



Solaris Trusted Extensions リ ファレンスマニュアル



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

Part No: 819-7615-11
2007年6月

Sun Microsystems, Inc. (以下米国 Sun Microsystems 社とします) は、本書に記述されている製品に含まれる技術に関連する知的財産権を所有します。特に、この知的財産権はひとつかそれ以上の米国における特許、あるいは米国およびその他の国において申請中の特許を含んでいることがあります。それらに限定されるものではありません。

本製品の一部は、カリフォルニア大学からライセンスされている Berkeley BSD システムに基づいていることがあります。UNIX は、X/Open Company, Ltd. が独占的にライセンスしている米国ならびに他の国における登録商標です。フォント技術を含む第三者のソフトウェアは、著作権により保護されており、提供者からライセンスを受けているものです。

U.S. Government Rights Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

この配布には、第三者によって開発された素材を含んでいることがあります。

本製品に含まれる HG-MinchoL、HG-MinchoL-Sun、HG-PMinchoL-Sun、HG-GothicB、HG-GothicB-Sun、および HG-PGothicB-Sun は、株式会社リコーがリョービマジックス株式会社からライセンス供与されたタイプフェースマスタをもとに作成されたものです。HeiseiMin-W3H は、株式会社リコーが財団法人日本規格協会からライセンス供与されたタイプフェースマスタをもとに作成されたものです。フォントとして無断複製することは禁止されています。

Sun、Sun Microsystems、Sun のロゴマーク、Solaris のロゴマーク、Java Coffee Cup のロゴマーク、docs.sun.com、ToolTalk、Sun Ray、Java および Solaris は、米国およびその他の国における米国 Sun Microsystems 社の商標、登録商標もしくは、サービスマークです。

すべての SPARC 商標は、米国 SPARC International, Inc. のライセンスを受けて使用している同社の米国およびその他の国における商標または登録商標です。SPARC 商標が付いた製品は、米国 Sun Microsystems 社が開発したアーキテクチャに基づくものです。

OPENLOOK、OpenBoot、JLE は、サン・マイクロシステムズ株式会社の登録商標です。

Wnn は、京都大学、株式会社アステック、オムロン株式会社で共同開発されたソフトウェアです。

Wnn8 は、オムロン株式会社、オムロンソフトウェア株式会社で共同開発されたソフトウェアです。Copyright(C) OMRON Co., Ltd. 1995-2006. All Rights Reserved. Copyright(C) OMRON SOFTWARE Co., Ltd. 1995-2006 All Rights Reserved.

「ATOK for Solaris」は、株式会社ジャストシステムの著作物であり、「ATOK for Solaris」にかかる著作権、その他の権利は株式会社ジャストシステムおよび各権利者に帰属します。

「ATOK」および「推測変換」は、株式会社ジャストシステムの登録商標です。

「ATOK for Solaris」に添付するフェイスマーク辞書は、株式会社ビレッジセンターの許諾のもと、同社が発行する『インターネット・パソコン通信フェイスマークガイド』に添付のものを使用しています。

「ATOK for Solaris」に含まれる郵便番号辞書(7桁/5桁)は日本郵政公社が公開したデータを元に制作された物です(一部データの加工を行なっています)。

Unicode は、Unicode, Inc. の商標です。

本書で参照されている製品やサービスに関しては、該当する会社または組織に直接お問い合わせください。

OPEN LOOK および Sun Graphical User Interface は、米国 Sun Microsystems 社が自社のユーザおよびライセンス実施権者向けに開発しました。米国 Sun Microsystems 社は、コンピュータ産業用のビジュアルまたはグラフィカル・ユーザインタフェースの概念の研究開発における米国 Xerox 社の先駆者としての成果を認めるものです。米国 Sun Microsystems 社は米国 Xerox 社から Xerox Graphical User Interface の非独占的ライセンスを取得しており、このライセンスは、OPEN LOOK のグラフィカル・ユーザインタフェースを実装するか、またはその他の方法で米国 Sun Microsystems 社との書面によるライセンス契約を遵守する、米国 Sun Microsystems 社のライセンス実施権者にも適用されます。

本書で言及されている製品や含まれている情報は、米国輸出規制法で規制されるものであり、その他の国の輸出入に関する法律の対象となることがあります。核、ミサイル、化学あるいは生物兵器、原子力の海洋輸送手段への使用は、直接および間接を問わず厳しく禁止されています。米国が禁輸の対象としている国や、限定はされませんが、取引禁止顧客や特別指定国民のリストを含む米国輸出排除リストで指定されているものへの輸出および再輸出は厳しく禁止されています。

本書は、「現状のまま」をベースとして提供され、商品性、特定目的への適合性または第三者の権利の非侵害の黙示の保証を含みそれに限定されない、明示的であるか黙示的であるかを問わない、なんらの保証も行われぬものとします。

本製品が、外国為替および外国貿易管理法(外為法)に定められる戦略物資等(貨物または役務)に該当する場合、本製品を輸出または日本国外へ持ち出す際には、サン・マイクロシステムズ株式会社の事前の書面による承諾を得ることのほか、外為法および関連法規に基づく輸出手続き、また場合によっては、米国商務省または米国所轄官庁の許可を得ることが必要です。

原典: Solaris Trusted Extensions Reference Manual

Part No: 819-3219-11

Revision A

目次

はじめに	7
序章	9
Intro(3TSOL)	10
ユーザーコマンド	13
dtappsession(1)	14
getlabel(1)	16
getzonepath(1)	17
plabel(1)	18
setlabel(1)	19
システム管理コマンド	21
add_allocatable(1M)	22
atohexlabel(1M)	25
chk_encodings(1M)	26
hextoalabel(1M)	27
remove_allocatable(1M)	28
smtnrhdb(1M)	29
smtnrhtp(1M)	33
smtnzonedcfg(1M)	37
tnchkdb(1M)	42
tnctl(1M)	44
tnd(1M)	47
tninfo(1M)	49
updatehome(1M)	51

システムコール	53
getlabel(2)	54
Trusted Extensions ライブラリ	57
blcompare(3TSOL)	58
blminmax(3TSOL)	59
bltcolor(3TSOL)	60
bltos(3TSOL)	62
btohex(3TSOL)	65
getdevicerange(3TSOL)	67
getpathbylabel(3TSOL)	68
getplabel(3TSOL)	70
getuserange(3TSOL)	71
getzonelabelbyid(3TSOL)	72
getzonerootbyid(3TSOL)	74
hextob(3TSOL)	75
labelbuilder(3TSOL)	76
labelclipping(3TSOL)	81
label_to_str(3TSOL)	83
m_label(3TSOL)	85
sbltos(3TSOL)	86
setflabel(3TSOL)	88
stobl(3TSOL)	91
str_to_label(3TSOL)	94
tsol_getrhtype(3TSOL)	96
X ライブラリ 拡張	97
XTSOLgetClientAttributes(3XTSOL)	98
XTSOLgetPropAttributes(3XTSOL)	99
XTSOLgetPropLabel(3XTSOL)	100
XTSOLgetPropUID(3XTSOL)	101
XTSOLgetResAttributes(3XTSOL)	102
XTSOLgetResLabel(3XTSOL)	104
XTSOLgetResUID(3XTSOL)	105
XTSOLgetSSHeight(3XTSOL)	107

XTSOLgetWorkstationOwner(3XTSOL)	108
XTSOLIsWindowTrusted(3XTSOL)	109
XTSOLMakeTPWindow(3XTSOL)	110
XTSOLsetPolyInstInfo(3XTSOL)	111
XTSOLsetPropLabel(3XTSOL)	112
XTSOLsetPropUID(3XTSOL)	113
XTSOLsetResLabel(3XTSOL)	114
XTSOLsetResUID(3XTSOL)	115
XTSOLsetSessionHI(3XTSOL)	116
XTSOLsetSessionLO(3XTSOL)	117
XTSOLsetSSHheight(3XTSOL)	118
XTSOLsetWorkstationOwner(3XTSOL)	119
ファイル形式	121
label_encodings(4)	122
sel_config(4)	127
tnrhdb(4)	129
tnrhtp(4)	132
tnzonecfg(4)	136
TrustedExtensionsPolicy(4)	140
標準、環境、マクロ	143
labels(5)	144
pam_tsol_account(5)	146
索引	149

はじめに

Solaris オペレーティングシステムの初心者でも、熟練したユーザーでも、オンラインのマニュアルページを使ってシステムおよびその機能に関する情報を入手できます。マニュアルページの目的は、「これは何をするのか」という質問に簡潔な答えを提供することです。通常、マニュアルページには、リファレンスマニュアルの内容が含まれています。これは、チュートリアルとして使用するためのものではありません。

Solaris Trusted Extensions マニュアルページの概要

次に、Trusted Extensions の各マニュアルページセクションを示します。

- セクション 1 では、Solaris Trusted Extensions ソフトウェア独自のコマンドについて説明します。このセクションには、CDE の機能を拡張する `dtappsession` のマニュアルページが含まれています。
- セクション 1M では、システムの保守および管理で主に使用する Trusted Extensions のコマンドについて説明します。
- セクション 2 では、Trusted Extensions のシステムコールについて説明します。
- セクション 3TSOL では、Trusted Extensions ソフトウェア独自の関数について説明します。
- セクション 3XTSOL では、Solaris Trusted Extensions 用の X Windows ソフトウェアを拡張する関数について説明します。これらの関数は、Trusted Extensions ソフトウェアに独自のものです。
- セクション 4 では、Trusted Extensions のファイル形式の概要を説明します。該当する部分では、ファイル形式の C 構造体宣言を示します。
- セクション 5 には、PAM モジュールおよびラベルの説明が含まれます。

Solaris Trusted Extensions のマニュアルページの形式は、Solaris OS のマニュアルページで一般に使用される形式に従っています。各セクションの詳細は、`man(1)` および各セクションの `Intro` マニュアルページを参照してください。

参照
序章

名前	Intro – Trusted Extensions インタフェースの紹介
機能説明	<p>このページでは、接尾辞が 3TSOL のマニュアルページだけではなく、Trusted Extensions のマニュアルページをすべて紹介します。Trusted Extensions のマニュアルページには、ユーザーとシステム管理者が使用可能なコマンド、Trusted Extensions に固有のファイル、および開発者が使用可能なインタフェースが含まれます。Trusted Extensions のマニュアルページは、Solaris OS のマニュアルページの形式に従っています。</p> <p>Trusted Extensions ソフトウェア専用のインタフェースは、このリファレンスマニュアルの印刷物に記載されています。既存の Solaris インタフェースに対する Trusted Extensions の変更内容については、このリファレンスマニュアルの印刷物には含まれません。</p> <p>Trusted Extensions により Solaris インタフェースが拡張されている部分については、該当する Solaris のマニュアルページに説明が記載されています。たとえば、Trusted Extensions 専用の監査クラスについては、<code>audit_class(4)</code> のマニュアルページに記載されています。マニュアルページのセクションの詳細は、<code>man(1)</code>、および Solaris OS マニュアルページの各セクションの Intro マニュアルページを参照してください。</p>
Solaris Trusted Extensions インタフェースの概要	<p>次に、Trusted Extensions の各マニュアルページセクションについて説明します。</p> <ul style="list-style-type: none">■ セクション 1 は、Trusted Extensions ソフトウェアに固有のコマンドについて説明します。このセクションには、CDE の機能を拡張する <code>dtappsession(1)</code> のマニュアルページが含まれています。■ セクション 1M は、システム保守や管理用として主に使用される Trusted Extensions コマンドについて説明します。■ セクション 2 は、Trusted Extensions のシステムコールについて説明します。■ セクション 3TSOL は、Trusted Extensions ソフトウェア専用の関数について説明します。■ セクション 3XTSOL は、Trusted Extensions 用に X Window ソフトウェアを拡張する関数について説明します。これらは、Trusted Extensions ソフトウェア専用の関数です。■ セクション 4 は、Trusted Extensions ファイル形式の概要を説明します。該当する部分では、ファイル形式の C 構造体宣言を示します。■ セクション 5 には、PAM モジュールおよびラベルの説明が含まれます。
Trusted Extensions ライブラリインタフェースおよびヘッダー	<p>Trusted Extensions では、3つのライブラリが追加されています。</p> <p>(3TSOL) これらの関数は、Trusted Extensions ライブラリ <code>libtsol</code>、および Trusted Extensions ソフトウェアでのみ使用されるほかのライブラリ内のさまざまな関数を構成します。</p>

`libtsol.so` は、共有オブジェクトとして実装されていますが、C 言語処理系により自動的にリンクされません。`libtsol` ライブラリとリンクさせるには、`cc` コマンド行で `-ltsol` を指定します。

