Solaris Trusted Extensions ラベルの管理

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

Part No: 819–7608–11
2008 年 4 月

原典: Solaris Trusted Extensions Label Administration

Part No: 819-0873-11

Revision A

080416@19860

目次

はじめに 11

1 Trusted Extensions ソフトウェアのラベル 17
ラベルとセキュリティーポリシー 17
ラベルの型、構成要素、および使用方法 19
ラベル範囲によるアクセス制限 19
アクセス制御の決定に使用されるラベル 20
ラベルの構成要素 21
ラベルの優位性 23
認可範囲、ラベル範囲、および有効なラベル 23
システム認可範囲 24
ユーザー認可範囲 25
アカウントラベル範囲 26
アカウントラベル範囲の例 27
セッション範囲 29
Trusted Extensions セッションでのラベルの使用可能性 32
ラベル付けされたワークスペース 33
ラベルの管理 34
ラベルの表示/非表示 34
印刷出力のラベル 34
情報の再ラベル付けの承認 35
ラベルを変換する特権 35

2 ラベルの計画 (手順) 37
ラベルの計画 (作業マップ) 37
▼ ラベルに関する戦略を立てる 38
▼ エンコーディングファイルを計画する 38

エンコーディングファイルのソース 42
Solaris Trusted Extensions パッケージのラベルファイル 42
label_encodings ファイルの Sun の拡張機能 46

3 ラベルエンコーディングファイルの作成 (手順) 47
エンコーディングファイルの構文 47
語句の順番 48
格付け名の構文 49
ラベルエンコーディングの管理 (作業マップ) 55
▼ label_encodings ファイルを作成する 55
▼ label_encodings ファイルを分析し、検証する 56
▼ label_encodings ファイルを配布する 57
▼ 格付けを追加または名前変更する 57
▼ デフォルト語句およびインバース語句を指定する 59
▼ 単一ラベルのエンコーディングファイルを作成する 60
▼ Sun の拡張機能をエンコーディングファイルに追加する 62
▼ label_encodings ファイルをデバッグする 63

4 プリンタ出力のラベル付け (手順) 65
本文ページのラベル 65
バナーページとトレーラページのセキュリティーテキスト 66
機密保護の格付けの指定 68
プリンタバナーの指定 69
チャネルの指定 71
印刷ジョブでのセキュリティーテキストの設定 (作業マップ) 76
▼ PRINTER BANNERS の語句を指定する 76
▼ CHANNELS の取り扱い指示を指定する 77
▼ 最下位の機密保護の格付けを設定する 78

5 LOCAL DEFINITIONS のカスタマイズ 81
LOCAL DEFINITIONS セクション 81
LOCAL DEFINITIONS セクションの内容 82
ラベルビルダーのカラムヘッダーの変更 82
ラベルの色の指定 83

Sun 拡張機能の変更 (作業マップ) 86
▼デフォルトのユーザーラベルを指定する 86
▼ラベルや語句に色を割り当てる 87
▼ラベルビルダーのカラムヘッダーに名前を付ける 88

6 例:組織のラベルの計画 89
自分のサイトにおけるラベルの条件の確認 89
情報保護の目標の達成 89
ラベル付けとアクセスを処理する Trusted Extensions の機能 90
セキュリティーの学習曲線 94
各ラベルの条件の分析 95
CONFIDENTIAL: INTERNAL_USE_ONLY の条件 95
CONFIDENTIAL: NEED_TO_KNOW の条件 95
CONFIDENTIAL: REGISTERED の条件 96
NEED_TO_KNOW ラベルのグループの名前 96
ラベルのセットの概要 97
ラベルのセットの定義 98
格付けの計画 99
コンパートメントの計画 99
MAC における語句の使用の計画 99
システム出力のラベル付けにおける語句の使用の計画 100
ラベルなしのプリンタ出力の計画 100
サポート手順の計画 101
ワークシートによる格付け値の計画 102
ワークシートによるコンパートメント値と組み合わせ制約の計画 103
ワークシートによる認可上限の計画 104
ワークシートによるプリンタバナーの計画 105
ワークシートによるチャネルの計画 106
認可範囲の最下位の計画 107
ワークシートによる色の計画 108
label_encodings ファイルの編集とインストール 109
バージョンのエンコーディング 109
格付けのエンコーディング 109
機密ラベルのエンコーディング 110
情報ラベルのエンコーディング 110

認可上限のエンコーディング 111
チャネルのエンコーディング 112
プリンタバナーのエンコーディング 113
認可範囲のエンコーディング 114
ローカル定義のエンコーディング 115
ラベルビルダーのカラムヘッダーのエンコーディング 115
色名のエンコーディング 115
ラベルに関するユーザーおよびプリンタの設定 116

A ラベルエンコーディングファイルのサンプル 119
格付けとコンパートメント 119
`label_encodings.example` ファイル 120

索引 127

図目次

図 1–1 テキストエディタのラベルとファイルのラベルの比較 21
図 1–2 CIPSO ラベル定義 22
図 1–3 TS、TS A、TS B、TS AB ラベルの表現 23
図 1–4 システム認可範囲が規則によって制約される様子 25
図 1–5 label_encodings ファイルの ACCREDITATION RANGE 部分 26
図 1–6 アカウントラベル範囲に対する制約 28
図 1–7 セッション範囲の比較 31
図 1–8 セッション範囲に対する制約の段階的効果 32
図 1–9 ワークスペーススイッチ領域 33
図 2–1 ラベルの関係を示す計画ボードの例 41
図 2–2 デフォルト label_encodings ファイルの格付け 44
図 2–3 デフォルト label_encodings ファイルのコンパートメント 44
図 4–1 本文ページに自動的に印刷されたラベル 66
図 4–2 典型的な印刷ジョブのバナーページ 67
図 4–3 トレーラページでの違い 67
図 4–4 機密保護の文 68
図 4–5 バナーページの PRINTER BANNERS の民間使用 70
図 4–6 バナーページの PRINTER BANNERS の官公庁使用 70
図 4–7 バナーページの CHANNELS の民間使用 72
図 4–8 バナーページの CHANNELS 指定の米国政府での使用 72
図 5–1 ラベルビルダーのカラムヘッダー 83
図 5–2 COLOR NAMES による色のウィンドウラベル 84
図 6–1 印刷ジョブの自動ラベル付け機能 91
図 6–2 本文ページに自動的に印刷されたラベル 92
図 6–3 制限されたラベル範囲のプリンタによるジョブの処理方法 93
図 6–4 アカウントラベル範囲内の電子メールを受信するユーザー 94
図 6–5 ラベルの関係を示す計画ボードの例 98

表目次

表 1–1 認可範囲とアカウントラベル範囲の例 28
表 1–2 Trusted Extensions セッションでのラベル 32
表 3–1 ラベルエンコーディングのキーワード 47
表 4–1 最下位の機密保護の格付けがプリンタ出力に及ぼす効果 69
表 6–1 各場所に設置されているプリンタのラベル範囲の設定例 102
表 6–2 格付けの計画 102
表 6–3 コンパートメントとユーザー認可範囲の組み合わせの計画シート 103
表 6–4 コンパートメントビットの管理表 104
表 6–5 認可上限計画シート 105
表 6–6 SecCompany 社のプリンタバナー計画シート 106
表 6–7 SecCompany 社のチャネル計画シート 107
表 6–8 SecCompany 社の色名計画シート 108

はじめに

Solaris Trusted Extensions ソフトウェアを設定しているシステムでは、情報を保護するために、ラベル、認可上限、および取り扱い指示を使用します。ラベル、認可上限、および取り扱い指示の構成要素は、`label_encodings` ファイルで指定します。このマニュアルは、このファイルの作成または変更について説明します。例も示されているので、サイトに適した `label_encodings` ファイルの作成およびインストールに役立ちます。

読者対象

このマニュアルは、セキュリティー管理者を対象とします。セキュリティー管理者は、組織のラベルの定義を担当します。ラベルの実装も担当する場合があります。定義担当者および実装担当者がこのマニュアルの対象者です。

注 – Trusted Extensions では、ラベルを表示しないように設定できますが、常にラベルは使用されています。ラベルは必須アクセス制御 (MAC) を提供し、常に MAC が実行されます。そのため、ユーザーまたは役割を作成する前に、サイトの `label_encodings` ファイルが準備されている必要があります。

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。セキュリティー管理者は、サイトに適したファイルを提供しなければなりません。

ラベルを実装するセキュリティー管理者は、Solaris の管理にも通じている必要があります。必要なレベルの知識は、トレーニングとマニュアルによって得ることができます。詳細は、13 ページの「マニュアル、サポート、およびトレーニング」を参照してください。

Solaris Trusted Extensions の関連マニュアル

Solaris Trusted Extensions 1.0 マニュアルセットは、Solaris 10 5/08 リリースのマニュアルを補足します。Solaris Trusted Extensions をより完全に理解するには、両方のマニュアルセットをお読みください。Solaris Trusted Extensions マニュアルセットは、次のマニュアルで構成されています。

マニュアルタイトル	内容	対象
『Solaris Trusted Extensions 移行ガイド』	旧版。Trusted Solaris 8 ソフトウェア、Solaris 10 5/08 ソフトウェア、および Solaris Trusted Extensions ソフトウェアの違いの概要。 このリリースでは、Trusted Extensions の変更点を『Solaris OS の概要』のマニュアルで概説しています。	全員
『Solaris Trusted Extensions リファレンスマニュアル』	旧版。Solaris 10 11/06 および Solaris 10 8/07 リリースにおける Trusted Extensions の Solaris Trusted Extensions マニュアルページが記載されています。 このリリースでは、Trusted Extensions のマニュアルページは Solaris のマニュアルページに含まれています。	全員
『Solaris Trusted Extensions ユーザーズガイド』	Solaris Trusted Extensions の基本的な機能の説明。用語集があります。	一般ユーザー、管理者、および開発者
『Solaris Trusted Extensions インストールと構成』	旧版。Solaris 10 11/06 と Solaris 10 8/07 リリースの Trusted Extensions における Solaris Trusted Extensions を計画、インストール、および構成する方法について説明しています。	管理者、開発者
『Solaris Trusted Extensions 構成ガイド』	Solaris 10 5/08 リリース以降において、Solaris Trusted Extensions を有効化、および最初に構成する方法を説明しています。旧版の『Solaris Trusted Extensions インストールと構成』に替わるものです。	管理者、開発者
『Solaris Trusted Extensions 管理の手順』	特定の管理タスクの実行方法。	管理者、開発者
『Solaris Trusted Extensions 開発ガイド』	Solaris Trusted Extensions によるアプリケーションの開発方法の説明。	開発者、管理者
『Solaris Trusted Extensions ラベルの管理』	ラベルエンコーディングファイルのラベル構成要素の指定に関する情報。	管理者
『コンパートメントモードワークステーションのラベル作成: エンコード形式』	ラベルエンコーディングファイルで使用される構文の説明。この構文では、システムの適格な形式のラベルに関するさまざまな規則を定めます。	管理者

このマニュアルの構成

- 第 1 章では、サイトの label_encodings ファイルを準備するセキュリティー管理者のために、ラベル関連の諸概念について説明します。
- 第 2 章では、サイトの label_encodings ファイルを準備するセキュリティー管理者のために、計画の手順について説明します。Trusted Extensions が提供するエンコーディングファイルについても説明します。
- 第 3 章では、label_encodings ファイルの作成、カスタマイズ、および検査の方法について説明します。
- 第 4 章では、プリンタ出力されるラベルおよび取り扱い指示について説明し、それを変更する手順を示します。
- 第 5 章では、label_encodings ファイルの省略可能な LOCAL DEFINITIONS セクションについて説明します。
- 第 6 章では、サイトにおいてそのラベルの要件を分析する方法、およびサイトにおいて label_encodings ファイルを作成する方法について説明します。
- 付録 A では、第 6 章 の label_encodings ファイルの例を示します。

マニュアル、サポート、およびトレーニング

Sun の Web サイトでは、次のサービスに関する情報も提供しています。

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

表記上の規則

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

表 P–1 表記上の規則

字体または記号	意味	例
AaBbCc123	コマンド名、ファイル名、ディレクトリ名、画面上のコンピュータ出力、コード例を示します。	.login ファイルを編集します。 ls -a を使用してすべてのファイルを表示します。 system%

表 P–1 表記上の規則 *(続き)*

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

コード例は次のように表示されます。

- C シェル

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

- C シェルのスーパーユーザー

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

- Bourne シェルおよび Korn シェル

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

- Bourne シェルおよび Korn シェルのスーパーユーザー

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

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

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

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

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

◆ ◆ ◆ 第 1 章

Trusted Extensions ソフトウェアのラベル

この章では、セキュリティー管理者が Trusted Extensions 用のラベルをエンコーディングするファイルを作成できるように準備します。この章の内容は次のとおりです。

- 17 ページの「ラベルとセキュリティーポリシー」
- 19 ページの「ラベルの型、構成要素、および使用方法」

この章を読む前に、次の箇所を読んでください。

- 『Solaris Trusted Extensions 管理の手順』の第 3 章「Trusted Extensions 管理者としての作業の開始 (手順)」 (セキュリティー管理者がセキュリティー管理者役割になるための準備)
- 『Solaris Trusted Extensions 管理の手順』の「Trusted Extensions ソフトウェアのラベル」

ラベルとセキュリティーポリシー

サイトセキュリティーポリシーは、組織がその専有情報を保護するために設定するセキュリティーポリシーです。Trusted Extensions ソフトウェアでは、ラベルおよび必須アクセス制御 (MAC) をこのポリシーに含めることができます。ラベルによって、システムセキュリティーポリシーの一部である一連の規則が実装されます。システムセキュリティーポリシーは、システムで処理される情報を保護するためにシステムソフトウェアから強制される規則です。セキュリティーポリシーという用語は、ポリシー自体を指す場合と、ポリシーの実装を指す場合があります。

Trusted Extensions によって構成されるすべてのシステムにはラベルがあります。ラベルは、`label_encodings` ファイルで指定されます。このファイルについては、`label_encodings(4)` のマニュアルページを参照してください。Solaris Trusted Extensions パッケージで提供されるエンコーディングファイルについては、42 ページの「エンコーディングファイルのソース」を参照してください。

Trusted Extensions では、デフォルトバージョンの label_encodings ファイルがインストールされます。デフォルトバージョンはいくつかの商用ラベルを提供します。このバージョンは、場合によって、学習目的で本稼働環境以外でも使用されます。サイトでは、Solaris Trusted Extensions パッケージで提供されるラベルエンコーディングファイルのいずれかをカスタマイズすることもできます。サイト固有のファイルの例は、付録 A を参照してください。

Trusted Extensions ネットワークのすべてのコンピュータには、サイトの label_encodings ファイルのコピーが必要です。コンピュータ相互運用性のため、ネットワーク内のすべてのコンピュータの label_encodings ファイルは互換性のある必要があります。少なくとも、各コンピュータがネットワーク内のほかのすべてのコンピュータで使用されるラベルを認識できるようにします。

特定の型のラベルは定義する必要があります。セキュリティー管理者は、ラベルの内部表現を構成する数値とビットを指定します。ユーザーおよび役割は、ラベルのそのテキスト表現を参照します。ラベル付けソフトウェアによって、ラベルの内部形式とテキスト形式が変換されます。label_encodings ファイルは、ラベルの内部表現をテキスト文字列に変換するための規則を提供します。そのテキスト文字列はデスクトップに表示できます。内部表現は監査証跡に記録され、praudit コマンドによって解釈されます。

「セキュリティー管理者」は、組織のセキュリティーポリシーの実装を定義および計画します。セキュリティー管理者は情報保護のための手順を定め、コンピュータユーザーおよび管理者が適切なトレーニングを受けるようにし、ポリシーが遵守されているかを監視します。

ソフトウェア内にセキュリティー管理者役割を作成します。この役割は、Trusted Extensions の管理について十分に理解している 1 人以上の管理者に割り当てられます。Trusted Extensions によって処理される最高レベルの情報を表示および保護するために、この管理者が認可されます。セキュリティー管理者の責務の 1 つは、Sun によってインストールされる label_encodings ファイルの代わりとなる、サイト用のファイルを作成することです。管理者は、ラベルをデスクトップ上に表示するかどうかを決定することもできます。ラベルが表示されなくても、システム上のオブジェクトおよびプロセスにはラベルが付けられ、MAC が強制的に行われます。

Trusted Extensions では、組織のセキュリティーポリシーを実施するためのツールおよび機能がセキュリティー管理者役割に提供されています。この役割になるには、最初、一般ユーザーとしてログインしてください。サイトによっては、サイトのセキュリティーポリシーを定義するセキュリティー管理者が、ポリシーを実装する管理者と異なることもあります。

ラベルの型、構成要素、および使用方法

Trusted Extensions では、次の 2 つの型のラベルが定義されます。

- 認可上限ラベル (単に「認可上限」とも言う)
- 機密ラベル (単に「ラベル」とも言う)

機密ラベル、ラベル範囲、およびラベル制限 (認可上限) では、システム上のどのオブジェクトにだれがアクセスできるかが決定されます。認可上限ラベルはユーザーに割り当てられます。機密ラベルは、ユーザープロセスを含むプロセス、およびファイルやディレクトリに割り当てられます。

一部のオブジェクトにはラベル範囲があります。そのオブジェクトには、定義されたラベル範囲内の特定のラベルでアクセスできます。ラベル範囲が `ADMIN_LOW` から `ADMIN_HIGH` までの場合、すべてのラベルでアクセスできます。セキュリティー管理者はこのラベル範囲を狭めることができます。ラベル範囲があるオブジェクトは、次のとおりです。

- 通信が可能な全ホストおよびネットワーク
- ゾーン
- ユーザーおよび役割
- 割り当て可能なデバイス (テープドライブ、フロッピードライブ、CD-ROM や DVD のデバイス、オーディオデバイスなど)
- 割り当て不可能なその他のデバイス (フレームバッファーのラベル範囲によって制御されるプリンタ、ワークステーションなど)、およびログインデバイスとして使用される場合のシリアル回線

これらのオブジェクトにラベルを設定する場合のさまざまな方法については、『Solaris Trusted Extensions 管理の手順』を参照してください。『Solaris Trusted Extensions 管理の手順』の「デバイス割り当てマネージャー GUI」に、ラベル範囲をデバイスに設定する方法が説明されています。

ラベル範囲によるアクセス制限

ラベル範囲は、次のラベルに対して制限を設定します。

- ホストで情報の送受信を行うことができるラベル。
- ユーザーや役割に代わって動作しているプロセスがアクセスできるゾーン内のファイルやディレクトリのラベル。
- ユーザーがデバイスを割り当てることができるラベル。すなわち、そのデバイスの記憶媒体にファイルが書き込まれるラベルを制限します。
- ユーザーがジョブを送信できるプリンタのラベル。

- ユーザーがログインできるワークステーションのラベル。ユーザーのラベル範囲のほかに、フレームバッファーのラベル範囲を使用して、システムへのアクセスを制限することもできます。

ラベルは自動的に電子メールメッセージに割り当てられ、電子メールの出力に表示されます。

アクセス制御の決定に使用されるラベル

コンピュータのアクセスの実装およびアクセスの制御のために、ラベルが使用されます。ラベルは、必須アクセス制御 (MAC) を実装します。Trusted Extensions では、オブジェクトへのアクセスが許可される前に、任意アクセス制御 (DAC) 検査と MAC 検査に合格しなければなりません。Solaris OS の場合と同様、DAC は、アクセス権ビットとアクセス制御リスト (ACL) に基づきます。詳細は、『Solaris のシステム管理 (セキュリティサービス)』の第 6 章「ファイルアクセスの制御 (作業)」を参照してください。

MAC は、アプリケーションを実行しているプロセスのラベルと、そのプロセスがアクセスしようとしているオブジェクトのラベルまたはラベル範囲を比較します。ラベルに実装されている規則セットによって、ポリシーが実施されます。規則の 1 つに「下位読み取り、同位読み取り」があります。プロセスがオブジェクトにアクセスしようとすると、この規則が適用されます。プロセスのラベルは、次のようにオブジェクトのラベル以上である必要があります。

```
Label[Process] >= Label[Object]
```

Trusted Extensions によって構成されているシステムでは、ファイルとディレクトリのアクセス規則は相互に少し異なり、プロセスオブジェクト、ネットワーク終端オブジェクト、デバイスオブジェクト、および X ウィンドウオブジェクトとも少し異なります。また、オブジェクトへのアクセスには 3 つの方法があります。オブジェクトにアクセスする 3 つの方法には、それぞれ、次のように少しずつ異なる規則セットが適用されます。

- ファイル、ディレクトリ、またはデバイスの名前を表示できる
- ファイル、ディレクトリ、またはデバイスの内容または属性を表示できる
- ファイル、ディレクトリ、またはデバイスの内容または属性を変更できる

図 1–1 に、ラベルを使用してアクセス制御を決定するシステムを示します。

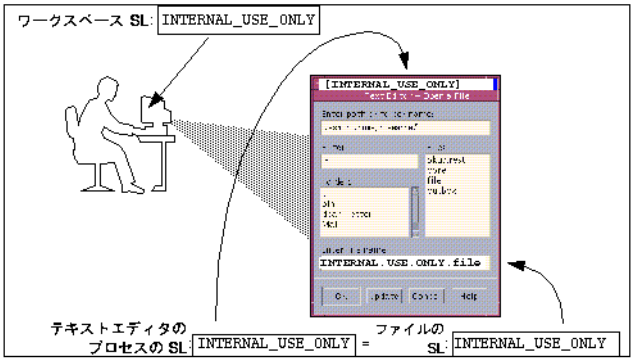


図 1–1 テキストエディタのラベルとファイルのラベルの比較

前の図で、ユーザーはラベル INTERNAL_USE_ONLY のワークスペースでテキストエディタを開いています。システムは、テキストエディタを実行しているプロセスのラベルを現在のワークスペースのラベルと同じに設定します。そのため、テキストエディタに INTERNAL_USE_ONLY のラベルが表示されます。編集のためにテキストエディタでファイルを開こうとすると、テキストエディタを実行しているプロセスのラベルとファイルのラベルが比較されます。2 つのラベルが等しい場合、書き込みアクセスが許可されます。

ファイルのラベルがテキストエディタのラベルより下位の場合、ファイルは読み取り専用で開かれます。たとえば、INTERNAL_USE_ONLY のテキストエディタは ADMIN_LOW のシステムファイルを開いて読み取ることができますが、変更はできません。また、下位読み取りの要件によって、現在の作業ラベルより上位のラベルのファイルをユーザーは参照できません。

ラベルの構成要素

ラベルと認可上限は、1 つの「格付け」と 0 または 1 つ以上の「コンパートメント」語句で構成されます。ラベルの格付け部分は、保護の相対レベルを示します。ラベルがオブジェクトに割り当てられると、ラベルの格付けが、オブジェクトに含まれている情報の機密度を示します。認可上限がユーザーに割り当てられると、認可上限ラベルの格付け部分が、ユーザーの信頼度を示します。

Trusted Extensions は CIPSO (Common IP Security Option) ラベルをサポートします。ラベルと認可上限ラベルのそれぞれには、256 個までの値を指定できる格付けフィールド、および 256 ビットのコンパートメントフィールドがあります。格付けに 0 (ゼロ) は使用できないので、合計 255 個の格付けを定義できます。CIPSO ラベルには、240 個のコンパートメントビットを使用できるので、合計 2^{240} のコンパートメントの組み合わせが可能です。これらの構成要素を次の図に示します。

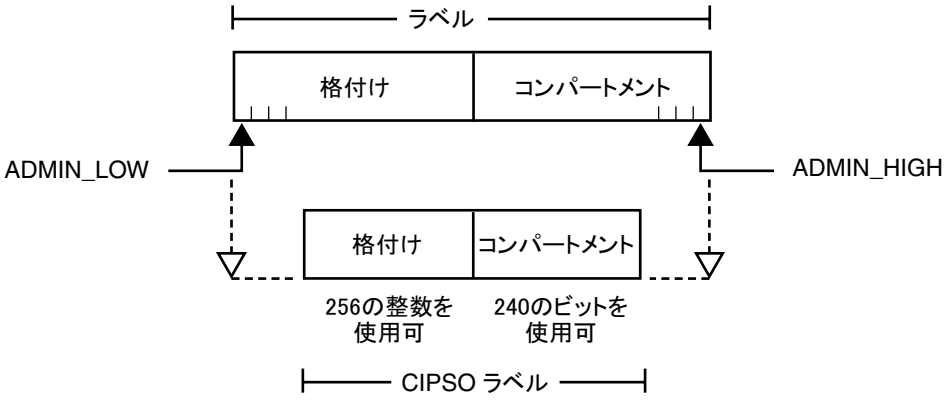


図 1–2 CIPSO ラベル定義

ADMIN_HIGH ラベルと ADMIN_LOW ラベルは管理ラベルです。これらのラベルはシステム上のすべてのラベルの上限と下限を定義します。

各コンパートメント語句には、1 ビット以上のコンパートメントビットが割り当てられています。同じコンパートメントビットを 1 つ以上の語句に割り当てることができます。

テキスト形式の格付けは、次のようになります。

```
CLASSIFICATIONS:

name= TOP SECRET; sname= TS; value= 6;initial compartments= 4-5;
```

ラベルのコンパートメント部分は省略可能です。ラベルのコンパートメント語句を使用して、ワークグループ、部、課、地理上区域などの異なる種類のグループを表すことができます。コンパートメント語句によって、情報の処理方法を指定することもできます。

初期コンパートメントが格付け定義の一部である場合、コンパートメントがそのラベルの一部になります。

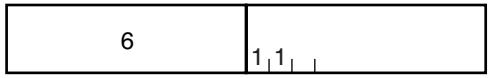
```
WORDS:

name= A;          compartments= 0;
name= B;          compartments= 1;
name= CNTRY1;      sname= c1;      compartments= ~4;
name= CNTRY2;    sname= c2;      compartments= ~5;
```

前の格付けおよびコンパートメントから使用可能なラベルには、TS、TS A、TS B、および TS AB があります。TS A のファイルは、TS 格付けと認可上限に A コンパートメントを持つユーザーのみが使用できます。説明図は、図 1–3 を参照してください。

ラベルの優位性

任意の型のラベルと別のラベルを比較したときに、前者のセキュリティーレベルが後者のそれと同等かそれよりも高い場合、前者が後者よりも「優位である」と言います。このセキュリティーレベルの比較は、ラベルの格付けとコンパートメントに基づきます。優位なラベルの格付けは、2 つ目のラベルの格付けと同等かそれよりも高くなければなりません。優位なラベルには、もう一方のラベルのコンパートメントのすべてが含まれていなければなりません。2 つのラベルが同等な場合は、「互いに優位である」と言います。

この基準により、TS A は TS より優位であり、TS は TS より優位です。TS ラベルの格付けとコンパートメントビットを次の図に示します。




```
TOP SECRET        A
value = 6         compartments = 0
                  B
                  compartments = 1
```

図 1–3　TS、TS A、TS B、TS AB ラベルの表現

別の種類の優位性である「完全な優位性」が、アクセスの際に必要とされる場合もあります。あるラベルのセキュリティーレベルが別のラベルのセキュリティーレベルより高い場合、そ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。完全な優位性には、同等の部分がありません。最初のラベルの格付けは、2 つ目のラベルの格付けより高いです。最初のラベルには、2 つ目のラベルのすべてのコンパートメントが含まれます。あるいは、両方のラベルの格付けが同じである場合、最初のラベルには 2 つ目のラベルのすべてのコンパートメントが含まれ、さらにその他のコンパートメントが 1 つ以上含まれます。

優位関係がないラベルは「無関係」であると言われます。無関係なラベルは、会社内の各部門を振り分けるのに適しています。たとえば、ラベル TS HR (人事) は TS Sales から分離しています。

認可範囲、ラベル範囲、および有効なラベル

label_encodings ファイルでは、ラベル構成要素の一定の組み合わせが規則によって無効とされます。組み合わせの規則によって、組織で使用可能なラベルが暗黙的に定義されます。組み合わせの規則はセキュリティー管理者が指定します。

「有効」または「適格な形式」のラベルとは、組み合わせの規則に従っているラベルのことです。セキュリティー管理者は、次のいずれかの方法によって組み合わせの規則を定義します。

