みアクセス権がありません。代わりに、ラベル付きゾーンは、そのシステムまたはネットワーク上の別のトラステッドシステムで実行されているマルチレベルプロキシサービスを介して、読み取りリクエストを送信します。Trusted Extensions では、ラベルごとに 1 つのディレクトリサーバーを使用する LDAP 構成もサポートされます。そのような構成は、ユーザーがラベルごとに異なる資格を持っている場合に必要になります。

Trusted Extensions は、LDAP サーバーに 2 つのトラステッドネットワークデータベース、tnrhdb および tnrhtp を追加します。

- Oracle Solaris での LDAP ネームサービスの使用については、『Oracle Solaris 11.2 ディレクトリサービスとネームサービスでの作業: LDAP 』を参照してください。
- Trusted Extensions に対する LDAP サーバーの設定については、第5章「Trusted Extensions 用の LDAP の構成」を参照してください。Trusted Extensions システムを Oracle Solaris LDAP サーバーのクライアントにするには、Trusted Extensions で構成されたプロキシを使用します。
- Trusted Extensions LDAP サーバーのクライアントの設定方法については、92 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。

ローカルで管理される Trusted Extensions システム

サイトで分散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と、name-service/switch SMF サービスの構成プロパティーによって保持されます。

Trusted Extensions LDAP データベース

Trusted Extensions では、LDAP 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 の LDAP ネームサービスに関するクイックリファレンス

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 11.2 ディレクトリサービスとネームサービスでの作業: LDAP 』の第 6 章「LDAP のトラブルシューティング」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、263 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 接続に関するその他のトラブルシューティングについては、『Oracle Solaris 11.2 ディレクトリサービスとネームサービスでの作業: LDAP 』の第 6 章「LDAP のトラブルシューティング」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

18 Trusted Extensions のマルチレベルメールについて

この章では、Trusted Extensions が構成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 11.2 での sendmail サービスの管理 』の第 2 章「メールサービスの管理」の手順に従ってメールサーバーを設定および管理します。また、Trusted Extensions メール機能をどのように構成する必要があるかもセキュリティー管理者が決定します。

次の説明は、Trusted Extensions に固有のメール管理です。

- `.mailrc` などのユーザーのローカル構成ファイルは、ユーザーの最小ラベルにあります。

したがって、最小ラベルのディレクトリの .mailrc ファイルを上位レベルの各ディレクトリにコピーまたはリンクしない限り、複数のラベルで作業するユーザーには、上位レベルのラベルの .mailrc はありません。

セキュリティー管理者役割または個々のユーザーは、.mailrc ファイルを .copy_files または .link_files に追加できます。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 220 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

この章では、Trusted Extensions を使用してラベル付き印刷を構成する方法について説明します。また、ラベル付けオプションを使用せずに Trusted Extensions 印刷ジョブを構成する方法も説明します。

ラベル、プリンタ、および印刷

Trusted Extensions は、ラベルを使用してプリンタへのアクセスを制御します。ラベルは、プリンタへのアクセスと、待ち行列に入った印刷ジョブに関する情報へのアクセスの制御に使用されます。ソフトウェアは、印刷出力のラベル付けも行います。本文ページにラベルが付けられ、必須のバナーページとトレーラページにもラベルが付けられます。バナーページとトレーラページに処理方法を含めることもできます。

システム管理者は、基本的なプリンタ管理を担当します。セキュリティー管理者役割は、ラベル付き出力の処理方法とラベルも含めてプリンタのセキュリティーを管理します。管理者は Oracle Solaris の基本的なプリンタ管理手順に従います。ラベルの適用、印刷ジョブのラベル範囲の制限、印刷するラベル付きゾーンの構成、および印刷制限の緩和を行うには、構成が必要です。

Trusted Extensions は、マルチレベルとシングルレベルの両方の印刷をサポートします。デフォルトでは、Trusted Extensions システムの大域ゾーンで構成されているプリンタサーバーは、ラベルの全範囲を印刷できます。つまり、このプリンタサーバーはマルチレベルです。そのプリンタサーバーに到達できるラベル付きゾーンまたはシステムは、接続されているプリンタに印刷できます。ラベル付きゾーンはシングルレベル印刷をサポートできます。ゾーンは大域ゾーンを

介してプリンタに接続できます。あるいは、ゾーンをプリンタサーバーとして構成できます。そのラベル付きゾーンに到達できるそのラベルのゾーン、およびそのプリンタサーバーは、接続されているプリンタに印刷できます。任意のラベルが割り当てられているラベルなしシステム上のプリンタサーバーを使用して、シングルレベル印刷も可能です。これらの印刷ジョブは、ラベルなしで印刷されます。

Oracle Solaris 10 と Oracle Solaris 11 の Trusted Extensions 印刷の相違点

Oracle Solaris 10 のデフォルトの印刷プロトコルは、LP 印刷サービスです。Oracle Solaris 11 のデフォルトは、Common UNIX Printing System (CUPS) です。Oracle Solaris の CUPS の包括的なガイドについては、『Oracle Solaris 11.2 での印刷の構成と管理 』を参照してください。次の表に、CUPS 印刷プロトコルと LP 印刷プロトコルの主要な相違点を示します。

表 19-1 CUPS と LP の相違点

相違点の領域	CUPS	LP
IANA ポート番号	631	515
両面印刷	片面	両面
カスケード印刷	プリンタサーバー上のプリンタを共有する必要があります	プリンタへの経路を構成する必要があります
ネットワークプリンタへのアクセス	プリンタおよびプリンタサーバーの IP アドレスを正常に `ping` できる必要があります	プリンタへの経路を構成する必要があります
リモート印刷ジョブ	ラベルなしで印刷できません	ラベルなしで印刷できます
クライアントへのリモートプリンタの追加	`lpadmin -p` *printer-name* `-E \ -v ipp://`*print-server-IP-address*`/printers/`*printer-name-on-server*	`lpadmin -p` *printer-name* `\ -s` *server-name*
プリンタサーバーの有効化と受け入れ	`lpadmin -E` オプション	`accept` および `enable` コマンド
PostScript 保護	デフォルトで提供されます	承認が必要です
バナーページの有効化	`-o job-sheets=labeled` オプション	デフォルトで提供されます
バナーページとトレーラページの無効化	`-o job-sheets=none` オプション	`-o nobanner` オプション
`lp -d` *printer* `file1 file2`	印刷ジョブあたり 1 バナーページと 1 トレーラページ	印刷ジョブの各ファイルに 1 バナーページと 1 トレーラページ

相違点の領域	CUPS	LP
ジョブページのラベル方向	常に縦長	常にジョブの向き
印刷サービス	svc:/application/cups/scheduler .../in-lpd:default	svc:/application/print/service-selector .../server .../rfc1179 .../ipp-listener svc:/network/device-discovery/printers:snmp

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 が構成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サーバーにのみ受け入れられます。ラベルは、プリンタサーバー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。

ラベル付きプリンタ出力

Trusted Extensions は、本文ページおよびバナーページとトレーラページにセキュリティー情報を印刷します。この情報は、`/etc/security/tsol/label_encodings` ファイルと `/usr/lib/cups/filter/tsol_separator.ps` ファイルから取得されます。80 文字より長いラベルは短縮されて、すべてのページの最上部と最下部に印刷されます。短縮は、矢印 (->) で示されます。本文ページが横長で印刷される場合でも、ヘッダーおよびフッターのラベルは縦長方向で印刷されます。例については、図19-4「本文ページがランドスケープモードで印刷されるとき、ジョブのラベルはポートレイトモードで印刷される」を参照してください。

印刷ジョブに表示されるテキスト、ラベル、および警告は構成可能です。テキストは、ローカライズのために別の言語のテキストで置き換えることもできます。セキュリティー管理者は次の構成を行うことができます。

- バナーページとトレーラページのテキストをローカライズまたはカスタマイズする
- 本文ページまたはバナーページとトレーラページの各種フィールドに印刷される代替ラベルを指定する