非公開ライブラリ `libtsnet` からの関数は、このセクションに含まれています。`libtsnet` ライブラリとリンクさせるには、`cc` コマンド行で `-ltsnet` を指定します。これらのライブラリについては、Solaris のマニュアルページ `libtsol(3LIB)` および `libtsnet(3LIB)` を参照してください。

(3XTSOL) これらの関数は、X Window ライブラリへの Trusted Extensions である `libXtsol` です。`libXtsol.so` は共有オブジェクトとして実装されていますが、C コンパイラシステムによって自動的にリンクはされません。`libXtsol` ライブラリをリンクする場合は、`cc` コマンド行上で `-lX11` のあとに `-lXtsol` を指定します (`cc -lX11 -lXtsol`)。

関連項目

Intro(1), man(1)

『Solaris Trusted Extensions 開発ガイド』

『Solaris Trusted Extensions 管理の手順』

参照
ユーザーコマンド

名前	dtapssession - 新規アプリケーションマネージャーセッションの起動
形式	<code>/usr/dt/bin/dtapssession [hostname]</code>
機能説明	<p>dtapssession は、Xsession シェルスクリプトの特殊なバージョンです。これは、CDE リモートログインの代わりに使用できます。これを使うと、現在の CDE セッションからログアウトせずに遠隔ホストにアクセスできます。dtapssession は、CDE アプリケーションマネージャーの新規インスタンスを、独自の ToolTalk™ セッション内で開始します。これを使用すると、<code>rlogin(1)</code> コマンドを使って遠隔ホストにログインしたあとで、リモートのアプリケーションマネージャーをローカルのディスプレイに表示できます。</p> <p><code>ttssession(1)</code> の独立した新規インスタンスにより、簡略化されたセッション管理ウィンドウが起動されます。このウィンドウのタイトルは次のようになります。</p> <p><code>remote_hostname</code>: Remote Administration</p> <p>ここで、<code>remote_hostname</code> はアクセス対象のシステムです。ウィンドウには、「終了」ボタンも表示されます。「終了」をクリックすると、ToolTalk セッションおよびこのセッションに含まれるウィンドウがすべて終了します。</p> <p>表示されるアプリケーションマネージャーを使用して、リモートの CDE アクションを起動し、このセッション内で実行できます。アプリケーションマネージャーを終了しても、このセッションは終了しません。このため、この方法は推奨されていません。「終了」をクリックして、セッションを終了することをお勧めします。リモートの CDE アプリケーションをローカルのアプリケーションと混同しないように、リモートセッション内のクライアント用に CDE ワークスペースを新規作成することをお勧めします。</p> <p>遠隔ホスト上で <code>DISPLAY</code> 環境変数がローカルホストに設定されている場合、<code>hostname</code> は不要です。</p> <p>Trusted Extensions を使って設定されたシステムでは、遠隔ホストにログイン可能な管理役割によって、dtapssession を使用してリモート管理を実行できます。</p> <p>dtapssession の実行には、いかなる特権も必要ありません。また、Trusted Extensions を使って設定されたシステム上でこのコマンドを使用する必要はありません。dtapssession を <code>startApp.ds</code> ファイルとともに Solaris システムの <code>/usr/dt/bin</code> にインストールした場合、Trusted Extensions を使って設定されたローカルシステムからリモートの Solaris システムを管理できます。ただし、この場合、リモート表示に使用する CDE ワークスペースは、役割ワークスペースではなく、通常のワークスペースでなければなりません。</p>
使用例	<p>例1 リモートログインと dtapssession</p> <p>CDE ワークスペースを新規作成したあとで、端末のウィンドウに次のように入力します。</p>

例1 リモートログインと dtapssession (続き)

```
# rlogin remote_hostname
password: /* リモートパスワードを入力 */

# dtapssession local_hostname /* リモートホスト上で実行 */
```

属性

次の属性については、attributes(5)を参照してください。

属性タイプ	属性値
使用条件	SUNWdttsu

ファイル

/usr/dt/bin/startApp.ds セッションマネージャーウィンドウ用の dt Korn
シェルスクリプト

使用上の留意点

ToolTalk セッションマネージャーに登録されない X11/CDE アプリケーションは、セッションが終了しても自動的に終了しません。この種のアプリケーションは、明示的に終了する必要があります。

関連項目

dtfile(1), rlogin(1), ttssession(1), attributes(5)

『Solaris Trusted Extensions 管理の手順』の第8章「Trusted Extensions での遠隔管理」

- 名前 getlabel – ファイルのラベルの表示
- 形式 /usr/bin/getlabel [-sS] filename...
- 機能説明 getlabel は、各 *filename* に関連付けられているラベルを表示します。オプションを省略すると、ラベルはデフォルト形式で表示されます。
- オプション -s *filename* に関連付けられているラベルを短形式で表示します。
 -S *filename* に関連付けられているラベルを長形式で表示します。
- 戻り値 getlabel は、終了時に次のいずれかの値を返します。
- 0 正常終了。
 - 1 使用方法の誤りのためエラー終了した。
 - 2 ラベルを変換できなかった。
- 属性 次の属性については、[attributes\(5\)](#) を参照してください。

属性タイプ	属性値
使用条件	SUNWtsu
安定性(コマンド行)	安定
安定性(出力)	非インタフェース

関連項目 [setlabel\(1\)](#), [label_encodings\(4\)](#), [attributes\(5\)](#)

- 名前** getzonepath - 指定したラベルに対応するゾーンのルートパスの表示
- 形式** /usr/bin/getzonepath {*sensitivity-label*}
- 機能説明** getzonepath は、指定した機密ラベルに対応する、実行中のラベル付きゾーンのルートパス名を表示します。返されるパス名は、呼び出し元のルートパス名に対する相対パスで、指定された機密ラベルが付けられています。
- 呼び出し元が大域ゾーン内に存在する場合、呼び出し側のプロセスが `file_dac_search` 特権を保持しない限り、返されるパスをたどることはできません。
- 呼び出し側がラベル付きのゾーン内に存在する場合、呼び出し側のラベルが指定したラベルよりも優位でなければなりません。返されたパス名内部のファイルへのアクセスは、読み取り専用操作に限定されています。
- 属性** 次の属性については、`attributes(5)` を参照してください。

属性タイプ	属性値
使用条件	SUNWtsu
安定性	安定

- 診断** getzonepath は、終了時に次のいずれかの値を返します。
- 0 正常終了
 - 1 使用上のエラー
 - 2 異常終了。エラーメッセージとして `getzonerootbylabel(3TSOL)` のシステムエラー番号が返される
- 関連項目** [getzonerootbylabel\(3TSOL\)](#), [attributes\(5\)](#)

『Solaris Trusted Extensions 開発ガイド』の「機密ラベルの取得」

- 名前 plabel – プロセスのラベルの取得
- 形式 /usr/bin/plabel [-sS] [pid...]
- 機能説明 plabel は、プロセスのラベルを取得するプロセスツールコマンドです。pid を指定しない場合は、plabel コマンドのラベルが表示されます。オプションを省略すると、ラベルはデフォルト形式で表示されます。
- オプション -s pid に関連付けられているラベルを短形式で表示します。
 -S pid に関連付けられているラベル長形式で表示します。
- 戻り値 plabel は、終了時に次のいずれかの値を返します。
- 0 正常終了。
 - 1 使用方法の誤りのためエラー終了した。
 - 2 ラベルを変換できなかった。
 - 3 メモリーを割り当てられなかった。
- 属性 次の属性については、attributes(5) を参照してください。

属性タイプ	属性値
使用条件	SUNWtsu
安定性	安定
安定性 (出力)	非インタフェース

関連項目 [proc\(1\)](#), [getplabel\(3TSOL\)](#), [attributes\(5\)](#)

名前	setlabel - 対応する機密ラベルを持つゾーンへのファイルの移動
形式	<code>/usr/bin/setlabel newlabel filename...</code>
機能説明	<p>setlabel は、<i>newlabel</i> に対応するラベルを持つゾーンにファイルを移動します。古いファイルパス名は、新規ゾーンのルートパス名との相対位置になるように調整されます。ファイルの親ディレクトリの古いパス名が、新規ゾーン内にディレクトリとして存在しない場合、ファイルは移動されません。移動後は、現在のゾーン内でファイルにアクセスすることはできなくなります。</p> <p><i>newlabel</i> および <i>filename</i> が指定されない場合、ラベルは設定されません。</p> <p>ラベルの定義は、サイトのセキュリティー管理者により行われます。ラベルは、システム内で常に大文字で表示されます。ユーザーは、大文字と小文字を任意に組み合わせるラベルを入力できます。ラベルの内容の追加や削除も可能です。</p> <p>このコマンドを実行するのに必要な条件および必要な特権についての説明は、setlabel(3TSOL) を参照してください。</p>
戻り値	<p>setlabel は、終了時に次のいずれかの値を返します。</p> <ul style="list-style-type: none"> 0 正常終了。 1 使用方法上のエラー。 2 ラベルの取得、設定、または変換中にエラー発生。
属性	次の属性については、 attributes(5) を参照してください。

属性タイプ	属性値
使用条件	SUNWtsu
安定性	安定

使用方法

コマンド行では、1つの単語だけから成るラベルを指定する場合を除き、ラベル全体を二重引用符で囲みます。引用符がないと、空白の次の単語または文字は、新たな引数として解釈されます。

```
% setlabel SECRET somefile
% setlabel "TOP SECRET" somefile
```

ラベルの内容は大文字でも、小文字でも、両者を混在させてもかまいません。ラベル内に複数の項目を記述する場合には、空白、タブ、コンマ、スラッシュ (/) のいずれかで区切ります。それ以外の文字や記号は区切り文字とは見なされません。

```
% setlabel "ts a b" somefile
% setlabel "ts,a,b" somefile
% setlabel "ts/a b" somefile
% setlabel " TOP SECRET A B " somefile
```

使用例

例1 ラベルを設定する

somefile のラベルを SECRET A に設定する

```
example% setlabel "Secret a" somefile
```

例2 コンパートメントを有効にする

プラス記号とマイナス記号を使って、既存のラベルを変更できます。プラス記号を使用すると、*somefile* のラベル用の指定したコンパートメントが有効になります。

```
example% setlabel +b somefile
```

例3 コンパートメントを無効にする

マイナス記号を使用すると、格付け部に関連付けられたコンパートメントが無効になります。次のようにして、*somefile* のラベル内のコンパートメント A を無効にします。

```
example% setlabel -A somefile
```

既存ラベルの内容を追加または削除する場合で、ラベルの先頭文字がハイフン(-)のときは、その前に二重ハイフン(--)を指定する必要があります。

次のようにして、*somefile* のラベル内のコンパートメント -A を無効にします。

```
example% setlabel -- -A somefile
```

注意事項

ラベル設定に関するこの実装は、米国国防情報局 (DIA) の必須アクセス制御 (MAC) ポリシーにとって重要です。詳細は、[label_encodings\(4\)](#) を参照してください。

関連項目

[setlabel\(3TSOL\)](#), [label_encodings\(4\)](#), [attributes\(5\)](#)

参照

システム管理コマンド

名前	add_allocatable - 割り当てデータベースへのエントリの追加
形式	<code>/usr/sbin/add_allocatable [-f] [-s] [-d] -n name -t type -l device-list [-a authorization] [-c clean] [-o key=value]</code>
機能説明	<p>add_allocatable は、ユーザーが割り当て可能なデバイス用の新規エントリを作成します。このデバイスは、デバイス割り当て機構により管理されます。</p> <p>add_allocatable を使用して、この種のデバイスの既存エントリを更新することもできます。</p> <p>add_allocatable を使用して、デバイス割り当て機構によりラベル範囲が管理される、プリンタなどの割り当て不可能なデバイスのエントリを作成および更新することもできます。</p> <p>add_allocatable をシェルスクリプト (ドライバパッケージのインストールスクリプトなど) 内で実行して、新規デバイスの設定に関する管理作業を自動化できます。</p> <p>割り当て可能なデバイスの名前とタイプ、属性、およびデバイスパスについては、list_devices(1) を参照してください。</p>
オプション	<p>-f 指定された情報を使って、既存のエントリを強制的に更新します。このオプションを指定しない場合、指定したデバイス名を持つエントリが既に存在すると、add_allocatable はエラーを出力して終了します。</p> <p>-s サイレントモードを有効にします。add_allocatable は、エラーや警告メッセージを一切出力しません。</p> <p>-d このオプションが指定されている場合、add_allocatable は、-t で指定されたデバイスタイプのシステム指定のデフォルト属性を更新します。</p> <p>-n name name で指定されたデバイスのエントリを追加または更新します。</p> <p>-t type type で指定されたタイプのデバイスエントリを追加または更新します。</p> <p>-l device-list -n で指定されたデバイスへのデバイスパスを追加または更新します。device-list 内の複数のパスは、空白文字で区切る必要があります。また、リストは引用符で囲む必要があります。</p> <p>-a authorization -n で指定されたデバイス、または -t で指定されたタイプのデバイスに関連付けられている承認を追加または更新します。複数の承認を指定する場合は、リストをコンマで区切り、引用符で囲む必要があります。デバイスが割り当て不可能な場合、authorization をアスタリスク (*) を使って指定し、引用符で囲む必要があります。すべてのユーザーがデバイスを割り当て可能</p>