- 「初期コンパートメント」(コンパートメントビット) を格付けに割り当てることができます。

  初期コンパートメントビットは、ラベル内で常にこの格付けに関連付けられます。詳細は、49 ページの「格付け名の構文」を参照してください。
- 「最下位の格付け」、「出力の最下位の格付け」、「最上位の格付け」を任意の語句に関連付けることができます。
- 各語句に選択する「ビットパターン」によって、語句間の「階層」を定義します。
- 語句の「必須組み合わせ」を指定します。
- 「組み合わせ制約」を語句に指定します。
- 「*minimum clearance* (最下位の認可上限)」および「*minimum sensitivity label* (最下位の機密ラベル)」 を指定する必要があります。

  システム全体に関わるこれらの最下位の指定によって、一般ユーザーに認められる`minimum clearance` (最下位の認可上限) および最下位ラベルが定められます。

`label_encodings` ファイルには、次の 2 つの「認可範囲」が暗黙的に指定されています。

- 24 ページの「システム認可範囲」
- 25 ページの「ユーザー認可範囲」

「認可範囲」という用語は、ユーザーアカウント、役割アカウント、プリンタ、ホスト、ネットワークなどのオブジェクトに割り当てられているラベル範囲も指します。規則は一連の有効なラベルを制約できるので、ラベル範囲および認可範囲には、範囲内のラベル構成要素のすべての可能な組み合わせが含まれないことがあります。

システム認可範囲

システム認可範囲には、管理ラベルの `ADMIN_HIGH` および `ADMIN_LOW` が含まれます。さらに、システム認可範囲には、`label_encodings` ファイルのラベル構成要素から構成されるすべての適格な形式のラベルも含まれます。

管理役割アカウントは、通常、システム認可範囲内のすべてのラベルで作業可能な唯一のアカウントです。組織では、管理ラベルを必要とするタスクを実行可能な一般ユーザーアカウントを設定することもできます。

次の図は、システム認可範囲で許可されるラベルが規則によってどのように制約されるかを示しています。

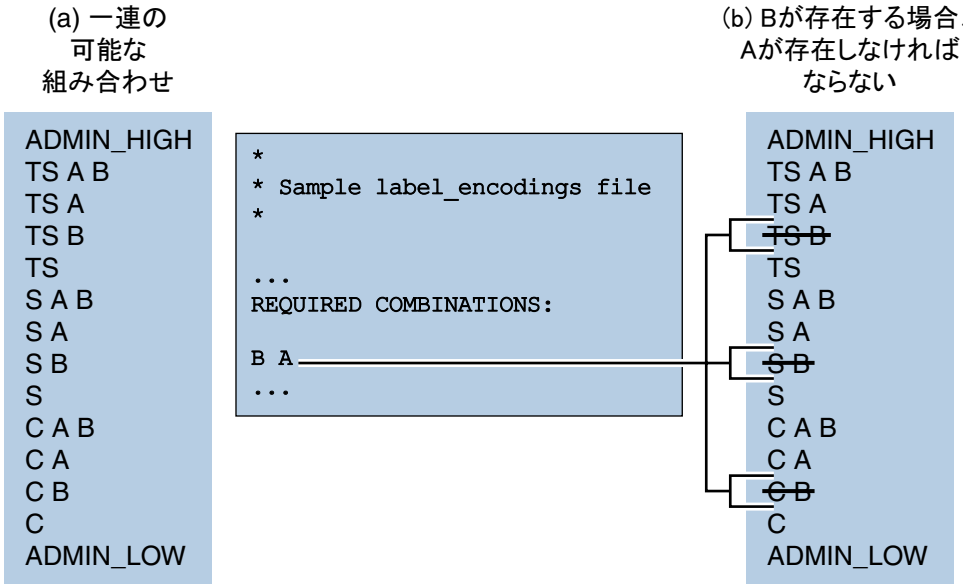


図 1–4 システム認可範囲が規則によって制約される様子

図 1–4 (a) は、格付け TS (TOP SECRET)、S (SECRET)、 C (CONFIDENTIAL)、およびコンパートメント A、 B によるすべての可能な組み合わせを示します。

図 1–4 (b) は、SENSITIVITY LABELS セクションの REQUIRED COMBINATIONS サブセクションによる代表的な規則とその結果を示します。矢印は規則によって無効にされるラベルを示します。無効にされるラベルは上に線が引かれています。REQUIRED COMBINATIONS 構文 B A は、コンパートメントとして B を持つラベルには A が含まれていなければならないことを示します。その逆は当てはまりません。コンパートメント A に、その他のコンパートメントを組み合わせる必要はありません。コンパートメント B は A がある場合にのみ許可されるので、ラベル TS B、S B、および C B は適格な形式ではありません。適格な形式でないラベルはシステム認可の範囲外です。

ユーザー認可範囲

「ユーザー認可範囲」は、Trusted Extensions の使用時に、一般ユーザーがアクセスできる最大のラベルセットです。ユーザー認可範囲では、ADMIN_HIGH および ADMIN_LOW が常に除外されます。ユーザー認可範囲は、24 ページの「システム認可範囲」を制約するすべての規則によってさらに制約されます。また、ACCREDITATION RANGE セクションの規則によってユーザー認可範囲を制約することもできます。図 1–5 は図 1–4 の例から続きます。図 1–5 は、ACCREDITATION RANGE セクションの 3 つの異なるタイプの規則と、そのユーザー認可範囲の結果を示します。矢印は特定の規則が許可する適格な形式のラベルを示します。

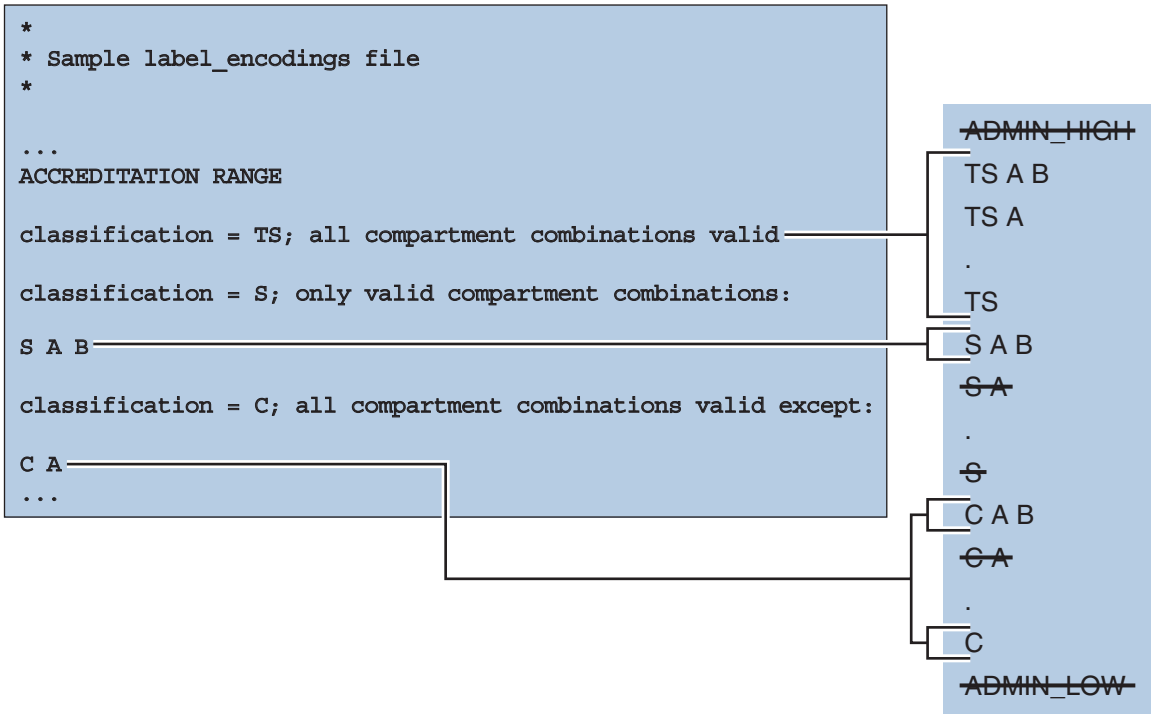


図 1–5 label_encodings ファイルの ACCREDITATION RANGE 部分

右側のボックスに示すように、ユーザー認可範囲は ADMIN_HIGH および ADMIN_LOW を除外します。TS 格付けの規則には、TS B を除くすべての TS の組み合わせが含まれます。ただし、図 1–4 に示すように TS B、S B、および C B は REQUIRED COMBINATIONS 規則 B A によって以前に無効にされているため、TS の組み合わせで許可されるのは、TS A B、TS A、および TS のみです。S A B が S 格付けの唯一の有効な組み合わせとして定義されているため、S B はやはり除外されます。C 格付けの規則に従えば、C A を除くすべての C の組み合わせが有効です。ただし、C B は以前に無効にされているので、C 格付けの許可される組み合わせは C A B および C のみです。

アカウントラベル範囲

「アカウントラベル範囲」は、各ユーザーまたは役割アカウントが使用可能なラベルの範囲です。システムへのログイン時にユーザーが作業できるラベルを、この範囲で制御します。

アカウントラベル範囲で使用可能なラベルには、次の制約があります。

- ユーザー認可上限がアカウントラベル範囲の最上位を定める。

  認可上限は有効なラベルである必要はありません。認可上限は、アカウントが作業するすべてのラベルより優位である必要があるため、アカウントが作業するすべてのラベルのすべての構成要素を含んでいなければなりません。
- 最下位のラベルがアカウントラベル範囲の最下位を定める。

  `label_encodings` ファイルの `minimum sensitivity label` (最下位の機密ラベル) は、ユーザーが作業可能なラベルの絶対最下位を決定します。
- ユーザー認可範囲が、ユーザーの認可上限からユーザーの最下位のラベルまでの有効なラベルのセットを定める。

例 1–1 有効なラベルではない有効な認可上限の定義

たとえば、`label_encodings` ファイルで、ラベルのコンパートメント `A`、`B`、および `C` の組み合わせを禁止できます。

- 最下位のラベルはコンパートメントがない `TS` になる。
- `TS A B C` が有効な認可上限になる。`TS A B C` は有効なラベルでなくなる。
- ユーザーの有効なラベルは `TS`、`TS A`、`TS B`、および `TS C` になる。

アカウントラベル範囲の例

アカウントに割り当てることができる認可上限および最下位のラベルを、次の図に示します。これらのラベルは、これまでの節で説明した認可の例に基づいています。

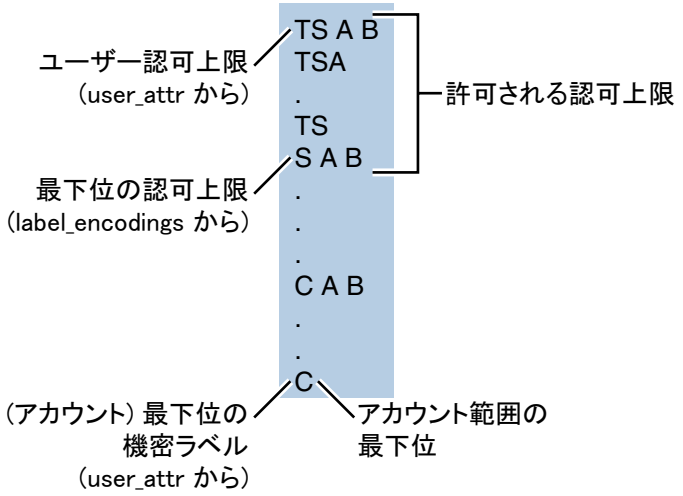


図1–6 アカウントラベル範囲に対する制約

この例で、TS A B がユーザー認可範囲の最上位ラベルです。このラベルには、どの格付けのラベルでも一緒に表示されることが許可される 2 つのコンパートメント A および B のみが含まれます。左側に示されているアカウント範囲は、TS A B によって最上位が定められています。TS A B はアカウントに割り当てられている認可上限です。C はアカウントの最下位のラベルです。これらの定義によって、ラベル TS A B、TS A、TS、S A B、C A B、または C で作業するアカウントが制約されます。許可される認可上限は TS A B、TS A、TS、および S A B です。minimum clearance (最下位の認可上限) の S A B が label_encodings ファイルに設定されます。

TS A B が有効なラベルではなかったとしても、セキュリティー管理者はそのラベルを認可上限として割り当てることができます。この割り当てによって、TS のほうが優位であり、かつ語句 A および B を含む、任意の有効なラベルを、アカウントで使用できるようになります。逆に、TS をアカウント認可上限として割り当てた場合、ユーザーはラベル TS および C でのみ作業できます。コンパートメントを持たない TS は S A B または C A B に対して優位になりません。

表1–1 認可範囲とアカウントラベル範囲の例

	認可範囲		アカウントラベル範囲		
可能なラベル	システム	ユーザー	TS A B 認可上限、S A B 最下位のラベル	TS 認可上限、C 最下位のラベル	ADMIN_LOW 認可上限および最下位のラベル、solaris.label.range 承認
ADMIN_HIGH	ADMIN_HIGH				
TS A B	TS A B		TS A B		
TS A	TS A	TS A	TS A		

表 1–1 認可範囲とアカウントラベル範囲の例 (続き)

	認可範囲		アカウントラベル範囲		
可能なラベル	システム	ユーザー	TS A B 認可上限、S A B 最下位のラベル	TS 認可上限、C 最下位のラベル	ADMIN_LOW 認可上限および最下位のラベル、solaris.label.range 承認
TS	TS	TS	TS	TS	
S A B	S A B	S A B	S A B		
S A					
S				S	
C A B	C A B				
C A	C A				
C	C	C		C	
ADMIN_LOW	ADMIN_LOW				ADMIN_LOW

表 1–1 は、可能なラベルの組み合わせ、システム認可範囲、ユーザー認可範囲、およびいくつかのアカウントラベル範囲の例における違いを示しています。

- 何も承認されていない一般ユーザーは、ユーザー認可範囲の列にあるラベルでしか作業できません。
- 4 列目は、認可上限 TS A B および最下位のラベル S A B のユーザーのアカウントラベル範囲を示します。この範囲では、ユーザーはラベル TS A B、TS A、TS、および S A B で作業できます。
- 表 1–1 の 5 列目は、認可上限 TS および最下位のラベル C のアカウントを示します。TS が優位になるその他のすべての有効なラベルには語句 A および B が含まれるので、このアカウントは TS、S、および C のラベルでのみ作業できます。A および B は認可上限にありません。
- 6 列目は、ユーザー認可範囲外で作業することが承認されているユーザーを示します。このユーザーには 1 つのラベル ADMIN_LOW が割り当てられます。

セッション範囲

「セッション範囲」は、Trusted Extensions セッション時にユーザーアカウントで使用できるラベルのセットです。セッション範囲は次を対象として制約します。

- ユーザーのラベル範囲
- ユーザーが選択したラベル
- ローカルシステムのラベル範囲

単一ラベルアカウントのセッション範囲は、アカウントのラベルです。ユーザーアカウントが複数のラベルを使用できるように設定されている場合にのみ、一連のラベルからの選択が可能です。複数のラベルを使用できるように設定されているユーザーアカウントは、セッション中に異なるラベルを選択できます。ラベルの指定については『Solaris Trusted Extensions ユーザーズガイド』の「ワークスペースのラベルを変更する」を参照してください。

ログイン時に選択した単一のラベルまたはセッションの認可上限は、ログアウトするまでのそのセッションを通じて有効です。マルチラベルセッションでは、セッション認可上限からユーザーの最下位ラベルまでの間の任意の有効なラベルで、ユーザーが作業できます。

図 1–6 の例は図 1–7 に続きます。この例では、ユーザーは TS A B と S A B の間の適格な形式のラベルを使用するセッション認可上限を指定できます。

図 1–7 の (a) は、ユーザーがセッション認可上限 S A B のマルチラベルセッションを選択した場合に使用可能なラベルを示します。S A B と C の中間にあるその他のラベルは適格な形式ではないので、ユーザーは S A B、C A B、または C でのみ作業できます。

図 1–7 の (b) は、ユーザーがセッションラベル C A B の単一ラベルセッションを選択した場合に使用可能なラベルを示します。C A B は minimum clearance (最下位の認可上限) より下位にあります。ただし、ユーザーは認可上限ではなくセッションラベルを選択するので、C A B はアクセス可能です。セッションは単一ラベルなので、ユーザーは 1 つのラベルでのみ作業できます。ユーザーは S A B または C を選択することも可能でしたが、この例では C A B を指定しました。

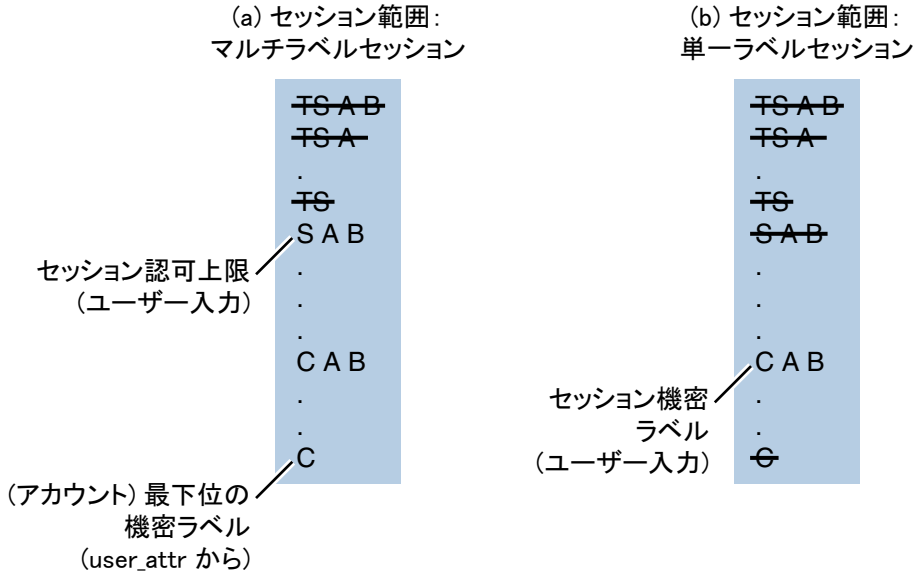


図 1–7 セッション範囲の比較

次の図に、この例で使用可能なラベルを段階的に除外して示します。それぞれの範囲で除外されるラベルは上に線が引かれます。除外されたラベルは、それ以降の範囲では表示されません。

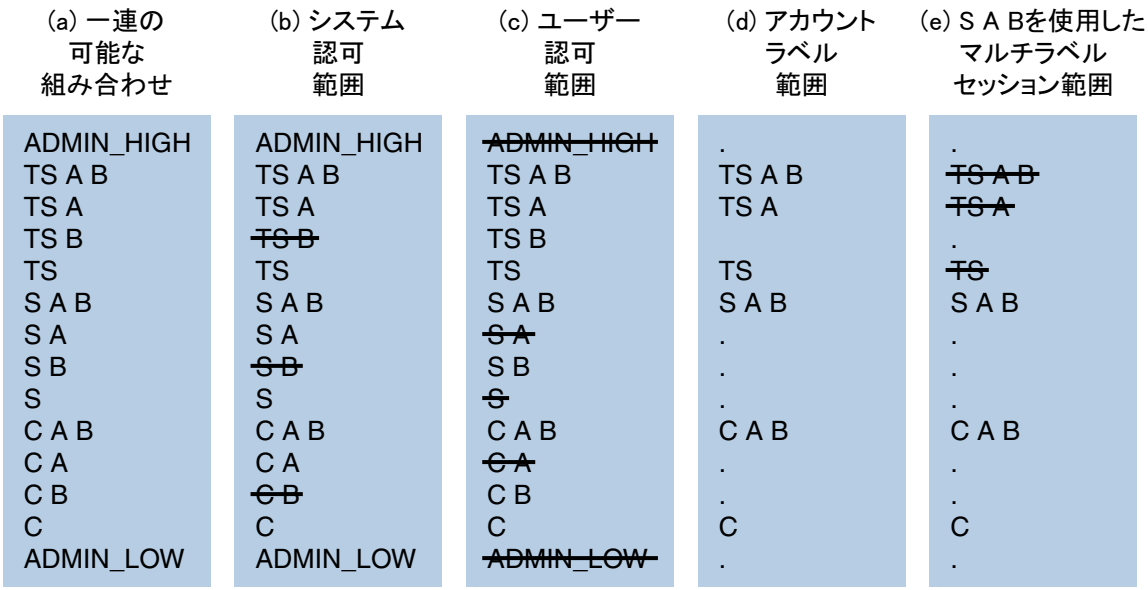


図 1–8　セッション範囲に対する制約の段階的効果

Trusted Extensions セッションでのラベルの使用可能性

次の表は、ユーザーのセッション選択に基づくセッションラベルの制限および使用可能性を示しています。この表は、図 1–8 の例から続くものです。

表 1–2　Trusted Extensions セッションでのラベル

	マルチレベルセッション		単一レベルセッション	
	通常の場合	例 #1	通常の場合	例 #2
		認可上限 SECRET A B のマルチレベル		セッションラベル SECRET A B の単一レベル
初期ワークスペースラベル (最初のログイン時)	アカウントラベル範囲の最下位ラベル	CONFIDENTIAL	セッションラベルはユーザーによって指定されます	SECRET A B
使用可能なワークスペースラベル	セッション認可上限までのアカウントラベル範囲のラベル	CONFIDENTIAL CONFIDENTIAL A B SECRET A B	セッションラベルはユーザーによって指定されます	SECRET A B

- 左の列はセッションに使用されるラベル設定のタイプを示します。

- 真ん中の 2 つの列はマルチレベルセッションに適用されます。
- 右の 2 つの列は単一レベルセッションに適用されます。
- 「通常の場合」の列はラベルタイプの決定方法を示します。
- 「例」の列はログイン時のユーザーの代表的なセッション選択を示します。

例 #1 では、初期ワークスペースラベルが CONFIDENTIAL に設定され、それがユーザーのアカウントラベル範囲の最下位ラベルになります。ユーザーはラベル CONFIDENTIAL、CONFIDENTIAL A B、または SECRET A B で作業できます。

例 #2 では、ユーザーの初期ワークスペースラベルは SECRET A B です。セッションが単一レベルなので、使用可能なワークスペースラベルは SECRET A B のみです。

ラベル付けされたワークスペース

ラベル付けされた「ワークスペース」では、ユーザーは単一セッションで複数のラベルで作業できます。

ユーザーがセッションについてラベルの範囲を選択した場合、最初に表示されるワークスペースは、ユーザーの「最下位ラベル」です。CDE では、フロントパネルのワークスペーススイッチ部分に、同じ最下位ラベルで 3 つの追加ワークスペース用のボタンが作成されます。

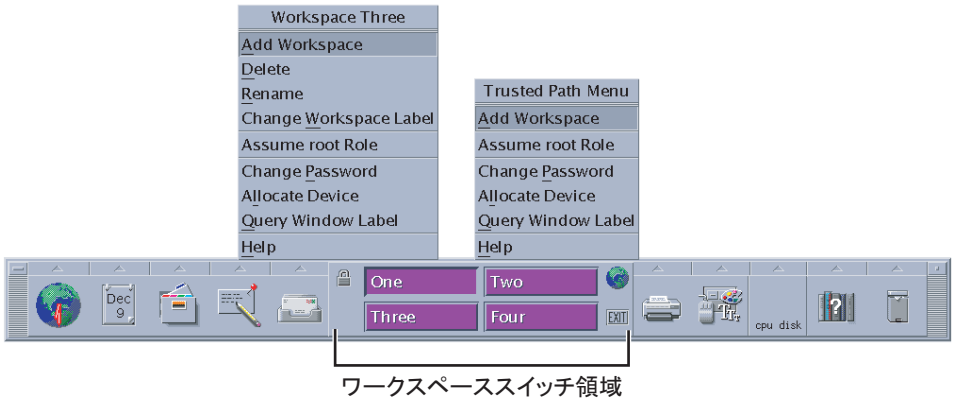


図 1–9　ワークスペーススイッチ領域

ラベル付けされたシステムでの作業についての詳細は、『Solaris Trusted Extensions ユーザーズガイド』を参照してください。

ラベルの管理

ユーザーに対するラベルの表示方法を設定できます。ラベルの表示/非表示、ラベルの色、印刷出力のラベルが設定可能です。ラベルに対する操作には、承認または特権が必要なものがあります。オブジェクトのラベルのアップグレードまたはダウングレードには承認が必要です。ラベルの内部表現とテキスト表現の間でラベルを操作するには、特権が必要な場合があります。

ラベルの表示/非表示

33 ページの「ラベル付けされたワークスペース」の説明のように、ラベルはデスクトップのウィンドウに表示されます。単一ラベルのシステムでは、ラベルを表示しないようにすることもできます。ラベルの表示/非表示は、システムの `policy.conf` ファイルおよび各ユーザーの Solaris 管理コンソールで設定します。設定の手順については、55 ページの「ラベルエンコーディングの管理 (作業マップ)」を参照してください。

通常、下位ラベルのファイルの内容は上位ラベルのユーザーが読み取ることができます。たとえば、システムファイルおよび一般使用の実行可能ファイルには `ADMIN_LOW` ラベルが割り当てられます。「下位読み取り、同位読み取り」の規則に従い、どのラベルで作業するアカウントも、`ADMIN_LOW` ファイルを読み取ることができます。Solaris OS と同様に、DAC の権限によって、読み取りアクセスをできないようにすることが可能です。ゾーンでも、ファイルが読み取られないように保護できます。下位レベルのゾーンがマウントされていない場合、上位レベルのゾーンのユーザーはファイルにアクセスして読み取ることができません。

システムログファイルや `label_encodings` ファイルなど、一般ユーザーに表示すべきでないデータが含まれるファイルは、`ADMIN_HIGH` で保守します。保護されているシステムファイルに管理者がアクセスできるようにするには、`ADMIN_LOW` および `ADMIN_HIGH` の管理ラベルを役割の最下位ラベルおよび認可上限として割り当てます。

印刷出力のラベル

印刷ジョブのバナーページ、トレーラページ、および本文ページに印刷されるラベルはカスタマイズできます。さらに、バナーページおよびトレーラページに現れる付随のテキストもカスタマイズできます。詳細は、第 4 章を参照してください。

情報の再ラベル付けの承認

現在の情報のラベルよりも優位のラベルに情報をアップグレードするための承認は、「ファイルラベルのアップグレード」承認と呼ばれます。現在の情報のラベルよりも下位のラベルに情報をダウングレードするための承認は、「ファイルラベルのダウングレード」承認と呼ばれます。これらの承認の定義については、`/etc/security/auth_attr` を参照してください。

ラベルを変換する特権

プログラムがラベルの操作を行うたびにラベルの変換が行われます。ラベルの変換はテキスト文字列と内部表現とで行われます。たとえば、`getlabel` などのプログラムがファイルのラベルを取得する場合、ラベルがユーザーに表示される前に、ラベルの内部表現が人間の理解できる形に変換されます。コマンド行で指定したラベルを `setlabel` プログラムが設定する場合、ラベル名のテキスト文字列がラベルの内部表現に変換されます。Trusted Extensions では、変換されるラベルに対して呼び出しプロセスのラベルが優位である場合にのみラベル変換が許可されます。プロセスのラベルが、変換を試みた対象のラベルよりも優位でない場合、変換は許可されません。この制限を無効にするには、`sys_trans_label` 特権が必要です。

◆ ◆ ◆ 第 2 章

2 ラベルの計画 (手順)

この章の内容は次のとおりです。

- 37 ページの「ラベルの計画 (作業マップ)」
- 42 ページの「エンコーディングファイルのソース」

詳細およびその他の参照は、『コンパートメントモードワークステーションのラベル作成: エンコード形式』: 国防情報局 (DIA) 文書 [DDS-2600-6216-93] を参照してください。DIA 参考資料は Trusted Extensions のマニュアルセットに含まれています。DIA 参考資料を使用する場合、Trusted Extensions では情報ラベルおよびその構成要素は使用しないことに注意してください。

ラベルの計画 (作業マップ)

ラベルを計画するには、サイトセキュリティーに関する一般的な知識、および `label_encodings` ファイルの構文に関する具体的な知識が必要です。

作業	内容	説明
ラベルエンコーディングファイルの検討とその概略	サイトセキュリティーポリシーを実施するラベルエンコーディングファイルを作成します。	38 ページの「ラベルに関する戦略を立てる」
拡張可能な `label_encodings` ファイルの作成	既存のラベル定義に影響を与えずに変更できるファイルを作成します。	38 ページの「エンコーディングファイルを計画する」