- テキストまたはラベルを変更または省略する

ラベルなしプリンタに割り当てられたユーザーは、ラベルなしで印刷できます。独自のプリンタサーバーを持つラベル付きゾーンのユーザーは、`solaris.print.unlabeled` 承認が割り当てられていれば、ラベルなしで印刷できます。Trusted Extensions プリンタサーバーで制御されているローカルプリンタにラベルなしで印刷するよう、役割を構成することができます。補足情報については、292 ページの「Trusted Extensions の印刷制限の引き下げ」を参照してください。

ラベル付きのバナーページとトレーラページ

次の図は、デフォルトのバナーページを示し、デフォルトのトレーラページがどのように異なるかを示しています。コールアウトは各種セクションを示しています。これらのセクションのテキストのソースについては、『Trusted Extensions Label Administration 』の第 4 章「Labeling Printer Output」を参照してください。トレーラページでは、外側の線が異なっています。

図 19-1　　ラベル付き印刷ジョブの一般的なバナーページ

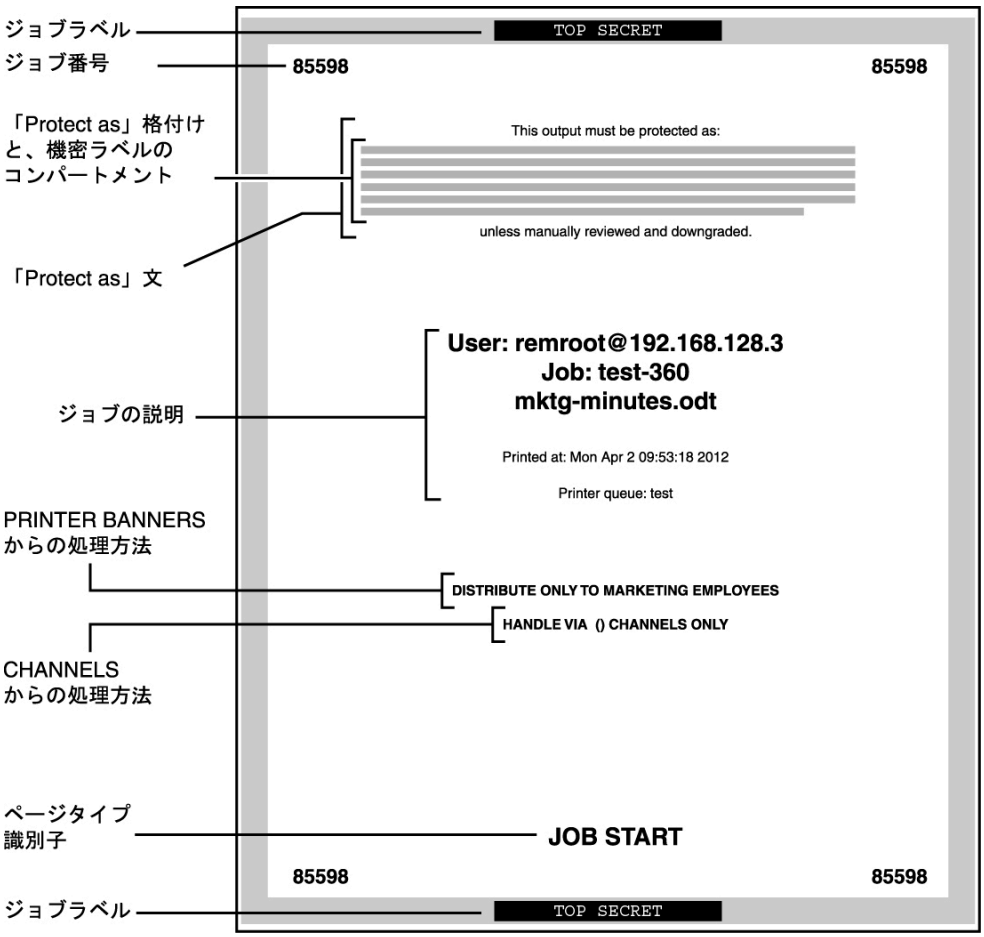
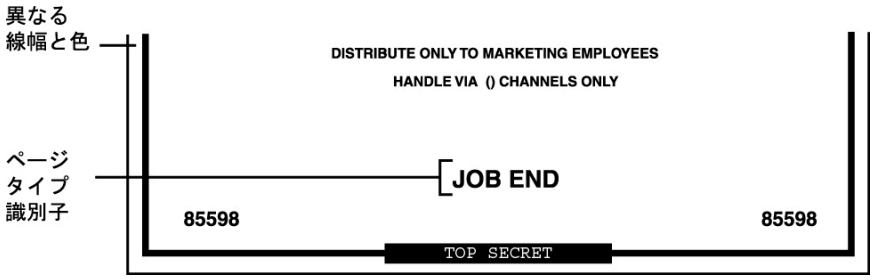


図 19-2 トレーラページの相違点

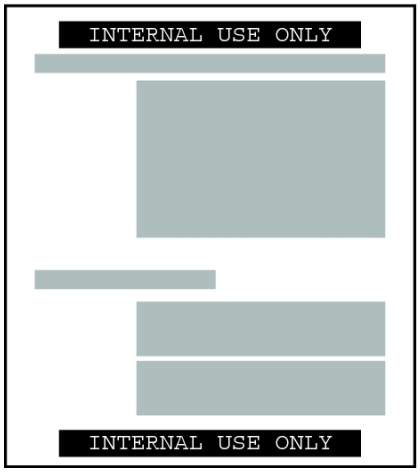


ラベル付きの本文ページ

デフォルトでは、各本文ページの最上部と最下部に「Protect as」格付けが印刷されます。「Protect as」格付けは、ジョブのラベルの格付けが `minimum protect as` 格付けと比較される際の優位格付けです。`minimum protect as` 格付けは `label_encodings` ファイルで定義されます。

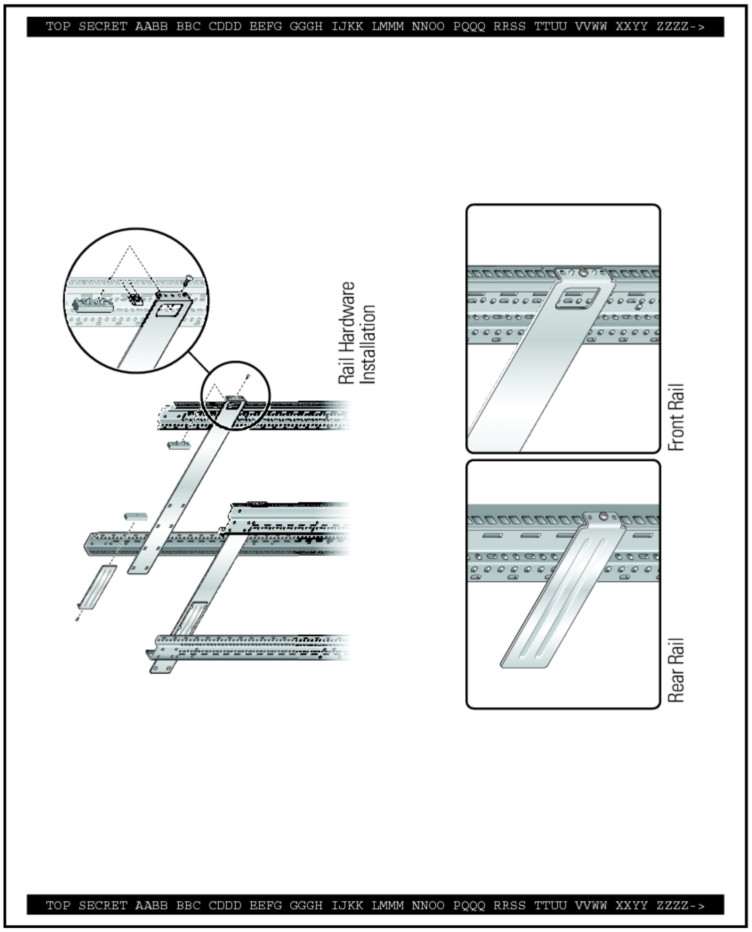
たとえば、ユーザーが `Internal Use Only` セッションにログインしている場合、ユーザーの印刷ジョブはそのラベルになります。`label_encodings` ファイル内の `minimum protect as` 格付けが `Public` の場合は、`Internal Use Only` ラベルが本文ページに印刷されます。