である場合は、*authorization* をアットマーク (@) を使って指定し、引用符で囲む必要があります。デフォルトの承認は '@' です。

-c clean -n で指定されたデバイス、または -t で指定されたデバイスタイプに対して *device_clean*(5) プログラム *clean* を使用するように指定します。デフォルトの *clean* プログラムは */bin/true* です。

-o key= value -n で指定されたデバイス、または -t で指定されたデバイスタイプに対して、コロンで区切られた *key=value* ペアの文字列を受け入れます。現在、システムにより解釈されるキーを次に示します。

minlabel デバイスを使用可能な最下位のラベル。

maxlabel デバイスを使用可能な最上位のラベル。

class デバイスの論理グループを指定します。たとえば、すべての Sun Ray™ デバイスの、すべてのデバイスタイプは論理グループです。class キーワードにはデフォルト値はありません。

xdpi Xセッションの表示名を指定します。このキーワードは、Xセッションに関連するデバイスを特定するために使用します。xdpi キーワードにはデフォルト値はありません。

エラー

成功した場合、*add_allocate* は終了ステータス 0 (真) を返します。エラーが発生した場合、*add_allocate* は、0 以外の終了ステータスを返します。終了コードとその意味を次に示します。

- 1 呼び出し時の構文エラー
- 2 原因不明のシステムエラー
- 3 指定されたデバイスのエントリは既に存在する。このエラーは、-f オプションが指定されていない場合にのみ発生する。
- 4 アクセス権が拒否された。ユーザーは、DAC または MAC アクセス記録の更新を保持していない。

属性

次の属性については、*attributes*(5) を参照してください。

属性タイプ	属性値
使用条件	SUNWtsu
インタフェースの安定性	下記を参照

呼び出しは不確実です。オプションは不確実です。出力は非インタフェースです。

関連項目

allocate(1), deallocate(1), list_devices(1), [remove_allocatable\(1M\)](#), attributes(5), device_clean(5)

名前	atohexlabel – 人間が読めるラベルの内部テキスト形式への変換						
形式	<code>/usr/sbin/atohexlabel [human-readable-sensitivity-label]</code> <code>/usr/sbin/atohexlabel -c [human-readable-clearance]</code>						
インタフェースレベル	このファイルは、米国国防情報局 (DIA) の必須アクセス制御 (MAC) ポリシーの一部です。このファイルは、Solaris Trusted Extensions ソフトウェアの将来のリリース向けに作成されるその他の MAC ポリシーには適用されない可能性があります。						
機能説明	<p>atohexlabel は、人間が読むことのできるラベルを、公開オブジェクトに安全に格納可能な内部テキスト表現に変換します。オプションが指定されない場合、ラベルは機密ラベルと見なされます。</p> <p>内部変換をあとで構文解析することで、同じ値に戻すことができます。多くの場合、内部形式は 16 進数で記述されます。変換されたラベルは、標準出力ファイルに書き込まれます。人間が読めるラベルを指定しない場合、標準入力ファイルからラベルが読み取られます。このコマンドは、内部データベース内に格納されているラベルを緊急に修復する場合に使用できます。</p>						
オプション	<code>-c</code> 人間の読めるラベルを認可上限として識別します。						
終了ステータス	次の終了ステータスが返されます。 <ul style="list-style-type: none"> 0 正常終了。 1 エラーが発生した。診断は標準エラーファイルに書き込まれる。 						
ファイル	<code>/etc/security/tsol/label_encodings</code> ラベルエンコーディングファイルには、このシステムの定義済みラベルに対する格付け名、語句、制約、および値が含まれます。						
属性	次の属性については、 <code>attributes(5)</code> を参照してください。						
	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center;">属性タイプ</th> <th style="text-align: center;">属性値</th> </tr> </thead> <tbody> <tr> <td>使用条件</td> <td>SUNWtsu</td> </tr> <tr> <td>安定性レベル</td> <td>後述の「注意事項」を参照</td> </tr> </tbody> </table>	属性タイプ	属性値	使用条件	SUNWtsu	安定性レベル	後述の「注意事項」を参照
属性タイプ	属性値						
使用条件	SUNWtsu						
安定性レベル	後述の「注意事項」を参照						
関連項目	hextoalabel(1M) , label_to_str(3TSOL) , str_to_label(3TSOL) , label_encodings(4) , attributes(5)						
	『Solaris Trusted Extensions 管理の手順』の「ラベルの 16 進値を求める」						
注意事項	コマンド出力の安定性は、同一の <code>label_encodings</code> ファイルを使用する場合は「安定」です。コマンド呼び出しの安定性は、DIA MAC ポリシーを実装するシステムでは「安定」です。						

- 名前** chk_encodings - ラベルエンコーディングファイルの構文の検査
- 形式** /usr/sbin/chk_encodings [-a] [-c *maxclass*] [*pathname*]
- インタフェースレベル** このファイルは、米国国防情報局 (DIA) の必須アクセス制御 (MAC) ポリシーの一部です。このファイルは、Solaris Trusted Extensions ソフトウェアの将来のリリース向けに作成されるその他の MAC ポリシーには適用されない可能性があります。
- 機能説明** chk_encodings は、*pathname* で指定されたラベルエンコーディングファイルの構文を検査します。-a オプションを使用すると、chk_encodings は、*pathname* で指定されたラベルエンコーディングファイルの意味解析も出力します。*pathname* が指定されない場合、chk_encodings は /etc/security/tsol/label_encodings ファイルを検査および解析します。
- ラベルエンコーディングファイルの解析が要求された場合、エラーが検出された場合でも、実施可能な解析が標準出力ファイルに書き込まれます。
- オプション**
- a ラベルエンコーディングファイルの意味解析を実行します。
 - c *maxclass* ラベルエンコーディングファイルの CLASSIFICATIONS セクションに指定可能な最大格付け値 *maxclass* (デフォルトは 255) を指定します。
- エラー** 正常終了時、chk_encodings は終了ステータス 0 (真) を返し、*pathname* 内にエラーが検出されなかったことを示すメッセージを標準出力ファイルに書き込みます。エラーが検出された場合、chk_encodings はゼロ以外 (偽) の終了コードを返し、診断メッセージを標準出力ファイルに書き込みます。
- 属性** 次の属性については、attributes(5) を参照してください。

属性タイプ	属性値
使用条件	SUNWtsu
安定性レベル	混在。後述の「注意事項」を参照

- ファイル** /etc/security/tsol/label_encodings
ラベルエンコーディングファイルには、このシステムの定義済みラベルに対する格付け名、語句、制約、および値が含まれます。

- 関連項目** [label_encodings\(4\)](#), [attributes\(5\)](#), [labels\(5\)](#)

『Solaris Trusted Extensions ラベルの管理』の「label_encodings ファイルを分析し、検証する」

- 注意事項** 構文検査の安定性は標準と考えられており、DIA ドキュメント DDS-2600-6216-93、『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』(1993 年 9 月) により制御されています。コマンド出力の安定性は、未定義です。コマンド呼び出しの安定性は、DIA MAC ポリシーを実装するシステムでは、安定です。

名前	hextoalabel – 内部テキストラベルの人間が読める形式への変換
形式	<code>/usr/sbin/hextoalabel [internal-text-sensitivity-label]</code> <code>/usr/sbin/hextoalabel -c [internal-text-clearance]</code>
インタフェース レベル	このファイルは、米国国防情報局 (DIA) の必須アクセス制御 (MAC) ポリシーの一部です。このファイルは、Solaris Trusted Extensions ソフトウェアの将来のリリース向けに作成されるその他の MAC ポリシーには適用されない可能性があります。
機能説明	hextoalabel は、内部テキストラベルを人間が読める形式に変換し、結果を標準出力ファイルに書き込みます。多くの場合、内部形式は 16 進数で記述されます。オプションが指定されない場合、ラベルは機密ラベルと見なされます。 内部テキストラベルを指定しない場合、標準入力ファイルからラベルが読み取られます。このコマンドは、内部データベース内に格納されているラベルを緊急に修復する場合に使用できます。
オプション	<code>-c</code> 内部テキストラベルを認可上限として識別します。
終了ステータス	次の終了ステータスが返されます。 0 正常終了。 1 エラーが発生した。診断は標準エラーファイルに書き込まれる。
属性	次の属性については、attributes(5) を参照してください。

属性タイプ	属性値
使用条件	SUNWtsu
安定性レベル	後述の「注意事項」を参照

ファイル	<code>/etc/security/tsol/label_encodings</code> ラベルエンコーディングファイルには、このシステムの定義済みラベルに対する格付け名、語句、制約、および値が含まれます。
関連項目	atohexlabel(1M) , label_to_str(3TSOL) , str_to_label(3TSOL) , label_encodings(4) , attributes(5) 『Solaris Trusted Extensions 管理の手順』の「可読のラベルを 16 進形式から求める」
注意事項	コマンド出力の安定性は、同一の label_encodings ファイルを使用する場合は「安定」です。コマンド呼び出しの安定性は、DIA MAC ポリシーを実装するシステムでは「安定」です。

名前	remove_allocatable - 割り当てデータベースからのエントリの削除
形式	<code>/usr/sbin/remove_allocatable [-f] -n name</code> <code>/usr/sbin/remove_allocatable [-f] [-d] -t dev-type</code>
機能説明	remove_allocatable は、デバイス割り当て機構からユーザーが割り当て可能なデバイスのエントリを削除します。remove_allocatable は、この機構によりラベル範囲が管理される、一部の割り当て不可能なデバイス(プリンタなど)のエントリも削除します。
オプション	<p>-d -t で指定されたデバイスタイプの、システム提供のデフォルト属性を削除します。</p> <p>-f エントリを強制的に削除します。このオプションを指定しない場合、指定したデバイス名を持つエントリがもはや存在しないと、remove_allocatable はエラーを出力して終了します。</p> <p>-n name デバイス <i>name</i> のエントリを削除します。</p> <p>-t dev-type デバイスタイプが <i>dev-type</i> であるデバイスを削除します。</p>
エラー	<p>成功した場合、remove_allocatable は終了ステータス 0 (真) を返します。エラーが発生した場合、remove_allocatable は、0 以外の終了ステータスを返します。終了コードとその意味を次に示します。</p> <ol style="list-style-type: none"> 1 呼び出し時の構文エラー 2 原因不明のシステムエラー 3 デバイス <i>name</i> または <i>dev-type</i> が見つからない。このエラーは、-f オプションが指定されていない場合にのみ発生する。 4 アクセス権が拒否された。ユーザーは、データベースに対する DAC または MAC アクセス権を持っていない。
属性	次の属性については、attributes(5) を参照してください。

属性タイプ	属性値
使用条件	SUNWtsu
インタフェースの安定性	下記を参照

呼び出しは不確実です。オプションは不確実です。出力は非インタフェースです。

関連項目 allocate(1), deallocate(1), [add_allocatable\(1M\)](#), attributes(5), device_clean(5)