▼ ラベルに関する戦略を立てる

1. 正確な label_encodings ファイルを作成するために時間的な余裕を持ちます。

   サイトのエンコーディングを作成したりその正確さを高めるには、時間がかかります。正確な label_encodings ファイルをインストールするまで、システムを構成できません。

2. 自分のサイトのセキュリティポリシーを確認します。

   多くのサイトは、政府方針に従って開発されたセキュリティーポリシーをすでに持っています。民間企業は、ラベル付けされたセキュリティーの計画に関して経験が浅い場合でも、情報保護の目的の検討から始めることができます。その目的から判断して、ラベルの使用方法に対する常識的な決定を行えます。印刷物や電子メールにラベル付けをする法的な必要が企業に生じた場合、こうしたガイドラインから始めるのがよいでしょう。

   - 例として、第 6 章を参照してください。
   - 必要なサイトセキュリティーポリシーの設定については、『Solaris Trusted Extensions 構成ガイド』の付録 A「サイトのセキュリティーポリシー」を参照してください。

3. 米国政府のラベルエンコーディングファイルを検討します。

   ファイルについての政府の説明は、『コンパートメントモードワークステーションのラベル作成: エンコード形式』: 国防情報局文書 [DDS-2600-6216-93] にあります。

4. サイト用に LOCAL DEFINITIONS セクションをカスタマイズします。

   参考および例は、第 5 章を参照してください。

5. **Trusted Extensions** のインストールの前にエンコーディングを最終確認します。

   稼働中のシステムで label_encodings ファイルを変更するのは危険です。詳細は、label_encodings(4) のマニュアルページを参照してください。

▼ エンコーディングファイルを計画する

次の手順は、あとで安全に拡張できる正確な label_encodings ファイルの作成に役立ちます。

注 – CLASSIFICATIONS および COMPARTMENTS は、あとでセキュリティー管理者役割がテキスト表現を変更できます。ただし、整数値およびビット値を変更すると、重大な問題が発生する可能性があります。

---

1. `label_encodings` ファイルを作成します。

   参考として、42 ページの「エンコーディングファイルのソース」を参照してください。手順については、55 ページの「ラベルエンコーディングの管理 (作業マップ)」を参照してください。

2. 項目を追加する余地を残します。

   a. 格付けの番号付けの際に間を空けます。

      たとえば、格付けを番号付けする際に 10 ずつ間を空けます。このように間を空けておけば、あとから格付けを追加できます。

   b. コンパートメントビットに間を空けます。

      あとで追加する場合に備えて、コンパートメントビット番号の間を空けておきます。

   c. 一部の初期コンパートメントビットを使用しないで、 あとで定義できるようにします。

      インバースコンパートメントを使用する場合は、51 ページの「デフォルト語句とインバース語句」を参照してください。インバースコンパートメントについての詳細は、DIA 参考資料『コンパートメントモードワークステーションのラベル作成: エンコード形式』を参照してください。

3. サイトの格付けを決定します。

   図 1–2 に示すように、定義可能な格付けの総数は 254 です。 格付けに 0 は使用しないでください。

   システムは、格付け値 10 は 2 よりセキュリティー上重要であると判断します。セキュリティーレベルの決定にはテキスト表現は使用されません。

   同じ格付け値を異なる名前に割り当てることはできません。格付けは、互いに高低の差があるか、無関係である必要があります。2 つのラベルが同一レベルとして評価されることはありません。

   格付けの計画のために、表を使用できます。記入例は、表 6–2 を参照してください。

4. コンパートメントを決定します。

   データおよびプログラムのグループ化の方法を決定します。データやプログラムを混在させるかどうかを決定します。たとえば、発注データは、人事ファイルを管理するプログラムから参照できないようにします。また、出荷追跡問題を処理するプログラムからは、発注データにアクセスできるようにします。

   ここでユーザーは考慮に入れません。「だれが」ではなく「何を」を検討します。

5 名前を設計します。

`label_encodings` ファイルの `CLASSIFICATIONS` および `WORDS` には、必須の長形式名と省略可能な短形式名があります。ラベルを指定する場合、短形式名を長形式名に代えて使用できます。

6 関係を調整します。

コンパートメントは、本来、階層構造ではありません。ただし、コンパートメントが階層関係を持つように設定できます。関係を設定する前に、『コンパートメントモードワークステーションのラベル作成: エンコード形式』の例を参照してください。

この手順を簡単に実行する 1 つの方法として、大きなボード、および格付けとコンパートメントを記した紙片を使用します。例については、図 2–1 を参照してください。この方法によって、関係を視覚化し、満足のいくまで各部分を再調整できます。

注 – ほかの組織のラベルとの互換性が必要なエンコーディングを作成するのでなければ、任意の有効値をコンパートメントビットとして割り当てることができます。ただし、自分の使用している番号とその相互関係を把握しておいてください。

---

7 どの認可上限をどのユーザーに割り当てるかを決定します。

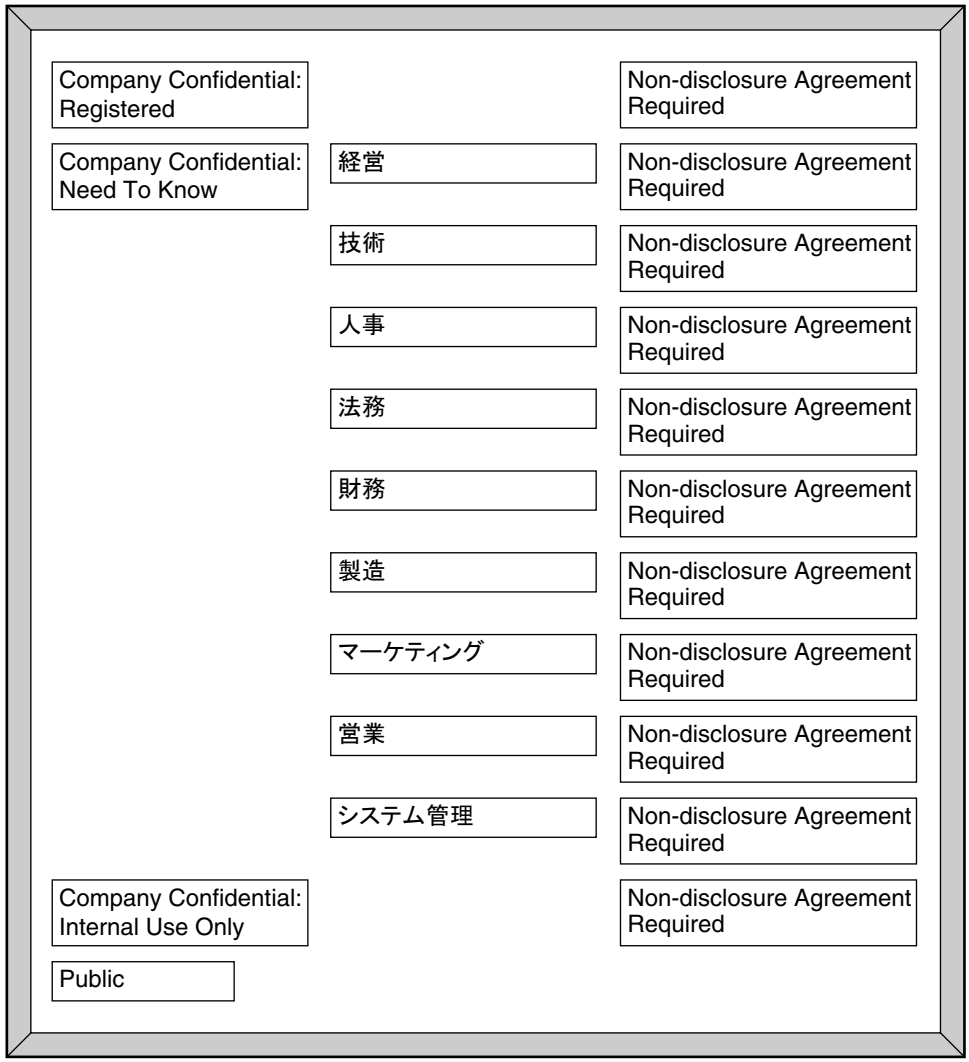


図 2–1 ラベルの関係を示す計画ボードの例

認可上限を計画するために表を使用できます。記入例は、表 6–5 を参照してください。

認可上限をユーザーに割り当てる場合、その格付けはユーザーが作業できるすべての格付けより優位にします。認可上限は、ユーザーの最高の作業格付けと同じにできます。認可上限のコンパートメントには、ユーザーが必要とする可能性があるすべてのコンパートメントを含めます。

8 機密度の低い順からラベルを並べます。

9 それぞれの語句の定義を、整数、ビットパターン、論理関係式のいずれかの、内部形式と関連付けます。

コンパートメントビットの割り当てを管理するために表を使用できます。記入例は、表 6–4 を参照してください。

10 SENSITIVITY LABELS の WORDS セクションを INFORMATION LABELS セクションにコピーします。

Trusted Extensions で情報ラベルはサポートされませんが、エンコーディングファイルを有効にするため、INFORMATION LABELS: WORDS: セクションと SENSITIVITY LABELS: WORDS: セクションを同じにする必要があります。

11 どの色をどのラベルに関連付けるかを決定します。

参考および例は、83 ページの「ラベルの色の指定」を参照してください。

12 ラベルの関係を分析します。

Trusted Extensions を設定しているシステムでは、chk_encodings -a コマンドを使用して、ラベルの関係に関する詳細なレポートをファイルに書き込みます。

```
# chk_encodings -a encodings-file
```

エンコーディングファイルのソース

label_encodings ファイルはフラットなテキストファイルです。Trusted Extensions を設定しているシステムでは、このファイルのラベルが ADMIN_HIGH であるため、一般ユーザーが読み取ることはできません。label_encodings ファイルの 1 行の最大長は、256 バイトです。このファイルは任意のテキストエディタで編集できます。セキュリティー管理者は、label_encodings ファイルの作成および配布を担当します。

注 – label_encodings ファイルは、どんなシステムでも作成および編集できます。ただし、Trusted Extensions を設定しているホストでファイルを検査およびテストします。

組織によっては、国防情報局 (DIA) の仕様に基づいた政府提供の label_encodings ファイルを使用しています。また、Trusted Extensions パッケージで提供されているエンコーディングファイルのいずれかを基にする組織もあります。

Solaris Trusted Extensions パッケージのラベルファイル

Trusted Extensions では、/etc/security/tsol ディレクトリにサンプルファイルがインストールされます。サンプルをサイトの要件に合わせて変更できます。

label_encodings.simple ファイル	Solaris Trusted Extensions ソフトウェアによってインストールされます。
label_encodings.example ファイル	付録 A の例とほぼ同じです。 付録の初めにファイルのラベル構成要素が説明されています。第 6 章に、ファイルの作成手順が説明されています。
label_encodings.gfi.single ファイル	米国政府の単一レベルファイルです。
label_encodings.single ファイル	米国政府の単一レベルファイルの Sun バージョンです。色の割り当てが異なります。
label_encodings.gfi.multi ファイル	米国政府のマルチレベルファイルです。
label_encodings.multi ファイル	米国政府のマルチレベルファイルの Sun バージョンです。組み合わせの制限が少なく、minimum clearance (最下位の認可上限) が高く、デフォルトユーザーラベルが低く、色が異なります。

あるいは、label_encodings ファイルを最初から作成することもできます。label_encodings ファイルの構文および構造は、47 ページの「エンコーディングファイルの構文」に示されています。

デフォルトのラベルエンコーディングファイル

デフォルトでは、label_encodings.simple ファイルは /etc/security/tsol/label_encodings としてインストールされます。

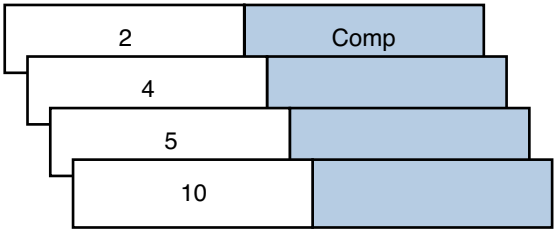
```
ACCREDITATION RANGE:  classification= public;
only valid compartment combinations:  public
minimum clearance= needtoknow;
minimum sensitivity label= public;
minimum protect as classification= public;
```

ACCREDITATION RANGE 定義は、ユーザーを次のラベルに制限します。

- only classification (唯一の格付け) として、PUBLIC が定義されています。
- only valid compartment combination (唯一の有効なコンパートメント組み合わせ) として、PUBLIC が定義されています。
- minimum clearance (最下位の認可上限) として、NEEDTOKNOW が定義されています。
- minimum sensitivity label (最下位の機密ラベル) として、PUBLIC が定義されています。

- `minimum protect as classification` (最下位の機密保護の格付け) として、`PUBLIC` が定義されています。

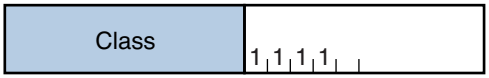
格付けセクションを次の図に示します。




```
CLASSIFICATIONS:
PUBLIC         value = 2
CONFIDENTIAL   value = 4
SANDBOX        value = 5
MAX LABEL      value = 10
```

図 2–2 デフォルト `label_encodings` ファイルの格付け

ファイルのコンパートメントを次の図に示します。




```
SENSITIVITY LABELS:
WORDS:
INTERNAL USE ONLY   compartments = 1 ~2
NEED TO KNOW        compartments = 1-2 ~3
RESTRICTED          compartments = 1-3
PLAYGROUND          compartments = 0 ~1 ~2 ~3
```

図 2–3 デフォルト `label_encodings` ファイルのコンパートメント

GFI ラベルエンコーディングファイルの違い

政府提供ファイルには、`label_encodings.single` と `label_encodings.multi` の 2 つがあります。`label_encodings.single` ファイルは単一レベルであり、`label_encodings.multi` ファイルは単一レベルファイルのマルチレベルバージョンです。`ACCREDITATION RANGE` セクションの設定も異なります。`ACCREDITATION RANGE` セクションは、どの格付けおよびどのコンパートメントが一般ユーザーで使用可能かを定義します。

GFI マルチレベルのラベルエンコーディングファイル

label_encodings.multi ファイルの ACCREDITATION RANGE 設定を次の抜粋に示します。

```
ACCREDITATION RANGE:
classification= u;   all compartment combinations valid;
classification= c;   all compartment combinations valid;
classification= s;   all compartment combinations valid;
classification= ts;   all compartment combinations valid;

minimum clearance= c;
minimum sensitivity label= u;
minimum protect as classification= u;
```

ACCREDITATION RANGE で次のように定義されているため、label_encodings.multi ファイルに定義されているすべての格付けおよびコンパートメントの語句をサイトで使用できます。

- all compartment combinations valid (すべてのコンパートメント組み合わせが有効) として、UNCLASSIFIED、CLASSIFIED、SECRET、および TOP SECRET が定義されています。
- minimum clearance (最下位の認可上限) として、CLASSIFIED が定義されています。
- minimum sensitivity label (最下位の機密ラベル) として、UNCLASSIFIED が定義されています。
- minimum protect as classification (最下位の機密保護の格付け) として、UNCLASSIFIED が定義されています。

GFI 単一レベルのラベルエンコーディングファイル

label_encodings.single ファイルの ACCREDITATION RANGE 設定を次の抜粋に示します。

```
ACCREDITATION RANGE:  classification= s;
only valid compartment combinations:  s a b rel cntry1
minimum clearance= s Able Baker NATIONALITY: CNTRY1;
minimum sensitivity label= s A B REL CNTRY1;
minimum protect as classification= s;
```

ACCREDITATION RANGE 定義は、ユーザーを次のラベルに制限します。

- only classification (唯一の格付け) として、SECRET が定義されています。
- only valid compartment combination (唯一の有効なコンパートメント組み合わせ) として、SECRET A B REL CNTRY1 が定義されています。
- minimum clearance (最下位の認可上限) として、SECRET ABLE BAKER NATIONALITY: CNTRY1 が定義されています。

- minimum sensitivity label (最下位の機密ラベル) として、SECRET A B REL CNTRY1 が定義されています。
- minimum protect as classification (最下位の機密保護の格付け) として、SECRET が定義されています。

label_encodings ファイルの Sun の拡張機能

label_encodings ファイルの Sun の実装は、LOCAL DEFINITIONS セクションをサポートします。このセクションは省略可能です。このセクションを既存の label_encodings ファイルに追加できます。セクション冒頭のキーワード内の LOCAL という語は「Sun の実装に対してローカル」であることを意味します。

LOCAL DEFINITIONS セクションのオプションは、ラベル変換オプションを設定し、色をラベルに関連付けます。アプリケーションウィンドウのタイトルバーには、関連付けられている色を背景にしてラベルが表示されます。COLOR NAMES オプションに無効な色が指定されていたり、色が指定されていない場合は、デフォルトの色が表示されます。第 5 章に、サイトに合わせて Sun の拡張機能を変更する方法が説明されています。

◆ ◆ ◆ 第 3 章

3 ラベルエンコーディングファイルの作成 (手順)

この章では、label_encodings ファイルの作成と変更について説明します。

- 47 ページの「エンコーディングファイルの構文」
- 55 ページの「ラベルエンコーディングの管理 (作業マップ)」

エンコーディングファイルの構文

label_encodings ファイルには、VERSION 指定と 7 つの必須セクション (CLASSIFICATIONS、 INFORMATION LABELS、 SENSITIVITY LABELS、 CLEARANCES、 CHANNELS、 PRINTER BANNERS、 ACCREDITATION RANGE) があります。これらのセクションの順序は決められています。省略可能な LOCAL DEFINITIONS セクションを続けることもできます。

次の表の「必須キーワード」は、必ず存在しなければならないことを意味します。すべてのキーワードに定義がある必要はありません。セクションごとの注釈に、必要な定義と省略可能な定義を示します。

表 3–1 ラベルエンコーディングのキーワード

セクション	注釈
VERSION=	必須キーワード。バージョン指定は、1 つのキーワード VERSION= の後ろに、エンコーディングの特定バージョンを示す文字列を続けます。
CLASSIFICATIONS:	必須キーワード。少なくとも 1 つの格付けを定義します

表 3–1 ラベルエンコーディングのキーワード (続き)

セクション	注釈
INFORMATION LABELS: WORDS: REQUIRED COMBINATIONS: COMBINATION CONSTRAINTS:	必須キーワード。Trusted Extensions ソフトウェアで情報ラベルが使用されていなくても、機密ラベル語句に割り当てる各ビットに対して、情報ラベル語句に 1 ビットを割り当てます。機密ラベル語句は次のセクションで定義されます。
SENSITIVITY LABELS: WORDS: REQUIRED COMBINATIONS: COMBINATION CONSTRAINTS	必須キーワード。WORDS の定義は省略可能です。機密ラベル語句を定義する場合、INFORMATION LABELS と CLEARANCES セクションの WORDS に同じビットを割り当てます。ビットに割り当てる語句は同じである必要はありません。
CLEARANCES: WORDS: REQUIRED COMBINATIONS: COMBINATION CONSTRAINTS	必須キーワード。定義した機密ラベル語句に対して、認可上限語句に 1 ビットを割り当てます。認可上限ラベルでは、機密ラベル語句の定義で許可されていない語句の組み合わせが可能です。
CHANNELS:	必須キーワード。
PRINTER BANNERS:	必須キーワード。
ACCREDITATION RANGE:	必須キーワード。格付け名ごとに規則を定義します。minimum clearance (最下位の認可上限)、minimum sensitivity label (最下位の機密ラベル)、および minimum protect as classification (最下位の機密保護の格付け) を定義します。
LOCAL DEFINITIONS:	省略可能キーワード。

すべての必須セクションで、前の表に示したキーワードが存在しなければなりませんが、すべてのセクションに定義がある必要はありません。たとえば、CLASSIFICATIONS と ACCREDITATION RANGE の定義だけの label_encodings ファイルも有効です。

語句の順番

機密ラベルおよび認可上限に関して設定される語句に強制的な順番はありません。ただし、語句間の関係の設定ではこの順番が重要です。通常、SENSITIVITY LABELS セクションの WORDS は、重要度の低い順に並べます。

語句の順番がどのように影響するかについては、第 4 章の71 ページの「チャネルの指定」 を参照してください。詳細は、『コンパートメントモードワークステーションのラベル作成: エンコード形式』を参照してください。

label_encodings ファイルで、コンパートメント語句を 1 つまたは複数のビットに割り当てることによって、ある型のラベルにコンパートメント語句が定義されている場合、ほかの型のラベルの定義で同じビットを語句に割り当てます。すべての型のラベルは同じ格付け名を使用しますが、各型のラベルに使用される語句は異なっていても構いません。語句が同じビットでエンコーディングされ、まったく同じオブジェクトを参照するのであっても、語句は異なるものにできます。認可上限ラベルでは、機密ラベル語句の定義で許可されていない語句の組み合わせが可能です。

格付け名の構文

格付けは、ラベルの階層を表します。各ラベルには、それぞれ 1 つの格付けがあります。1 つのサイトで最大 255 の格付けを定義できます。label_encodings ファイルで、1 ～ 255 の整数値を格付けに割り当てることができます。値 0 は ADMIN_LOW 管理ラベル用に予約されています。値 32,767 は ADMIN_HIGH 管理ラベル用に予約されています。説明図は、図 1–2 を参照してください。

格付けは、label_encodings ファイルの CLASSIFICATIONS セクションで、認可上限と機密ラベルに対して一度定義されます。

高い値の格付けは、低い値の格付けよりも優位です。次の表は、異なるエンコーディングファイルの、同じ値が割り当てられている 2 セットのラベル名を示しています。左の列は、label_encodings.example ファイルの機密ラベルの例を示します。真ん中の列は、label_encodings.gfi.multi ファイルのラベルを示します。Registered または Top Secret の格付け (値 6) のラベルは、それぞれの列に示されているラベルよりも優位です。

民間の例	米国政府の例	値
Registered	Top Secret	6
Need to Know	Secret	5
Internal Use Only	Confidential	4
Public	Unclassified	1

格付けのキーワード

格付けとして定義されるキーワードを次のリストで説明します。初期コンパートメントの定義例は、51 ページの「デフォルト語句とインバース語句」を参照してください。

name=　(/)、(,)、および (;) を含むことはできません。それ以外の英数字および空白文字は使用できます。ラベルを指定する場合、name、sname、または aname を指定できます。

sname=	格付けのみで必要とされます。短形式名が機密ラベルで [ ] 内に表示されます。
aname=	省略可能。格付けが必要とされる場合に入力可能な名前。
value=	割り当てる値は、格付けの実際の階層を表します。今後の拡張に備えて、割り当てる値に余裕をもたせます。0 は ADMIN_LOW 用に予約されています。値は 1 〜 255 の範囲です。
initial compartments=	省略可能。デフォルトのコンパートメント語句のビット番号を指定します。デフォルトのコンパートメント語句は、関連付けられた格付けがあるラベルで最初に表示されます。 応用: インバース語句のビット番号を指定します。最下位格付けには初期コンパートメントはありません。
initial markings=	廃止。定義しないでください。

次の例は、label_encodings.multi ファイルの冒頭部分です。

例 3–1 label_encodings.multi の初期コンパートメントがある格付け

```
VERSION= Trusted Solaris Multi-Label Sample Version - 5.6 05/07/27

*
*    WARNING:  If CIPSO Tag Type 1 network labels are to be used:
*
*        a) All CLASSIFICATIONS values must be less than or equal to 255.
*        b) All COMPARTMENTS bits must be less than or equal to 239.
*

CLASSIFICATIONS:

*
name= UNCLASSIFIED;  sname= U;  value= 1;
name= CONFIDENTIAL;  sname= C;  value= 4; initial compartments= 4-5 190-239;
name= SECRET;        sname= S;  value= 5; initial compartments= 4-5 190-239;
name= TOP SECRET;    sname= TS; value= 6; initial compartments= 4-5 190-239;
```

各格付けには必須の name、sname 、value フィールドがあります。CONFIDENTIAL、SECRET、および TOP SECRET の格付けには初期コンパートメントがあります。最下位の格付け UNCLASSIFIED には初期コンパートメントはありません。

初期コンパートメントのビット割り当て 4-5 および 190-239 は、ビット 4、5、および 190 ～ 239 がオンであることを表します。これらのビットは、この格付けによってラベルで 1 に設定されます。

初期コンパートメントの一部は、デフォルト語句およびインバース語句を定義するためにあとで使用します。インバース語句をあとで定義するために予約されている初期コンパートメントもあります。

次の例は、初期コンパートメントがない格付けのセットです。

例 3–2 label_encodings.example の初期コンパートメントがない格付け

```
CLASSIFICATIONS:

name= PUBLIC; sname= PUBLIC; value= 1;
name= INTERNAL_USE_ONLY; sname= INTERNAL; aname= INTERNAL; value= 4;
name= NEED_TO_KNOW; sname= NEED_TO_KNOW; aname= NEED_TO_KNOW; value= 5;
name= REGISTERED; sname= REGISTERED; aname= REGISTERED; value= 6;
```

デフォルト語句とインバース語句

初期コンパートメントとしてビットを定義すると、その格付けを含むすべてのラベルで、そのビットが 1 に設定されます。初期コンパートメントとして指定したビットは、あとから label_encodings ファイルで、「デフォルト語句」または「インバース語句」として定義できます。

- 「デフォルトコンパートメント語句」は、その格付けを含むすべてのラベルに表示されます。
- インバースコンパートメント語句は、インバースコンパートメントのビットによって定義する別の語句がない場合に、関連付けられている格付けがあるラベルに表示されます。

例 3–3 初期コンパートメントの割り当て

この例で、PUBLIC 格付けに初期コンパートメントは割り当てられず、WEB COMPANY 格付けに初期コンパートメント 4 および 5 が割り当てられます。PUBLIC 格付けを含むラベルにはデフォルトコンパートメントはありません。WEB COMPANY 格付けを含むラベルは、常にコンパートメントビット 4 および 5 がオンです。

```
name= PUBLIC;  sname= P;  value= 1;
name= WEB COMPANY;  sname= WEBCO;  value= 4; initial compartments= 4-5
```

次の節では、これらの初期コンパートメントビットを語句に割り当てる方法を示します。

例 3–4 SENSITIVITY LABELS のデフォルト語句とインバース語句の定義

この例では、コンパートメントビット 4 および 5 が語句 DIVISION ONLY に割り当てられます。各コンパートメントビットは、インバース語句にも関連付けられます。WEBC AMERICA がインバースコンパートメントビット ~4 に割り当てられます。WEBC WORLD がインバースコンパートメントビット ~5 に割り当てられます。これらの割り当ての結果は次のとおりです。

- WEB COMPANY 格付けの機密ラベルには、最初、語句 DIVISION ONLY が含まれます。ラベルのバイナリ表現で、コンパートメントビット 4 および 5 はオンになります。
- PUBLIC 格付けの機密ラベルは、常にコンパートメントビット 4 および 5 がオフです。語句 WEBC AMERICA および WEBC WORLD がラベルに含まれます。

  インバース語句に IUO の minclass が指定されているので、WEBC AMERICA および WEBC WORLD は PUBLIC 機密ラベルに表示されません。これら 2 つのインバース語句の存在は暗黙となります。

```
SENSITIVITY LABELS:

WORDS:

name= DIVISION ONLY;  sname= DO;       minclass= WEB COMPANY; compartments= 4-5;
name= WEBC AMERICA;   sname= WEBCA;    minclass= WEB COMPANY; compartments= ~4;
name= WEBC WORLD;     sname= WEBCW;    minclass= WEB COMPANY; compartments= ~5;
```

コンパートメント語句

コンパートメントはラベルに表示されるように定義できる、省略可能な語句です。ほかのトラステッドシステムでは、コンパートメントをカテゴリと呼ぶことがあります。コンパートメントを使用することによって、そのコンパートメントがラベルに含まれている情報に対する特別な取り扱い手順や、その情報にアクセスできる人の一般的なクラスを示すことができます。

コンパートメント語句は非階層的なビットに割り当てられますが、コンパートメント語句間に階層を設定できます。その階層は、あるコンパートメント語句のビットを別のコンパートメント語句に定義されているビットに含めるための規則に基づいて形成されます。

コンパートメント語句は、ラベルの型ごとに WORDS サブセクションでオプションとして定義されます。各コンパートメント語句は、1 つまたは複数のビットに割り当てられます。