図 19-3 本文ページの最上部と最下部に印刷されたジョブのラベル



本文ページがランドスケープモードで印刷されるとき、ラベルはポートレイトモードで印刷されます。次の図は、ランドスケープモードで印刷された本文ページの「Protect As」ラベルがページ境界を越えている様子を示しています。ラベルは 80 文字に短縮されます。

図 19-4 本文ページがランドスケープモードで印刷されるとき、ジョブのラベルはポートレイトモードで印刷される



`tsol_separator.ps` 構成ファイル

次の表は、セキュリティー管理者が `/usr/lib/cups/filter/tsol_separator.ps` ファイルの変更によって変更できるトラステッド印刷の項目を示しています。

表 19-2 tsol_separator.ps ファイルで構成可能な値

出力	デフォルト値	定義の方法	変更するには
PRINTER BANNERS	/Caveats Job_Caveats	/Caveats Job_Caveats	『Trusted Extensions Label Administration 』の「Specifying Printer Banners」を参照してください。
CHANNELS	/Channels Job_Channels	/Channels Job_Channels	『Trusted Extensions Label Administration 』の「Specifying Channels」を参照してください。
バナーページおよびトレーラページの最上部のラベル	/HeadLabel Job_Protect def	/PageLabel の説明を参照してください。	/PageLabel の変更と同じです。 『Trusted Extensions Label Administration 』の「Specifying the “Protect As” Classification」も参照してください。
本文ページの最上部と最下部のラベル	/PageLabel Job_Protect def	ジョブのラベルと、label_encodings ファイルのminimum protect as classification とを比較します。より優位な方の格付けを印刷します。 印刷ジョブのラベルにコンパートメントがある場合は、コンパートメントを含みます。	/PageLabel 定義を変更して別の値を指定します。 または、選択した文字列を入力します。 または、何も印刷しないようにします。
「Protect as」格付け文のテキストとラベル	/Protect Job_Protect def /Protect_Text1 () def /Protect_Text2 () def	/PageLabel の説明を参照してください。 ラベルの上に表示するテキスト。 ラベルの下に表示するテキスト。	/PageLabel の変更と同じです。 Protect_Text1 と Protect_Text2 の () をテキスト文字列で置き換えます。

セキュリティー情報の PostScript 印刷

Trusted Extensions でのラベル付き印刷は、Oracle Solaris 印刷からの機能に依存します。Oracle Solaris OS の場合と同様に、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。ラベル付けを実装するために、フィルタによって印刷ジョブが 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。

注記 - CUPS は PostScript ファイルの変更を防止します。したがって、熟練した PostScript プログラマが、印刷出力のラベルを変更する PostScript ファイルを作成することはできません。

Trusted Extensions 印刷インタフェース (リファレンス)

Trusted Extensions は、次の印刷承認を追加して Trusted Extensions セキュリティーポリシーを実装します。これらの承認はプリンタサーバー上で検査されます。したがって、ラベル付きゾーンのユーザーなどのリモートユーザーは、承認検査に合格できません。

- `solaris.print.admin` – 役割が印刷を管理できるようにします
- `solaris.print.list` – 役割がその役割に属さない印刷ジョブを表示できるようにします
- `solaris.print.nobanner` – 役割が大域ゾーンからバナーページとトレーラページなしでジョブを印刷できるようにします
- `solaris.print.unlabeled` – 役割が大域ゾーンからページラベルなしでジョブを印刷できるようにします

次のユーザーコマンドは、Trusted Extensions セキュリティーポリシーに準拠するように拡張されています。

- `cancel` – 印刷ジョブを取り消すには、呼び出し元はそのジョブのラベルと等しくなければなりません。一般ユーザーは自分のジョブだけを取り消すことができます。
- `lp` – 本文ページをラベルなしで印刷する `-o nolabel` オプションには、`solaris.print.unlabeled` 承認が必要です。バナーページとトレーラページなしでジョブを印刷する `-o job-sheets=none` オプションには、`solaris.print.nobanner` 承認が必要です。
- `lpstat` – 印刷ジョブのステータスを取得するには、呼び出し元はそのジョブのラベルと等しくなければなりません。一般ユーザーは自分の印刷ジョブだけを表示できます。

次の管理コマンドは、Trusted Extensions セキュリティーポリシーに準拠するように拡張されています:Oracle Solaris OS の場合と同様に、これらのコマンドは Printer Management 権利プロファイルを含む役割だけが実行できます。

- `lpmove` – 印刷ジョブを移動するには、呼び出し元はそのジョブのラベルと等しくなければなりません。デフォルトでは、一般ユーザーは自分の印刷ジョブだけを移動できます。
- `lpadmin` – 大域ゾーンの場合、このコマンドはすべてのジョブに対して機能します。ラベル付きゾーンの場合、印刷ジョブを表示するには、呼び出し元はそのジョブのラベルより優位でなければならず、変更するには等しくなければなりません。

- `lpsched` – 大域ゾーンの場合、このコマンドは常に成功します。Oracle Solaris OS の場合と同様に、`svcadm` コマンドを使用して、印刷サービスを有効化、無効化、起動、または再起動します。ラベル付きゾーンの場合、印刷サービスを変更するには、呼び出し元はその印刷サービスのラベルと等しくなければなりません。サービス管理機能の詳細は、`smf`(5)、`svcadm`(1M)、および `svcs`(1) のマニュアルページを参照してください。

Trusted Extensions での印刷の管理

Oracle Solaris のプリンタの設定を完了したあと、Trusted Extensions で印刷の構成手順を実行します。これらの手順には、基本的な設定の一部が含まれます。詳細は、『Oracle Solaris 11.2 での印刷の構成と管理 』の第 2 章「CUPS を使用したプリンタの設定 (タスク)」を参照してください。ラベル付き印刷を管理する主要なタスクへのリンクを次に示します。

- 285 ページの「ラベル付き印刷の構成」
- 292 ページの「Trusted Extensions の印刷制限の引き下げ」

ラベル付き印刷の構成

次のタスクマップでは、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。

表 19-3 ラベル付き印刷を構成するためのタスクマップ

タスク	説明	手順
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。	286 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」
ネットワークプリンタを構成します。	プリンタを共有します。	288 ページの「ネットワークプリンタを構成する方法」
ラベル付きゾーンから印刷を構成します。	ラベル付きゾーンに、シングルラベルのプリンタサーバーを作成します。	289 ページの「ゾーンをシングルレベルのプリンタサーバーとして構成する方法」
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。	290 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に接続されたプリンタは、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。プリンタが共有されている場合、プリンタサーバーに到達できる Trusted Extensions ホストは、その共有プリンタを使用できます。

始める前に 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. **プリンタの製造元とモデルを判定します。**

   ```
   # lpinfo -m | grep printer-manufacturer
   ```

   たとえば、すべての Xerox プリンタを見つけるには、次の構文を使用します。

   ```
   # lpinfo -m | grep Xerox
   gutenprint.5.2://xerox-able_1406/expert Xerox Able 1406 - CUPS+Gutenprint v5.2.4
   gutenprint.5.2://xerox-able_1406/simple Xerox Able 1406 - CUPS+Gutenprint v5.2.4 ...
   gutenprint.5.2://xerox-dc_400/expert Xerox Document Centre 400 - ...
   gutenprint.5.2://xerox-dc_400/simple Xerox Document Centre 400 - ...
   gutenprint.5.2://xerox-dp_4508/expert Xerox DocuPrint 4508 - ...
   gutenprint.5.2://xerox-dp_4508/simple Xerox DocuPrint 4508 - ...
   ...
   ```