名前	smtnrhdb - tnrhdb データベース内のエントリの管理
形式	<code>/usr/sadm/bin/smtnrhdb subcommand [auth_args] -- subcommand_args</code>
機能説明	<p>smtnrhdb コマンドは、tnrhdb データベース内のエントリの追加、変更、削除、および一覧表示を行います。</p> <p>smtnrhdb のサブコマンドを次に示します。</p> <p>add tnrhdb データベースに新規エントリを追加します。エントリを追加するには、管理者が <code>solaris.network.host.write</code> および <code>solaris.network.security.write</code> 承認を保持している必要があります。</p> <p>delete tnrhdb データベース内のエントリを削除します。エントリを削除するには、管理者が <code>solaris.network.host.write</code> および <code>solaris.network.security.write</code> 承認を保持している必要があります。</p> <p>list tnrhdb データベース内のすべてのエントリを一覧表示します。エントリを一覧表示するには、管理者が <code>solaris.network.host.read</code> および <code>solaris.network.security.read</code> 承認を保持している必要があります。</p> <p>modify tnrhdb データベース内のエントリを変更します。エントリを変更するには、管理者が <code>solaris.network.host.write</code> および <code>solaris.network.security.write</code> 承認を保持している必要があります。</p>
オプション	<p>smtnrhdb の認証引数 <code>auth_args</code> は、<code>smc</code> 引数セットから派生します。これらの引数は、使用するサブコマンドに関係なく同じです。smtnrhdb コマンドを成功させるには、Solaris 管理コンソールを初期化する必要があります <code>smc(1M)</code> を参照)。Solaris 管理コンソールサーバーのリポート後に、最初の <code>smc</code> 接続がタイムアウトする可能性があります。この場合は、コマンドを再度実行してください。</p> <p>サブコマンド固有のオプション <code>subcommand_args</code> の前に、<code>--</code> オプションを指定する必要があります。</p>
<code>auth_args</code>	<p>有効な <code>auth_args</code> は <code>-D</code>、<code>-H</code>、<code>-l</code>、<code>-p</code>、<code>-r</code>、および <code>-u</code> です。これらの指定は任意です。<code>auth_args</code> を指定しない場合、デフォルト値が指定されたものと見なされて、認証用パスワードなどの追加情報の入力が必要と求められることがあります。これらの文字の代わりに、二重ダッシュ記号に続けて等価の単語を指定することもできます。たとえば、<code>-D</code> または <code>--domain</code> を使用できます。</p> <p><code>-D --domain domain</code> 管理対象のデフォルトドメインを指定します。 <code>domain</code> の構文は、<code>type:/host_name/domain_name</code> です。ここで、<code>type</code> は <code>dns</code>、<code>ldap</code>、<code>file</code> のいずれか、<code>host_name</code> はサーバーの名前、<code>domain_name</code> は管理対象のドメインの名前です。</p>

このオプションを指定しない場合、Solaris 管理コンソールは、管理対象として選択したサーバーの `file` デフォルトドメインと見なします。つまり、変更はサーバーに対してローカルであることとなります。ツールボックスでは、ドメインをツールごとに変更できます。このオプションにより、その他すべてのツール用のドメインが指定されます。

`-H | --hostname host_name:port`

接続先の `host_name` および `port` を指定します。`port` を指定しない場合、システムはデフォルトポート 898 に接続されます。`host_name:port` を指定しない場合、Solaris 管理コンソールは、ローカルホストのポート 898 に接続します。

`-l | --rolepassword role_password`

`role_name` のパスワードを指定します。`role_name` を指定するが、`role_password` を指定しない場合、システムにより `role_password` の入力が必要と求められます。コマンド行に指定したパスワードは、システムのすべてのユーザーが表示できます。このため、このオプションは安全ではないと見なされます。

`-p | --password password`

`user_name` のパスワードを指定します。パスワードを指定しない場合、システムによりパスワードの入力が求められます。コマンド行に指定したパスワードは、システムのすべてのユーザーが表示できます。このため、このオプションは安全ではないと見なされます。

`-r | --rolename role_name`

認証に使用する役割名を指定します。このオプションを指定しない場合、役割なしと見なされます。

`-u | --username user_name`

認証に使用するユーザー名を指定します。このオプションを指定しない場合、コンソールプロセスを実行しているユーザーの ID が想定されます。

`--`

このオプションは必須であり、常に先行するオプションのあとに指定する必要があります。先行するオプションを入力しない場合でも、`--` オプションを入力する必要があります。

subcommand_args

注: 空白文字を含む説明およびその他の引数オプションは、二重引用符で囲む必要があります。

- h コマンドの使用方法を表示します。
 - H *hostname* ホストの名前を指定します。list サブコマンドの場合は、*hostname* 引数は指定しません。ipaddress サブコマンド引数を指定した場合、この指定は不要です。
 - i *ipaddress* ホストのIPアドレスを指定します。hostname サブコマンド引数を指定した場合、この指定は不要です。
 - n *templatename* テンプレートの名前を指定します。
 - p *prefixlen* IPアドレスのワイルドカード表現の接頭辞の長さを指定します(単位はビット)。接頭辞は、IPアドレスの一番左の部分です。
 - w *ipaddress-wildcard* ワイルドカードを使ってサブネットのIPアドレスを指定します。
- サブコマンド add では、次のいずれかの引数セットを指定する必要があります。
 - H *hostname* -n *templatename* |
 - i *ipaddress* -n *templatename* |
 - w *ipaddress-wildcard* -n *templatename* [-p *prefixlen*] |
 - h
 - サブコマンド modify では、次のいずれかの引数セットを指定する必要があります。
 - H *hostname* -n *templatename* |
 - i *ipaddress* -n *templatename* |
 - w *ipaddress-wildcard* -n *templatename* [-p *prefixlen*] |
 - h
 - サブコマンド delete では、次のいずれかの引数セットを指定する必要があります。
 - H *hostname* |
 - i *ipaddress* |
 - w *ipaddress-wildcard* [-p *prefixlen*] |
 - h
 - サブコマンド list には次の引数を指定します。
 - h

使用例

例1 ワイルドカードIPアドレスのテンプレート名を指定する

管理役割は、ローカルのファイルシステム上でIPアドレスワイルドカード 192.168.113.0 を使用する一連のホストに対して、テンプレート名 *cipso_lan* を指定します。認証引数が指定されなかったため、管理者は、デフォルトの *file* ドメイン

例1 ワイルドカードIPアドレスのテンプレート名を指定する (続き)

タイプを使用して、ローカルサーバー上のローカルホストのポート 898 に接続します。管理者には、管理パスワードの入力が求められます。

```
$ /usr/sadm/bin/smtnrhdb add -- -w 192.168.113.0 -n cipso_lan
```

例2 tnrhdb データベース内のエントリを削除する

管理役割は、LDAP サーバーのポート 898 (デフォルト、これ以外のポートも使用可) に接続し、IP アドレス 192.168.113.8 を指定して、データベースからホストエントリを削除します。ドメインが指定されていないため、デフォルトの file ドメインタイプおよびローカルサーバーが使用されます。管理者には、管理パスワードの入力が求められます。

```
/usr/sadm/bin/smtnrhdb delete \  
-D ldap:/example.domain -i 192.168.113.8
```

終了ステータス 次の終了ステータスが返されます。

- 0 正常終了。
- 1 無効なコマンド構文。使用方法を示すメッセージが表示される。
- 2 コマンドの実行中にエラーが発生した。エラーメッセージが表示される。

ファイル smtnrhdb コマンドにより、次のファイルが使用されます。

```
/etc/security/tsol/tnrhdb トラストドネットワーク遠隔ホストデータベース。  
tnrhdb(4) を参照。
```

属性 次の属性については、attributes(5) を参照してください。

属性タイプ	属性値
使用条件	SUNWmgts

関連項目 smc(1M), [tnrhdb\(4\)](#), [attributes\(5\)](#)

このオプションを指定しない場合、Solaris 管理コンソールは、管理対象として選択したサーバーの `file` デフォルトドメインと見なします。つまり、変更はサーバーに対してローカルであることとなります。ツールボックスでは、ドメインをツールごとに変更できます。このオプションにより、その他すべてのツール用のドメインが指定されます。

`-H | --hostname host_name:port`

接続先の `host_name` および `port` を指定します。`port` を指定しない場合、システムはデフォルトポート 898 に接続されます。`host_name:port` を指定しない場合、Solaris 管理コンソールは、ローカルホストのポート 898 に接続します。

`-l | --rolepassword role_password`

`role_name` のパスワードを指定します。`role_name` を指定するが、`role_password` を指定しない場合、システムにより `role_password` の入力が必要と求められます。コマンド行に指定したパスワードは、システムのすべてのユーザーが見ることができます。このため、このオプションは安全ではないと考えられます。

`-p | --password password`

`user_name` のパスワードを指定します。パスワードを指定しない場合、システムによりパスワードの入力が求められます。コマンド行に指定したパスワードは、システムのすべてのユーザーが見ることができます。このため、このオプションは安全ではないと考えられます。

`-r | --rolename role_name`

認証に使用する役割名を指定します。このオプションを指定しない場合、役割なしと見なされます。

`-u | --username user_name`

認証に使用するユーザー名を指定します。このオプションを指定しない場合、コンソールプロセスを実行しているユーザーの ID が想定されます。

`--`

このオプションは必須であり、常に先行するオプションのあとに指定する必要があります。先行するオプションを入力しない場合でも、`--` オプションを入力する必要があります。

`subcommand_args`

注: 空白文字を含む説明およびその他の引数オプションは、二重引用符で囲む必要があります。

- h コマンドの使用方法を表示します。
- n *templatename* テンプレートの名前を指定します。
- t *hosttype* 新規ホストのホストタイプを指定します。有効な値は、unlabeled および cipso です。
- x *doi=doi-value* DOI 値を指定します。
- x *max=maximum-label* 最上位のラベルを指定します。値は、16 進数値または文字列 (admin_high など) で指定できます。
- x *min=minimum-label* 最下位のラベルを指定します。値は、16 進数値または文字列 (admin_low など) で指定できます。
- x *label=default-label* ホストタイプが unlabeled の場合の、デフォルトラベルを指定します。hosttype が CIPSO の場合、このオプションは適用されません。値は、16 進数値または文字列 (admin_low など) で指定できます。
- x *slset=l1, l2,l3,l4* 機密ラベルのセットを指定します。4 つまでのラベル値を、コンマで区切って指定できます。値は、16 進数値または文字列 (admin_low など) で指定できます。
- サブコマンド add では、次のいずれかの引数セットを指定する必要があります。
 - n *template name* (
 - t cipso [-x *doi=doi-value* -x *min=minimum-label* -x *max=maximum-label* -x *slset=l1,l2,l3,l4*] |
 - t unlabeled [-x *doi=doi-value* -x *min=minimum-label* -x *max=maximum-label* -x *label=default-label* -x *slset=l1,l2,l3,l4*] |
 - h
 - サブコマンド modify では、次のいずれかの引数セットを指定する必要があります。
 - n *template name* (
 - t cipso [-x *doi=doi-value* -x *min=minimum-label* -x *max=maximum-label* -x *slset=l1,l2,l3,l4*] |
 - t unlabeled [-x *doi=doi-value* -x *min=minimum-label* -x *max=maximum-label* -x *label=default-label* -x *slset=l1,l2,l3,l4*] |
 - h

注: ホストタイプを変更した場合は、新規ホストタイプ用のすべてのオプションを指定する必要があります。

- サブコマンド `delete` では、次のいずれかの引数セットを指定する必要があります。

```
-n templatename |
-h
```

- サブコマンド `list` では、次の引数を指定できます。

```
-n templatename |
-h
```

使用例

例1 ネットワークテンプレートデータベースに新規エントリを追加する

管理役割は LDAP サーバーのポート 898 に接続して、`tnrhtp` データベース内に `unlabeled_ntk` エントリを作成します。新規テンプレートには、ホストタイプ `unlabeled`、解釈ドメイン 1、最下位のラベル `public`、最上位のラベル `restricted`、デフォルトラベル `needtoknow` が割り当てられます。管理者には、管理パスワードの入力が求められます。

```
$ /usr/sadm/bin/smtnrhtp \
add -D ldap:directoryname -H servername:898 -- \
-n unlabeled_ntk -t unlabeled -x DOI=1 \
-x min=public -x max=restricted -x label="need to know"
```

終了ステータス

次の終了ステータスが返されます。

- 0 正常終了。
- 1 無効なコマンド構文。使用方法を示すメッセージが表示される。
- 2 コマンドの実行中にエラーが発生した。エラーメッセージが表示される。

ファイル

`smtnrhtp` コマンドにより、次のファイルが使用されます。

`/etc/security/tsol/tnrhtp` トラストドネットワーク遠隔ホストテンプレート。[tnrhtp\(4\)](#) を参照。

属性

次の属性については、[attributes\(5\)](#) を参照してください。

属性タイプ	属性値
使用条件	SUNWmgts

関連項目

[smc\(1M\)](#), [tnrhtp\(4\)](#), [attributes\(5\)](#)