すべての型のラベルは同じ格付けを使用しますが、それぞれの型のラベルに使用される語句は異なっていても構いません。語句が同じビットでエンコーディングされ、まったく同じオブジェクトを参照するのであっても、語句は異なるものにできます。

次の例は WEB COMPANY コンパートメント語句です。この語句は、短形式名 (sname) WEBCO およびコンパートメントビット 40 〜 50 によって指定されています。

例 3–5 機密ラベルのコンパートメント定義の例

```
WORDS:

name= WEB COMPANY; sname= WEBCO; compartments= 40-50;
```

各ラベルには、格付けフィールドとともに、256 ビットのコンパートメントフィールドがあり、そのうちの 239 ビットを CIPSO ラベルに使用できます。各ビットには、コンパートメント語句をまったく割り当てないことも、1 つ以上割り当てることもできます。各語句には、1 つまたは複数のコンパートメントビットを割り当てることができます。使用可能な 239 ビットによって、多数のコンパートメント語句を作成できます。例として、表 6–3 に示すコンパートメント計画シートを参照してください。

格付け、コンパートメント、および組み合わせの要件が認可範囲に影響します。各格付け設定の ACCREDITATION RANGE (認可範囲) は、次の文字列のいずれかです。

- only valid compartment combinations; (唯一の有効なコンパートメントの組み合わせ)
- all compartment combinations valid; (すべてのコンパートメント組み合わせが有効)
- all compartment combinations valid except; (次のものを除くすべてのコンパートメント組み合わせが有効)

階層コンパートメント語句

階層コンパートメントを使用することによって、大きなグループの全員が使用可能な文書とサブグループのみが使用可能な文書を区別できます。

例 3–6 階層を設定するためのビット組み合わせの使用

1 つのビットを使用する語句と、その同じビットをもう 1 つのビットとともに使用する別の語句を定義することによって、2 つの語句の階層関係を定義します。一般的なコンパートメント語句は特殊な語句より下に定義します。たとえば、ビット番号 1 を使用する語句、およびビット番号 1 と 2 を使用する別の語句を定義することによって、2 つの語句に階層関係を設定できます。

例 3–6 階層を設定するためのビット組み合わせの使用 (続き)

この例では、Sales (営業) コンパートメントが定義されています。これには、Direct Sales (直接営業) と Indirect Sales (間接営業) の 2 つのサブコンパートメントがあります。WebCo という名前の 1 つの格付けが前に定義されています。

```
name= Direct_Sales;   compartments= 1, 2
name= Indirect_Sales;   compartments= 1, 3
name= Sales;   compartments= 1
```

この定義によって、WebCo 社では、販売員のだれもがアクセスできる文書、間接販売員のみがアクセスできる文書、および直接販売員のみがアクセスできる文書を区別できます。

- セキュリティー管理者は、直接販売の従業員に WebCo Direct_Sales 認可上限を設定します。WebCo Indirect_Sales 認可上限が間接販売の従業員に設定されます。
- WebCo Direct_Sales ラベルで作業した人員によって作成された文書は同じラベルになるので、その文書には直接販売部の従業員のみがアクセスできます。
- コンパートメント語句 Sales は Direct_Sales 語句および Indirect_Sales 語句の下にあるので、間接販売部および直接販売部のだれもが WebCo Sales ラベルで作業できます。WebCo Sales ラベルで作成した文書は販売部のだれもがアクセスできます。

例 3–7 階層を設定するための REQUIRED COMBINATIONS の使用

2 つの語句が REQUIRED COMBINATIONS セクションに指定されている場合、最初の語句が使用されると必ず 2 番目のラベルがラベルに追加されます。

この例の Direct Sales、Indirect_Sales、Sales の定義は、例 3–6 と原則的に同じ働きをします。異なるのは、Direct_Sales 語句に必ず Sales 語句が伴う点です。

```
name= Direct_Sales;   compartments= 2
name= Indirect_Sales;   compartments= 3
name= Sales;   compartments= 1

REQUIRED COMBINATIONS:

Direct_Sales            Sales
Indirect_Sales          Sales
```

ラベルエンコーディングの管理 (作業マップ)

注意 – label_encodings ファイルをもっとも安全に変更できるのは、最初のホストをインストールするときです。使用中のファイルを変更する場合は注意して進めてください。詳細は、label_encodings(4) のマニュアルページを参照してください。

作業	説明
label_encodings ファイルを作成または変更する	55 ページの「label_encodings ファイルを作成する」
label_encodings ファイルをテストする	56 ページの「label_encodings ファイルを分析し、検証する」
label_encodings ファイルを配布する	57 ページの「label_encodings ファイルを配布する」
label_encodings ファイルをデバッグする	63 ページの「label_encodings ファイルをデバッグする」
格付け定義を変更する	57 ページの「格付けを追加または名前変更する」
デフォルト語句またはインバース語句を作成する	59 ページの「デフォルト語句およびインバース語句を指定する」
単一ラベルのファイルをカスタマイズする	60 ページの「単一ラベルのエンコーディングファイルを作成する」
ラベル名を指定する	例 3–9
LOCAL DEFINITIONS セクションを追加する	62 ページの「Sun の拡張機能をエンコーディングファイルに追加する」
特定ユーザーにラベルを表示しない	『Solaris Trusted Extensions 管理の手順』の「ユーザーに対してラベルを非表示にする」
特定システムのすべてのユーザーにラベルを表示しない	『Solaris Trusted Extensions 管理の手順』の「policy.conf のデフォルトを修正する」

▼ label_encodings ファイルを作成する

サンプルファイルは、インストールしたシステムの /etc/security/tsol ディレクトリを参照してください。ファイルについては、42 ページの「Solaris Trusted Extensions パッケージのラベルファイル」で説明しています。

始める前に　このファイルは、最初のシステムに Trusted Extensions をインストールする前に、作成できます。その最初のシステムでファイルをチェックします。Trusted Extensions をインストールする最初のシステムでこのファイルを作成することもできます。この手順は、2 番目のコンピュータに Trusted Extensions を設定する前に完了してください。

Trusted Extensions が設定されているシステムでは、大域ゾーンでセキュリティー管理者役割にならなければなりません。その他のシステムでは、任意のエディタでこのファイルを作成または編集できます。

1. 元のファイルのバックアップコピーを作成します。
2. 新しいファイルまたは既存のバージョンのファイルを開きます。
   - **Trusted Extensions** が設定されていないシステムでは、任意のエディタを使用してファイルを作成します。
   - **Trusted Extensions** が設定されているシステムでは、「エンコーディングの編集 **(Edit Encodings)**」アクションを使用してファイルを作成します。

     CDE のアプリケーションマネージャーの Trusted_Extensions フォルダには、エンコーディングファイル用の 2 つのアクションがあります。

     Edit Encodings (エンコーディングの編集)
     指定された `label_encodings` ファイルの構文を編集し、検査します。

     Check Encodings (エンコーディングの検査)
     指定された `label_encodings` ファイルの構文を検査します。
3. ファイルを変更します。

   詳細は、38 ページの「エンコーディングファイルを計画する」を参照してください。
4. **56** ページの「`label_encodings` ファイルを分析し、検証する」に進みます。

▼ label_encodings ファイルを分析し、検証する

始める前に　大域ゾーンでセキュリティー管理者役割になります。

1. ラベルの構文および関係を検査します。

   端末で `chk_encodings -a` コマンドを使用して、ラベルの関係を分析し、レポートします。

   ```
   $ chk_encodings -a encodings-file
   ```
2. ファイルを検証します。

   「エンコーディングの検査 (Check Encodings)」アクションは、指定されたファイルに対して `chk_encodings` コマンドを実行します。
   - ファイルが合格したら、インストールします。

     ```
     Do you want to install this label_encodings file? yes
     ```

- ファイルが合格しない場合は、63 ページの「label_encodings ファイルをデバッグする」を参考にしてください。

3 エンコーディングファイルをテストします。
できれば、サイトのすべてのシステム用にファイルを承認する前に、少数のシステムでファイルをテストしてください。

4 マスターコピーを作成します。
コピーの手順については、『Solaris Trusted Extensions 構成ガイド』の「Trusted Extensions でファイルをポータブルメディアにコピーする方法」を参照してください。

5 ファイルのコピーにラベルを付けて、安全な場所に保管します。

▼ label_encodings ファイルを配布する

1 マスターコピーを作成します。
コピーの手順については、『Solaris Trusted Extensions 構成ガイド』の「Trusted Extensions でファイルをポータブルメディアにコピーする方法」を参照してください。

2 **Trusted Extensions** をシステムにインストールしたら、すぐにマスターファイルをそのシステムにコピーします。
コピーの手順については、『Solaris Trusted Extensions 構成ガイド』の「Trusted Extensions でポータブルメディアからファイルをコピーする方法」を参照してください。

▼ 格付けを追加または名前変更する

始める前に 大域ゾーンでセキュリティー管理者役割になります。

1 label_encodings ファイルを編集します。
「エンコーディングの編集 (Edit Encodings)」アクションを使用します。詳細は、55 ページの「label_encodings ファイルを作成する」を参照してください。

2 バージョン番号を指定します。
VERSION= セクションにサイト名、ファイルのタイトル、バージョン番号、および日付を入力します。

```
VERSION= Sun Microsystems, Inc. Example Version - 5.10 04/05/28
```

Sun では、バージョン番号および日付に SCCS キーワードを使用します。詳細は、sccs(1) のマニュアルページを参照してください。

```
VERSION= Sun Microsystems, Inc. Example Version - %I% %E%
```

3 格付けを指定します。

CLASSIFICATIONS セクションに新しい格付けの長形式名、短形式名、および数値を入力します。

```
name= NEW_CLASS; sname= N; value= 2;
```

4 新しい格付けを認可範囲に含めます。

新しい格付けを ACCREDITATION RANGE セクションに追加します。

次の例では、新しい 3 つの格付けが ACCREDITATION RANGE セクションに追加されています。それぞれの格付けに、all compartment combinations valid (すべてのコンパートメントの組み合わせが有効) が指定されています。

```
ACCREDITATION RANGE:

classification= UNCLASSIFIED;        all compartment combinations valid;

* i is new in this file
classification= INTERNAL_USE_ONLY;   all compartment combinations valid;

* n is new in this file
classification= NEED_TO_KNOW;        all compartment combinations valid;

classification= CONFIDENTIAL;        all compartment combinations valid except:
c
c a
c b

classification= SECRET;               only valid compartment combinations:
. . .
* r is new in this file
classification= REGISTERED;           all compartment combinations valid;
```

5 必要であれば、ACCREDITATION RANGE セクションを調整します。

新しい格付けを最下位格付けにすることが必要になる場合があります。

```
minimum clearance= u;
minimum sensitivity label= u;
minimum protect as classification= u;
```

注 – ユーザーへの割り当てを計画しているすべての認可上限のほうが優位となるよう、`minimum clearance` (最下位の認可上限) を設定する必要があります。同様に、ユーザーへの割り当てを計画しているすべての最下位ラベルのほうが優位となるよう、`minimum sensitivity label` (最下位の機密ラベル) を設定する必要があります。

6 変更を保存します。

▼ デフォルト語句およびインバース語句を指定する

始める前に 大域ゾーンでセキュリティー管理者役割になります。

1 `label_encodings` ファイルを編集します。

「エンコーディングの編集 (Edit Encodings)」アクションを使用します。詳細は、55 ページの「`label_encodings` ファイルを作成する」を参照してください。

2 初期コンパートメントを指定します。

`CLASSIFICATIONS` セクションで、格付け定義の一部としてコンパートメントを指定します。

```
CLASSIFICATIONS:
name= PUBLIC;  sname= P;  value= 1;
name= WEB COMPANY;  sname= WEBCO;  value= 2; initial compartments= 4-5 ;
```

3 デフォルト語句を指定します。

初期コンパートメントビットを語句に割り当てます。

```
name= DIVISION ONLY;  sname= DO;  minclass=  IUO; compartments= 4-5;
name= WEBC AMERICA;  sname= WEBCA; minclass= IUO; compartments= 4;
name= WEBC WORLD;  sname= WEBCW; minclass= IUO; compartments= 5;
```

4 インバース語句を指定します。

初期コンパートメントの前にチルド (~) を付けることによって、インバース語句が作成されます。

```
name= DIVISION ONLY;  sname= DO;  minclass=  IUO; compartments= 4-5;
name= WEBC AMERICA;  sname= WEBCA; minclass= IUO; compartments= ~4;
name= WEBC WORLD;  sname= WEBCW; minclass= IUO; compartments= ~5;
```

5 変更を保存します。

注意事項　以後の割り当てに予約されていないコンパートメントビットの場合、次のセクションのビットに語句を割り当てる必要があります。

- SENSITIVITY LABELS: WORDS:
- INFORMATION LABELS: WORDS:
- COMPARTMENTS: WORDS:

▼ 単一ラベルのエンコーディングファイルを作成する

label_encodings ファイルには、次のような特定のラベルが常に必要です。

- ユーザー認可範囲の機密ラベル 1 つ
- ユーザー認可範囲の認可上限 1 つ
- ユーザー認可範囲の情報ラベル 1 つ

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. エンコーディングファイルを編集します。

   「エンコーディングの編集 (Edit Encodings)」アクションを使用します。詳細は、55 ページの「label_encodings ファイルを作成する」を参照してください。インストールした label_encodings ファイルとは異なる名前を指定します。

2. 格付けが 1 つだけで、必要なコンパートメントだけのエンコーディングファイルを作成します。

   たとえば、INTERNAL_USE_ONLY 格付けのエンコーディングファイルを設定し、語句を指定しないことも可能です。

```
VERSION= Single-Label Encodings

. . .
CLASSIFICATIONS:

name= INTERNAL_USE_ONLY;       sname= INTERNAL;  value= 5;

INFORMATION LABELS:

WORDS:

SENSITIVITY LABELS:

WORDS:

CLEARANCES:
```

```
WORDS:

CHANNELS:

WORDS:

PRINTER BANNERS:

WORDS:
```

3 ACCREDITATION RANGE セクションに指定するのは、格付けは 1 つだけ、コンパートメントの有効な組み合わせも 1 つだけです。

次の例は、INTERNAL 格付けをエンコーディングしています。

```
ACCREDITATION RANGE:

classification= INTERNAL;
only valid compartment combinations:

INTERNAL

minimum clearance= INTERNAL;
minimum sensitivity label= INTERNAL;
minimum protect as classification= INTERNAL;
```

4 LOCAL DEFINITIONS セクションをエンコーディングします。

詳細は、第 5 章を参照してください。

5 ファイルの構文が正しいことを確認します。

- ファイルが chk_encodings に合格しない場合は、63 ページの「label_encodings ファイルをデバッグする」を参照してください。
- それ以外の場合は、56 ページの「label_encodings ファイルを分析し、検証する」に進みます。

6 (省略可能) ラベルがユーザーに表示されないように設定します。

手順は、『Solaris Trusted Extensions 管理の手順』の「ユーザーに対してラベルを非表示にする」を参照してください。

例 3–8 単一ラベルのエンコーディングファイルでの認可範囲の定義

次の例は、ACCREDITATION RANGE: セクションの設定を示します。単一の ANY_CLASS 格付けが定義されています。コンパートメント語句 A、B、および REL CNTRY 1 がすべての型のラベルに指定されます。

```
ACCREDITATION RANGE:

classification= ANY_CLASS;      only valid compartment combinations:

ANY_CLASS A B REL CNTRY1

minimum clearance= ANY_CLASS A B REL CNTRY1;
minimum sensitivity label= ANY_CLASS A B REL CNTRY1;
minimum protect as classification= ANY_CLASS;
```

例 3–9 単一ラベル名の変更

この例では、単一ラベルの会社を扱うように label_encodings.example ファイルが変更されます。name= 値が SECRET から INTERNAL_USE_ONLY に変更されています。sname= 値が s から INTERNAL に変更されています。value= および initial compartments= の定義は変更されていません。

```
CLASSIFICATIONS:
name= INTERNAL_USE_ONLY;  sname= INTERNAL;  value= 5; initial compartments= 4-5
190-239;
```

ACCREDITATION RANGE セクションで、格付けの短形式名が置き換えられます。また、最下位の定義が新しい sname に置き換えられます。

```
ACCREDITATION RANGE:

classification= INTERNAL;      only valid compartment combinations:

INTERNAL

minimum clearance= INTERNAL;
minimum sensitivity label= INTERNAL;
minimum protect as classification= INTERNAL;
```

▼ Sun の拡張機能をエンコーディングファイルに追加する

始める前に　大域ゾーンでセキュリティー管理者役割になります。LOCAL DEFINITIONS セクションのないエンコーディングファイルが必要です。

1. LOCAL DEFINITIONS セクションをファイルに追加します。

   Sun 提供の label_encodings ファイルのセクションを追加します。Sun 提供のファイルは /etc/security/tsol ディレクトリにあります。

2 拡張機能をサイトに合わせてカスタマイズします。
詳細は、86 ページの「Sun 拡張機能の変更 (作業マップ)」を参照してください。

▼ label_encodings ファイルをデバッグする

始める前に 大域ゾーンでセキュリティー管理者役割になります。

1 label_encodings ファイルを編集します。
「エンコーディングの編集 (Edit Encodings)」アクションを使用します。詳細は、55 ページの「label_encodings ファイルを作成する」を参照してください。

2 INFORMATION LABELS: WORDS: セクションのエントリをチェックします。
このエントリは、SENSITIVITY LABELS: WORDS: セクションのエントリと完全に一致する必要があります。

ヒント – 機密ラベル語句をエンコーディングし、その語句を INFORMATION LABELS セクションにコピーします。

---

3 コンパートメントビットを持たない値 0 のラベルが、ユーザー認可範囲にないことをチェックします。
この手順によって、ラベル ADMIN_HIGH と区別できないラベルがなくなります。

4 0 ～ 239 のすべてのコンパートメントビットを持つ、値 255 のラベルが、ユーザー認可範囲にないことをチェックします。
この手順によって、ラベル ADMIN_HIGH と区別できないラベルがなくなります。

5 コンパートメントに 239 を超える値がないことをチェックします。
この手順によって、すべてのラベルが確実に CIPSO ラベルにマッピングされます。

6 解決されないラベルに対しては、次のように実行してください。

a. 新しいラベルを持つオブジェクトがある場合、低いシステムラベル ADMIN_LOW にリセットします。

b. バックアップから、既知の使用可能な label_encodings ファイルを復元します。

c. chk_encodings -a コマンドを使用して、不良なファイルのラベルに関する問題を分析します。

◆ ◆ ◆ 第 4 章

4 プリンタ出力のラベル付け (手順)

この章では、ラベルおよび取り扱いガイドラインのプリンタ出力について説明します。また、セキュリティー管理者役割がデフォルト設定を変更する方法も説明します。この章の内容は次のとおりです。

- 65 ページの「本文ページのラベル」
- 66 ページの「バナーページとトレーラページのセキュリティーテキスト」
- 68 ページの「機密保護の格付けの指定」
- 69 ページの「プリンタバナーの指定」
- 71 ページの「チャネルの指定」
- 76 ページの「印刷ジョブでのセキュリティーテキストの設定 (作業マップ)」

本文ページのラベル

デフォルトでは、各印刷ジョブのラベルがすべての本文ページの一番上と一番下に印刷されます。

図 4–1 は、印刷ジョブの本文ページの一番上と一番下に印刷されるラベル `PUBLIC` を示します。

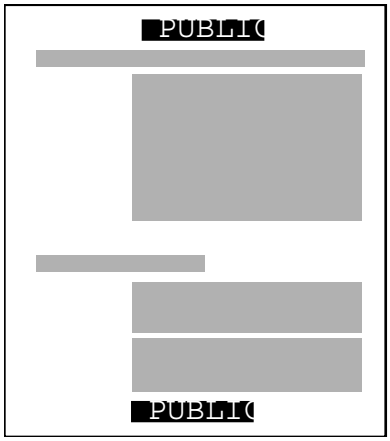


図 4–1 本文ページに自動的に印刷されたラベル

セキュリティー管理者役割は、デフォルトを変更して、印刷ジョブのラベルではなくより高位のラベルを印刷するようにできます。より高位のラベルを印刷するには、71 ページの「チャネルの指定」を参照してください。ラベルをまったく印刷しない場合は、『Solaris Trusted Extensions 管理の手順』の「Trusted Extensions の印刷制限の引き下げ (作業マップ)」を参照してください。

バナーページとトレーラページのセキュリティーテキスト

デフォルトでは、「バナーページ」と「トレーラページ」が印刷ジョブごとに自動的に作成されます。バナーページとトレーラページには、ラベル関連のテキストやプリンタ出力を保護するためのその他のガイドラインが含まれます。

バナーページに印刷されるフィールドやテキストを図 4–2 に示します。デフォルトで表示されるラベル名や文字列を引き出し線で説明しています。

バナーページとトレーラページのすべてのテキストおよびラベルは設定が可能です。

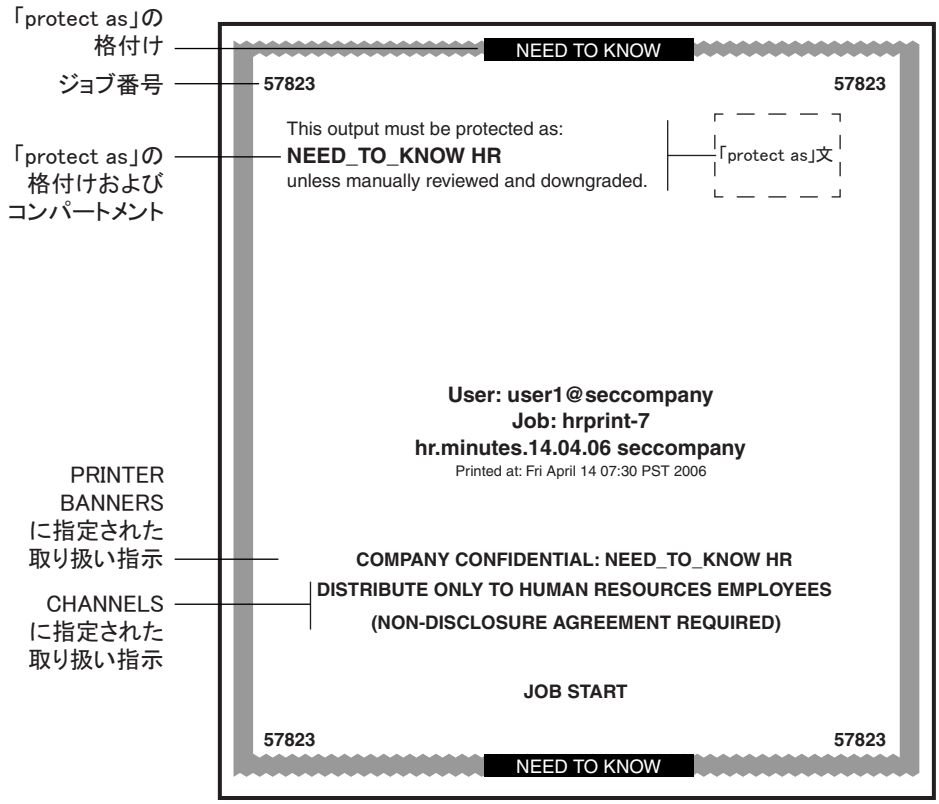


図 4–2　典型的な印刷ジョブのバナーページ

トレーラページでの違いを図 4–3 に示します。バナーページでは太いグレーのフレームですが、トレーラページではそれよりは細い黒のフレームです。トレーラページのページタイプ識別子は JOB END です。

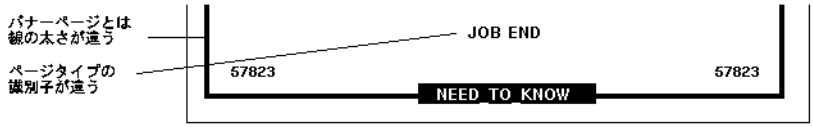


図 4–3　トレーラページでの違い

セキュリティー管理者役割が設定できるバナーページとトレーラページの部分を、次の節で説明します。

- 68 ページの「機密保護の格付けの指定」
- 69 ページの「プリンタバナーの指定」
- 71 ページの「チャネルの指定」

さらに、セキュリティー管理者役割は、/usr/lib/lp/postscript ライブラリの tsol_separator.ps という印刷設定ファイルで、次の変更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の日本語化
- 本文ページの一番上と一番下に印刷されるデフォルトラベルとは別のラベルの指定
- テキストまたはラベルの変更、削除

設定ファイルをカスタマイズするには、/usr/lib/lp/postscript ディレクトリの tsol_separator.ps ファイルのコメントを参照してください。詳細は、『Solaris Trusted Extensions 管理の手順』の第 15 章「ラベル付き印刷の管理 (手順)」を参照してください。

機密保護の格付けの指定

protect as (機密保護) の格付けは、次の 2 つの場所に印刷されます。

- バナーページとトレーラページの一番上と一番下
- 「機密保護の文」の中央 (ジョブのラベルのコンパートメントとともに)

次の図では、protect as (機密保護) の格付けの NEED_TO_KNOW がバナーページの一番上に印刷されています。

protect as statement (機密保護の文) は、次のとおりです。

```
This output must be protected as:
```

この文の後ろは、次のように、ラベルのコンパートメントを伴う protect as classification (機密保護の格付け) です。

```
NEED_TO_KNOW HR
```

この文の後ろは、次のように続きます。

```
unless manually reviewed and downgraded.
```

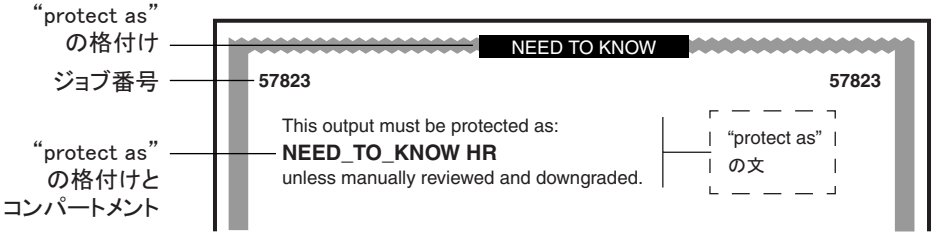


図 4–4 機密保護の文

たとえば、あるサイトが minimum protect as classification (最下位の機密保護の格付け) として INTERNAL_USE_ONLY を使用するとします。このサイトには、次の表の 1 列目と 2 列目が示す値を持つ 3 つの格付けがあります。3 列目は protect as (機密保護) の格付けです。 左の列の格付けが印刷ジョブのラベルにある場合に、そのジョブのバナーページとトレーラページにこの格付けが印刷されます。

表 4–1 最下位の機密保護の格付けがプリンタ出力に及ぼす効果

印刷ジョブの格付け	値	バナーページとトレーラページに印刷される機密保護の格付け
NEED_TO_KNOW	3	NEED_TO_KNOW
INTERNAL_USE_ONLY	2	INTERNAL_USE_ONLY
PUBLIC	1	INTERNAL_USE_ONLY

この表に示すように、ラベルに PUBLIC または INTERNAL_USE_ONLY の格付けが含まれる印刷ジョブでは、Protect as statement (機密保護の文)、およびバナーページとトレーラページの一番上と一番下に INTERNAL_USE_ONLY が印刷されます。ラベルに NEED_TO_KNOW 格付けが含まれる印刷ジョブでは、同じ場所に NEED_TO_KNOW が印刷されます。

プリンタバナーの指定

PRINTER BANNERS (プリンタバナー) フィールドは、バナーページとトレーラページの下部 3 分の 1 に表示される取り扱い指示の最初の行に印刷されます。

民間サイトでは、セキュリティー管理者役割は PRINTER BANNERS セクションのテキストをコンパートメントビットに関連付けることができます。そのコンパートメントビットは、label_encodings ファイルの SENSITIVITY LABELS セクションの語句に割り当てられている必要があります。次の例で、プリンタバナーは COMPANY CONFIDENTIAL: NEED_TO_KNOW HR の行です。

印刷ジョブのラベルのコンパートメントは、印刷ジョブの protect as (機密保護) の格付けとともに protect as (機密保護) フィールドに印刷されます。ラベルのすべてのコンパートメントはアクセス関連として扱われるので、次の例で、コンパートメント HR は protect as (機密保護) の格付けとともにアクセス関連語句として印刷されます。