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 -E -v socket://printer-IP-address -m printer-make-and-model
   -
   ```

   -E オプションは、指定したプリンタが印刷リクエストのキューを受け入れられるようにします。また、プリンタをアクティブ化または有効化します。

3. **ネットワークプリンタを作成するには、プリンタを共有します。**

   ```
   # lpadmin -p printer-name -o printer-is-shared=true
   ```

   プリンタがほかのシステムによって使用されないようにする場合は、この手順を省略します。

4. **プリンタのデフォルトを表示します。**

   ```
   # lpoptions -p printer-name
   ```

5. **デフォルトを調整します。**

   たとえば、両面の二段組印刷にすることができます。

ヒント - CUPS Web インタフェース `http://localhost:631` を使用して、プリンタを構成できます。

6. **印刷サーバーに接続されている各プリンタを、ラベル付きバナーページおよびトレーラページで構成します。**

```
# lpadmin -p printer-name -o job-sheets=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、ラベル構成はこれで完了です。

7. **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. **プリンタを追加します。**

```
# lpadmin -p zone-printer-name -E \
-v ipp://global-zone-IP-address/printers/printer-name-in-global-zone
```

c. **(オプション) プリンタをデフォルトとして設定します。**

```
# lpadmin -d zone-printer-name
```

8. **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. **コマンド行からテキストファイルと PostScript ファイルを印刷します。**

```
# lp /etc/motd ~/PostScriptTest.ps
% lp $HOME/file1.txt $HOME/PublicTest.ps
```

b. **メール、Oracle OpenOffice、Adobe Reader、ブラウザなどのアプリケーションからファイルを印刷します。**

c. **バナーページ、トレーラページ、および本文ページの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 – 292 ページの「Trusted Extensions の印刷制限の引き下げ」
- このゾーンをプリンタサーバーとして使用する – 290 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」

▼ ネットワークプリンタを構成する方法

プリンタが共有されている場合、プリンタサーバーに到達できる Trusted Extensions ホストは、その共有プリンタを使用できます。

始める前に 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. **ネットワークプリンタの特性を定義します。**

   ステップ 1のステップ 6 から286 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」に従って、ネットワークプリンタを構成します。

   ステップ 3 でプリンタを共有したあとは、プリンタサーバーに到達できるネットワーク上のすべてのシステムが、このプリンタに印刷できます。

2. **ネットワークプリンタをテストします。**

   このプリンタサーバーを使用するシステムから、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. **コマンド行からテキストファイルと PostScript ファイルを印刷します。**

   ```
   # lp /etc/motd ~/PostScriptTest.ps
   % lp $HOME/file1.txt $HOME/PublicTest.ps
   ```

   b. **メール、Oracle OpenOffice、Adobe Reader、ブラウザなどのアプリケーションからファイルを印刷します。**

   c. **バナーページ、トレーラページ、および本文ページの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場合は、292 ページの「Trusted Extensions の印刷制限の引き下げ」を参照してください。

▼ ゾーンをシングルレベルのプリンタサーバーとして構成する方法

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 ユーザーズガイド 』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 ユーザーズガイド 』の「ワークスペースのラベルを変更する」を参照してください。

3. **接続されているすべてのプリンタの特性を定義します。**

   ステップ 1のステップ 6 から 286 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」 に従って、ゾーンプリンタを構成します。

   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。

4. **プリンタをテストします。**

   注記 - 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. **コマンド行からテキストファイルと PostScript ファイルを印刷します。**

   ```
   # lp /etc/motd ~/PostScriptTest.ps
   % lp $HOME/file1.txt $HOME/PublicTest.ps
   ```

   b. **メール、Oracle OpenOffice、Adobe Reader、ブラウザなどのアプリケーションからファイルを印刷します。**

c. **バナーページ、トレーラページ、および本文ページの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 – 292 ページの「Trusted Extensions の印刷制限の引き下げ」
- このゾーンをプリンタサーバーとして使用する – 290 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共有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共有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、同じラベルのリモートゾーンが構成されている共有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共有プリンタへのアクセスを追加します。

始める前に プリンタサーバーがラベル範囲またはシングルラベルで構成されています。また、プリンタサーバーに接続されているプリンタの構成と共有が完了しています。詳細は、次を参照してください。

- 286 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」
- 289 ページの「ゾーンをシングルレベルのプリンタサーバーとして構成する方法」
- 294 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. **プリンタに ping を実行できることを確認します。**

```
# ping printer-IP-address
```

このコマンドが失敗する場合は、ネットワーク接続に問題があります。接続の問題を修正してから、この手順に戻ります。補足情報については、258 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」を参照してください。

2. **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. **リモートの Trusted Extensions 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 -p printer-name -E \
     -v ipp://print-server-IP-address/printers/printer-name-on-server
     ```

   - **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 ユーザーズガイド 』の「ワークスペースのラベルを変更する」を参照してください。

     b. **プリンタへのアクセスを追加します。**

     ```
     # lpadmin -p printer-name -E \
     -v ipp://print-server-IP-address/printers/printer-name-on-print-server
     ```

   - **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構成します。**

     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. **リモート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 -p printer-name -E \
-v ipp://zone-print-server-IP-address/printers/printer-name-on-zone-print-server
```

- **ラベルなしプリンタサーバーを使用してセキュリティー情報なしで印刷するよう、ラベル付きゾーンを構成します。**

  手順については、294 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」を参照してください。

3. **プリンタをテストします。**

注記 - 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。

すべてのクライアント上で、大域ゾーンにアクセスできるすべてのアカウントおよびラベル付きゾーンにアクセスできるすべてのアカウントに対して、印刷が正しく機能することをテストします。

a. **コマンド行からテキストファイルと PostScript ファイルを印刷します。**

```
# lp /etc/motd ~/PostScriptTest.ps
% lp $HOME/file1.txt $HOME/PublicTest.ps
```

b. **メール、Oracle OpenOffice、Adobe Reader、ブラウザなどのアプリケーションからファイルを印刷します。**

c. **バナーページ、トレーラページ、および本文ページのラベルが正しく印刷されることを確認します。**

Trusted Extensions の印刷制限の引き下げ

以下のタスクはオプションです。これらは、Trusted Extensions で提供される印刷のセキュリティーを引き下げます。

表 19-4　Trusted Extensions の印刷制限の引き下げ (タスクマップ)

タスク	説明	手順
出力にラベルを付けないようプリンタを構成します。	大域ゾーンからの印刷出力にセキュリティー情報が印刷されないようにします。	293 ページの「バナーページとトレーラページを削除する方法」
プリンタをシングルラベルでラベルなし出力に構成します。	ユーザーが特定のラベルで印刷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。	294 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。	ラベルなしのプリンタサーバーに印刷します。 ラベル付けを抑制する印刷承認を割り当てます。	294 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」 295 ページの「特定のユーザーと役割が印刷出力のラベルを省略できるようにする方法」
バナーページとトレーラページを抑制します。	バナーページとトレーラページを削除して、それらのページの追加のセキュリティー情報を削除します。	293 ページの「バナーページとトレーラページを削除する方法」
印刷承認を割り当てます。	特定のユーザーと役割に、ラベルなしのジョブの印刷を許可します。	295 ページの「特定のユーザーと役割が印刷出力のラベルを省略できるようにする方法」

▼ バナーページとトレーラページを削除する方法

`job-sheets` オプションが `none` に設定されているプリンタは、バナーページまたはトレーラページを印刷*しません*。

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。

- **該当するラベルで、プリンタをバナーページやトレーラページなしで構成します。**

```
# lpadmin -p print-server-IP-address -o job-sheets=none,none
```

または、`none` を 1 回指定します。

```
# lpadmin -p print-server-IP-address -o job-sheets=none
```

本文ページにはまだラベルが付いたままです。本文ページからラベルを削除するには、295 ページの「特定のユーザーと役割が印刷出力のラベルを省略できるようにする方法」を参照してください。

▼ ラベルなしのプリンタサーバーにラベルを割り当てる

Trusted Extensions システムは、Oracle Solaris プリンタサーバーにラベルを割り当てることにより、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。ジョブは、割り当てられたラベルで、ラベルなしで印刷されます。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。ユーザーは割り当てられたラベルで、ラベルなしのプリンタにジョブを印刷できます。

始める前に 大域ゾーンでセキュリティー管理者役割になります。

1. **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、236 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。
   ラベルなしテンプレートでプリンタサーバーに割り当てられているラベルで作業しているユーザーは、Oracle Solaris プリンタにそのラベルで印刷ジョブを送信できます。

2. **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。**

3. **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 ユーザーズガイド 』の「ワークスペースのラベルを変更する」を参照してください。

4. **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 -p printer-name -E \
   -v ipp://print-server-IP-address/printers/printer-name-on-print-server
   ```