名前	smtzonecfg – Trusted Extensions ネットワーキング用ゾーン構成データベース内のエントリの管理
形式	<code>/usr/sadm/bin/smtzonecfg subcommand [auth_args] -- [subcommand_args]</code>
機能説明	smtzonecfg コマンドは、tzonecfg データベース内のエントリの追加、変更、削除、および一覧表示を行います。

smtzonecfg のサブコマンドを次に示します。

add	tzonecfg データベースに新規エントリを追加します。エントリを追加するには、管理者が <code>solaris.network.host.write</code> および <code>solaris.network.security.write</code> 承認を保持している必要があります。
modify	tzonecfg データベース内のエントリを変更します。エントリを変更するには、管理者は <code>solaris.network.host.write</code> および <code>solaris.network.security.write</code> 承認を保持している必要があります。
delete	tzonecfg データベースからエントリを削除します。エントリを削除するには、管理者は <code>solaris.network.host.write</code> および <code>solaris.network.security.write</code> 承認を保持している必要があります。
list	tzonecfg データベース内のエントリを一覧表示します。エントリを一覧表示するには、管理者が <code>solaris.network.host.read</code> および <code>solaris.network.security.read</code> 承認を保持している必要があります。

オプション

smtzonecfg の認証引数 `auth_args` は、smc 引数セットから派生し、使用するサブコマンドに関係なく同じです。smtzonecfg コマンドを成功させるには、Solaris 管理コンソールを初期化する必要があります (smc(1M) を参照)。Solaris 管理コンソールサーバーのリポート後に、最初の smc 接続がタイムアウトする可能性があります。この場合は、コマンドを再度実行してください。

サブコマンド固有のオプション `subcommand_args` の前に、`--` オプションを指定する必要があります。

`auth_args`

有効な `auth_args` は `-D`、`-H`、`-l`、`-p`、`-r`、および `-u` です。これらの指定は任意です。`auth_args` を指定しない場合、デフォルト値が指定されたものと見なされて、認証用パスワードなどの追加情報の入力が必要と求められることがあります。これらの文字の代わりに、二重ダッシュ記号に続けて等価の単語を指定することもできます。たとえば、`-D` または `--domain` を使用できます。

`-D | --domain domain` 管理対象のデフォルトドメインを指定します。
`domain` の構文は、`type:/host_name/domain_name` です。ここで、`type` は `dns`、`ldap`、`file` のいずれか、`host_name` はサーバーの名前、`domain_name` は管理対象のドメインの名前です。

このオプションを指定しない場合、Solaris 管理コンソールは、管理対象として選択したサーバーの `file` デフォルトドメインと見なします。つまり、変更はサーバーに対してローカルであることとなります。ツールボックスを使用すると、ドメインをツール単位で変更できます。このオプションでは、その他すべてのツール用のドメインを指定します。

`-H | --hostname host_name:port`

接続先の `host_name` および `port` を指定します。`port` を指定しない場合、システムはデフォルトポート 898 に接続されます。`host_name:port` を指定しない場合、Solaris 管理コンソールは、ローカルホストのポート 898 に接続します。

`-l | --rolepassword role_password`

`role_name` のパスワードを指定します。`role_name` を指定するが、`role_password` を指定しない場合、システムにより `role_password` の入力が必要と求められます。コマンド行に指定したパスワードは、システムのすべてのユーザーが表示できます。このため、このオプションは安全ではないと考えられます。

`-p | --password password`

`user_name` のパスワードを指定します。パスワードを指定しない場合、システムによりパスワードの入力が求められます。コマンド行に指定したパスワードは、システムのすべてのユーザーが表示できます。このため、このオプションは安全ではないと考えられます。

`-r | --rolename role_name`

認証に使用する役割名を指定します。このオプションを指定しない場合、役割なしと見なされます。

`-u | --username user_name`

認証に使用するユーザー名を指定します。このオプションを指定しない場合、コンソールプロセスを実行しているユーザーの ID が想定されます。

`--`

このオプションは必須であり、常に先行するオプションのあとに指定する必要があります。先行するオプションを入力しない場合でも、`--` オプションを入力する必要があります。

`subcommand_args`

注: 空白文字を含む説明およびその他の引数オプションは、二重引用符で囲む必要があります。

- h コマンドの使用方法を表示します。
- n *zonename* エントリのゾーン名を指定します。この名前は、ゾーンの構成時に使用されます。*zonename* では、大文字と小文字が区別されます。指定するゾーン名は、システムの構成済みのゾーンのいずれかである必要があります。次のコマンドは、構成済みのゾーンの一覧を返します。
- ```
/usr/sbin/zoneadm list -c
```
- l *label* ゾーンのラベルを指定します。このフィールドは、ゾーン起動時のゾーンへのラベル付けで使用されます。
- x *polycymatch=0* | 1 非トランスポートトラフィックのポリシー一致レベルを指定します。指定可能な値は、0 (ラベルに一致する) または 1 (ゾーンのラベル範囲内にある) だけです。詳細は、[tnzonecfg\(4\)](#) を参照してください。このサブコマンド引数は省略可能です。指定しない場合、デフォルト値の 0 が使用されます。
- x *mlpzone= ""* | *port/protocol* ゾーン固有 IP アドレス用のマルチレベルポート構成エントリを指定します。複数の *port/protocol* を、セミコロンで区切って指定できます。既存の MLP ゾーン値すべてを削除する場合は、空の文字列を指定できます。このサブコマンド引数は省略可能です。
- x *mlpshared= ""* | *port/protocol* 共有 IP アドレス用のマルチレベルポート構成エントリを指定します。複数の *port/protocol* を、セミコロンで区切って指定できます。既存の MLP 共有値すべてを削除する場合は、空の文字列を指定できます。このサブコマンド引数は省略可能です。
- サブコマンド `add` では、次のいずれかの引数セットを指定する必要があります。
 

```
-n zonename -l label [-x polycymatch=policy-match-level \
-x mlpzone=port/protocol;... | -x mlpshared=port/protocol;...]
```
- h
- サブコマンド `modify` では、次のいずれかの引数セットを指定する必要があります。

```
-n zonename [-l label] [-x policymatch=policy-match-level \
-x mlpzone=port/protocol;... | -x mlpshared=port/protocol;...]
```

```
-h
```

- サブコマンド `delete` では、次のいずれかの引数を指定する必要があります。

```
-n zonename |
```

```
-h
```

- サブコマンド `list` では、次の引数を指定できます。

```
-n zonename |
```

```
-h
```

## 使用例

例1 ゾーン構成データベースに新規エントリを追加する

管理役割は、ラベル `public`、ポリシー一致レベル 1、共有 MLP ポート 666、およびプロトコル TCP を使って、新規ゾーンエントリ `public` を作成します。管理者には、管理パスワードの入力が求められます。

```
$ /usr/sadm/bin/smtntzonecfg add -- -n public -l public \
-x policymatch=1 -x mlpshared=666/tcp
```

例2 ゾーン構成データベース内のエントリを変更する

管理役割は、`tnzonecfg` データベース内の `public` エントリを `needtoknow` に変更します。管理者には、管理パスワードの入力が求められます。

```
$ /usr/sadm/bin/smtntzonecfg modify -- -n public -l needtoknow
```

例3 ゾーン構成データベースを一覧表示する

管理役割は、`tnzonecfg` データベース内のエントリを一覧表示します。管理者には、管理パスワードの入力が求められます。

```
$ /usr/sadm/bin/smtntzonecfg list --
```

終了ステータス 次の終了ステータスが返されます。

- 0 正常終了。
- 1 無効なコマンド構文。使用方法を示すメッセージが表示される。
- 2 コマンドの実行中にエラーが発生した。エラーメッセージが表示される。

## ファイル

`smtntzonecfg` コマンドにより、次のファイルが使用されます。

```
/etc/security/tso1/tnzonecfg トラストッドゾーン構成データベース。
tnzonecfg(4) を参照。
```

属性 次の属性については、[attributes\(5\)](#)を参照してください。

| 属性タイプ | 属性値      |
|-------|----------|
| 使用条件  | SUNWmgts |

関連項目 [smc\(1M\)](#), [tzonecfg\(4\)](#), [attributes\(5\)](#)

|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 名前    | tnchkdb - トラストドネットワークデータベースのファイル構文の検査                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 形式    | <code>/usr/sbin/tnchkdb [-h path] [-t path] [-z path]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 機能説明  | <p>tnchkdb は、<a href="#">tnrhtp(4)</a>、<a href="#">tnrhdb(4)</a>、および <a href="#">tnzonecfg(4)</a> データベースの構文を検査します。デフォルトでは、各ファイルのパスは次のとおりです。</p> <ul style="list-style-type: none"> <li>■ <code>/etc/security/tsol/tnrhtp</code></li> <li>■ <code>/etc/security/tsol/tnrhdb</code></li> <li>■ <code>/etc/security/tsol/tnzonecfg</code></li> </ul> <p>コマンド行で <code>-h(tnrhdb)</code>、<code>-t(tnrhtp)</code>、および <code>-z(tnzonecfg)</code> オプションとともにパスを指定することで、一部またはすべてのファイルの代替パスを指定できます。このオプションは、変更したファイルセットを新規システムデータベースとしてインストールする前にテストする場合に便利です。</p> <p>3つのデータベースファイルすべての整合性が検査されます。すべてのファイルが構文的に正しく、かつ可能な範囲内で意味的に正しい場合、tnchkdb は終了ステータス 0 を返します。1つ以上のファイルにエラーが存在する場合、終了ステータス 1 が返されます。ファイルを読み込むことができないなど、コマンド行の指定に問題がある場合は、終了ステータス 2 が返されます。エラーは、標準エラーに書き込まれます。</p> <p>tnrhtp 内にエラーが存在する場合、エラーが階層的に発生することを防ぐために、tnrhdb 内のテンプレート名は検査されません。</p> <p>tnchkdb は任意のラベルで実行できますが、標準の <code>/etc/security/tsol</code> ファイルを表示できるのは大域ゾーンだけです。</p> |
| オプション | <p><code>-h [path]</code> <i>path</i> を検査して、tnrhdb の構文が適切かどうかを調べます。<i>path</i> が指定されない場合は、<code>/etc/security/tsol/tnrhdb</code> を検査します。</p> <p><code>-t [path]</code> <i>path</i> を検査して、tnrhtp の構文が適切かどうかを調べます。<i>path</i> が指定されない場合は、<code>/etc/security/tsol/tnrhtp</code> を検査します。</p> <p><code>-z [path]</code> <i>path</i> を検査して、tnzonecfg の構文が適切かどうかを調べます。<i>path</i> が指定されない場合は、<code>/etc/security/tsol/tnzonecfg</code> を検査します。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 使用例   | <p>例1 エラーメッセージの例</p> <p>tnchkdb コマンドは、CIPSO エラーを検査します。この例では、<code>admin_low</code> テンプレートのデフォルトラベルが、不正な値 <code>ADMIN_HIGH</code> です。</p> <pre># tnchkdb checking /etc/security/tsol/tnrhtp ... tnchkdb: def_label classification 7fff is invalid for cipso labels: line 14 entry admin_low tnchkdb: def_label compartments 241-256 must be zero for cipso labels: line 14 entry admin_low</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

## 例1 エラーメッセージの例 (続き)

```
checking /etc/security/tsol/tnrhdb ...
checking /etc/security/tsol/tnzonecfg ...
```

## 属性

次の属性については、attributes(5)を参照してください。

| 属性タイプ      | 属性値     |
|------------|---------|
| 使用条件       | SUNWtsu |
| 安定性(コマンド行) | 開発中     |
| 安定性(出力)    | 不安定     |

## ファイル

/etc/security/tsol/tnrhdb トラステッドネットワーク遠隔ホストデータベース

/etc/security/tsol/tnrhtp トラステッドネットワーク遠隔ホストテンプレート

/etc/security/tsol/tnzonecfg トラステッドゾーン構成データベース

## 関連項目

[tnd\(1M\)](#), [tnctl\(1M\)](#), [tnrhdb\(4\)](#), [tnrhtp\(4\)](#), [tnzonecfg\(4\)](#), [attributes\(5\)](#)