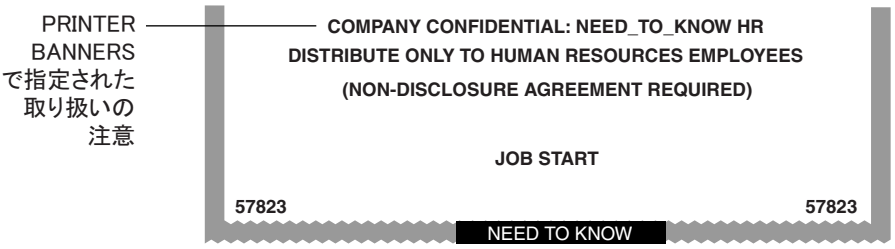


図 4–5　バナーページの PRINTER BANNERS の民間使用

米国政府でのインストールの通例では、プリンタバナーの行は、ジョブの機密ラベルの「サブコンパートメント」に関連付けられている警告を示します。次の例では、官公庁のインストールしたシステムの典型的な PRINTER BANNER (プリンタバナー) を示します。ここに示した文字列 (FULL SA NAME) 以外の文字列を指定することもできます。

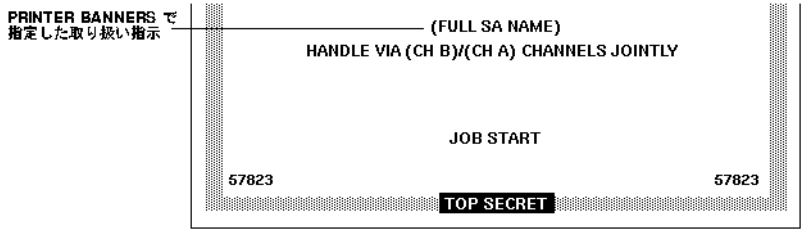


図 4–6　バナーページの PRINTER BANNERS の官公庁使用

次のエンコーディングは、図 4–6 のプリンタバナー行 (FULL SA NAME) です。

最初に、label_encodings の PRINTER BANNERS セクションで、語句 (FULL SA NAME) が、コンパートメントビット 2 に関連付けられています。

例 4–1　PRINTER BANNERS セクションの語句の定義

```
PRINTER BANNERS:

WORDS:
. . .
name= (FULL SA NAME);                    compartments= 2;
```

例 4–2 は、図 4–6 の PRINTER BANNER の定義に使用されるのと同じコンパートメントを指定する SENSITIVITY LABELS の定義です。この例で、コンパートメントビット 2 はサブコンパートメント語句 SA に関連付けられています。

プリンタバナーは (FULL SA NAME) として印刷されます。その理由は、次のとおりです。

- ラベルにサブコンパートメント語句 SA が含まれている。
- コンパートメントビット 2 がサブコンパートメント語句 SA に関連付けられている。
- PRINTER BANNERS エンコーディングで、コンパートメントビット 2 が文字列 (FULL SA NAME) に関連付けられている。

例 4–2 PRINTER BANNERS の定義に関連付けられた機密ラベル WORDS

```
SENSITIVITY LABELS:

WORDS:
  .
  .
  .
name= SB;                       minclass= TS; compartments= 3-5;
name= SA;                       minclass= TS; compartments= 2;
```

PRINTER BANNERS 計画シートの例は、105 ページの「ワークシートによるプリンタバナーの計画」を参照してください。

チャネルの指定

label_encodings ファイルの CHANNELS (チャネル) セクションでは、バナーページとトレーラページの下部 3 分の 1 のうち、PRINTER BANNER 行の下に表示される行を定義します。印刷ジョブのラベルに特定のコンパートメントが含まれる場合に文字列が印刷されるように、CHANNELS セクションを指定できます。

民間サイトでは、CHANNELS セクションの、任意のコンパートメントビットのテキストをカスタマイズできます。図 4–7 は、民間サイトにおける印刷ジョブのバナーページの CHANNELS 警告を示しています。

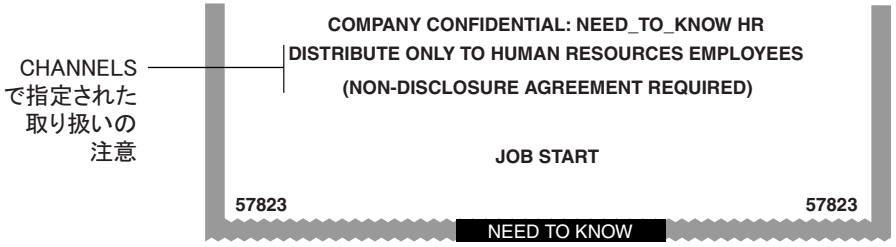


図 4–7 バナーページの CHANNELS の民間使用

米国政府のインストールでは、バナーページのチャネル行に、ジョブのラベルの「コンパートメント」に関連付けられている警告が慣例として表示されます。図 4–8 は、官公庁のインストールにおける印刷ジョブのバナーページに表示される典型的な CHANNELS 警告 (HANDLE VIA (CH B)/(CH A) CHANNELS JOINTLY) を示します。

次の説明で、ラベルにコンパートメント語句 A および B が含まれるジョブに対して、CHANNELS 文字列 HANDLE VIA (CH B)/(CH A) CHANNELS JOINTLY がどのように指定されるかを示します。例として (CH A) および (CH B) のみを適用します。ただし、3 つ目のチャネル (CH C) に対するコンパートメントビットがそれらの定義に含まれているため、 (CH C) についても説明します。

この例には、次のような特徴があります。

- 2 つのコンパートメントビットがある語句のセットに個別に関連付けられ、また、別の語句のセットに一緒に関連付けられています
- 3 つ目のコンパートメントビットが、最初の 2 つのビットのエンコーディングに含まれています
- 「1 つまたは複数のチャネルの語句の組み合わせ」がラベルにあるときに使用する接尾辞が 1 つ定義されています
- 「1 つだけ」のチャネル語句がラベルにあるときに使用する、もう 1 つ の接尾辞が定義されています
- 2 つ以上のチャネル語句が印刷ジョブのラベルにあるときに使用する、3 つ目の接尾辞が定義されています

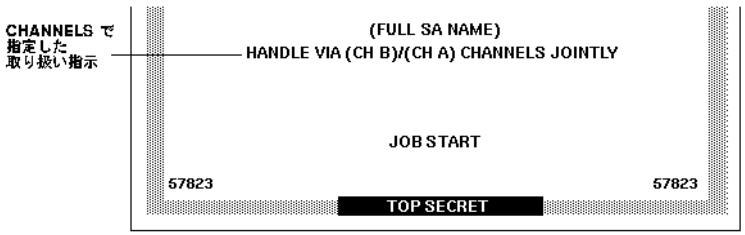


図 4–8 バナーページの CHANNELS 指定の米国政府での使用

次の例に示すように、2 つの接尾辞 CHANNELS JOINTLY と CHANNELS ONLY、および接頭辞 HANDLE VIA が定義されています。

例 4–3　官公庁の label_encodings ファイルの CHANNELS セクションの接尾辞と接頭辞

```
CHANNELS:

WORDS:
name= CHANNELS JOINTLY;         suffix;
name= CHANNELS ONLY;            suffix;
name= HANDLE VIA;               prefix;
```

例 4–3 のように接頭辞と接尾辞を定義したあと、次の結果を得るためにチャネル名 (CH A)、(CH B)、および(CH C) を 2 つの異なる方法で指定します。

- チャネルに関連付けられた 3 つのコンパートメントビットのうちの最低 1 つがラベルにある場合、HANDLE VIA: 接頭辞が印刷されます。
- チャネルに関連付けられた 3 つのコンパートメントビットのうちの 1 つだけがラベルにある場合、CHANNELS ONLY 接尾辞が、チャネル名 (CH A)、(CH B)、または (CH C) の後ろに印刷されます。
- チャネルに関連付けられている複数のコンパートメントビットがラベルにある場合、接頭辞の後ろにスラッシュ(/) によって区切られたチャネル名が続きます。さらに、このチャネル名の後ろに CHANNELS JOINTLY 接尾辞が続きます。

  例 4–3 の CHANNELS WORDS を定義する最初の 3 行が例 4–4 でも繰り返されます。この 2 つ目の例は、(CH A)、(CH B)、および (CH C) がどのようにエンコーディングされて CHANNELS ONLY 接尾辞と一緒に表示されるかを中心に示します。

- (CH A) のエンコーディングは、ビット 0 をオンにし、チルド (~) を使用してビット 1 とビット 6 を明示的にオフにします: 0 ~1 ~6
- (CH B) のエンコーディングは、ビット 1 をオンにし、チルド (~) を使用してビット 0 とビット 6 を明示的にオフにします: ~0 1 ~6
- (CH C) のエンコーディングは、ビット 6 をオンにし、チルド (~) を使用してビット 0 とビット 1 を明示的にオフにします: ~0 ~1 6

例 4–4　個々のチャネルと単独で表示されるように定義された CHANNELS ONLY 接尾辞

```
CHANNELS:

WORDS:

name= CHANNELS JOINTLY;         suffix;
name= CHANNELS ONLY;            suffix;
name= HANDLE VIA;               prefix;
name= (CH A);   prefix= HANDLE VIA; suffix= CHANNELS ONLY;
compartments= 0 ~1 ~6;
```

例 4–4 個々のチャネルと単独で表示されるように定義された CHANNELS ONLY 接尾辞 *(続き)*

```
name= (CH B);   prefix= HANDLE VIA; suffix= CHANNELS ONLY;
compartments= ~0 1 ~6;
name= (CH C);   prefix= HANDLE VIA; suffix= CHANNELS ONLY;
compartments= ~0 ~1 6;
```

例 4–4 に示す CHANNELS セクションのチャネル名定義の最初の 3 行による結果は、次のとおりです。

- label_encodings の別の箇所で、ビット 0、1、および 6 に関連付けられている語句の「1 つ」がジョブのラベルにある場合、HANDLE VIA 接頭辞と CHANNELS ONLY 接尾辞が印刷される
- HANDLE VIA 接頭辞と CHANNELS ONLY 接尾辞が次のように印刷される
  - ラベルの中でコンパートメントビット 0 がオンで、コンパートメントビット 1 と 6 がオフの場合は、(CH A) とともに印刷される
  - ラベルの中でコンパートメントビット 1 がオンで、コンパートメントビット 0 と 6 がオフの場合は、(CH B) とともに印刷される
  - ラベルの中でコンパートメントビット 6 がオンで、コンパートメントビット 0 と 1 がオフの場合は、(CH C) とともに印刷される

    例 4–4 の CHANNELS WORDS を定義する最後の 3 行が例 4–5 でも繰り返されます。この繰り返しは、ビット 0、1、6 に関連付けられた複数の語句がジョブのラベルにある場合、(CH A)、(CH B)、および (CH C) がどのようにエンコーディングされて CHANNELS JOINTLY 接尾辞と一緒に表示されるかを示します。チャネルセクションに定義されているビットが、ジョブのラベルに複数存在する場合は、チャネル名の間にスラッシュが挿入されます。

例 4–5 官公庁エンコーディングファイルの CHANNELS セクションにおける複数チャネルのエンコーディング

```
name= (CH A);   prefix= HANDLE VIA; suffix= CHANNELS ONLY; compartments= 0 ~1 ~6;
name= (CH B);   prefix= HANDLE VIA; suffix= CHANNELS ONLY; compartments= ~0 1 ~6;
name= (CH C);   prefix= HANDLE VIA; suffix= CHANNELS ONLY; compartments= ~0 ~1 6;

name= (CH C);   prefix= HANDLE VIA; suffix= CHANNELS JOINTLY; compartments= 6;
name= (CH B);   prefix= HANDLE VIA; suffix= CHANNELS JOINTLY; compartments= 1;
name= (CH A);   prefix= HANDLE VIA; suffix= CHANNELS JOINTLY; compartments= 0;
```

例 4–5 の CHANNELS 指定は、コンパートメントをエンコーディングする場合の順序の重要性を示します。最初の 3 行が、チャネルコンパートメントビットの 1 つだけがオンである場合を扱い、複数のビットがオンである場合は最後の 3 行が扱います。したがって、最後の 3 行では、どのコンパートメントビットも明示的に 0 に設定する必

要はありません。この最後の 3 行の結果として、チャネルに関連付けられた 3 つのコンパートメント語句の中のどれか 2 つ以上がラベルにある場合に、接尾辞 CHANNELS JOINTLY が常に印刷されます。

- ビット 6 がオンで、ビット 0 とビット 1 の少なくとも一方もオンである場合、(CH C) が CHANNELS JOINTLY とともに印刷される。
- ビット 1 がオンで、ビット 0 とビット 6 の少なくとも一方もオンである場合、(CH B) が CHANNELS JOINTLY とともに印刷される。
- ビット 0 がオンで、ビット 6 とビット 1 の少なくとも一方もオンである場合、(CH A) が CHANNELS JOINTLY とともに印刷される。

次の例は、コンパートメントビット 6 がラベル語句 CC に関連付けられていることを示しています。

例 4–6 コンパートメントビット 6 に関連付けられたラベル WORDS

```
SENSITIVITY LABELS:


WORDS:
  .
  .
  .
name= CC;                       minclass= TS; compartments= 6;
```

例 4–7 は、コンパートメントビット 1 が機密ラベル語句 B に関連付けられていることを示しています。

例 4–7 コンパートメントビット 1 に関連付けられたラベル WORDS

```
SENSITIVITY LABELS:

WORDS:
  .  .  .
name= B;                        minclass=  C; compartments= 1;
```

例 4–8 は、コンパートメントビット 0 が機密ラベル語句 A に関連付けられていることを示しています。

例 4–8 コンパートメントビット 0 に関連付けられたラベル WORDS

```
SENSITIVITY LABELS:

WORDS:
   .   .   .
```

例 4–8 コンパートメントビット 0 に関連付けられたラベル WORDS (続き)

```
name= A;                        minclass=  C; compartments= 0;
```

これをまとめると、次の指示によって、チャネル行が HANDLE VIA (CH B)/(CH A) CHANNELS JOINTLY と印刷されます。

- HANDLE VIA が CHANNELS 語句とともに常に表示されるように定義されている。
- 機密ラベルに A と B の 2 つのアクセス関連語句があり、コンパートメントビット 0 と 1 の 2 つのビットに関連付けられている。
- CHANNELS 語句として定義されたビットがジョブのラベルに 2 つあるため、CHANNELS WORDS (CH A) と (CH B) に続いて CHANNELS JOINTLY が表示される。

  チャネル名の前に印刷する文字列は「接頭辞」として指定する。チャネル名の後ろに印刷する文字列は「接尾辞」として指定する。

CHANNELS 計画シートの例は、106 ページの「ワークシートによるチャネルの計画」を参照してください。

印刷ジョブでのセキュリティーテキストの設定 (作業マップ)

作業	説明
印刷出力のフロントページの語句の印刷	76 ページの「PRINTER BANNERS の語句を指定する」
取り扱い指示の印刷	77 ページの「CHANNELS の取り扱い指示を指定する」
印刷ジョブより高位のラベルの印刷出力の保護	78 ページの「最下位の機密保護の格付けを設定する」
ラベル出力のためのプリンタの設定	『Solaris Trusted Extensions 管理の手順』の「ラベル付き印刷の構成 (作業マップ)」

▼ PRINTER BANNERS の語句を指定する

バナーページの一番上に表示される文字列、および一番下の取り扱い指示の最初に表示される文字列を作成します。

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 プリンタバナーを計画します。
参考として、69 ページの「プリンタバナーの指定」を参照してください。

105 ページの「ワークシートによるプリンタバナーの計画」も参照してください。

2. label_encodings ファイルを編集します。
   「エンコーディングの編集 (Edit Encodings)」アクションを使用します。

3. ファイルの PRINTER BANNERS セクションを変更します。

   a. 接頭辞と接尾辞を作成します。
      これらの文字列を、バナーページとトレーラページのプリンタバナー行の WORDS に関連付けます。

```
PRINTER BANNERS:

WORDS:

name= ORCON;                    prefix;
```

   b. 機密ラベルの定義済みコンパートメントに関連付ける語句の名前を入力します。
      コンパートメントを特定の接頭辞および接尾辞に関連付けることができます。

```
name= (FULL SB NAME);           compartments= 3;
name= (FULL SA NAME);           compartments= 2;
```

4. 56 ページの「label_encodings ファイルを分析し、検証する」に進みます。

▼ CHANNELS の取り扱い指示を指定する

プリンタバナーページに出力する取り扱い指示の文字列を作成します。

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. 接頭辞と接尾辞を計画します。
   参考として、106 ページの「ワークシートによるチャネルの計画」を参照してください。

2. label_encodings ファイルを編集します。
   「エンコーディングの編集 (Edit Encodings)」アクションを使用します。

3 ファイルの CHANNELS セクションを変更します。

```
CHANNELS:

WORDS:
```

a. 接頭辞または接尾辞を入力します。

バナーページとトレーラページの CHANNELS 行の WORDS が接頭辞または接尾辞となります。

```
CHANNELS:

WORDS:
name= CHANNELS JOINTLY;         suffix;
name= CHANNELS ONLY;            suffix;
name= HANDLE VIA;               prefix;
```

b. 機密ラベルの定義済みコンパートメントに関連付ける語句の名前を入力します。

定義済み接頭辞および接尾辞を使用できます。

```
name= (CH C);   prefix= HANDLE VIA; suffix= CHANNELS JOINTLY;
compartments= 6;
name= (CH B);   prefix= HANDLE VIA; suffix= CHANNELS JOINTLY;
compartments= 1;
name= (CH A);   prefix= HANDLE VIA; suffix= CHANNELS JOINTLY;
compartments= 0;
```

4 56 ページの「label_encodings ファイルを分析し、検証する」に進みます。

▼ 最下位の機密保護の格付けを設定する

minimum protect as classification (最下位の機密保護の格付け) によって、指定された最下位の格付け以上のすべてのプリンタ出力が保護されます。低レベルの情報を高位のラベルで保護しなければならない場合、サイトセキュリティーポリシーでこの設定が必要になることがあります。

始める前に 大域ゾーンでセキュリティー管理者役割になります。

1 minimum protect as classification (最下位の機密保護の格付け) を設定します。

この格付けは、エンコーディングファイルの ACCREDITATION RANGE セクションで定義します。

2 56 ページの「label_encodings ファイルを分析し、検証する」に進みます。

例 4–9 label_encodings ファイルの最下位の機密保護の格付け

この例は、minimum protect as classification (最下位の機密保護の格付け) を示します。この格付けは、label_encodings.simple ファイルの ACCREDITATION RANGE セクションで定義されています。この設定によって、INTERNAL ラベルのファイルの印刷で、バナーページとトレーラページに NEED_TO_KNOW が表示されます。

```
minimum protect as classification= NEED_TO_KNOW;
```

◆ ◆ ◆ 第 5 章

LOCAL DEFINITIONS のカスタマイズ

この章では、label_encodings ファイルの LOCAL DEFINITIONS セクションをカスタマイズする方法について説明します。この章の内容は次のとおりです。

- 81 ページの「LOCAL DEFINITIONS セクション」
- 86 ページの「Sun 拡張機能の変更 (作業マップ)」

LOCAL DEFINITIONS セクション

Sun は、政府支給の『コンパートメントモードワークステーションのラベル作成: エンコード形式』には定義されていない追加キーワードを提供します。Sun のキーワード拡張は LOCAL DEFINITIONS セクションにあります。

```
*
* Local site definitions and locally configurable options.
*

LOCAL DEFINITIONS:

Classification Name= Classification;
Compartments Name= Sensitivity;

Default User Sensitivity Label= PUB;
Default User Clearance= CNF NEED TO KNOW;

COLOR NAMES:

     label= Admin_Low;           color= #bdbdbd;

     label= PUB;                 color= blue violet;
     label= SBX PLAYGROUND;      color= yellow;
     label= CNF;                 color= navy blue;
     label= CNF : INTERNAL USE ONLY;  color= blue;
```

```
        label= CNF : NEED TO KNOW;  color= #00bfff;
        label= CNF : RESTRICTED;    color= #87ceff;

        label= Admin_High;          color= #636363;

*

* End of local site definitions
*
```

LOCAL DEFINITIONS セクションの内容

セキュリティー管理者役割は、LOCAL DEFINITIONS セクションで次の指定を行えます。

- ACCREDITATION RANGE: セクションの定義と異なるユーザー認可上限およびユーザー最下位ラベルの指定。

  手順については、86 ページの「デフォルトのユーザーラベルを指定する」を参照してください。
- ラベルビルダーのダイアログボックスにあるカラムヘッダーの名前の指定。カラムヘッダーは格付けとコンパートメントを示します。

  手順については、88 ページの「ラベルビルダーのカラムヘッダーに名前を付ける」を参照してください。
- ラベルに割り当てる色の指定。

  色の定義はオプションです。しかし、ラベルに色を割り当てることを強くお勧めします。

  手順については、87 ページの「ラベルや語句に色を割り当てる」を参照してください。

Trusted Extensions が提供するラベルエンコーディングのキーワードに対する機能拡張についての詳細は、label_encodings(4) のマニュアルページを参照してください。

ラベルビルダーのカラムヘッダーの変更

次の図は、Solaris 管理コンソールによって表示されるラベルビルダーのカラムヘッダー Classification および Category を示します。

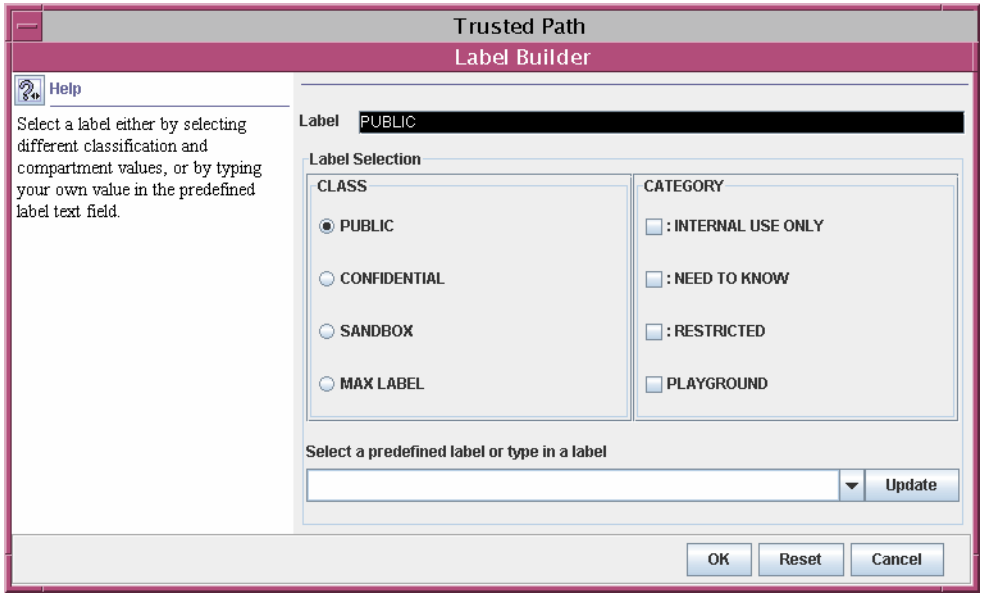


図 5–1 ラベルビルダーのカラムヘッダー

カラムヘッダーを変更するには、88 ページの「ラベルビルダーのカラムヘッダーに名前を付ける」を参照してください。

ラベルの色の指定

LOCAL DEFINITIONS セクションでは、COLOR NAMES キーワードに続いて、0 個以上の色の割り当てを行うことができます。label_encodings ファイルの COLOR NAMES セクションで格付けに対応する色を定義しないと、黒が使用されます。次の抜粋に色のデフォルト値を示します。

```
COLOR NAMES:

     label= Admin_Low;           color= #bdbdbd;

     label= PUB;                 color= blue violet;
     label= SBX PLAYGROUND;      color= yellow;
     label= CNF;                 color= navy blue;
     label= CNF : INTERNAL USE ONLY;  color= blue;
     label= CNF : NEED TO KNOW;  color= #00bfff;
     label= CNF : RESTRICTED;    color= #87ceff;

     label= Admin_High;          color= #636363;
```

ラベルおよびラベル内の語句への配色には、次の構文を使用します。

```
label= label-name;       color= color-name;
word= label-name;       color= color-name;
```

color-name の値は、テキストで表した色の名前または 16 進数で表した色の値です。色は、語句またはラベルに関連付けられます。指定されたラベル構成要素がラベルに含まれる場合は、ラベル構成要素に割り当てられている色が必ず背景色として表示されます。文字の補色の計算は、ウィンドウのソフトウェアによって行われます。

色の値については、86 ページの「色の値」を参照してください。色の指定方法については、本書では完全には説明していません。詳細は、`/usr/openwin/share/man` ディレクトリにある X11(5) のマニュアルページを参照してください。さらに詳しくは、『X ウィンドウ・システム・ユーザ・ガイド』(ソフトバンククリエイティブ発行、1993) の「カラー指定」を参照してください。

色は、次の項で説明する順序規則に従ってラベル構成要素に割り当てられます。色を使用したデスクトップの例を図 5–2 に示します。`PUBLIC`、`INTERNAL`、および `NTK_SALES` のワークスペースボタンに、互いに異なり、標準のワークスペースボタンとも異なる色を使用しています。

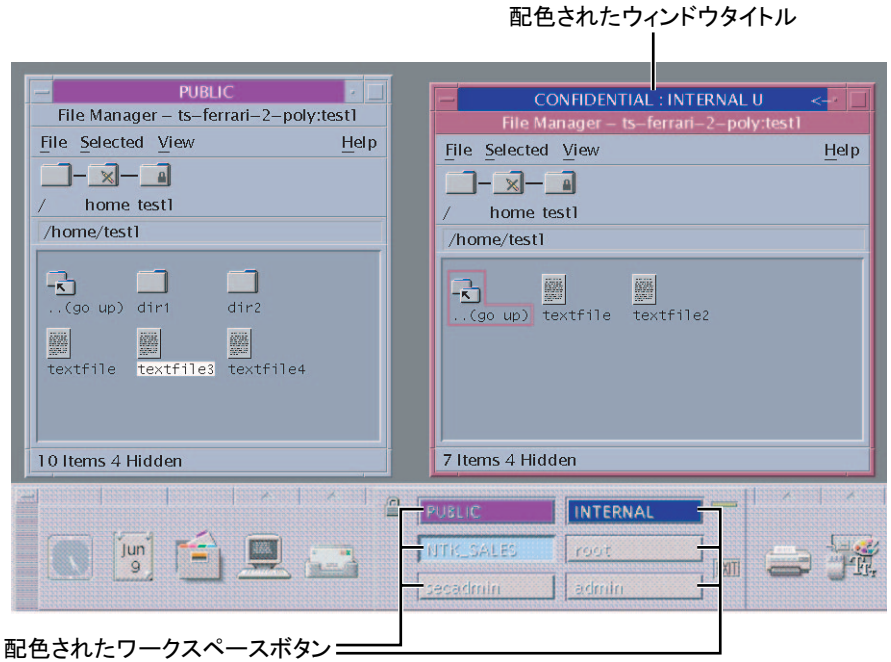


図 5–2 COLOR NAMES による色のウィンドウラベル

色指定の順序

ラベルに使用される色は、次の規則に従って決定されます。

1. 1 つまたは複数の色を指定したコンパートメント語句がラベルにあれば、最初の word= 値に関連付けられた色の値が使用される。
2. 色に関連付けられたコンパートメント語句がラベルにない場合でも、ラベル名に一致するものがあれば、その指定した色が使用される。
3. ラベル名に一致するものがない場合は、ラベルの格付けとして最初に指定した label= 値に関連付けられた色が使用される。
4. 格付けに色が割り当てられていない場合は、同じ格付けの最初のラベルに割り当てられた色が使用される。

例 5–1 順序規則に従って割り当てられた色

この例では、システムの色定義は次のとおりです。

```
label= u;       color= green
label= c;       color= blue
label= S;       color= red;
word= B;        color= orange;
label= TS;      color= yellow;
label= TS SA;   color= khaki;
```

規則の結果、色は次のとおり表示されます。

- 黄が TS 格付けに割り当てられているので、ラベル TS A は黄の背景で表示される。規則 3。
- ラベルに語句 B が含まれない限り、C 格付けのラベルは青で表示される。規則 2。
- 語句 B がオレンジであるので、C B 格付けのラベルはオレンジで表示される。規則 1。
- U 格付けのラベルは常に緑で表示される。エンコーディングファイルで、語句 B は格付け U では表示されない。規則 2。