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ドキュメント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、256 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」を参照してください。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。

▼ 特定のユーザーと役割が印刷出力のラベルを省略できるようにする方法

ユーザーと役割がラベルなしでジョブを印刷できるようにするには、セキュリティー管理者による承認が必要で、承認されたユーザーまたは役割の側では、印刷ジョブの送信時に操作が必要です。

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. **ユーザーまたは役割に印刷承認を割り当てます。**

   - **ユーザーまたは役割がバナーページとトレーラページからラベルを削除できるようにするには、solaris.print.nobanner 承認を割り当てます。**

     ```
     # usermod -A +solaris.print.nobanner username
     # rolemod -A +solaris.print.nobanner rolename
     ```

   - **ユーザーまたは役割が本文ページからラベルを削除できるようにするには、solaris.print.unlabeled 承認を割り当てます。**

     ```
     # usermod -A +solaris.print.unlabeled username
     # rolemod -A +solaris.print.unlabeled rolename
     ```

   - **ユーザーまたは役割が印刷出力からすべてのラベルを削除できるようにするには、両方の承認を割り当てます。**

     ```
     # usermod -A +solaris.print.unlabeled,+solaris.print.nobanner username
     # rolemod -A +solaris.print.unlabeled,+solaris.print.nobanner rolename
     ```

2. **ラベルのない出力を印刷するための準備を行います。**

   プリンタがローカルであることを確認します。

   つまり、ユーザーの場合は、そのゾーン用のプリンタサーバーを持っているラベル付きゾーンから印刷する必要があります。役割は大域ゾーンまたはラベル付きゾーンから印刷できます。

3. **ラベルのない出力を印刷するには、ラベルを削除するオプションをコマンド行で指定します。**

   ラベルのない出力の印刷を承認されている必要があります。

   - **バナーなしで印刷するには、`job-sheets=none` オプションを使用します。**

     ```
     # lp -o job-sheets=none file
     ```

   - **本文ページをラベルなしで印刷するには、`nolabel` オプションを使用します。**

     ```
     # lp -o nolabels file
     ```

   - **出力をラベルなしで印刷するには、両方のオプションを使用します。**

     ```
     # lp -o job-sheets=none -o nolabels file
     ```

♦ ♦ ♦ 第 20 章

20 Trusted Extensions のデバイスについて

この章では、Trusted Extensions システムでの周辺デバイスの保護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 機能が構成されたシステムは、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。

注記 - 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 11.2 でのシステムおよび接続されたデバイスのセキュリティー保護 』の第 4 章「デバイスアクセスの制御」を参照してください。

Trusted Extensions が構成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、テープドライブや CD-ROM 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。デバイスをリモートで割り当てるには、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 11.2 でのシステムおよび接続されたデバイスのセキュリティー保護 』の「デバイスポリシーの構成」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、テープドライブおよび CD-ROM 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 11.2 でのシステムおよび接続されたデバイスのセキュリティー保護 』の「デバイスクリーンスクリプト」を参照してください。

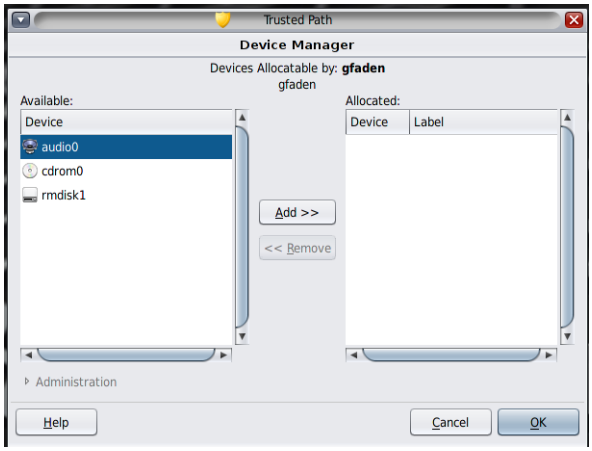
Trusted Extensions ソフトウェアの場合、デバイスクリーンスクリプトは一定の要件を満たさなくてはなりません。この要件については、`device_clean`(5) のマニュアルページを参照してください。

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。

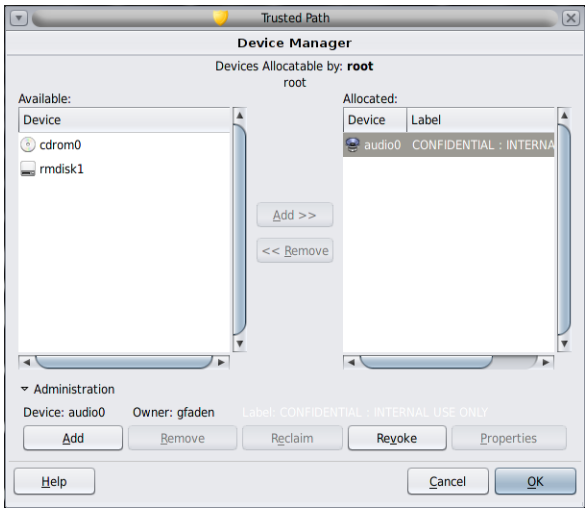
この GUI はデバイスマネージャーと呼ばれます。この GUI は、トラステッドパスメニューから「デバイスの割り当て」を選択することによって起動します。次の図は、`audio` デバイスを割り当てることのできるユーザーがデバイスマネージャーを開いたところです。

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 CD 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。CD 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 CD-ROM 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 11.2 でのシステムおよび接続されたデバイスのセキュリティー保護 』の「デバイス保護リファレンス」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 11.2 でのシステムおよび接続されたデバイスのセキュリティー保護 』の「デバイスを強制的に割り当てる方法」および『Oracle Solaris 11.2 でのシステムおよび接続されたデバイスのセキュリティー保護 』の「デバイスの割り当てを強制的に解除する方法」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

21 Trusted Extensions のデバイスの管理

この章では、Trusted Extensions が構成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

周辺デバイスを取り扱う管理者とユーザーのタスクマップは、次のとおりです。

表 21-1 Trusted Extensions でデバイスを処理するためのタスクマップ

タスク	説明	手順
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。	304 ページの「Trusted Extensions でデバイスを使用するためのタスクマップ」
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。	304 ページの「Trusted Extensions でのデバイスの管理」
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、新しいデバイス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。	312 ページの「Trusted Extensions でのデバイス承認のカスタマイズ」

Trusted Extensions でデバイスを使用するためのタスクマップ

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。次のタスクマップでは、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。

表 21-2 Trusted Extensions でデバイスを使用するためのタスクマップ

タスク	手順
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 ユーザーズガイド 』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。	79 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 」 78 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

次のタスクマップでは、サイトのデバイスを保護する手順について説明します。

表 21-3 Trusted Extensions でデバイスを管理するためのタスクマップ

タスク	説明	手順
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 11.2 でのシステムおよび接続されたデバイスのセキュリティー保護 』の「デバイスポリシーの構成」
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 11.2 でのシステムおよび接続されたデバイスのセキュリティー保護 』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。	312 ページの「Trusted Extensions でのデバイス承認のカスタマイズ」
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。	305 ページの「Trusted Extensions でデバイスマネージャーを使用してデバイスを構成する方法」
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。	309 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 11.2 でのシステムおよび接続されたデバイスのセキュリティー保

タスク	説明	手順
		護 』の「デバイスを強制的に割り当てる方法」 『Oracle Solaris 11.2 でのシステムおよび接続されたデバイスのセキュリティー保護 』の「デバイスの割り当てを強制的に解除する方法」
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「きめ細かいデバイス承認の作成」
	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「オーディオデバイスのリモート割り当ての禁止」
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。	311 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。	312 ページの「Trusted Extensions で Device_Clean スクリプトを追加する」