『Solaris Trusted Extensions 管理の手順』の「トラステッドネットワークデータベースの構文をチェックする」

## 注意事項

LDAP を使って欠落したテンプレートを提供する場合、tnrhtp および tnrhdb の構成が一貫してはいなくても有効であることがあります。

|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 名前    | tnctl – Trusted Extensions ネットワークパラメータの構成                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 形式    | <code>/usr/sbin/tnctl [-dfv] [-h host [/prefix] [:template]] [-m zone:mlp:shared-mlp] [-t template [:key=val [;key=val]]] [-HTz] file]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 機能説明  | <p>tnctl は、Solaris カーネル内のトラステッドネットワークパラメータを操作するためのインタフェースを提供します。</p> <p>システムの起動時に、Solaris Trusted Extensions の初期化処理の一部として、smf(5) スクリプトにより tnctl が大域ゾーン内で実行されます。tnctl は、通常のシステム管理での使用を意図したコマンドではありません。Solaris 管理コンソールを使用せずにローカルのトラステッドネットワークデータベースファイルが変更された場合、管理者は最初に <a href="#">tnchkdb(1M)</a> を発行して構文を検査してから、このコマンドを使ってカーネルのコピーを更新します。</p> <pre># svcadm restart svc:/network/tnctl</pre> <p>実行中のシステム上の遠隔ホストおよびテンプレート情報を変更することの危険については、「警告」を参照してください。</p>                                                                                                                                                                                                                                                                                                                              |
| オプション | <p><b>-d</b><br/>一致するエントリをカーネルから削除します。デフォルトでは、新規エントリを追加します。</p> <p>MLP を削除する場合は、MLP の範囲が正確に一致している必要があります。MLP の指定は、次の形式で行います。</p> <pre>port[-port]/protocol</pre> <p>ここで、<i>port</i> には 1 ～ 65535 の範囲の値、または既知の任意のサービスを指定できます (<a href="#">services(4)</a> を参照)。<i>protocol</i> には、1 ～ 255 の範囲の値または既知の任意のプロトコルを指定できます (<a href="#">protocols(4)</a> を参照)。</p> <p><b>-f</b><br/>コマンド行で指定されたエントリをロードする前に、すべてのカーネルエントリをフラッシュします。1 つ以上のエントリの構文解析が成功しない場合、フラッシュは実行されません。</p> <p><b>-v</b><br/>冗長モードを有効にします。</p> <p><b>-h host[/ prefix][:template]</b><br/>指定された <i>host</i> についてのカーネル遠隔ホストキャッシュを更新します。テンプレート名が指定されている場合は、指定された <i>template</i> を使ってカーネルのキャッシュを変更します。<i>prefix</i> が指定されていない場合、<a href="#">tnrhdb(4)</a> の解釈に使用した規則に従って、示された接頭辞の長さが決定されます。<b>-d</b> を指定する場合は、テンプレート名は指定できません。</p> |

**-m zone: mlp:shared-mlp**

指定された *zone* に対するカーネルのマルチレベルポート (MLP) 構成キャッシュを変更します。 *zone* には、更新するゾーンを指定します。 *mlp* および *shared-mlp* は、ゾーン固有および共有の IP アドレス用の MLP を指定します。 *shared-mlp* フィールドは、大域ゾーンのみで有効です。

**-t template[ key=val[;key=val]]**

*template* のカーネルテンプレートキャッシュを更新します。また、 *key=val* ペアのリストが指定された場合は、カーネルのキャッシュを変更して指定されたエントリを使用します。 *-d* が指定された場合は、 *key=val* ペアは指定できません。エントリの形式については、 [tnrhttp\(4\)](#) を参照してください。

**-T file**

*file* 内のテンプレートエントリすべてをカーネルキャッシュに読み込みます。

**-H file**

*file* 内の遠隔ホストエントリすべてをカーネルキャッシュに読み込みます。

**-z file**

大域ゾーンの MLP だけを *file* からカーネルキャッシュに読み込みます。非大域ゾーンの MLP の再読み込みを行うには、ゾーンを再起動します。

```
zoneadm -z non-global zone reboot
```

## 属性

次の属性については、 [attributes\(5\)](#) を参照してください。

| 属性タイプ  | 属性値     |
|--------|---------|
| 使用条件   | SUNWtsu |
| 安定性レベル | 不安定     |

## ファイル

|                                           |                         |
|-------------------------------------------|-------------------------|
| <code>/etc/security/tsol/tnrhdb</code>    | トラステッドネットワーク遠隔ホストデータベース |
| <code>/etc/security/tsol/tnrhttp</code>   | トラステッドネットワーク遠隔ホストテンプレート |
| <code>/etc/security/tsol/tnzonecfg</code> | トラステッドゾーン構成データベース       |
| <code>/etc/nsswitch.conf</code>           | ネームサービススイッチの構成ファイル      |

## 関連項目

[svcs\(1\)](#), [svcadm\(1M\)](#), [tninfo\(1M\)](#), [tnd\(1M\)](#), [tnchkdb\(1M\)](#), [zoneadm\(1M\)](#), [nsswitch.conf\(4\)](#), [protocols\(4\)](#), [services\(4\)](#), [tnrhdb\(4\)](#), [tnrhttp\(4\)](#), [tnzonecfg\(4\)](#), [attributes\(5\)](#), [smf\(5\)](#)

『Solaris Trusted Extensions 管理の手順』の「カーネルキャッシュとネットワークデータベースを同期する」

## 注意事項

tnctl サービスは、サービス管理機能 [smf\(5\)](#) により、サービス識別子の下で管理されます。

```
svc:/network/tnctl
```

サービスのステータスは、`svcs(1)` を使って問い合わせることができます。このサービスに対する管理操作 (カーネルキャッシュの更新など) は、`svcadm(1M)` を使って実行できます。次に例を示します。

```
svcadm refresh svc:/network/tnctl
```

**警告**

ネットワークの稼働中にテンプレートを変更すると、不特定数のホストのセキュリティ表示が変更される可能性があります。

|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 名前    | tnd - トラストッドネットワークデーモン                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 形式    | <code>/usr/sbin/tnd [-p poll-interval]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 機能説明  | <p>tnd (トラストッドネットワークデーモン) は、トラストッドネットワークデータベースを使ってカーネルを初期化し、また要求に従って LDAP サーバーおよびローカルファイルからデータベースの再読み込みを行います。tnd は、設定データベースを読み込む際、<code>nsswitch.conf(4)</code> は、ブート処理の冒頭で起動されます。tnd は、ブート処理の冒頭で起動されます。</p> <p>tnd は、次の 2 つのデータベースをカーネルに読み込みます。遠隔ホストデータベース <code>tnrhdb(4)</code> および遠隔ホストテンプレートデータベース <code>tnrhtp(4)</code> です。これらのデータベースの内容、およびデータベースがトラストッドネットワークに与える影響については、それぞれのマニュアルページを参照してください。関連する LDAP データベースまたはローカルデータベースが変更されると、tnd はローカルカーネルのキャッシュを、決められた間隔で更新します。</p> <p>ローカルのトラストッドネットワークデータベースファイルが変更された場合、管理者は <code>tnchkdb(1M)</code> を実行して構文を検査するとともに、<code>svcadm refresh svc:/network/tnd</code> を実行して tnd によるデータベース走査をすぐに開始する必要があります。</p> <p>tnd は <code>smf(5)</code> スクリプトから起動され、大域ゾーンで実行されることを前提としています。次に示すシグナルは、svcadm の特定の処理を引き起こします。</p> <p><b>SIGHUP</b>      <code>svcadm refresh svc:/network/tnd</code> を実行します。</p> <p>ローカルおよび LDAP <code>tnrhdb</code> と <code>tnrhtp</code> データベースの再走査が開始されます。tnd は、検出された変更点を使ってカーネルデータベースを更新します。</p> <p><b>SIGTERM</b>      <code>svcadm disable svc:/network/tnd</code> を実行します。</p> <p>tnd デーモンを停止します。カーネルデータベースは変更されません。</p> |
| オプション | <p><code>-p poll-interval</code>      ポーリング間隔を <code>poll-interval</code> 秒に設定します。デフォルトの <code>poll-interval</code> は 1800 秒 (30 分) です。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 使用例   | <p>例1 ポーリング間隔の変更</p> <p>次のコマンドは、ポーリング間隔を 1 時間に変更して、この間隔を SMF リポジトリに格納します。次のブート時に、tnd のポーリング間隔は 1 時間になります。</p> <pre># svccfg -s network/tnd setprop tnd/poll_interval=3600</pre> <p>次のコマンドは、ポーリング間隔を変更しますが、リポジトリの更新は行いません。次のブート時、tnd のポーリング間隔はデフォルトの 30 分のままです。</p> <pre># tnd -p 3600</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

属性 次の属性については、[attributes\(5\)](#) を参照してください。

| 属性タイプ        | 属性値       |
|--------------|-----------|
| 使用条件         | SUNWtsu   |
| 安定性レベル(コマンド) | 安定        |
| 安定性レベル(サービス) | プロジェクト非公開 |

ファイル

|                                           |                         |
|-------------------------------------------|-------------------------|
| <code>/etc/security/tsol/tnrhdb</code>    | トラステッドネットワーク遠隔ホストデータベース |
| <code>/etc/security/tsol/tnrhtp</code>    | トラステッドネットワーク遠隔ホストテンプレート |
| <code>/etc/security/tsol/tnzonecfg</code> | トラステッドゾーン構成データベース       |
| <code>/etc/nsswitch.conf</code>           | ネームサービススイッチの構成ファイル      |

関連項目 [svcs\(1\)](#), [svcadm\(1M\)](#), [tninfo\(1M\)](#), [tnctl\(1M\)](#), [tnchkdb\(1M\)](#), [tnrhdb\(4\)](#), [tnrhtp\(4\)](#), [tnzonecfg\(4\)](#), [nsswitch.conf\(4\)](#), [attributes\(5\)](#), [smf\(5\)](#)

『Solaris Trusted Extensions 管理の手順』の「カーネルキャッシュとネットワークデータベースを同期する」

注意事項 tnd サービスは、サービス管理機能 [smf\(5\)](#) により、サービス識別子の下で管理されます。

```
svc:/network/tnd
```

サービスの状態は、[svcs\(1\)](#) を使って問い合わせることができます。このサービスに対する管理操作(デーモンの再起動要求など)は、[svcadm\(1M\)](#) を使って実行できます。次に例を示します。

```
svcadm restart svc:/network/tnd
```

|       |                                                                                                                                                                                                                                                                                                                          |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 名前    | tninfo - カーネルレベルのネットワークに関する情報と統計の出力                                                                                                                                                                                                                                                                                      |
| 形式    | /usr/sbin/tninfo [-h <i>hostname</i> ] [-m <i>zone-name</i> ] [-t <i>template</i> ]                                                                                                                                                                                                                                      |
| 機能説明  | tninfo は、カーネルレベルのネットワーク情報と統計を取得して表示するためのインタフェースを提供します。                                                                                                                                                                                                                                                                   |
| オプション | <p>-h <i>hostname</i>      遠隔ホストキャッシュ内にある、指定されたホストのセキュリティ構造を表示します。出力には、tnrhdb データベース内で指定された内容が反映されます。</p> <p>-m <i>zone-name</i>      指定したゾーンに関連付けられた MLP 構成を表示します。出力には、tnzonecfg データベース内で指定された内容が反映されます。</p> <p>-t <i>template</i>      指定した <i>template</i> に関連付けられている構造を表示します。出力には、tnrhtp データベース内で指定された内容が反映されます。</p> |

## 使用例

例1 カーネル内にキャッシュされた遠隔ホスト構造を表示する

この例では、カーネル内にキャッシュされた遠隔ホスト構造を表示します。出力には、tnrhdb データベース内の定義が反映されます。

```
tninfo -h machine1
 IP address= 192.168.8.61
 Template = cipso
```

例2 大域ゾーンのマルチレベルポートを表示する

この例では、カーネルでキャッシュされた大域ゾーンの MLP を表示します。出力には、tnzonecfg データベース内の定義、および動的に割り当てられたすべての MLP が反映されます。private は、ゾーン固有の MLP を示します。

```
tninfo -m global
private:23/tcp;111/tcp;111/udp;515/tcp;2049/tcp;6000-6003/tcp;
 32812/tcp;36698/ip;38634/tcp;64365/ip
shared: 6000-6003/tcp
```

例3 cipso テンプレート定義を表示する

この例では、カーネルでキャッシュされた cipso テンプレート定義を表示します。出力には、tnrhtp データベース内の定義が反映されます。

```
tninfo -t cipso
=====
 Remote Host Template Table Entries:

 template: cipso
 host_type: CIPSO
```

## 例3 cipso テンプレート定義を表示する (続き)

```

doi: 1
min_sl: ADMIN_LOW
hex: ADMIN_LOW
max_sl: ADMIN_HIGH
hex: ADMIN_HIGH

```

## 属性

次の属性については、[attributes\(5\)](#) を参照してください。

| 属性タイプ      | 属性値     |
|------------|---------|
| 使用条件       | SUNWtsu |
| 安定性(コマンド行) | 開発中     |
| 安定性(出力)    | 不安定     |