例 5–2 色の割り当てがないラベルに割り当てられる色

この例は規則 4 を示しています。TS SA が TS 格付けを含む唯一のラベルであるので、ラベル TS の色表示はカーキです。TS SA の色表示はカーキに定義されています。

```
label= u;       color= green
label= c;       color= blue
label= S;       color= red;
word= B;        color= orange;
label= TS SA;   color= khaki;
```

色の値

/usr/openwin/lib/rgb.txt データベースは、色の名前を赤、緑、および青の値に変換します。rgb.txt ファイルでは、サイトのラベルに使用する色の名前を参照できます。16 進数の色の値も使用できます。

色の値の主な要点を簡潔に説明すると、次のとおりです。

- 色の値によって、その色を構成する赤、緑、青 (RGB) の割合を指定できます。
- RGB 値は、0 から FF までの 16 進数を 3 つ組み合わせることによって指定できます。それぞれの 16 進数が、その色に含まれる赤、緑、および青の量を示します。

  たとえば、純粋な赤は #FF0000、純粋な緑は #00FF00、純粋な青は #0000FF、純粋な白は #FFFFFF、そして純粋な黒は #000000 です。詳細は、/usr/openwin/share/man ディレクトリにある X11(5) のマニュアルページを参照してください。
- 画面で使用できる色の数は、次の要因によって決まります。
  - 色の指定に使用できるメモリーの容量
  - カラープレーンの数
  - カラーセルを使用しているクライアントの数
  - ほかのアプリケーションが専用のカラーマップを使用しているかどうか

色名計画シートの例については、表 6–8 を参照してください。色の割り当てについては、87 ページの「ラベルや語句に色を割り当てる」を参照してください。

Sun 拡張機能の変更 (作業マップ)

目的	説明
ユーザーに対するラベルと認可上限のデフォルトの変更	86 ページの「デフォルトのユーザーラベルを指定する」
ラベルの色の指定	87 ページの「ラベルや語句に色を割り当てる」
ラベルビルダーのヘッダーのカスタマイズ	88 ページの「ラベルビルダーのカラムヘッダーに名前を付ける」

▼ デフォルトのユーザーラベルを指定する

始める前に　大域ゾーンでセキュリティー管理者役割になります。

1. label_encodings ファイルを編集します。

   「エンコーディングの編集 (Edit Encodings)」アクションを使用します。詳細は、55 ページの「label_encodings ファイルを作成する」を参照してください。

2 LOCAL DEFINITIONS セクションで、Default User Sensitivity Label で始まる行を探します。

```
Default User Sensitivity Label= u;
Default User Clearance= c;
```

3 機密ラベルを目的の最下位ユーザーラベルに置き換えます。

次の例では、新しい最下位ラベル c が示されます。

```
Default User Sensitivity Label= c;
```

4 認可上限を目的のユーザー認可上限に置き換えます。

次の例では、新しい認可上限 s が示されます。

```
Default User Clearance= s;
```

▼ ラベルや語句に色を割り当てる

色化けを最小限にとどめるには、ほかのアプリケーションで指定したことが明らかな色の名前や 16 進数の色の値を使用します。色に関する留意として、デフォルトの色の値はメモリーの制限によって選択されています。

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。

1 label_encodings ファイルを編集します。

「エンコーディングの編集 (Edit Encodings)」アクションを使用します。詳細は、55 ページの「label_encodings ファイルを作成する」を参照してください。

2 COLOR NAMES セクションを見つけます。

```
COLOR NAMES:
          label= Admin_Low;       color= #bdbdbd;
          ...
          label= Admin_High;      color= #636363;
```

3 格付けごとに色を定義します。

この例では、格付け REGISTERED に赤が割り当てられます。格付け NEED_TO_KNOW SYSADM には青が割り当てられます。

```
label= REGISTERED;  color= red;
label= NEED TO KNOW; color= blue;
```

4 (省略可能) 個々のコンパートメント語句の色を定義します。

特定のコンパートメント語句を、それが関連している格付けとは無関係に区別するには、それらの語句に別の色を割り当てます。

a. システムで使用可能な色の名前を決定します。

名前は、ローカルの色データベースに定義されます。詳細は、/usr/openwin/share/man ディレクトリにある X11(5) のマニュアルページを参照してください。

```
% grep Red /usr/openwin/lib/X11/rgb.txt
...
255  69   0            OrangeRed
219 112 147            PaleVioletRed
...
139   0   0            DarkRed
```

b. 色の名前を割り当てます。

```
word= EMGT; color= OrangeRed;
```

5 (省略可能) ラベルの色を定義します。

この例では、色 MediumPurple4 がラベルに割り当てられます。

```
label= NEED TO KNOW SYSADM; color= MediumPurple4;
```

▼ ラベルビルダーのカラムヘッダーに名前を付ける

始める前に 大域ゾーンでセキュリティー管理者役割になります。

1 label_encodings ファイルを編集します。

「エンコーディングの編集 (Edit Encodings)」アクションを使用します。詳細は、55 ページの「label_encodings ファイルを作成する」を参照してください。

2 LOCAL DEFINITIONS セクションで「**Classification Name**」の行を探します。

この行と次の行によって、ラベルビルダーのカラムヘッダーが定義されます。

```
Classification Name= Classification;
Compartments Name= Sensitivity;
```

3 カラムヘッダーに別の名前を割り当てます。

次の例は、label_encodings.simple のカラムヘッダーです。

```
Classification Name= Classification;
Compartments Name= Department;
```

◆ ◆ ◆ 第 6 章

例: 組織のラベルの計画

この章では、情報保護に関する会社の目標に合ったラベルの作成について説明します。

- 89 ページの「自分のサイトにおけるラベルの条件の確認」
- 94 ページの「セキュリティーの学習曲線」
- 95 ページの「各ラベルの条件の分析」
- 98 ページの「ラベルのセットの定義」
- 109 ページの「label_encodings ファイルの編集とインストール」
- 116 ページの「ラベルに関するユーザーおよびプリンタの設定」

自分のサイトにおけるラベルの条件の確認

次の例でラベル要件を設計する企業を、かりに SecCompany 社とします。自社の知的財産を保護するため、SecCompany 社の法務部門では、機密度の高い電子メールや印刷物に対する 3 種類のラベルの使用を全社員に義務付けています。3 種のラベルは、機密度の高い順に次のとおりです。

- SecCompany Confidential: Registered
- SecCompany Confidential: Need To Know
- SecCompany Confidential: Internal Use Only

法務部門では、省略可能な第 4 のラベル Public の使用も認めています。Public ラベルは制限なしにだれにでも配布可能な情報に使用します。

情報保護の目標の達成

SecCompany 社の情報の機密保護の担当責任者は、可能な限りあらゆる方法を利用してラベルの必要性を説いています。しかし、その必要性を理解しない従業員もいます。それを忘れたり、無視したりする従業員もいます。ラベルが正しく使用された場合でも、その情報が常に正しく扱われ、保管され、配布されているとは限りませ

ん。たとえば、Registered 扱いの情報でさえも、だれもいないところに見つかることのあることが報告されています。Registered 扱いの情報のコピーが、コピー機やプリンタの横に置いてあったり、休憩室やロビーに置いてあったりするのです。

法務部門では、従業員の意識に全面的に頼らずに、情報が適切にラベル付けされる確実な方法を求めています。システム管理者は、次のことを制御するためのより良い方法を求めています。

- 機密情報をだれが参照または変更できるか
- どの情報をどのプリンタに出力するか
- プリンタ出力をどのように扱うか
- さまざまなセキュリティーレベルの電子メールが会社の内外にどのように配信されるか

ラベル付けとアクセスを処理する Trusted Extensions の機能

Trusted Extensions ソフトウェアは、ラベル付けをコンピュータユーザー任せにしません。Trusted Extensions によって設定されているプリンタサーバーからのすべてのプリンタ出力は、サイトの要件に従って自動的にラベル付けされます。

セキュリティーに対する社内の理解は十分ではありませんでしたが、Trusted Extensions のいくつかの機能を即座に実装できることに、経営陣は気付きました。

- 印刷ジョブの自動ラベル付け機能
- ラベルによりアクセスが制限されるプリンタ
- ラベルによりアクセスが制限される電子メール

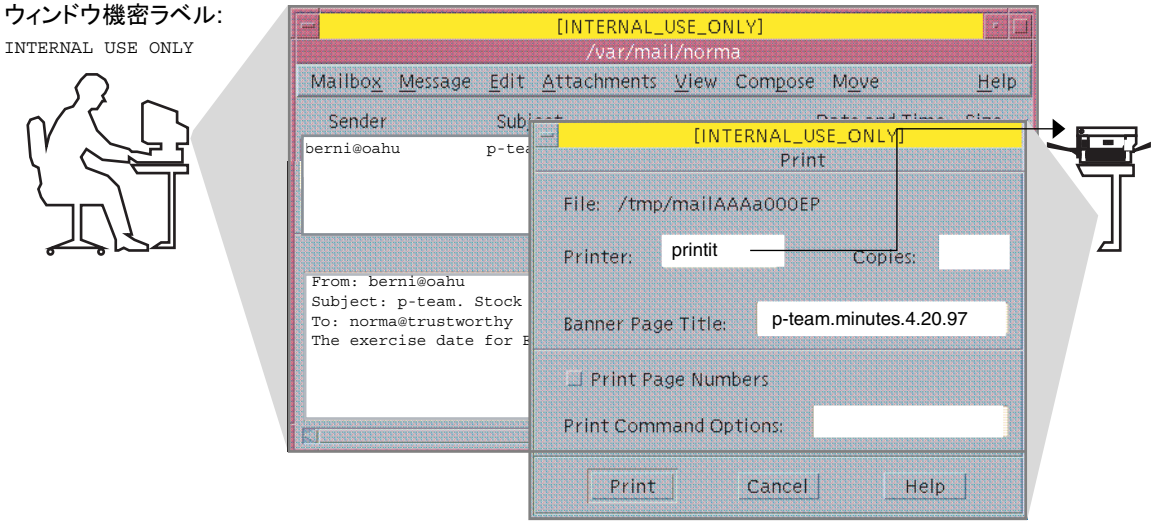


図 6–1 印刷ジョブの自動ラベル付け機能

各印刷ジョブには「ラベル」が自動的に割り当てられます。 これは、ユーザーが作業をしている「レベル」、またはユーザーの責任のレベルに対応します。

図 6–1 は、INTERNAL_USE_ONLY のレベルで作業する従業員を示します。このレベルでは、SecCompany 社の従業員および機密保持契約に署名した者のみがその作業にアクセスできます。この従業員がプリンタに電子メールを送信すると、印刷ジョブにはラベル INTERNAL_USE_ONLY が自動的に割り当てられます。

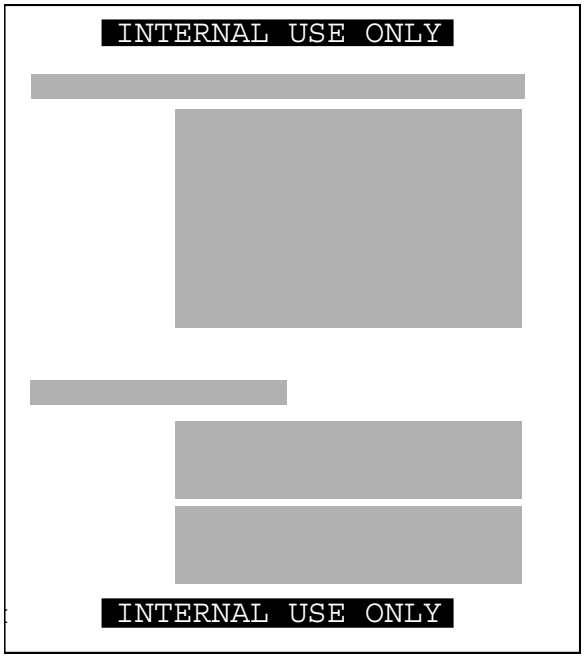


図 6–2 本文ページに自動的に印刷されたラベル

プリンタによって、会社指定のラベルが、印刷出力の各ページの一番上と一番下に自動的に印刷されます。

図 6–2 は、図 6–1 でプリンタに送信して、ユーザーの作業ラベルで印刷された文書を示します。ラベル INTERNAL_USE_ONLY が各ページの一番上と一番下に印刷されます。

例 6–1 バナーページとトレーラページの取り扱いガイドライン

この例は、機密レベルの格付けが NEED_TO_KNOW であり、部門が HUMAN_RESOURCES である印刷ジョブの語句を示します。どの印刷ジョブにもバナーページとトレーラページが自動的に作成され、会社が指定した取り扱いガイドラインとともに出力されます。

```
NEED_TO_KNOW HR

DISTRIBUTE ONLY TO HUMAN RESOURCES (NON-DISCLOSURE AGREEMENT REQUIRED)
```

「取り扱い指示」が機密ラベルの下に印刷され、印刷物の配布上の注意が示されます。この注意には、その情報を必要としている人事担当者のみに配布すること、また、それを読む人は機密保持契約に署名した者に限ることが記されています。

制限されたラベル範囲内のジョブだけを出力するようにプリンタを設定できます。たとえば、図 6–3 は、法務部門のプリンタが、次の 3 つのラベルのいずれかが割り当てられたジョブのみを出力するように設定されていることを示します。

- NEED_TO_KNOW LEGAL – 法務部門でこの情報を知る必要のある従業員のみが閲覧できる
- INTERNAL_USE_ONLY – SecCompany 社の常勤従業員および機密保持契約に署名した顧客が閲覧できる
- PUBLIC – 全員が閲覧できる

このプリンタの設定では、それ以外のラベルで送信されるジョブは除外されます。たとえば、ラベル NEED_TO_KNOW MARKETING および REGISTERED のジョブは拒否されます。

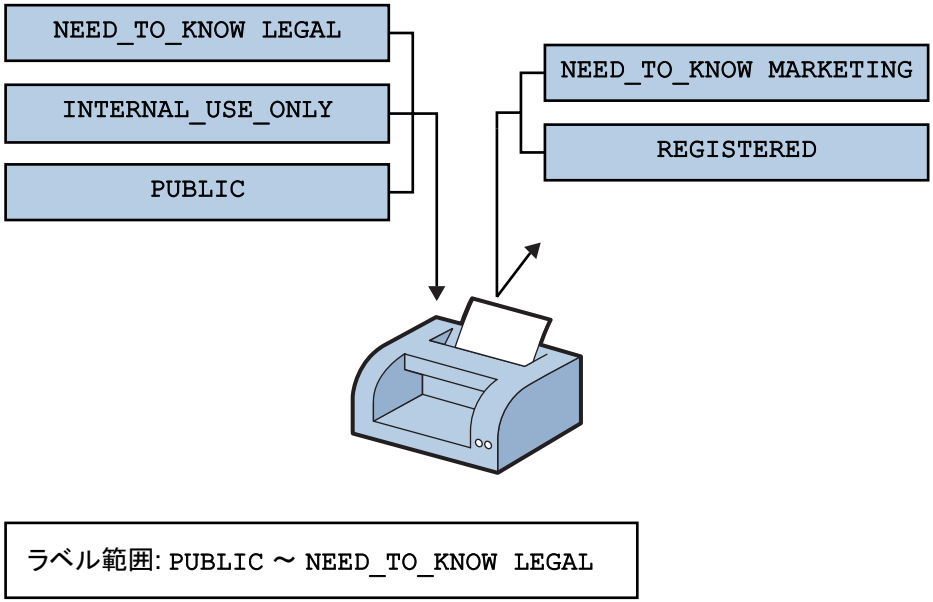


図 6–3 制限されたラベル範囲のプリンタによるジョブの処理方法

すべての従業員が使用できる場所にあるプリンタを、同様に制限できます。たとえば、すべての従業員が見ることができる 2 つのラベル INTERNAL_USE_ONLY および PUBLIC のみのジョブを印刷するように設定できます。

どのジョブを特定のプリンタで印刷できるかをプリンタラベル範囲で制御する方法と同様に、ユーザーの「アカウント機密ラベル範囲」 で、ユーザーが扱える電子メールを制限します。図 6–4 は、ユーザーの電子メールアプリケーションの機密ラベルでラベル付けされる電子メールを示します。電子メールはそのラベルで電子メールアプリケーションに送信されます。

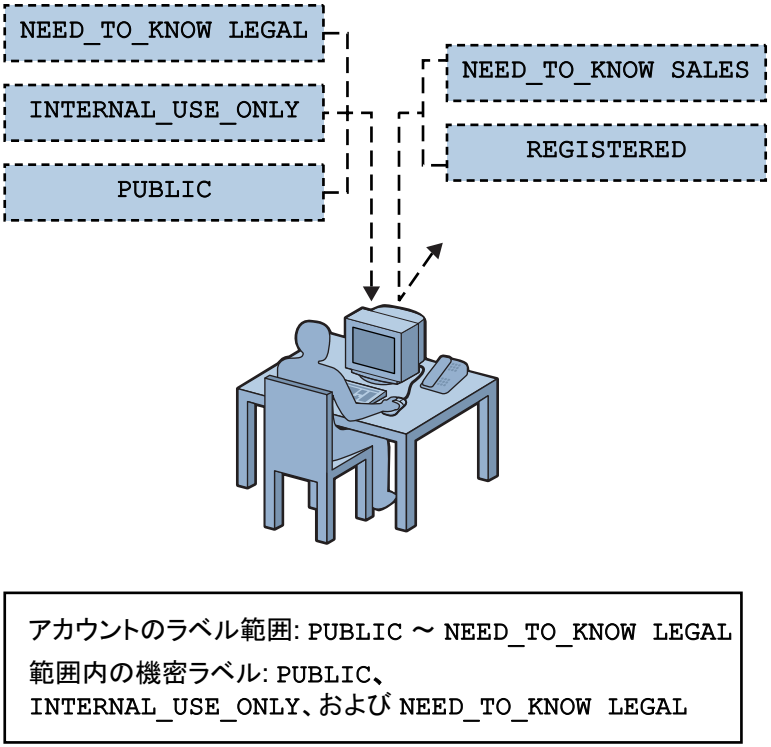


図 6–4 アカウントラベル範囲内の電子メールを受信するユーザー

インターネットへのゲートウェイが電子メールを選別するように設定されているので、不適切なラベルの電子メールは社外に送信されません。PUBLIC 以外のラベルがすべて不適切です。

セキュリティーの学習曲線

経営陣は、次のような条件に該当する、経験豊富な管理者を選び出します。

- 信頼性がある
- Solaris システムの管理方法を知っている
- 組織の情報処理の目標を十分に理解し、サイトのセキュリティーを監督または実装できる

このような人が、セキュリティー管理者としての業務に割り当てられます。

セキュリティー管理者は、Trusted Extensions ソフトウェアをインストールするずっと前から、セキュリティーについて学習し、サイトのセキュリティーポリシーの計画を準備します。セキュリティー管理者は、最初に次のマニュアルを読みます。

- 『Solaris Trusted Extensions 構成ガイド』の「サイトセキュリティーの実現」 – サイトのセキュリティーポリシー作成のガイダンスとして
- 『Solaris Trusted Extensions ユーザーズガイド』 – ラベルの型とその表示について
- 『Solaris Trusted Extensions 管理の手順』 – セキュリティー管理者の責任とツールについて
- 第 1 章 – ラベルの概念の確認として

次に、セキュリティー管理者はサイトのラベルの計画を開始します。計画については、次の節で説明します。

各ラベルの条件の分析

セキュリティ管理者は、法務部門が指定するラベルから開始することが適切だと認めていますが、それをエンコーディングする前にさらに分析する必要があります。

CONFIDENTIAL: INTERNAL_USE_ONLY の条件

CONFIDENTIAL: INTERNAL_USE_ONLY ラベルは、会社所有の情報のうち、機密レベルが低いので全従業員に配布できます。全従業員は雇用の開始前に機密保持契約に署名しています。このラベルの情報はその他のユーザーにも配布できます。たとえば、機密保持契約に署名したベンダーの従業員や契約社員も、この情報を受け取ることができます。インターネット上では情報がのぞき見される場合があるので、このラベルを持つ情報はインターネット経由で送信することはできません。社内で電子メールで送信することはできます。

CONFIDENTIAL: INTERNAL_USE_ONLY ラベルが適した情報は、次のとおりです。

- 出費ガイドラインを含むメモ
- 社内作業の割り当て

CONFIDENTIAL: NEED_TO_KNOW の条件

CONFIDENTIAL: NEED_TO_KNOW は、会社所有の情報のうち、INTERNAL_USE_ONLY より機密レベルが高く、利用者がより限定される情報向けのラベルです。配布は、この情報を知る必要のある従業員に限定されます。従業員以外でも、機密保持契約に署名した、この情報を知る必要がある者に配布される場合があります。

たとえば、特定のプロジェクトで作業をしているグループだけに情報を表示したい場合は、その情報に対して NEED_TO_KNOW を使用します。特定のグループに情報を限定する場合は、その情報の印刷出力にグループ名を明記します。

ラベルにグループ名を明記することによって、そのグループ外には情報を与えてはならないことが明らかになります。このラベルの情報は、インターネット経由で送信することはできませんが、社内では電子メールで送信できます。

NEED_TO_KNOW ラベルが適した情報は、次のとおりです。

- 製品設計ドキュメント
- プロジェクトの詳細
- 社員配置部署変更通知

CONFIDENTIAL: REGISTERED の条件

CONFIDENTIAL: REGISTERED は、会社所有の情報のうち、機密レベルが非常に高いので、この情報が社外に漏れた場合、会社に大きな損害を与える可能性があります。登録された (registered) 情報は、所有者が番号を振って追跡します。各コピーは特定の人に割り当てられます。読み終わったあとは所有者に戻されて廃棄されます。コピーはその情報の所有者だけが作成できます。紙の色は、赤茶色を使用されることをお勧めします。この色はコピーすることができません。

このラベルは、限られた 1 つのグループの人だけに会社所有の情報を提示するときに使用されます。この情報の所有者によって承認されている人以外には、この情報を提示できません。情報の所有者がその情報の提示を承認しても、機密保持契約に署名していないほかの会社の従業員には提示されません。このラベルが付いた情報は、電子メールで送信することはできません。

CONFIDENTIAL: REGISTERED ラベルが適した情報は、次のとおりです。

- 未発表の四半期末会計報告書
- 売り上げ予測
- 市場予測

NEED_TO_KNOW ラベルのグループの名前

セキュリティー管理者は、グループまたは部門の名前を NEED_TO_KNOW ラベルに含めようと決断しました。セキュリティー管理者が、組織内のグループまたは関心のある分野を定義するのに使用する語句について提案を求めた結果、次のような名前が挙がりました。

- 技術
- 経営
- 財務

- 人事
- 法務
- 製造
- マーケティング
- 営業
- システム管理

このあと、セキュリティー管理者は、技術とマーケティングのグループのすべてのメンバーがプロジェクトデータを共有できるように、プロジェクトチームグループを追加しました。

ラベルのセットの概要

次のステップでは、次の問題を解決します。

- 格付けとコンパートメントを使用してラベルと認可上限をエンコーディングする
- プリンタ出力上に印刷する取り扱い指示

セキュリティー管理者は、大きなボードを使用しました。図 6–5 に示すように、ラベルにする語句が紙片に記されました。これによって関係を視覚化することができ、満足のいくまで各部分を入れ替えたりして検討を加えることができます。

セキュリティー管理者は次の事実を発見しました。

- 4 つのラベルは階層構造になっていて、最上位が REGISTERED で、最下位が PUBLIC である。
- グループ名を関連付けられるラベルは 1 つだけである

  登録された情報を受け取れるように認可される者のリストは、それぞれの場合によって制限されます。そのため、REGISTERED にはグループ名は不要です。INTERNAL_USE_ONLY は全従業員と機密保持契約に署名した人を対象とし、PUBLIC ラベルは全員を対象としているため、これらのラベルはそれ以外の資格を必要としていません。 NEED_TO_KNOW ラベルは、NEED_TO_KNOW MARKETING や NEED_TO_KNOW ENGINEERING のように非階層的な語句と関連付ける必要があります。グループや部門を表す語句をそのユーザーの認可上限に含めることこともできます。 これは、そのユーザーの need to know (知る必要性) を確定するためです。
- PUBLIC 以外の各ラベルでは、その情報にアクセスするには機密保持契約に署名する必要があります。

  NON-DISCLOSURE AGREEMENT REQUIRED などのテキストがあれば、その必要性を気づかせる意味で有効です。
- バナーページやトレーラページに示す取り扱い指示は、情報の取り扱い方を明確な表現で示します。情報の取り扱い方は、格付けと、ラベル内のグループ名に基づきます。

  プリンタ出力の機密に関する情報に加えて、取り扱い指示には、ラベルが機密保持契約を必要とする場合にその条件を出力します。

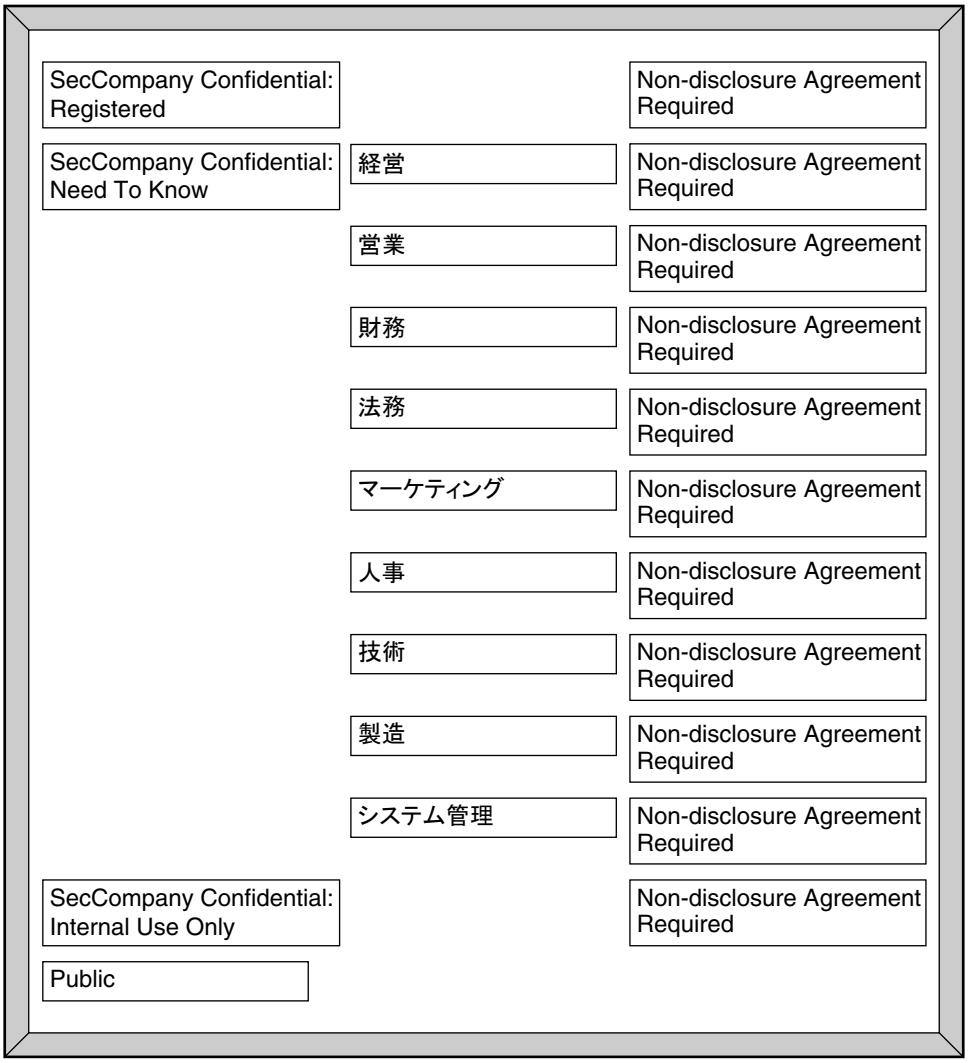


図 6–5　ラベルの関係を示す計画ボードの例

ラベルのセットの定義

この節では、ラベルに関して必要な次の事項をすべて含むリストで、ラベルのセットを定義します。

- 格付け
- その他の語句
- 語句同士の関係
- 各語句の使用に関連付けられた格付けの制約

- 機密ラベルおよび認可上限における語句の使用目的
- 印刷や電子メールなどのシステム出力の、ラベル付けにおける語句の使用目的

格付けの計画

4 つのラベルが階層構造になっているので、それらのラベルは階層的な格付けとしてエンコーディングされます。

法務部門からの承諾を得て、セキュリティー管理者は、ラベル名から SecCompany Confidential: を削除してラベルを短くしました。格付けが長いと、ウィンドウフレームでラベルを読み取るのが困難です。ウィンドウフレームに入りきらないラベル名は右端が切れます。PUBLIC より上位にあるラベル名の切り詰められた名前はすべて、SECCOMPANY という語句で始まるので、各ウィンドウのフレームを手動で拡張しなければ区別できません。