▼ Trusted Extensions でデバイスマネージャーを使用してデバイスを構成する方法

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、ウィンドウシステム上で変更できます。デスクトップのないシステムでは、大域ゾーン内の役割だけが割り当て可能なデバイスを構成および使用できます。

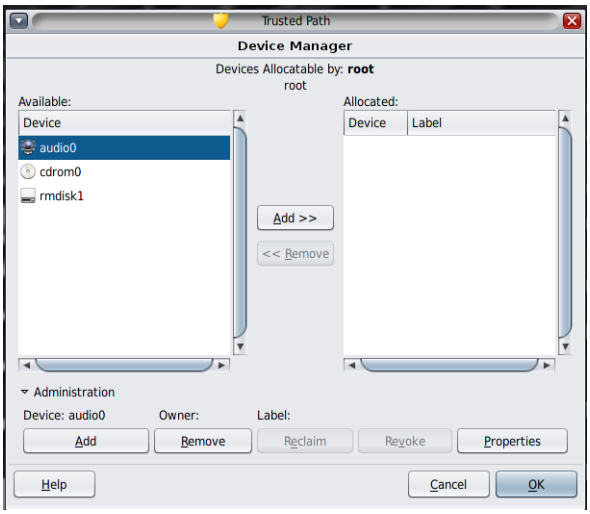
ウィンドウシステムでは、次のデバイスを割り当てて使用できます。

- `audio`*n* – マイクロフォンとスピーカーを表します
- `cdrom`*n* – CD-ROM ドライブを表します
- `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。

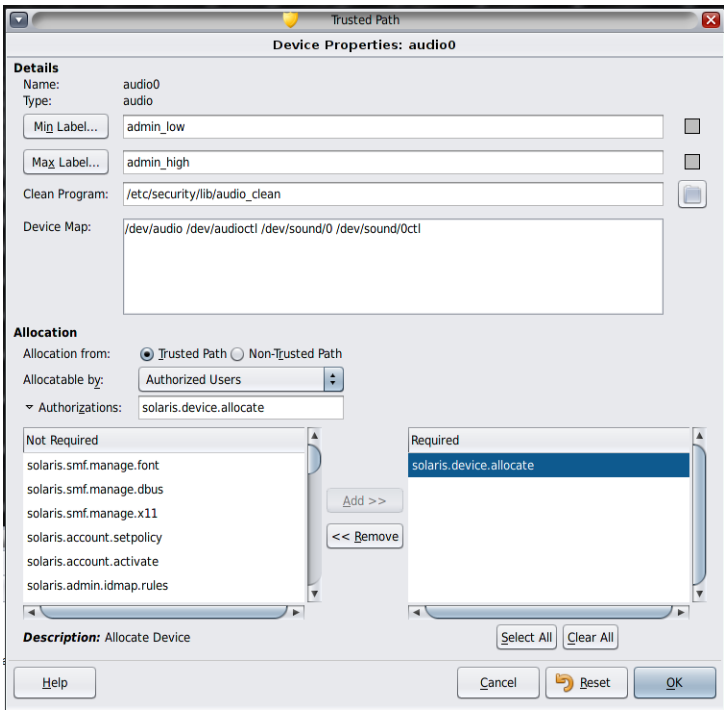
1. **「トラステッドパス」メニューから「デバイスの割り当て」を選択します。**

   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. **(オプション) 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。**

  フレームバッファー、または割り当て可能にしてはいけないほかのデバイスを構成する場合は、「なし」を選択します。

注記 - プリンタを割り当て用に構成することはできません。

- **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。**

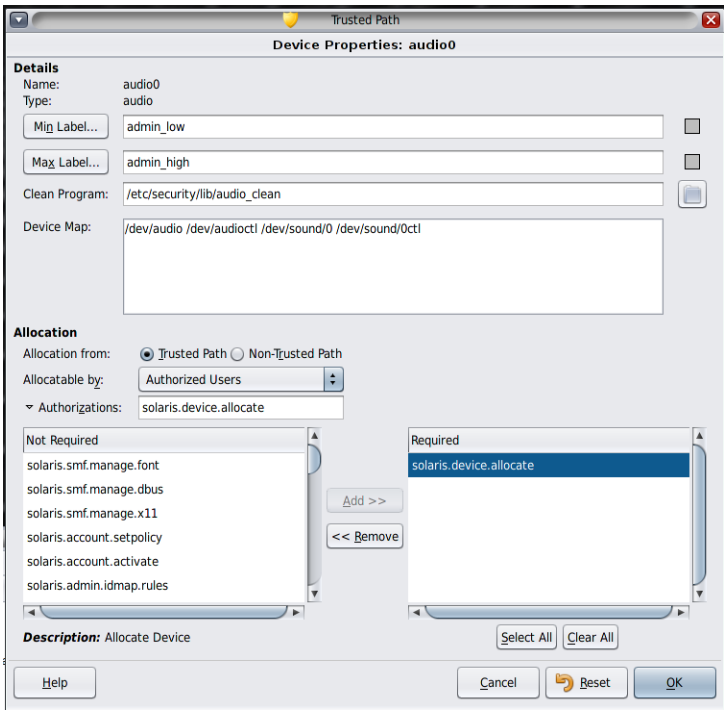
5. **デバイスがリモートで割り当て可能かどうかを指定します。**

   「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。**
   - **リモート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を作成および使用する場合は、312 ページの「Trusted Extensions でのデバイス承認のカスタマイズ」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。**

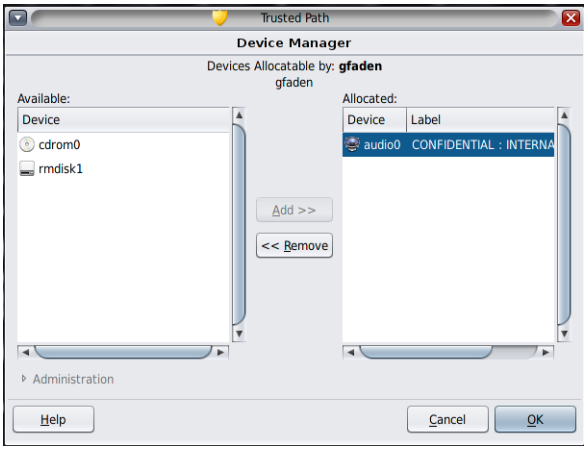
▼ Trusted Extensions でデバイスを解除または再利用する

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. **デバイスのステータスをチェックします。**

   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. **(オプション) 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リモート割り当ての禁止

「割り当てを行えるユーザー」セクションの「なし」オプションは、リモートユーザーがリモートシステムの周囲の会話を聞くことを禁止します。

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

次のタスクマップでは、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。

表 21-4　Trusted Extensions でデバイス承認をカスタマイズするためのタスクマップ

タスク	説明	手順
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。	313 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。	316 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。	317 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

デバイスが承認を必要としない場合、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。承認が必要な場合は、承認されたユーザーのみがそのデバイスを使用できます。

割り当て可能なデバイスへのアクセスをすべて拒否するには、例21-1「オーディオデバイスのリモート割り当ての禁止」を参照してください。新しい承認を作成して使用するには、例21-3「トラステッドパスデバイス承認と非トラステッドパスデバイス承認の作成と割り当て」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. **(オプション) 新しいデバイス承認ごとにヘルプファイルを作成します。**

   ヘルプファイルは HTML 形式です。命名規則は *AuthName*`.html` で、たとえば `DeviceAllocateCD.html` となります。

2. **デバイス承認を作成します。**

   ```
   # auths add -t "Authorization description" -h /full/path/to/helpfile.html authorization-name
   ```

3. **新しい承認を適切な権利プロファイルに追加します。**

   ```
   # profiles rights-profile
   profiles:rights-profile > add auths="authorization-name"...
   ```

4. **そのプロファイルをユーザーと役割に割り当てます。**

   ```
   # usermod -P "rights-profile" username
   # rolemod -P "rights-profile" rolename
   ```

5. **承認を使用して、選択したデバイス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、316 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

この例で、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作成します。

```
Newco.html
NewcoDevAllocateCDVD.html
NewcoDevAllocateUSB.html
```