## ファイル

[/etc/security/tsol/tnrhdb](#)      トラストドネットワーク遠隔ホストデータベース  
[/etc/security/tsol/tnrhtp](#)      トラストドネットワーク遠隔ホストテンプレート  
[/etc/security/tsol/tzonecfg](#)      トラストドゾーン構成データベース

## 関連項目

[tnd\(1M\)](#), [tnctl\(1M\)](#), [tnrhdb\(4\)](#), [tnrhtp\(4\)](#), [tzonecfg\(4\)](#), [attributes\(5\)](#)

『Solaris Trusted Extensions 管理の手順』の「カーネルキャッシュとネットワークデータベースを同期する」

|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 名前    | updatehome - 現在のラベル用のホームディレクトリのコピーファイルとリンクファイルの更新                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 形式    | /usr/bin/updatehome [-cirs]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 機能説明  | <p>updatehome は、ユーザーの最下位ラベルのコピーおよびリンク制御ファイル (.copy_files と .link_files) を読み込みます。これらのファイルには、コピーするファイルの一覧、およびユーザーの最下位ラベルのホームディレクトリから現在のラベルのホームディレクトリへシンボリックリンクするファイルの一覧が含まれます。</p> <p>Solaris Trusted Extensions dtsession プログラムは、新たにラベル付けされたワークスペースが作成されるたびに updatehome を実行します。これにより、ユーザーが使用したいファイルが利用可能になります。たとえば、たいていの場合、ユーザーは .profile、.login、.cshrc、.exrc、.mailrc、および ~/bin などのファイルへのシンボリックリンクを必要とします。updatehome は、このシンボリックリンクを実現する便利な機構を提供します。ユーザーは、コピーするファイルのリスト (.copy_files) およびシンボリックリンクを設定するファイルのリスト (.link_files) にファイルを追加できます。</p> |
| オプション | <ul style="list-style-type: none"> <li>-c 現在のラベルを持つ既存のホームディレクトリのコピーを置換します。デフォルトでは、既存のコピーの置換は実行しません。</li> <li>-i エラーが発生しても無視します。デフォルトでは、エラー発生時は異常終了します。</li> <li>-r 現在のラベルを持つ既存のホームディレクトリのコピーまたはシンボリックリンクを置換します。このオプションは、-c および -s オプションを合わせた意味を持ちます。デフォルトでは、既存のコピーやシンボリックリンクの置換は実行しません。</li> <li>-s 現在のラベルを持つ既存のホームディレクトリのシンボリックリンクを置換します。デフォルトでは、既存のシンボリックリンクの置換は実行しません。</li> </ul>                                                                                                                                                          |
| 戻り値   | 正常終了時に、updatehome は 0 を返します。エラー終了時には、updatehome は 1 を返して、診断メッセージを標準エラー出力に書き込みます。                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 使用例   | <p>例1 .copy_files ファイルの例</p> <p>.copy_files に記述されているファイルは、すべてのユーザーラベルで変更できません。</p> <pre>.cshrc .mailrc .mozilla/bookmarks.html</pre>                                                                                                                                                                                                                                                                                                                                                                                                          |

## 例2 .link\_files ファイルの例

.link\_files に記述されているファイルは、最下位のラベルで変更できます。変更は、ユーザーが利用可能なほかのラベルに伝達されます。

```
~/bin
.mozilla/preferences
.xrc
.rhosts
```

## 例3 リンクファイルとコピーファイルを更新する

.copy\_files および .link\_files は、ユーザーにより最下位のラベルで更新されました。ユーザーは、より高位のラベルでコピーおよびリンクを更新します。このコマンドを実行するのに権限は不要です。

```
% updatehome -r
```

## 属性

次の属性については、attributes(5)を参照してください。

| 属性タイプ | 属性値     |
|-------|---------|
| 使用条件  | SUNWtsu |
| 安定性   | 安定      |

## ファイル

\$HOME/.copy\_files コピーするファイルのリスト

\$HOME/.link\_files シンボリックリンクを作成するファイルのリスト

## 関連項目

attributes(5)

『Solaris Trusted Extensions 管理の手順』の「.copy\_files ファイルと .link\_files ファイル」

参照

システムコール

名前 getlabel, fgetlabel – ファイル機密ラベルの取得

形式 `cc [flags...] file... -ltsol [library...]`

```
#include <tsol/label.h>
```

```
int getlabel(const char *path, m_label_t *label_p);
```

```
int fgetlabel(int fd, m_label_t *label_p);
```

### 機能説明

`getlabel()` は、*path* で指定されたファイルの機密ラベルを取得します。*path* の最終構成要素への任意の読み取り、書き込み、または実行アクセス権は必要ありませんが、*path* のパス接頭辞内のすべてのディレクトリが検索可能である必要があります。

`fgetlabel()` は、引数の記述子から参照される、開いたファイルのラベルを取得します。取得は、`open(2)` の呼び出しなどを使って行われます。

*label\_p* は、隠されたラベル構造へのポインタです。呼び出し側は、`m_label_alloc(3TSOL)` を使用して、*label\_p* 用の領域を割り当てる必要があります。

### 戻り値

`getlabel()` および `fgetlabel()` は、次のいずれかの値を返します。

0 成功の場合。

-1 エラーが発生。エラーを表す `errno` が設定される。

### エラー

次の条件のどれかが該当する場合、`getlabel()` の処理は失敗します。

**EACCES** *path* のパス接頭辞の構成要素に対する検索権限が拒否されています。この制約を除くには、呼び出し元プロセスで `PRIV_FILE_DAC_SEARCH` 特権を表明します。

**EFAULT** *label\_p* または *path* が無効なアドレスを指しています。

**EIO** ファイルシステムに対する読み取りまたは書き込みで I/O エラーが発生しました。

**ELOOP** *path* を変換するときに検出されたシンボリックリンクの数が多すぎます。

**ENAMETOOLONG** パス引数の長さが `PATH_MAX` を超えています。

`_POSIX_NO_TRUNC` が有効な状態で、パス名の構成要素の長さが `NAME_MAX` を超えています (`pathconf(2)` を参照)。

**ENOENT** *path* で参照されているファイルが存在しません。

**ENOTDIR** *path* のパス接頭辞に、ディレクトリでない構成要素があります。

次の条件のどれかが該当する場合、`fgetlabel()` の処理は失敗します。

**EBADF** *fd* は、開いたファイルの有効な記述子ではありません。

EFAULT *label\_p* が、無効なアドレスを指しています。

EIO ファイルシステムに対する読み取りまたは書き込みで I/O エラーが発生しました。

## 属性

次の属性については、`attributes(5)` を参照してください。

| 属性タイプ       | 属性値      |
|-------------|----------|
| 使用条件        | SUNWcslr |
| インタフェースの安定性 | 安定       |

## 関連項目

`open(2)`, `pathconf(2)`, `m_label_alloc(3TSOL)`, `attributes(5)`, `labels(5)`

『Solaris Trusted Extensions 開発ガイド』の「ファイルラベルの取得」



参 照

Trusted Extensions ライブラリ

名前 blcompare, blequal, bldominates, blstrictdom, blinrange – バイナリラベルの比較

```
形式 cc [flag...] file... -ltsol [library...]
#include <tsol/label.h>

int blequal(const m_label_t *label1, const m_label_t *label2);
int bldominates(const m_label_t *label1, const m_label_t *label2);
int blstrictdom(const m_label_t *label1, const m_label_t *label2);
int blinrange(const m_label_t *label, const brange_t *range);
```

機能説明 これらの関数は、バイナリラベルを比較して、特定の条件を満たしているかどうかを調べます。

blequal() は、2つのラベルが同等かどうかを比較します。

bldominates() は、ラベル *label1* がラベル *label2* より優位かどうかを比較します。

blstrictdom() は、ラベル *label1* がラベル *label2* より完全に優位かどうかを比較します。

blinrange() は、ラベル *label* が *range*→*lower\_bound* より優位かどうか、および *range*→*upper\_bound* がラベル *label* より優位かどうかを比較します。

戻り値 これらの関数は、それぞれの条件が満たされた場合にはゼロ以外の値を、条件どおりでなかった場合はゼロを返します。

属性 次の属性については、attributes(5)を参照してください。

| 属性タイプ       | 属性値     |
|-------------|---------|
| 使用条件        | SUNWtsu |
| MTレベル       | MT-安全   |
| インタフェースの安定性 | 安定      |

関連項目 [ucred\\_getlabel\(3C\)](#), [getlabel\(3TSOL\)](#), [label\\_to\\_str\(3TSOL\)](#), [label\\_encodings\(4\)](#), [attributes\(5\)](#), [labels\(5\)](#)

『Solaris Trusted Extensions 開発ガイド』の「2つのラベル間の関係の判別」

名前 blminmax, blmaximum, blminimum - 2つのラベルの上限と下限

形式 `cc [flag...] file... -ltsol [library...]`

```
#include <tsol/label.h>
```

```
void blmaximum(m_label_t *maximum_label, const m_label_t *bounding_label);
```

```
void blminimum(m_label_t *minimum_label, const m_label_t *bounding_label);
```

機能説明

`blmaximum()` は、ラベル `maximum_label` の内容を、ラベル `maximum_label` および `bounding_label` のいずれか低い方の上限と置き換えます。低い方の上限とは、格付けと両方のラベルのすべてのコンパートメントのうちの上位の方を指します。これは、元の両方のラベルより優位な最下位のラベルです。

`blminimum()` は、ラベル `minimum_label` の内容をラベル `minimum_label` と `bounding_label` のいずれか高い方の下限と置き換えます。高い方の下限とは、格付けと両方のラベルに含まれているコンパートメントのうちの下位の方を指します。これは、元の両方のラベルより下位の最大のラベルです。

属性

次の属性については、`attributes(5)` を参照してください。

| 属性タイプ   | 属性値     |
|---------|---------|
| 使用条件    | SUNWtsu |
| MT レベル  | MT-安全   |
| インタフェース | 安定      |

関連項目

[label\\_to\\_str\(3TSOL\)](#), [sbltos\(3TSOL\)](#), [attributes\(5\)](#)

|                |                                                                                                                                                                                                                                     |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 名前             | bltcolor, bltcolor_r – ラベルの文字形式のカラー名を取得する                                                                                                                                                                                           |
| 形式             | cc [ <i>flag...</i> ] <i>file...</i> -ltsol [ <i>library...</i> ]<br><pre>#include &lt;tsol/label.h&gt;  char *bltcolor(const m_label_t *label);  char *bltcolor_r(const m_label_t *label, const int size, char *color_name);</pre> |
| インタフェース<br>レベル | bltcolor() および bltcolor_r() 関数は、廃止または互換性がなくなる可能性があります。代わりに <a href="#">label_to_str(3TSOL)</a> 関数を使用してください。                                                                                                                         |
| 機能説明           | 呼び出し元のプロセスは、現在のプロセスの機密ラベルより優位にあるラベルのカラー名を取得する PRIV_SYS_TRANS_LABEL を有効な特権のセット内に保持している必要があります。                                                                                                                                       |
|                | bltcolor() および bltcolor_r() は、バイナリラベル <i>label</i> と関連付けられた文字形式のカラー名を取得します。                                                                                                                                                         |
| 戻り値            | bltcolor() は、 <i>label</i> に指定された文字形式のカラー名を含む静的に割り当てられた文字列へのポインタを返すか、何らかの理由でバイナリラベルで文字形式のカラー名が利用できない場合は (char *)0 を返します。                                                                                                            |
|                | bltcolor_r() は、 <i>label</i> に指定された文字形式のカラー名を含む <i>color_name</i> 文字列へのポインタを返すか、何らかの理由でバイナリラベルで文字形式のカラー名が利用できない場合は (char *)0 を返します。 <i>color_name</i> は、少なくとも <i>size</i> 文字の文字列を提供する必要があります。                                       |
| ファイル           | /etc/security/tsol/label_encodings<br>ラベルエンコーディングファイルには、このシステムの定義済みラベルに対する格付け名、語句、制約、および値が含まれます。                                                                                                                                    |
| 属性             | 次の属性については、 <a href="#">attributes(5)</a> を参照してください。                                                                                                                                                                                 |

| 属性タイプ  | 属性値                |
|--------|--------------------|
| 使用条件   | SUNWtsu            |
| 安定性レベル | 廃止または互換性がなくなる可能性あり |
| MT レベル | 例外付き MT-安全         |

関連項目 [label\\_to\\_str\(3TSOL\)](#), [attributes\(5\)](#)

注意事項 これらの関数は旧式であり、移植を容易にする目的で維持されています。将来の Solaris Trusted Extensions リリースでは、これらの関数は削除される可能性があります。