セキュリティー管理者は、次のラベルを定義しました。

- REGISTERED
- NEED_TO_KNOW
- INTERNAL_USE_ONLY
- PUBLIC

コンパートメントの計画

グループ名は、非階層的な「コンパートメント」としてエンコーディングします。コンパートメントは、NEED_TO_KNOW 格付けを持つラベルだけに現れるように制限されます。コンパートメントの制限は、COMBINATION CONSTRAINTS の ACCREDITATION RANGE セクションにエンコーディングされます。

ユーザー「認可上限」は、ラベルにグループ名があるファイルおよびディレクトリをどのユーザーが作成できるかを制御します。 さらに、NEED_TO_KNOW 格付けとともに複数のグループ名があるラベルを持つドキュメントをどのユーザーが作成できるかも制御します。

MAC における語句の使用の計画

ユーザー認可上限および機密ラベルでの格付けやコンパートメントが、必須アクセス制御 (MAC) で使用されます。したがって、法務部門における階層的なラベルやグループ名は、格付けやコンパートメントとしてエンコーディングする必要があります。そうすることによって、これらをラベルで使用して、どの従業員がファイルにアクセスしたりその他の作業を行なったりできるかを制御できるようになります。

SecCompany 社は、ある機密ラベルを PUBLIC の格付けで定義し、そのラベルをユーザー認可範囲の最下位に割り当てています。 また、別の機密ラベルは、PUBLIC のすぐ上位の INTERNAL_USE_ONLY の格付けで定義しています。

認可上限が PUBLIC、最下位ラベルが PUBLIC であり、承認を持たない従業員は、システムを次の範囲で使用できます。

- PUBLIC のワークスペースのみでの作業。
- PUBLIC のみでのファイルの作成。
- PUBLIC のみでの電子メールの読み取り。
- ラベル範囲が PUBLIC のプリンタの使用。

  それに対して、承認を持たなくても、認可上限が INTERNAL_USE_ONLY の従業員は、システムを次の範囲で使用できます。
- PUBLIC または INTERNAL_USE_ONLY のいずれかのワークスペースでの作業。
- PUBLIC または INTERNAL_USE_ONLY のいずれか (従業員の現在のワークスペースによって異なる) でのファイルの作成。
- いずれかの機密ラベルの電子メールの送受信。
- PUBLIC のラベル範囲のプリンタによる PUBLIC とラベル付けされたファイルの印刷。INTERNAL_USE_ONLY のラベル範囲のプリンタへの INTERNAL_USE_ONLY とラベル付けされたファイルの送信。

システム出力のラベル付けにおける語句の使用の計画

プリンタジョブの機密ラベルにグループ名のコンパートメントが含まれていれば、必須プリンタバナーページとトレーラページの文面は次のようになります。

```
Distribute Only To Group Name (Non-Disclosure Agreement Required)
```

ラベルなしのプリンタ出力の計画

「ラベルなしの印刷」承認を持つユーザーや役割は、lp -o nolabels オプションを使用できます。このオプションを使用すると、印刷ジョブの本文ページの一番上と一番下のラベルが印刷されません。セキュリティー管理者役割は、この「ラベルなしの印刷」承認を全員に許可するか、まったく許可しないかを決定できます。

「PostScript ファイルの印刷」承認によって、ユーザーは PostScript ファイルをプリンタに送信できます。十分な知識を持つユーザーによって PostScript ファイルのラベルが変更されてしまう危険性があるので、通常は PostScript 印刷は許可されません。

ラベルが印刷されない文書のマスターコピーの製作をテクニカルライターに許可するには、セキュリティー管理者は「ラベルなしの印刷」と「PostScript ファイルの印刷」の 2 つの承認をすべてのテクニカルライターに与えます。

サポート手順の計画

セキュリティー管理者は、ラベル付けの計画を実行するためにセキュリティーポリシーを作成します。

REGISTERED ファイルまたはディレクトリを保護するための規則

語句 REGISTERED を含む認可上限を持つユーザーであれば、社内のすべての場所にあるすべての登録された情報にアクセスできることを、セキュリティー管理者は認識しています。そこで、追加の対策が必要です。たとえば、認可上限に REGISTERED を持つユーザーに対し、UNIX のアクセス権を使用して自分のファイルを保護するよう指示します。ファイルの参照または変更を作成者のみができるようにアクセス権を設定します。次の例は、任意アクセス制御 (DAC) を適用して REGISTERED ディレクトリの内容を保護するユーザーの場合です。

例 6–2　DAC の使用による登録情報の保護

```
% plabel
REGISTERED
% mkdir registered.dir
% chmod 700 registered.dir
% cd registered.dir
% touch registered.file
% ls -l
-rwxrwxrwx registered.file
% chmod 600 registered.file
% ls -l
-rw------- registered.file
```

この例に示すように、機密ラベル REGISTERED で作業してファイルまたはディレクトリを作成するユーザーは、所有者のみにファイルの読み取りと書き込みの権限を設定する必要があります。ディレクトリのアクセス権は、読み取り、書き込み、および検索を、所有者のみが行うことができるように設定します。これによって、REGISTERED で作業できるほかのユーザーでもそのファイルを読み取れなくなります。

プリンタ設定の規則

次の表は、さまざまな作業グループによって使用されるプリンタの設定方法を示します。

表 6–1 各場所に設置されているプリンタのラベル範囲の設定例

プリンタの設置場所	アクセスのタイプ	ラベル範囲
ロビーや共有の会議室	全員	PUBLIC 〜 PUBLIC
社内プリンタルーム	全従業員および機密保持契約に署名した者	〜PUBLIC 〜 INTERNAL_USE_ONLY
1 つのグループに制限された区域	NEED_TO_KNOW *group-name* コンパートメントで指定されたグループのメンバー	NEED_TO_KNOW *group-name* 〜 NEED_TO_KNOW *group-name*
厳密に制限された区域	認可上限が REGISTERED に格付けされた者のみ	REGISTERED 〜 REGISTERED

詳細は、『Solaris Trusted Extensions 管理の手順』の第 15 章「ラベル付き印刷の管理 (手順)」を参照してください。

プリンタ出力の取り扱い上の規則

使用制限されているプリンタにアクセスする人に対して、次のように指示します。

- プリンタバナーページとトレーラページにある指示に従って情報を保護すること。
- バナーページもトレーラページもないジョブをシュレッダにかけること。また、バナーページにもトレーラページにも照合ジョブ番号が付与されていないジョブもシュレッダにかけること。

ワークシートによる格付け値の計画

次の表のワークシートは、4 つの格付けに定義されている名前および階層値を示しています。値 0 は管理ラベルの ADMIN_LOW のために予約されているので、PUBLIC 格付けの値は 1 に設定され、ほかの格付けの値は順次それよりも高く設定されています。

注 – ラベルのグループ名は、SENSITIVITY LABELS および CLEARANCES セクションの WORDS としてあとで指定します。

表 6–2 格付けの計画

name=	**sname=/aname=**	**value=**	**initial compartments=** ビット番号/語句
PUBLIC	PUB	1	なし
INTERNAL_USE_ONLY	IUO	4	なし

表 6–2 格付けの計画 (続き)

name=	sname=/aname=	value=	initial compartments= ビット番号/語句
NEED_TO_KNOW	NTK	5	なし
REGISTERED	REG	6	なし

ワークシートによるコンパートメント値と組み合わせ制約の計画

次の表では、語句と格付けの関係を定義します。この関係は、図 6–5 の計画ボードで検討して決定されました。PUBLIC および INTERNAL_USE_ONLY は、いずれのコンパートメントとも、1 つのラベル内で組み合わせることができません。NEED_TO_KNOW は、コンパートメントのいずれか、またはすべてのコンパートメントと、1 つのラベル内で組み合わせることができます。

表 6–3 コンパートメントとユーザー認可範囲の組み合わせの計画シート

格付け	コンパートメント名/短形式名/ビット	組み合わせの制約
PUBLIC		PUBLIC のみが有効な組み合わせ
INTERNAL_USE_ONLY		INTERNAL_USE_ONLY のみが有効な組み合わせ
NEED_TO_KNOW	SYSTEM ADMINISTRATION/ SYSADM/ 19	NEED_TO_KNOW すべての組み合わせが有効
	MANUFACTURING/ MANU/ 18	
	ENGINEERING/ ENG/ 17 20	
	HUMAN RESOURCES/ HR/ 16	
	MARKETING/ MKTG/ 15 20	
	LEGAL/ LEGAL/ 14	
	FINANCE/ FINANCE/ 13	
	SALES/ SALES/ 12	
	EXECUTIVE MANAGEMENT GROUP/ EMGT/ 11	
	ALL_DEPARTMENTS/ ALL/ 11-20	

表 6–3 コンパートメントとユーザー認可範囲の組み合わせの計画シート (続き)

格付け	コンパートメント名/短形式名/ビット	組み合わせの制約
REGISTERED		REGISTERED のみが有効な組み合わせ

セキュリティー管理者は次の表を使用して、コンパートメントに使用されたビットを追跡します。

表 6–4 コンパートメントビットの管理表

11	12	13	14	15	16	17	18	19	20	

ワークシートによる認可上限の計画

ラベルのコンポーネントは、認可上限のユーザーにも割り当てられています。ワークシートの認可上限計画シート (表 6–5) は、認可上限で使用されるラベルコンポーネントを定義します。

表 6–5 のキーは次の通りです。

略語	名前
REG	REGISTERED
NTK	NEED_TO_KNOW
IUO	INTERNAL_USE_ONLY
EMGT	EXECUTIVE MANAGEMENT GROUP
SALES	SALES
FIN	FINANCE
LEGAL	LEGAL
MKTG	MARKETING
HR	HUMAN RESOURCES
ENG	ENGINEERING
MANU	MANUFACTURING
SYSADM	SYSTEM ADMINISTRATION
NDA	NON-DISCLOSURE AGREEMENT

表 6–5 認可上限計画シート

CLASS (格付け)	COMP (コンパートメント)	COMP (コンパートメント)	COMP (コンパートメント)	COMP (コンパートメント)	COMP (コンパートメント)	COMP (コンパートメント)	COMP (コンパートメント)	COMP (コンパートメント)	COMP (コンパートメント)	注釈
REG	EMGT	ENG	FIN	HR	LEGAL	MANU	MKTG	SALES	SYSADM	最上位、使用されない *
REG										必要に応じて、限定したスタッフに割り当て **
NTK		ENG								ENG グループに割り当て
									SYSADM	システム管理者に割り当て
IUO										従業員に割り当て。および NDA に署名した者
PUB										全員に割り当て

*システムにおける最上位のラベルで、最上位の格付けと定義されたすべてのコンパートメントが含まれています。組織内の全部門のすべての情報にアクセスできる者はいないので、これは、ユーザー認可範囲には入りません。そのため、この格付けにはだれも割り当てないでください。

**REGISTERED 機密ラベルで作業するとき、ユーザーは所有者以外の全員に対してアクセス制限するようにアクセス権を設定します。ファイルアクセス権 600 およびディレクトリアクセス権 700 でアクセスを制限します。

ワークシートによるプリンタバナーの計画

SecCompany 社の法務部門は、プリンタバナーページとトレーラページに次のテキストを表示させたいと考えています。

```
SecCompany Confidential:
```

PRINTER BANNERS セクションを使用して、印刷ジョブの機密ラベルに表示される任意のコンパートメントに文字列を関連付けることができます。このエンコーディングでは、NEED_TO_KNOW 格付けだけがコンパートメントを持ちます。次の表は、必要な語句を接頭辞として指定し、各コンパートメントに割り当てる方法を示しています。各チャネルに NTK という略語を割り当てると、PRINTER BANNERS セクションの語句に次のようなグループ名が含まれます。

```
SecCompany Confidential: group-name
```

表 6–6　SecCompany 社のプリンタバナー計画シート

接頭辞	プリンタバナー (語句、接頭辞なし)
SECCOMPANY CONFIDENTIAL:	ALL_DEPARTMENTS
SECCOMPANY CONFIDENTIAL:	EXECUTIVE_MANAGEMENT_GROUP
SECCOMPANY CONFIDENTIAL:	SALES
SECCOMPANY CONFIDENTIAL:	FINANCE
SECCOMPANY CONFIDENTIAL:	LEGAL
SECCOMPANY CONFIDENTIAL:	MARKETING
SECCOMPANY CONFIDENTIAL:	HUMAN_RESOURCES
SECCOMPANY CONFIDENTIAL:	ENGINEERING
SECCOMPANY CONFIDENTIAL:	MANUFACTURING
SECCOMPANY CONFIDENTIAL:	SYSTEM_ADMINISTRATION
SECCOMPANY CONFIDENTIAL:	PROJECT_TEAM

ワークシートによるチャネルの計画

SecCompany 社の法務部門は、プリンタバナーページとトレーラページに次の取り扱い指示を表示させたいと考えています。

```
DISTRIBUTE ONLY TO group-name EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED)
```

そのためには、この例のグループ名に以前割り当てられたのと同じコンパートメントビットを CHANNELS セクションで割り当てます。SecCompany 社は、コンパートメントとチャネルの両方に同じグループ名を使用する計画です。

チャネル名の前にくる語句は「接頭辞」として指定され、チャネル名の後にくる語句は「接尾辞」として指定されます。セキュリティー管理者はワークシートで接頭辞と接尾辞を指定します。

表 6–7 SecCompany社のチャネル計画シート

接頭辞	チャネル	接尾辞
DISTRIBUTE_ONLY_TO	EXECUTIVE_MANAGEMENT_GROUP	EMPLOYEES (NON-DISCLOSURE_AGREEMENT_REQUIRED)
DISTRIBUTE_ONLY_TO	SALES	EMPLOYEES (NON-DISCLOSURE_AGREEMENT_REQUIRED)
DISTRIBUTE_ONLY_TO	FINANCE	EMPLOYEES (NON-DISCLOSURE_AGREEMENT_REQUIRED)
DISTRIBUTE_ONLY_TO	LEGAL	EMPLOYEES (NON-DISCLOSURE_AGREEMENT_REQUIRED)
DISTRIBUTE_ONLY_TO	MARKETING	EMPLOYEES (NON-DISCLOSURE_AGREEMENT_REQUIRED)
DISTRIBUTE_ONLY_TO	HUMAN_RESOURCES	EMPLOYEES (NON-DISCLOSURE_AGREEMENT_REQUIRED)
DISTRIBUTE_ONLY_TO	ENGINEERING	EMPLOYEES (NON-DISCLOSURE_AGREEMENT_REQUIRED)
DISTRIBUTE_ONLY_TO	MANUFACTURING	EMPLOYEES (NON-DISCLOSURE_AGREEMENT_REQUIRED)
DISTRIBUTE_ONLY_TO	SYSTEM_ADMINISTRATION	EMPLOYEES (NON-DISCLOSURE_AGREEMENT_REQUIRED)
DISTRIBUTE_ONLY_TO	PROJECT_TEAM	EMPLOYEES (NON-DISCLOSURE_AGREEMENT_REQUIRED)

認可範囲の最下位の計画

次の最下位値を設定する必要があります。

- minimun sensitivity label (最下位の機密ラベル)
- minimum clearance (最下位の認可上限)
- minimum protect as classification (最下位の機密保護の格付け)

SecCompany 社は、従業員がすべての定義済み機密ラベルを使用できるようにしようとしています。さらに、一部の従業員に PUBLIC 認可上限を割り当てられるようにしようとしています。そのため、「minimum sensitivity label (最下位の機密ラベル)」および「minimum clearance (最下位の認可上限)」を PUBLIC に設定する必要があります。

「minimum protect as classification (最下位の機密保護の格付け)」が、ジョブの機密ラベルの実際の格付けの代わりに、プリンタバナーページとトレーラページに出力されます。minimum protect as classification (最下位の機密保護の格付け) は、実際の最下位の格付けよりも高く設定できます。 しかし、SecCompany 社の要件では、minimum protect as classification (最下位の機密保護の格付け) を、印刷ジョブの機密ラベルの実際の格付けと常に等しくすることが許されています。セキュリティー管理者は、minimum sensitivity label (最下位の機密ラベル)、minimum clearance (最下位の認可上限)、およびminimum protect as classification (最下位の機密保護の格付け) に値 PUBLIC を指定します。

ワークシートによる色の計画

ラベル名がウィンドウの一番上に表示されるときは、ラベルに割り当てられている色が背景に表示されます。文字は、背景と補色の関係にある色で表示されます (補色はウィンドウシステムによって演算される)。この例でセキュリティー管理者は、デフォルトの label_encodings ファイルで管理ラベルにすでに割り当てられている色はそのまま使用しています。また管理者は、次の表に示すように、PUBLIC に緑、INTERNAL_USE_ONLY に黄、NEED_TO_KNOW を含むラベルに青 (コンパートメントの違いは青の濃淡で区別)、REGISTERED に赤を割り当てています。

表 6–8 SecCompany 社の色名計画シート

ラベルまたは名前 (label= または name=)	色
ADMIN_LOW	#BDBDBD
PUBLIC	緑
INTERNAL_USE_ONLY	黄色
NEED_TO_KNOW	青
NEED_TO_KNOW EMGT	#7FA9EB
NEED_TO_KNOW SALES	#87CEFF
NEED_TO_KNOW FINANCE	#00BFFF
NEED_TO_KNOW LEGAL	#7885D0
NEED_TO_KNOW MKTG	#7A67CD
NEED_TO_KNOW HR	#7F7FFF
NEED_TO_KNOW ENG	#007FFF
NEED_TO_KNOW MANU	#0000BF
NEED_TO_KNOW PROJECT_TEAM	#9E7FFF
NEED_TO_KNOW SYSADM	#5B85D0
NEED_TO_KNOW ALL	#4D658D
NEED_TO_KNOW SYSADM	#5B85D0
REGISTERED	赤
ADMIN_HIGH	#636363

label_encodings ファイルの編集とインストール

インストールチームは、インストールした label_encodings ファイルの印刷コピーおよびオンラインコピーを作成します。このコピーは、セキュリティー管理者役割が提供する新しいバージョンのファイルに問題がある場合に使用します。

セキュリティー管理者役割は、テキストエディタを使って label_encodings ファイルを作成し、「エンコーディングの検査 (Check Encodings)」アクションを使ってファイルを検査します。ファイルが「エンコーディングの検査 (Check Encodings)」アクションの検査に合格すると、新しいファイルをインストールするかどうかを選択できます。セキュリティー管理者役割がインストールを選択すると、「エンコーディングの検査 (Check Encodings)」アクションによって現在のバージョンの label_encodings ファイルがバックアップされ、新しい label_encodings ファイルが作成されます。

バージョンのエンコーディング

次の例は、社名、タイトル、バージョン番号、および日付を変更した、VERSION の文字列です。

例 6–3　SecCompany 社の VERSION エントリ

```
VERSION= SecCompany, Inc. Example Version - 2.2 00/04/18
```

格付けのエンコーディング

次の例は、表 6–2、表 6–3、および表 6–4 に示した SecCompany 社の格付けと値が追加された、CLASSIFICATIONS セクションです。

例 6–4　SecCompany 社の CLASSIFICATIONS セクション

```
CLASSIFICATIONS:

name= PUBLIC; sname= PUBLIC; value= 1;
name= INTERNAL_USE_ONLY; sname= INTERNAL; aname= INTERNAL; value= 4;
name= NEED_TO_KNOW; sname= NEED_TO_KNOW; aname= NEED_TO_KNOW; value= 5;
name= REGISTERED; sname= REGISTERED; aname= REGISTERED; value= 6;
```

注 – 格付けには、スラッシュ (/) やコンマ (,) は使用しないでください。格付けは、最下位から順に指定します。

機密ラベルのエンコーディング

表 6–3 のコンパートメントのエンコーディングを次の例に示します。ラベルに必須組み合わせおよび組み合わせ制約はありません。

例 6–5 SecCompany 社の SENSITIVITY LABELS セクションの WORDS

```
SENSITIVITY LABELS:

WORDS:

name= ALL_DEPARTMENTS; sname= ALL; compartments= 11-20;
minclass= NEED_TO_KNOW;
name= EXECUTIVE_MGT_GROUP; sname= EMGT; compartments= 11;
minclass= NEED_TO_KNOW;
name= SALES; sname= SALES; compartments= 12;
minclass= NEED_TO_KNOW;
name= FINANCE; sname= FINANCE; compartments= 13;
minclass= NEED_TO_KNOW;
name= LEGAL; sname= LEGAL; compartments= 14;
minclass= NEED_TO_KNOW;
name= MARKETING; sname= MKTG; compartments= 15 20; minclass= NEED_TO_KNOW;
name= HUMAN_RESOURCES; sname= HR; compartments= 16; minclass= NEED_TO_KNOW;
name= ENGINEERING; sname= ENG; compartments= 17 20; minclass= NEED_TO_KNOW;
name= MANUFACTURING; sname= MANUFACTURING; compartments= 18;
minclass= NEED_TO_KNOW;
name= SYSTEM_ADMINISTRATION; sname= SYSADM; compartments= 19;
minclass= NEED_TO_KNOW;
name= PROJECT_TEAM; sname= P_TEAM; compartments= 20; minclass= NEED_TO_KNOW;

REQUIRED COMBINATIONS:

COMBINATION CONSTRAINTS:
```

情報ラベルのエンコーディング

情報ラベルは使用されませんが、ファイルがエンコーディング検査に合格するためには、 INFORMATION LABELS: WORDS: セクションに値を指定する必要があります。セキュリティー管理者役割は、次の例に示すように、SENSITIVITY LABELS: WORDS: セクションの語句をコピーします。

例 6–6 SecCompany 社の INFORMATION LABELS セクションの WORDS

```
INFORMATION LABELS:

WORDS:
```

例 6–6　SecCompany 社の INFORMATION LABELS セクションの WORDS　(続き)

```
name= ALL_DEPARTMENTS; sname= ALL; compartments= 11-20;
minclass= NEED_TO_KNOW;
name= EXECUTIVE_MGT_GROUP; sname= EMGT; compartments= 11;
minclass= NEED_TO_KNOW;
name= SALES; sname= SALES; compartments= 12;
minclass= NEED_TO_KNOW;
name= FINANCE; sname= FINANCE; compartments= 13;
minclass= NEED_TO_KNOW;
name= LEGAL; sname= LEGAL; compartments= 14;
minclass= NEED_TO_KNOW;
name= MARKETING; sname= MKTG; compartments= 15 20; minclass= NEED_TO_KNOW;
name= HUMAN_RESOURCES; sname= HR; compartments= 16; minclass= NEED_TO_KNOW;
name= ENGINEERING; sname= ENG; compartments= 17 20; minclass= NEED_TO_KNOW;
name= MANUFACTURING; sname= MANUFACTURING; compartments= 18;
minclass= NEED_TO_KNOW;
name= SYSTEM_ADMINISTRATION; sname= SYSADM; compartments= 19;
minclass= NEED_TO_KNOW;
name= PROJECT_TEAM; sname= P_TEAM; compartments= 20; minclass= NEED_TO_KNOW;

REQUIRED COMBINATIONS:

COMBINATION CONSTRAINTS:
```

認可上限のエンコーディング

認可上限の語句は機密ラベルの語句と同じなので、次の例の語句は例 6–5 の語句と同じです。

例 6–7　SecCompany 社の CLEARANCES セクションの WORDS

```
CLEARANCES:

WORDS:

name= ALL_DEPARTMENTS; sname= ALL; compartments= 11-20; minclass= NEED_TO_KNOW;
name= EXECUTIVE_MANAGEMENT_GROUP; sname= EMGT; compartments= 11;
minclass= NEED_TO_KNOW;
name= SALES; sname= SALES; compartments= 12; minclass= NEED_TO_KNOW;
name= FINANCE; sname= FINANCE; compartments= 13; minclass= NEED_TO_KNOW;
name= LEGAL; sname= LEGAL; compartments= 14; minclass= NEED_TO_KNOW;
name= MARKETING; sname= MKTG; compartments= 15 20; minclass= NEED_TO_KNOW;
name= HUMAN_RESOURCES; sname= HR; compartments= 16; minclass= NEED_TO_KNOW;
name= ENGINEERING; sname= ENG; compartments= 17 20; minclass= NEED_TO_KNOW;
```

例 6–7 SecCompany 社の CLEARANCES セクションの WORDS (続き)

```
name= MANUFACTURING; sname= MANUFACTURING; compartments= 18; minclass= NEED_TO_KNOW;
name= SYSTEM_ADMINISTRATION; sname= SYSADM; compartments= 19; minclass= NEED_TO_KNOW;
name= PROJECT_TEAM; sname= P_TEAM; compartments= 20;
minclass= NEED_TO_KNOW;

REQUIRED COMBINATIONS:

COMBINATION CONSTRAINTS:
```

チャネルのエンコーディング

この例は、グループ名コンパートメントごとに 1 つのチャネルでエンコーディングされています。各チャネルは、SENSITIVITY LABELS: WORDS: セクションのコンパートメント語句に割り当てられているのと同じコンパートメントビットを使用します。接頭辞は DISTRIBUTE ONLY TO として定義されています。接尾辞は、(NON-DISCLOSURE AGREEMENT REQUIRED) として定義されています。

```
DISTRIBUTE ONLY TO group-name (NON-DISCLOSURE AGREEMENT REQUIRED)
```

次の例に示すチャネル指定によって、取り扱い指示セクションに目的の語句が作成されます。

注 – 次の例に示すように、接頭辞と接尾辞はセクションの冒頭で定義します。コンパートメントはそれらに割り当てられません。接頭辞と接尾辞を使用してチャネルを定義します。

例 6–8 SecCompany 社の CHANNELS セクションの WORDS

```
CHANNELS:

WORDS:

name= DISTRIBUTE_ONLY_TO;       prefix;
name= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
suffix;

name= EXECUTIVE_MANAGEMENT_GROUP;
prefix= DISTRIBUTE_ONLY_TO; compartments= 11;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= SALES; prefix= DISTRIBUTE_ONLY_TO; compartments= 12;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= FINANCE; prefix= DISTRIBUTE_ONLY_TO; compartments= 13;
```

例 6–8 SecCompany 社の CHANNELS セクションの WORDS (続き)

```
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= LEGAL; prefix= DISTRIBUTE_ONLY_TO; compartments= 14;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= MARKETING; prefix= DISTRIBUTE_ONLY_TO;
compartments= 15 20;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= HUMAN_RESOURCES; prefix= DISTRIBUTE_ONLY_TO;
compartments= 16;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= ENGINEERING; prefix= DISTRIBUTE_ONLY_TO;
compartments= 17 20;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= MANUFACTURING; prefix= DISTRIBUTE_ONLY_TO;
compartments= 18;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= SYSTEM_ADMINISTRATION; prefix= DISTRIBUTE_ONLY_TO;
compartments= 19;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= PROJECT_TEAM; prefix= DISTRIBUTE_ONLY_TO; compartments= 20;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
```

プリンタバナーのエンコーディング

注 – 「プリンタバナー」という用語は、label_encodings ファイルで特別な意味を持ちます。プリンタバナーは、それに関連付けられたコンパートメントがジョブのラベルに明記されているときにプリンタバナーページに表示される文字列のことです。

次のようにプリンタバナーを指定すると、必要な語句が PRINTER BANNERS セクションに作成されます。バナーページの例は、図 4–2 を参照してください。

注 – 次の例に示すように、接頭辞はセクションの冒頭で定義します。この接頭辞にはコンパートメントが割り当てられていません。

例 6–9 SecCompany 社の PRINTER BANNERS セクションの WORDS

```
PRINTER BANNERS:

WORDS:
```