次に、管理者はテンプレートヘルプファイルを作成します。ほかのヘルプファイルはこのテンプレートからコピーして変更します。

```
<HTML>
-- Copyright 2012 Newco.  All rights reserved.
-- NewcoDevAllocateCDVD.html
-->
<HEAD>
<TITLE>Newco Allocate CD or DVD Authorization</TITLE>
</HEAD>
<BODY>
The com.newco.dev.allocate.cdvd authorization enables you to allocate the
CD drive on your system for your exclusive use.
<p>
The use of this authorization by a user other than the authorized account
is a security violation.
<p>
</BODY>
</HTML>
```

ヘルプファイルを作成したあと、管理者は `auths` コマンドを使用して各デバイス承認を作成します。承認は会社全体で使用されるため、管理者は承認を LDAP リポジトリに置きます。コマンドにはヘルプファイルのパス名が含まれます。

管理者は 2 つのデバイス承認と Newco 承認ヘッダーを作成します。

- 1 つの承認は、ユーザーが CD-ROM または DVD ドライブを割り当てることを承認します。

```
# auths add -S ldap -t "Allocate CD or DVD" \
  -h /docs/helps/NewcoDevAllocateCDVD.html com.newco.dev.allocate.cdvd
```

- 1 つの承認は、ユーザーが USB デバイスを割り当てることを承認します。

```
# auths add -S ldap -t "Allocate USB" \
```

```
  -h /docs/helps/NewcoDevAllocateUSB.html com.newco.dev.allocate.usb
```

■ Newco 承認ヘッダーは、すべての Newco 承認を識別します。

```
# auths add -S ldap -t "Newco Auth Header" \
  -h /docs/helps/Newco.html com.newco
```

例 21-3 トラステッドパスデバイス承認と非トラステッドパスデバイス承認の作成と割り当て

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リモート CD-ROM および DVD 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.newco.dev.allocate.cdvd.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 および DVD ドライブ用です。com.newco.dev.allocate.cdvd.remote 承認は、トラステッドパス以外からの CD-ROM または DVD ドライブの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 データベースにデバイス承認を追加し、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。root 役割は、それらのプロファイルを、デバイスの割り当てを許可されているユーザーに割り当てます。

■ 次のコマンドは、デバイス承認を auth_attr データベースに追加します。

```
# auths add -S ldap -t "Allocate Local DVD or CD" \
  -h /docs/helps/NewcoDevAllocateCDVDLocal.html \
  com.newco.dev.allocate.cdvd.local
# auths add -S ldap -t "Allocate Remote DVD or CD" \
  -h /docs/helps/NewcoDevAllocateCDVDRemote.html \
  com.newco.dev.allocate.cdvd.remote
```

■ デバイスマネージャーの割り当ては次のとおりです。

CD-ROM ドライブのローカル割り当ては、トラステッドパスによって保護されます。

```
Device Name: cdrom_0
For Allocations From: Trusted Path
Allocatable By: Authorized Users
Authorizations: com.newco.dev.allocate.cdvd.local
```

リモート割り当てはトラステッドパスによって保護されないため、リモートユーザーは信頼できるユーザーでなければなりません。最後の手順で、管理者は 2 つの役割にのみリモート割り当てを承認します。

```
Device Name: cdrom_0
For Allocations From: Non-Trusted Path
Allocatable By: Authorized Users
Authorizations: com.newco.dev.allocate.cdvd.remote
```

- 次のコマンドは、これらの承認用の Newco 権利プロファイルを作成し、承認をプロファイルに追加します。

```
# profiles -S ldap "Remote Allocator"
profiles:Remote Allocator > set desc="Allocate Remote CDs and DVDs"
profiles:Remote Allocator > set help="/docs/helps/NewcoDevRemoteCDVD.html"
profiles:Remote Allocator > add auths="com.newco.dev.allocate.cdvd.remote"
profiles:Remote Allocator > end
profiles:Remote Allocator > exit

# profiles -S ldap "Local Only Allocator"
profiles:Local Only Allocator > set desc="Allocate Local CDs and DVDs"
profiles:Local Only Allocator > set help="/docs/helps/NewcoDevLocalCDVD.html"
profiles:Local Only Allocator > add auths="com.newco.dev.allocate.cdvd.local"
profiles:Local Only Allocator > end
profiles:Local Only Allocator > exit
```

- 次のコマンドは、承認されたユーザーに権利プロファイルを割り当てます。root 役割はプロファイルを割り当てます。このサイトでは、役割だけが周辺デバイスのリモート割り当てを承認されています。

```
# usermod -P "Local Only Allocator" jdoe
# usermod -P "Local Only Allocator" kdoe

# rolemod -P "Remote Allocator" secadmin
# rolemod -P "Remote Allocator" sysadmin
```

▼ 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、313 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. 305 ページの「Trusted Extensions でデバイスマネージャーを使用してデバイスを構成する方法」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、153 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 11.2 でのユーザーとプロセスのセキュリティー保護 』の「ユーザーへの権利の割り当て」を参照してください。
  次の権利プロファイルでは、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
  - 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21-2「きめ細かいデバイス承認の作成」は、承認を割り当てる方法を示しています。

♦ ♦ ♦ 第 22 章

22 Trusted Extensions と監査

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 での監査

Trusted Extensions ソフトウェアが構成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。計画の詳細は、『Oracle Solaris 11.2 での監査の管理 』の第 2 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62 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。

注記 - 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。構成に誤りがあると、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。

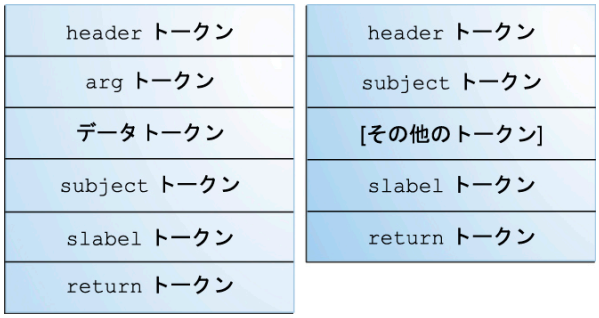
- セキュリティー管理者は、Trusted Extensions に固有の監査ポリシーである windata_down や windata_up を選択できます。
- システム管理者は、監査レコードの確認時に監査レコードをラベル別に選択できます。詳細は、auditreduce(1M) のマニュアルページを参照してください。

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
322 ページの「`label` トークン」	機密ラベル
323 ページの「`xatom` トークン」	X ウィンドウのアトム ID
323 ページの「`xcolormap` トークン」	X ウィンドウのカラー情報
323 ページの「`xcursor` トークン」	X ウィンドウのカーソル情報
323 ページの「`xfont` トークン」	X ウィンドウのフォント情報
324 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
324 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
324 ページの「`xproperty` トークン」	X ウィンドウのプロパティー情報
324 ページの「`xselect` トークン」	X ウィンドウのデータ情報
325 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

23 Trusted Extensions のソフトウェア管理

この章では、Trusted Extensions システムで、サードパーティー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 が構成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。ただし、ラベル付きゾーンで `pkg` コマンドを実行することにより、そのゾーンにパッケージをインストールすることができます。その場合は、そのゾーンが管理アカウントとパスワードプロンプトを処理できることを確認する必要があります。詳細は、24 ページの「ラベル付きゾーンに制限されているアプリケーション」を参照してください。パッケージとゾーンの詳細については、『Oracle Solaris ゾーンの作成と使用 』の第 9 章「ゾーンがインストールされている Oracle Solaris 11.2 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 11.2 でのユーザーとプロセスのセキュリティー保護 』の「ユーザー権利およびプロセス権利の基本情報」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 11.2 でのユーザーとプロセスのセキュリティー保護 』の第 1 章「権利を使用したユーザーとプロセスの制御について」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 ゾーンの作成と使用 』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 11.2 でのユーザーとプロセスのセキュリティー保護 』の「権利プロファイルの詳細」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オーバーライドが、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。このようなオーバーライドは、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、ポリシーのオーバーライド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 セキュリティー開発者ガイド 』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。`dtrace` を使用して、特権および承認の使用を評価することもできます。
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。

4. 新しいプログラムの権利プロファイルを作成して割り当てます。

♦ ♦ ♦ 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 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 ユーザーズガイド 』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 が構成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 が構成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ドキュメント化して、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。
- 操作ドキュメントと管理者ドキュメントは、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、報告およびドキュメント化して、原因を突き止めます。
- Trusted Extensions が構成されたシステムは、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 が構成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 が構成されたシステムへのアクセスをモニターおよびドキュメント化します。
- 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 (50 - 90˚F) 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、ドキュメント、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。
- 機密の印刷ドキュメント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。その他のセキュリティー関連の出版物は、UNIX セキュリティーの問題および解決方法を深く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。米国国土安全保障省 (http://www.us-cert.gov/security-publications)がセキュリティー情報を出版しています。また、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記事を発表しています。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 の安全な構成について解説。

- 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 の安全な構成について解説。
- 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 出版物

Sun Microsystems Security Engineers. *Solaris 10 Security Essentials*. Prentice Hall, 2009.