例 6–9 SecCompany 社の PRINTER BANNERS セクションの WORDS (続き)

```
name= COMPANY CONFIDENTIAL:;       prefix;

name= ALL_DEPARTMENTS; prefix= COMPANY CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 11-20;
name= EXECUTIVE_MANAGEMENT_GROUP; prefix= COMPANY CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 11;
name= SALES; prefix= COMPANY CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 12;
name= FINANCE; prefix= COMPANY CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 13;
name= LEGAL; prefix= COMPANY CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 14;
name= MARKETING; prefix= COMPANY CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 15 20;
name= HUMAN_RESOURCES; prefix= COMPANY CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 16;
name= ENGINEERING; prefix= COMPANY CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 17 20;
name= MANUFACTURING; prefix= COMPANY CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 18;
name= SYSTEM_ADMINISTRATION; prefix= COMPANY CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 19;
name= PROJECT_TEAM; prefix= COMPANY CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 20;
```

認可範囲のエンコーディング

表 6–3 の組み合わせ制約、および 107 ページの「認可範囲の最下位の計画」の minimum clearance (最下位の認可上限)、minimum sensitivity label (最下位の機密ラベル)、minimum protect as classification (最下位の機密保護の格付け) は、次の例に示す ACCREDITATION RANGE: セクションでエンコーディングされます。PUBLIC および INTERNAL_USE_ONLY は、いずれのコンパートメントとも、1 つのラベル内で組み合わされないように定義します。NEED_TO_KNOW は、任意の組み合わせのコンパートメントと、1 つのラベル内で組み合わせることができるように定義します。REGISTERED は、コンパートメントとともには表示されないように定義します。

例 6–10 SecCompany 社の ACCREDITATION RANGE セクション

```
ACCREDITATION RANGE:

classification= PUBLIC; only valid compartment combinations:

PUBLIC
```

例 6–10　SecCompany 社の ACCREDITATION RANGE セクション　(続き)

```
classification= INTERNAL_USE_ONLY; only valid compartment combinations:

INTERNAL

classification= NEED_TO_KNOW; all compartment combinations valid;

classification= REGISTERED; only valid compartment combinations:

REGISTERED


minimum clearance= PUBLIC;
minimum sensitivity label= PUBLIC;
minimum protect as classification= PUBLIC;
```

ローカル定義のエンコーディング

SecCompany 社は、LOCAL DEFINITIONS セクションにサイトカラムヘッダーおよび色をエンコーディングします。

ラベルビルダーのカラムヘッダーのエンコーディング

ラベルビルダーは、ラベルを設定する必要のあるときは必ず表示されます。次の例は、ラベルビルダーの格付け名およびコンパートメント名のデフォルト値の変更を示します。

例 6–11　SecCompany 社の label_encodings ファイルのヘッダー

次の抜粋は、ラベルビルダーのカラムヘッダーの変更を示します。SecCompany 社のセキュリティー管理者役割はコンパートメント名を変更しました。

```
Classification Name= Classification;
Compartments Name= Department;
```

色名のエンコーディング

例 6–12 で使用されている色名は、表 6–8 のワークシートから取られています。

例 6–12　SecCompany 社の COLOR NAMES セクション

```
COLOR NAMES:

        label= Admin_Low;       color= #bdbdbd;

        label= PUBLIC;        color= green;
        label= INTERNAL_USE_ONLY;  color= yellow;
        label= NEED_TO_KNOW;  color= blue;
        label= NEED_TO_KNOW EMGT;  color= #7FA9EB;
        label= NEED_TO_KNOW SALES;  color= #87CEFF;
        label= NEED_TO_KNOW FINANCE;  color= #00BFFF;
        label= NEED_TO_KNOW LEGAL;  color= #7885D0;
        label= NEED_TO_KNOW MKTG;  color= #7A67CD;
        label= NEED_TO_KNOW HR;  color= #7F7FFF;
        label= NEED_TO_KNOW ENG;  color= #007FFF;
        label= NEED_TO_KNOW MANUFACTURING;  color= #0000BF;
        label= NEED_TO_KNOW PROJECT_TEAM;  color= #9E7FFF;
        label= NEED_TO_KNOW SYSADM; color= #5B85D0;
        label= NEED_TO_KNOW ALL; color= #4D658D;
        label= REGISTERED;  color= red;

        label= Admin_High;      color= #636363;

*
* End of local site definitions
```

ラベルに関するユーザーおよびプリンタの設定

ラベル付けの決定は、ユーザーおよびプリンタにおいて実行される必要があります。

ユーザーアカウントを設定する場合、セキュリティー管理者役割はすべてのユーザーに対して次を指定する必要があります。

- 適切な認可上限

  ユーザー認可上限の計画については、104 ページの「ワークシートによる認可上限の計画」を参照してください。
- 適切な最下位ラベル
- ラベルの表示/非表示

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

セキュリティー管理者役割は、印刷出力にラベル付けするかどうかをカスタマイズできます。手順については、『Solaris Trusted Extensions 管理の手順』の「Trusted Extensions での印刷の管理 (作業マップ)」を参照してください。

◆ ◆ ◆ 付 録 A

ラベルエンコーディングファイルのサンプル

この付録では、第 6 章の例から発展させたlabel_encodings のサンプルファイルを取り扱います。

格付けとコンパートメント

このサンプルファイルには、次の 4 つの格付けがあります。

- PUBLIC
- INTERNAL_USE_ONLY
- NEED_TO_KNOW
- REGISTERED

このモデルでは、PUBLIC は、インターネット通信に使用する機密ラベルです。INTERNAL_USE_ONLY は、社内通信に使用する機密ラベルです。

サンプルファイルでは、NEED_TO_KNOW 格付けを持つラベルにだけ表示されるようにコンパートメントを定義しています。このサンプルファイルではまた、ラベルビルダー GUI のデフォルト語句の Comps を Departments に変更するように指定しています。

NEED_TO_KNOW のコンパートメントには、次のようなものがあります。

- ALL_DEPARTMENTS

  ALL_DEPARTMENTS コンパートメント語句は、定義されているコンパートメントビットがすべてオンの場合に有効化され、ラベルビルダーの切り換えスイッチとして機能します。
- EXECUTIVE_MGT_GROUP
- SALES
- FINANCE
- LEGAL

- MARKETING
- HUMAN_RESOURCES
- ENGINEERING
- MANUFACTURING
- SYSTEM_ADMINISTRATION
- PROJECT_TEAM

  PROJECT_TEAM は、階層的に ENGINEERING と MARKETING の両方より下位にあります。この階層によって、NEED_TO_KNOW ENGINEERING や NEED_TO_KNOW MARKETING で作業をしている社員は、NEED_TO_KNOW PROJECT_TEAM ラベルのファイルを読むことはできても、書き込みはできません。

label_encodings.example ファイル

このバージョンは、提供バージョンと少し異なります。

- CIPSO ラベル警告が追加されている。
- このマニュアルの例に合わせて、語句「proprietary」が削除されている。
- CMW ラベルの指示が削除されている。

```
* ident "@(#)label_encodings.example    5.13    06/08/04 SMI"
*
* Copyright 2006 Sun Microsystems, Inc.  All rights reserved.
* Use is subject to license terms.
*
*
* This version of the label_encodings file encodes the Sun
* confidential labels that are required by Sun's
* legal and information protection departments. The prefix
* COMPANY is omitted from the labels for
* brevity. This encodings includes some example department
* names that can be used for controlling access to information
* across department boundaries. Commercial sites with different
* requirements can copy this file and change the definitions to suit.

* This example shows how to specify labels that meet an actual
* site's legal information  protection requirements for
* labeling email and printer output. These labels can also
* be used to enforce mandatory access control checks that are
* based on user clearance labels, and on labels on files
* and directories.


VERSION= Sun Microsystems, Inc. Example Version - 5.13 06/08/04
```

```
*    WARNING:  If CIPSO Tag Type 1 network labels are to be used:
*
*        a) All CLASSIFICATIONS values must be less than or equal to 255.
*        b) All COMPARTMENTS bits must be less than or equal to 239.
*

CLASSIFICATIONS:

name= PUBLIC; sname= PUBLIC; value= 1;
name= INTERNAL_USE_ONLY; sname= INTERNAL; aname= INTERNAL; value= 4;
name= NEED_TO_KNOW; sname= NEED_TO_KNOW; aname= NEED_TO_KNOW; value= 5;
name= REGISTERED; sname= REGISTERED; aname= REGISTERED; value= 6;


INFORMATION LABELS:

WORDS:

name= SYSTEM_ADMINISTRATION; sname= SYSADM; compartments= 19;
minclass= NEED_TO_KNOW;
name= MANUFACTURING; sname= MANUFACTURING; compartments= 18;
minclass= NEED_TO_KNOW;
name= ENGINEERING; sname= ENG; compartments= 17 20;
minclass= NEED_TO_KNOW;
name= HUMAN_RESOURCES; sname= HR; compartments= 16;
minclass= NEED_TO_KNOW;
name= MARKETING; sname= MRKTG; compartments= 15 20;
minclass= NEED_TO_KNOW;
name= LEGAL; sname= LEGAL; compartments= 14;
minclass= NEED_TO_KNOW;
name= FINANCE; sname= FINANCE; compartments= 13;
minclass= NEED_TO_KNOW;
name= SALES; sname= SALES; compartments= 12;
minclass= NEED_TO_KNOW;
name= EXECUTIVE_MGMNT_GROUP; sname= EMG; compartments= 11;
minclass= NEED_TO_KNOW;
name= ALL_DEPARTMENTS; sname= ALL; compartments= 11-20;
minclass= NEED_TO_KNOW;
name= PROJECT_TEAM; sname= P_TEAM; compartments= 20;
minclass= NEED_TO_KNOW;

REQUIRED COMBINATIONS:

COMBINATION CONSTRAINTS:

SENSITIVITY LABELS:
```

```
WORDS:

name= ALL_DEPARTMENTS; sname= ALL; compartments= 11-20;
minclass= NEED_TO_KNOW;
name= EXECUTIVE_MGMNT_GROUP; sname= EMG; compartments= 11;
minclass= NEED_TO_KNOW;
name= SALES; sname= SALES; compartments= 12;
minclass= NEED_TO_KNOW;
name= FINANCE; sname= FINANCE; compartments= 13;
minclass= NEED_TO_KNOW;
name= LEGAL; sname= LEGAL; compartments= 14;
minclass= NEED_TO_KNOW;
name= MARKETING; sname= MRKTG; compartments= 15 20;
minclass= NEED_TO_KNOW;
name= HUMAN_RESOURCES; sname= HR; compartments= 16;
minclass= NEED_TO_KNOW;
name= ENGINEERING; sname= ENG; compartments= 17 20;
minclass= NEED_TO_KNOW;
name= MANUFACTURING; sname= MANUFACTURING; compartments= 18;
minclass= NEED_TO_KNOW;
name= SYSTEM_ADMINISTRATION; sname= SYSADM; compartments= 19;
minclass= NEED_TO_KNOW;
name= PROJECT_TEAM; sname= P_TEAM; compartments= 20;
minclass= NEED_TO_KNOW;

REQUIRED COMBINATIONS:

COMBINATION CONSTRAINTS:

CLEARANCES:

WORDS:

name= ALL_DEPARTMENTS; sname= ALL; compartments= 11-20;
minclass= NEED_TO_KNOW;
name= EXECUTIVE_MANAGEMENT_GROUP; sname= EMG; compartments= 11;
minclass= NEED_TO_KNOW;
name= SALES; sname= SALES; compartments= 12;
minclass= NEED_TO_KNOW;
name= FINANCE; sname= FINANCE; compartments= 13;
minclass= NEED_TO_KNOW;
name= LEGAL; sname= LEGAL; compartments= 14;
minclass= NEED_TO_KNOW;
name= MARKETING; sname= MRKTG; compartments= 15 20;
minclass= NEED_TO_KNOW;
name= HUMAN_RESOURCES; sname= HR; compartments= 16;
minclass= NEED_TO_KNOW;
name= ENGINEERING; sname= ENG; compartments= 17 20;
```

```
minclass= NEED_TO_KNOW;
name= MANUFACTURING; sname= MANUFACTURING; compartments= 18;
minclass= NEED_TO_KNOW;
name= SYSTEM_ADMINISTRATION; sname= SYSADM; compartments= 19;
minclass= NEED_TO_KNOW;
name= PROJECT_TEAM; sname= P_TEAM; compartments= 20;
minclass= NEED_TO_KNOW;

REQUIRED COMBINATIONS:

COMBINATION CONSTRAINTS:

CHANNELS:

WORDS:

name= DISTRIBUTE_ONLY_TO;       prefix;
name= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
suffix;

name= EXECUTIVE_MANAGEMENT_GROUP;
prefix= DISTRIBUTE_ONLY_TO; compartments= 11;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= SALES; prefix= DISTRIBUTE_ONLY_TO; compartments= 12;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= FINANCE; prefix= DISTRIBUTE_ONLY_TO; compartments= 13;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= LEGAL; prefix= DISTRIBUTE_ONLY_TO; compartments= 14;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= MARKETING; prefix= DISTRIBUTE_ONLY_TO;
compartments= 15 20;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= HUMAN_RESOURCES; prefix= DISTRIBUTE_ONLY_TO;
compartments= 16;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= ENGINEERING; prefix= DISTRIBUTE_ONLY_TO;
compartments= 17 20;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= MANUFACTURING; prefix= DISTRIBUTE_ONLY_TO;
compartments= 18;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= SYSTEM_ADMINISTRATION; prefix= DISTRIBUTE_ONLY_TO;
compartments= 19;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= PROJECT_TEAM; prefix= DISTRIBUTE_ONLY_TO; compartments= 20;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);

PRINTER BANNERS:
```

```
WORDS:

name= CONFIDENTIAL:;       prefix;

name= ALL_DEPARTMENTS;
prefix= CONFIDENTIAL:;
compartments= 11-20;
name= EXECUTIVE_MANAGEMENT_GROUP;
prefix= CONFIDENTIAL:;
compartments= 11;
name= SALES; prefix= CONFIDENTIAL:;
compartments= 12;
name= FINANCE; prefix= CONFIDENTIAL:;
compartments= 13;
name= LEGAL; prefix= CONFIDENTIAL:;
compartments= 14;
name= MARKETING; prefix= CONFIDENTIAL:;
compartments= 15 20;
name= HUMAN_RESOURCES;
prefix= CONFIDENTIAL:;
compartments= 16;
name= ENGINEERING;
prefix= CONFIDENTIAL:;
compartments= 17 20;
name= MANUFACTURING;
prefix= CONFIDENTIAL:;
compartments= 18;
name= SYSTEM_ADMINISTRATION;
prefix= CONFIDENTIAL:;
compartments= 19;
name= PROJECT_TEAM;
prefix= CONFIDENTIAL:;
compartments= 20;

ACCREDITATION RANGE:

classification= PUBLIC; only valid compartment combinations:

PUBLIC

classification= INTERNAL_USE_ONLY; only valid compartment combinations:

INTERNAL

classification= NEED_TO_KNOW; all compartment combinations valid;

classification= REGISTERED; only valid compartment combinations:
```

```
REGISTERED


minimum clearance= PUBLIC;
minimum sensitivity label= PUBLIC;
minimum protect as classification= PUBLIC;

*
* Local site definitions and locally configurable options.
*

LOCAL DEFINITIONS:


Classification Name= Classification;
Compartments Name= Departments;

Default User Sensitivity Label= public;
Default User Clearance= public;

COLOR NAMES:

     label= Admin_Low;       color= #bdbdbd;

     label= PUBLIC;               color= green;
     label= INTERNAL_USE_ONLY;    color= yellow;
     label= NEED_TO_KNOW;         color= blue;
     label= NEED_TO_KNOW EMG;     color= #7FA9EB;
     label= NEED_TO_KNOW SALES;   color= #87CEFF;
     label= NEED_TO_KNOW FINANCE;  color= #00BFFF;
     label= NEED_TO_KNOW LEGAL;    color= #7885D0;
     label= NEED_TO_KNOW MRKTG;    color= #7A67CD;
     label= NEED_TO_KNOW HR;       color= #7F7FFF;
     label= NEED_TO_KNOW ENG;      color= #007FFF;
     label= NEED_TO_KNOW MANUFACTURING;  color= #0000BF;
     label= NEED_TO_KNOW PROJECT_TEAM;   color= #9E7FFF;
     label= NEED_TO_KNOW SYSADM;   color= #5B85D0;
     label= NEED_TO_KNOW ALL;      color= #4D658D;
     label= REGISTERED;            color= red;

     label= Admin_High;      color= #636363;

*
* End of local site definitions
*
```

索引

A

ACCREDITATION RANGE キーワード，48
ACCREDITATION RANGE セクション
　説明，48
　例，114-115
ADMIN_HIGH ラベル
　格付け値，49
　数値に対応，21
ADMIN_LOW ラベル
　格付け値，49
　数値に対応，21
aname= 格付けキーワード，50

C

CHANNELS キーワード，48
CHANNELS セクション
　説明，48
　例，112-113
CIPSO (Common IP Security Option)，「CIPSO ラベル」を参照
CIPSO ラベル
　label_encodings ファイルの警告，120-125
　数値，21
　図示，21
　トラブルシューティング，63
CLASSIFICATIONS セクション
　説明，47
　例，109-110
CLEARANCES キーワード，48
CLEARANCES セクション
　説明，48
　例，111-112
COLOR NAMES セクション
　色計画シート，108
　説明，46, 83-86
　例，115-116
COMBINATION CONSTRAINTS キーワード，48
CONFIDENTIAL: INTERNAL_USE_ONLY ラベル, 条件，95
CONFIDENTIAL: NEED_TO_KNOW ラベル
　条件，95-96
　使用するグループ，96-97
CONFIDENTIAL: REGISTERED ラベル
　DAC 保護の追加，101
　条件，96

E

/etc/security/tsol ディレクトリ，42

G

GFI ファイル
　/etc/security/tsol ディレクトリ，42
　比較，44-46

I

INFORMATION LABELS キーワード，48

INFORMATION LABELS セクション
　説明，48
　例，110-111
initial compartments= 格付けキーワード，50

L

label_encodings.example ファイル，42, 120-125
label_encodings.gfi.multi ファイル，42
label_encodings.gfi.single ファイル，42
label_encodings.multi ファイル，42
label_encodings.simple ファイル，42, 43-44
label_encodings.single ファイル，42
label_encodings ファイル
　CHANNELS セクション，71, 76
　GFI エンコーディングに対する Sun の拡張機能，46
　LOCAL DEFINITIONS セクション，81-86
　アクセス関連の語句，68-69
　色のエンコーディングの例，108
　格付け名の構文，49-54
　格付けのキーワード，49-51
　格付けの例，50
　機密保護の格付け，68-69
　計画，37-42
　構文，47-54
　語句の順番，48-49
　作成の例，98
　商用の例，89-117
　説明，42-46
　提供バージョン，42-46
　デフォルトバージョン，42-46
　米国政府単一ラベルバージョン，45-46
　米国政府バージョン，44-46
　米国政府マルチラベルバージョン，45
　ラベルの色の指定，83-86, 87
　リスト，42-46
　例，119
label_encodings ファイルの構文，47-54
LOCAL DEFINITIONS キーワード，48
LOCAL DEFINITIONS セクション
　GFI エンコーディングファイルに追加，46
　説明，48, 81-86
　例，115

N

name= 格付けキーワード，49

P

PostScript ファイルの印刷承認，100-101
PRINTER BANNERS キーワード，48
PRINTER BANNERS セクション
　説明，48
　例，113-114

R

REQUIRED COMBINATIONS キーワード，48
rgb.txt ファイル，86

S

SENSITIVITY LABELS キーワード，48
SENSITIVITY LABELS セクション
　説明，48
　例，110
sname= 格付けキーワード，50
Sun 拡張機能の変更 (作業マップ)，86-88
Sun の拡張機能，「LOCAL DEFINITIONS セクション」を参照
sys_trans_label 特権，35

T

tsol_separator.ps ファイル，68

U

/usr/lib/lp/postscript/tsol_separator.ps ファイル，68
/usr/openwin/lib/rgb.txt ファイル，86

V

value= 格付けキーワード，50
VERSION= キーワード，47
VERSION セクション
　説明，47
　例，109

W

WORDS キーワード，48

あ

アカウント
　セッション範囲，29-31
　ラベル範囲の概要，26-27
　ラベル範囲の例，27
アクセス関連の語句, 定義済み，68-69
アクセス制御
　ラベル範囲による，19-20
　例，21
アクセスの決定, ラベルの使用，20-21
値
　格付け，49
　管理格付け，49
　コンパートメント，53

い

色
　値，86
　色の値を見つける，88
　ラベルでの使用に関する規則，84-86
　ラベルに対する指定，83-86
　ワークシートの例，108
　割り当て，87-88
印刷，「プリンタ出力」を参照
印刷ジョブでのセキュリティーテキストの設定 (作業マップ)，76-79
インバース語句, 定義済み，51-52

え

エンコーディングファイル，「label_encodings ファイル」を参照

か

格付け
　色の指定，87
　印刷のルール，69
　キーワード，49-51
　計画の例，99
　構文，49-54
　最大数，21, 49
　数値，49
　分析の例，95-97
　優位性，49
　ラベルビルダーのカラムヘッダーの変更，82-83
格付けのキーワード，49-51
カスタマイズ
　色の割り当て，108
　印刷出力のセキュリティーテキスト，66
　バナーページ，68
　プリンタ出力の取り扱い指示，77-78
　ラベルの表示，34-35
　ラベルへの色の割り当て，87-88
カラムヘッダー, ラベルビルダーの変更，82-83
関心がある分野, コンパートメントによって表現，52-53
完全な優位性，23
管理ラベル
　システム認可範囲内の，24-25
　名前表示の指定，34
　表示の設定，34-35

き

機密, ラベルの型，19-33
機密保護の格付け
　概要，68-69
　例，69, 114-115
機密ラベル，「ラベル」を参照

く
組み合わせ制約
　例，24, 26, 28, 114-115
組み合わせの規則，「組み合わせの制約」を参照
組み合わせの制約, 定義済み，23

け
計画シート，「ワークシート」を参照

こ
語句, 計画の例，99-100
国際化
　バナーページとトレーラページ，68
　プリンタバナーページとトレーラページ，66
語句の順番, label_encodings ファイル，48-49
国防情報局 (DIA), label_encodings 参考資料，42
コンパートメント
　階層の設定，53-54
　計画の例，99
　語句，52-53
　語句の例，53
　数値，53
　デフォルト語句とインバース語句，51-52
　ラベルビルダーのカラムヘッダーの変更，82-83
　ワークシートの例，103-104

さ
最下位機密ラベル, 例，114-115
最下位認可上限, 例，114-115
最下位の機密保護の格付け
　印刷出力，78-79
　例，68, 69
最下位の機密ラベル
　定義済み，26-27
　例，58, 61
最下位ラベル
　アカウントラベル範囲，26-27
　商用の例，107
作業マップ
　Sun 拡張機能の変更 (作業マップ)，86-88
　印刷ジョブでのセキュリティーテキストの設定 (作業マップ)，76-79
　ラベルエンコーディングの管理 (作業マップ)，55-63
　ラベルの計画 (作業マップ)，37-42

し
システムセキュリティーポリシー，17
システム認可範囲，24-25
承認
　PostScript ファイルの印刷，100-101
　ファイルラベルのアップグレード，35
　ファイルラベルのダウングレード，35
　ラベルなしの印刷，100-101
初期コンパートメント
　語句へのビットの割り当て，51
　定義済み，51-52
　割り当ての例，51

せ
セキュリティーポリシー
　最下位の機密保護の設定，78
　サイト固有，38
　サイトの条件の確認，89-94
　情報保護，89-90
　定義済み，17-18
セッション
　セッション範囲の定義，29-31
　ログイン時に選択したラベル制限の期間，30
接頭辞, チャネル，73
接尾辞, チャネル，73

ち
チャネル
　接頭辞と接尾辞，72
　バナーページとトレーラページの文字列，71, 76

チャネル (続き)
ワークシートの例，106-107
注意，「取り扱い指示」を参照

て
デバッグ, label_encodings ファイル，63
デフォルト語句, 定義済み，51-52
デモファイル
label_encodings.example ファイル，51
label_encodings.multi ファイル，50
label_encodings の例，42-46

と
特権, ラベルの変換，35
トラブルシューティング, label_encodings ファイル，63
取り扱い指示
指定，77-78
プリンタバナー，34
トレーラページ
格付けの計算，69
国際化，68
ラベル付け，66-68
例，67

に
認可上限
アカウントラベル範囲，26-27
ラベルの型，19-33
ワークシートの例，104-105
認可範囲
概要，24
システム，24-25
ユーザー，25-26

は
バナーページ
格付けの計算，69
カスタマイズ，68
国際化，68
表示，66
ラベル付け，66-68

ひ
比較
GFI ファイル，44-46
label_encodings ファイル，42-46
ラベル，20
必須アクセス制御 (MAC)
アクセスの決定での使用，21
定義済み，17-18
必要な組み合わせ，「組み合わせの制約」を参照

ふ
ファイル
label_encodings.example，120-125
label_encodings.simple，43-44
label_encodings のバージョン，42-46
/usr/lib/lp/postscript/tsol_separator.ps，68
/usr/openwin/lib/rgb.txt，86
ファイルラベルのアップグレード承認，35
ファイルラベルのダウングレード承認，35
プリンタ出力
印刷されたラベルの変更，34
最下位の機密保護の格付けの設定，78-79
接頭辞と接尾辞，73
チャネル，73
取り扱い上の規則，102
バナーテキスト，69
ラベルとテキストの設定，66
プリンタの出力, 計画の例，100
プリンタバナー
表示，66
ワークシートの例，105-106

へ
変換
「国際化」も参照
ラベルの表現，35

ほ
本文ページ
表示，65
ラベル，65-66

ゆ
優位性，23
ユーザー
印刷承認，100-101
ラベルの変更の承認，35
ワークスペースアクセス，100
ユーザー認可範囲，25-26

ら
ラベル
CIPSO，21, 53
CONFIDENTIAL: INTERNAL_USE_ONLY の条件，95
CONFIDENTIAL: NEED_TO_KNOW の条件，95-96
CONFIDENTIAL: REGISTERED の条件，96
label_encodings ファイルのソース，42-46
Sun 提供のファイル，42-46
アカウントラベル範囲，26-27
アクセスおよび印刷に関する必須事項，90-94
アクセスの決定，20-21
アクセスの制限，19-20
色の計画の例，108
色の指定，87
印刷される本文ページ，65-66
インストールの例，109-116
型，19-33
関係の調整，40
計画，38-42
計画の概要，37-42
構成要素，21-22
ラベル (続き)
構成要素の長さ，53
最下位の機密保護の格付け，78-79
システム認可範囲，24-25
商用の例，89-117
セッション中の使用可能性，32-33
セッション範囲，29-31
戦略，38
適格な形式，24
テキスト文字列，35
内部表現，35
認可範囲，24
バナーページとトレーラページ，66-68
範囲，23-24
比較，20
プリンタ出力の設定，34
分析の例，95-97
変換，35
変更の承認，35
優位性，23
有効，24
ユーザー認可範囲，25-26
ワークシートの例，102-103
ワークスペースで表示，33
ラベルエンコーディングの管理 (作業マップ)，55-63
ラベル制限, 認可上限，19-33
ラベルなしの印刷承認，100-101
ラベルの型，19-33
ラベルの計画
label_encodings ファイル，38-42
色，108
概要，37-42
サポート手順，101-102
商用の例，89-117
戦略，38
手順，38-42
ラベル付けされていないプリンタ出力，100-101
ラベルの計画 (作業マップ)，37-42
ラベル範囲, 概要，19
ラベルビルダー, カラムヘッダーの変更，82-83
ラベル変換，35

れ

例
ACCREDITATION RANGE セクション，114-115
CHANNELS セクション，112-113
CLASSIFICATIONS セクション，109-110
CLEARANCES セクション，111-112
COLOR NAMES セクション，115-116
label_encodings ファイル，119
LOCAL DEFINITIONS セクション，115
MAC 決定，21
PRINTER BANNERS セクション，113-114
SENSITIVITY LABELS セクション，110
ラベル計画，89-117
ラベルビルダーのカラムヘッダー，115

わ

ワークグループ, ラベルコンパートメントに
よって表現，52-53
ワークシート
色計画シート，108
格付け計画シート，102-103
コンパートメント計画シート，103-104
チャネル計画シート，106-107
認可上限計画シート，104-105
プリンタバナー計画シート，105-106
ワークスペース
ユーザーによるアクセス，32-33, 100
ラベル付け，33