Garfinkel, Simson, Gene Spafford, and Alan Schwartz. *Practical UNIX and Internet Security, 3rd Edition*. O'Reilly & Associates, Inc, Sebastopol, CA, 2006.

Nemeth, Evi, Garth Snyder, Trent R. Hein, and Ben Whaley. *UNIX and Linux System Administration Handbook (4th Edition)* Pearson Education, Inc. 2010.

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. *Toward Systemically Secure IT Architectures*. Archived Oracle Technical Paper, June 2006.

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.

McClure, Stuart, Joel Scambray, George Kurtz. *Hacking Exposed 7: Network Security Secrets & Solutions, Seventh Edition*. McGraw-Hill, 2012.

Stoll, Cliff. *The Cuckoo's Egg*. Doubleday, 1989.

♦ ♦ ♦ 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、このガイド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。
   - 97 ページの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。
   - 334 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。
   - リモート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。
   - Oracle Solaris OS をインストールします。
3. Trusted Extensions を有効にします。37 ページの「Trusted Extensions のインストールおよび有効化」を参照してください。
   a. システムでマルチレベルのデスクトップを実行するかしないかに合わせて、適切な Trusted Extensions パッケージセットをロードします。

b. `labeladm enable` *options* コマンドを実行して、Trusted Extensions サービスを有効にします。

c. (オプション) `labeladm encodings` *encodings-file* コマンドを実行して、エンコーディングファイルをインストールします。

d. リブートします。

4. (オプション) 大域ゾーンをカスタマイズします。43 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. `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。

b. サイトの `label_encodings` ファイルを確認してインストールします。

c. リブートします。

5. ラベル付きゾーンを追加します。48 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 用の LDAP の構成」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構成はありません。

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ルーティングを構成します。54 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. ネットワークを構成します。229 ページの「ホストおよびネットワークへのラベル付け」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構成します。

- 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構成します。61 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。68 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。
- (オプション) 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. 印刷を構成します。285 ページの「ラベル付き印刷の構成」を参照してください。

e. デバイスを構成します。303 ページの「Trusted Extensions でのデバイスの扱い」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。

- 監査を構成します。
- 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 でユーザーを構成します。
- LDAP でネットワークの役割を構成します。

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」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。`labeladm` コマンドは、`labeld` サービスを有効および無効にし、Trusted Extensions システム用の `label_encodings` ファイルを設定します。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。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、196 ページの「Trusted Extensions での NFS サーバーとクライアントの構成」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、320 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。 305 ページの「Trusted Extensions でデバイスマネージャーを使用してデバイスを構成する方法」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」および例4-1「コマンド行での label_encodings 構文の検査」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、178 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、134 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。

labeladm(1M)	Trusted Extensions ラベル付けサービスを有効および無効にして、label_encodings ファイルを設定できます。
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、167 ページの「リモート 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、305 ページの「Trusted Extensions でデバイスマネージャーを使用してデバイスを構成する方法」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」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構成。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「リモート管理のための CIPSO ホストタイプの割り当て」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。 259 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、205 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。 48 ページの「ラベル付きゾーンの作成」および258 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」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 ユーザーズガイド 』の「Trusted Extensions でデバイスを割り当てる」を参照してください。
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 11.2 での監査の管理 』の「表示する監査イベントの選択」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、198 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 ユーザーズガイド 』の「Trusted Extensions でデバイスを割り当てる」を参照してください。
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ステータス SO_MAC_EXEMPT の取得
getsockopt(3XNET)	ソケットの必須のアクセス制御ステータス 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、258 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 拡張を追加します。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)	ソケットとルーティング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、205 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、205 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。 201 ページの「Trusted Extensions でファイルをバックアップする」および201 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 clearance および min_label ユーザーセキュリティー属性の追加 26 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

.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`、`.firefox` 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。

.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`、`.firefox` 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。

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。

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
認可上限またはラベル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セキュリティー属性を付与する役割。役割は、バックアップ、監査など、Oracle Solaris `root` 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ラベル。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 ラベルの非階層コンポーネントで、格付け コンポーネントとともに使用して認可上限やラベルを形成します。コンパートメントは、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。セキュリティー管理者 ファイルの最下位ラベルのフィールドで`security administrator`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 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。

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 が構成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。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。

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、適切な管理役割を持つ 1 人以上に対してセキュリティー管理者

の認可上限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構成します。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、プロセス、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 Trusted Extensions ネットワークにアクセスできるホストのクラスのセキュリティー属性を定義する `tnrhtp` データベースのレコードの 1 つ。

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、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 が構成されているシステムのネットワーク。このネットワークは Trusted Extensions 以外のホストから切り離されています。Trusted Extensions ネットワークの外へ配線せずに物理的に切り離すことができます。あるいは、Trusted Extensions ホストが Trusted Extensions ホストのみを認識するようにソフトウェアで切り離すことができます。ネットワークの外側からのデータ入力は、Trusted Extensions ホストに接続された周辺機器に制限されます。オープンネットワークと比較。

特権 コマンドを実行中のプロセスに付与される権限。完全セットの特権は、基本機能から管理機能に至るまでのシステムの完全機能です。システムクロックの設定などのセキュリティーポリシーをバイパスする特権は、サイトのセキュリティー管理者が付与できます。

ドメイン インターネットのネーミング階層の一部。ローカルネットワーク上のシステムのグループであり、管理ファイルを共有します。

ドメイン名 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 (通常はリモート) 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構成されている場合、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リモート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リモート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リモート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。下限は最下位ラベルが割り当てるセキュリティー管理者です。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、各システムはローカルの `/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、または機密ラベルのデバイス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。

Trusted Extensions ソフトウェアでは、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 に認定されるための評価、および多数の保護プロファイルに対する評価を実施中です。

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システムまたはリモート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。

プロセス 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。

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システム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 認可上限によって割り当てられるセキュリティー管理者で、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 一般ユーザーがシステム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 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構成したかによって、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。

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、一方のシステムのラベル `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リモートホストには、機密ラベルが 1 つのラベルに制限するその他のホストと同様に、1 つのセキュリティー管理者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。

リモートホスト ローカルシステムとは異なるシステム。リモートホストは、ラベルなしホストまたはラベル付きホストになります。

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。

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。

DAC 任意アクセス制御を参照。

GFI 政府提供情報 (Government Furnished Information の略)。このマニュアルでは、米国政府提供の label_encodings ファイルを指します。Trusted Extensions ソフトウェアで GFI を使用するには、Oracle 固有の `LOCAL DEFINITIONS` セクションを GFI の末尾に追加する必要があります。詳細は、『Trusted Extensions Label Administration 』の第 5 章「Customizing the LOCAL DEFINITIONS Section」を参照してください。

IP アドレス インターネットプロトコルアドレス。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 ネットワーク上のシステム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_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。

MAC 必須アクセス制御を参照。

tnrhdb データベース トラステッドネットワークのリモート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リモート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リモートホストテンプレート。このデータベースは、リモート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。

索引

か

さ

た

な

は

ま

や

ら

わ

A

C

D

G

H

I

K

L

M

N

O

P

R

S

T

U

V

X

Z