---

関数 `bltcolor()` は、静的に割り当てられた文字列へのポインタを返します。次に関数を呼び出す際、文字列は新しい文字形式のカラー名で文字列で上書きされます。MT-安全ではありません。

マルチスレッドアプリケーションの場合は、関数 `bltcolor_r()` を使用するよう to してください。

*label* に指定された語句が含まれる場合、ラベルエンコーディングファイルで指定した最初の語に関連付けられた文字形式のカラー名が返されます。それ以外の場合、*label* に文字形式のカラー名が指定されていなければ、バイナリラベルと同じ格付けのラベルエンコーディングファイルで指定された最初の文字形式のカラー名が返されます。

名前 bltos, bsltos, bcleartos – バイナリラベルの文字形式のラベルへの変換

形式 `cc [flag...] file... -ltsol [library...]`

```
#include <tsol/label.h>
```

```
int bsltos(const m_label_t *label, char **string, const int str_len, const int flags);
```

```
int bcleartos(const m_label_t *label, char **string, const int str_len, const int flags);
```

インタフェースレベル bsltos() および bcleartos() 関数は、廃止または互換性がなくなる可能性があります。代わりに `label_to_str(3TSOL)` 関数を使用してください。

機能説明 呼び出し元プロセスは、現在のプロセスの機密ラベルより優位にあるラベルについてラベル変換を実行するには、有効な特権セットの中に `PRIV_SYS_TRANS_LABEL` を保持している必要があります。

これらのルーチンは、バイナリラベルを文字列に変換します。この文字列は `flags` パラメータの値によって制御されます。

出力される文字コード形式のラベルの汎用形式は次のとおりです。

```
CLASSIFICATION WORD1 WORD2 WORD3/WORD4 SUFFIX PREFIX WORD5/WORD6
```

CLASSIFICATION 名と WORD は大文字で表示します。格付け (Classifications) と Word は、文字コード形式のラベルにあるほかの Word と「」(空白文字) で区別されます。ただし、同じ PREFIX または SUFFIX を要求する複数の Word が存在する場合は例外です。この場合は、Word と Word の間は「/」(スラッシュ) で区切ります。

`string` は、事前に割り当てられたメモリーへのポインタ、値 (`char *`)`0` のうち、いずれかを指します。事前に割り当てられたメモリーへのポインタを指す場合は、`str_len` で、メモリーのサイズを示します。値 (`char *`)`0` を指す場合は、変換された文字コード形式のラベルを含むように、`malloc()` を使ってメモリーが割り当てられます。変換された `label` は、割り当てられた (または事前に割り当てられた) メモリーにコピーされます。

`flags` は `0` (ゼロ)、または次の論理和になります。

LONG\_WORDS `label` に定義されている Word の長形式名を使って変換します。

SHORT\_WORDS `label` に定義されている Word の短形式名を使って変換します。`label_encodings` ファイルの中に Word の短形式名が定義されていない場合は、長形式名が使用されます。

LONG\_CLASSIFICATION `label` に定義されている格付けの長形式名を使って変換します。

SHORT\_CLASSIFICATION `label` に定義されている格付けの短形式名を使って変換します。

|                   |                                                                                                                                                                                     |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ACCESS_RELATED    | 情報ラベル <i>label</i> に定義されている「アクセス関連の」エントリだけを変換します。                                                                                                                                   |
| VIEW_EXTERNAL     | ADMIN_LOW ラベルと ADMIN_HIGH ラベルを <i>label_encodings</i> ファイルに定義されている最下位ラベルと最上位ラベルに変換します。                                                                                              |
| VIEW_INTERNAL     | ADMIN_LOW ラベルと ADMIN_HIGH ラベルを、 <i>label_encodings</i> ファイルに指定されている <i>admin low name</i> 文字列と <i>admin high name</i> 文字列に変換します。文字列が指定されていない場合は、文字列「ADMIN_LOW」と「ADMIN_HIGH」が使用されます。 |
| NO_CLASSIFICATION | <i>label</i> に定義されている格付けは変換されません。                                                                                                                                                   |

*bsltos()* は、バイナリ機密ラベルを文字列に変換します。適用可能な *flags* は、LONG\_CLASSIFICATION または SHORT\_CLASSIFICATION、LONG\_WORDS または SHORT\_WORDS、VIEW\_EXTERNAL または VIEW\_INTERNAL、および NO\_CLASSIFICATION です。*flags* 値 0 は、(SHORT\_CLASSIFICATION | LONG\_WORDS) と同等です。

*bcleartos()* は、バイナリ許可上限を文字列に変換します。適用可能な *flags* は、LONG\_CLASSIFICATION または SHORT\_CLASSIFICATION、LONG\_WORDS または SHORT\_WORDS、VIEW\_EXTERNAL または VIEW\_INTERNAL、および NO\_CLASSIFICATION です。*flags* 値 0 は、(SHORT\_CLASSIFICATION | LONG\_WORDS) と同等です。認可上限の変換結果は、機密ラベルの変換結果と同じでないことがあります。これらの関数は、別々の *label\_encodings* ファイルテーブルを使用します。それぞれのテーブルに含まれる Word と制約条件は異なっている場合があります。

## 戻り値

これらのルーチンは次の値を返します。

- 1 ラベルのタイプが、有効な定義された必須のものでない場合、プロセスの機密ラベルがラベルより優位でなく、プロセスの有効な特権セットの中に PRIV\_SYS\_TRANS\_LABEL がない場合、または *label\_encodings* ファイルにアクセス不能な場合。
- 0 戻り文字列にメモリーを割り当てられない場合、または事前に割り当てられた戻り文字列のメモリーに文字列が収まらない場合。事前に割り当てられた文字列の値は NULL 文字列に設定されます (*\*string[0]='00'*;)。
- >0 成功の場合、NULL ターミネータを含む文字コード形式のラベルの長さが表示されます。

## プロセス属性

VIEW\_EXTERNAL または VIEW\_INTERNAL フラグが指定されていない場合、ADMIN\_LOW ラベルと ADMIN\_HIGH ラベルの変換は、ラベル表示プロセスの属性フラグによって制御されます。ラベル表示プロセスの属性フラグが定義されていない場合は、*label\_encodings* ファイルに設定されているラベル表示によって制御されます。External の値は、ADMIN\_LOW ラベルと ADMIN\_HIGH ラベルが *label\_encodings* ファイル

に定義されている最下位ラベルと最上位ラベルに割り当てられることを指定します。Internal の値は、ADMIN\_LOW ラベルと ADMIN\_HIGH ラベルが label\_encodings ファイルに指定されている admin low name 文字列と admin high name 文字列に変換されることを指定します。このような名前が指定されていない場合は、文字列「ADMIN\_LOW」と「ADMIN\_HIGH」が使用されます。

#### ファイル

/etc/security/tsol/label\_encodings

ラベルエンコーディングファイルには、このシステムの定義済みラベルに対する格付け名、語句、制約、および値が含まれます。

#### 属性

次の属性については、attributes(5) を参照してください。

| 属性タイプ  | 属性値                |
|--------|--------------------|
| 使用条件   | SUNWtsu            |
| 安定性    | 廃止または互換性がなくなる可能性あり |
| MT レベル | 例外付き MT-安全         |

#### 関連項目

free(3C), malloc(3C), label\_to\_str(3TSOL), label\_encodings(4), attributes(5)

#### 注意事項

これらの関数は旧式であり、移植を容易にする目的で維持されています。これらは、将来の Solaris Trusted Extensions リリースでは削除される可能性があります。

これらのルーチンでメモリーを割り当てている場合は、使用しなくなったメモリーは、呼び出し元で free() を使って解放します。

|            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 名前         | btohex, bsltoh, bcleartoh, bsltoh_r, bcleartoh_r, h_alloc, h_free – バイナリラベルの 16 進数への変換                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 形式         | <pre>cc [flag...] file... -ltsol [library...] #include &lt;tsol/label.h&gt;  char *bsltoh(const m_label_t *label); char *bcleartoh(const m_label_t *clearance); char *bsltoh_r(const m_label_t *label, char *hex); char *bcleartoh_r(const m_label_t *clearance, char *hex); char *h_alloc(const unsigned char type); void h_free(char *hex);</pre>                                                                                                                                                                                            |
| インタフェースレベル | bsltoh(), bcleartoh(), bsltoh_r(), bcleartoh_r(), h_alloc(), および h_free() 関数は、廃止または互換性がなくなる可能性があります。代わりに <a href="#">label_to_str(3TSOL)</a> 関数を使用してください。                                                                                                                                                                                                                                                                                                                                                                                      |
| 機能説明       | <p>これらの関数は、バイナリラベルを内部値を表す 16 進文字列に変換します。</p> <p>bsltoh() および bsltoh_r() は、バイナリ機密ラベルを次の形式の文字列に変換します。</p> <pre>[0xsensitivity_label_hexadecimal_value]</pre> <p>bcleartoh() および bcleartoh_r() は、バイナリ認可上限を次の形式の文字列に変換します。</p> <pre>0xclearance_hexadecimal_value</pre> <p>h_alloc() は、bsltoh_r() および bcleartoh_r() で使用する 16 進数値 <i>type</i> にメモリーを割り当てます。</p> <p><i>type</i> の有効な値は次のとおりです。</p> <p>SUN_SL_ID     <i>label</i> はバイナリ機密ラベルです。</p> <p>SUN_CLR_ID    <i>label</i> はバイナリ認可上限です。</p> <p>h_free() は、h_alloc() によって割り当てられたメモリーを解放します。</p> |
| 戻り値        | これらの関数は、変換結果を含む文字列へのポインタを返します。パラメータのタイプが要求されたものでない場合は、(char *)0 を返します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 属性         | 次の属性については、 <a href="#">attributes(5)</a> を参照してください。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| 属性タイプ  | 属性値                |
|--------|--------------------|
| 使用条件   | SUNWtsu            |
| 安定性レベル | 廃止または互換性がなくなる可能性あり |
| MT レベル | 例外付き MT-安全         |

関連項目 [atohexlabel\(1M\)](#), [hextoalabel\(1M\)](#), [label\\_to\\_str\(3TSOL\)](#), [attributes\(5\)](#), [labels\(5\)](#)

#### 注意事項

これらの関数は旧式であり、移植を容易にする目的で維持されています。これらは、将来の Solaris Trusted Extensions リリースでは削除される可能性があります。

関数 `bsltoh()` および `bcleartoh()` は、静的に割り当てられた同じ文字列記憶領域を共有します。MT-安全ではありません。これらの関数を呼び出すたびに、文字列は新しく変換された文字列で上書きされます。

マルチスレッドアプリケーションの場合は、関数 `bsltoh_r()` および `bcleartoh_r()` を使用してください。

|      |                                                                                                                                                                                                                                                     |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 名前   | getdevicerange – デバイスのラベル範囲の取得                                                                                                                                                                                                                      |
| 形式   | cc [ <i>flag...</i> ] <i>file...</i> -l <code>bsm</code> -l <code>tsol</code> [ <i>library...</i> ]<br>#include <tsol/label.h><br><br>blrange_t *getdevicerange(const char *device);                                                                |
| 機能説明 | getdevicerange() 関数は、ユーザーが割り当て可能なデバイスのラベル範囲を返します。<br><br><i>device</i> のラベルが指定されていない場合、getdevicerange() は、 <i>device</i> の下限として ADMIN_LOW のデフォルト値を、上限として ADMIN_HIGH のデフォルト値を返します。<br><br>コマンド行で list_devices(1) を使用して、 <i>device</i> のラベル範囲を表示できます。 |
| 戻り値  | getdevicerange() 関数は、失敗時に NULL を返して、errno を設定します。成功時には、blrange_t 構造体へのポインタを返します。呼び出し元は、次のようにしてこれを解放する必要があります。<br><br>blrange_t *range;<br>...<br>m_label_free(range->lower_bound);<br>m_label_free(range->upper_bound);<br>free(range);             |
| 属性   | 次の属性については、attributes(5) を参照してください。                                                                                                                                                                                                                  |

| 属性タイプ  | 属性値      |
|--------|----------|
| 使用条件   | SUNWcslr |
| 安定性    | 開発中      |
| MT レベル | MT-安全    |

|      |                                                                                                                                                                                                 |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| エラー  | getdevicerange() は、次の場合に失敗します。<br><br>EAGAIN 必須のバイトを割り当てるための十分なメモリーがありません。アプリケーションは、あとで再試行できます。<br><br>ENOMEM システムの物理的制限を超過したために、size バイトのメモリーを割り当てることができません。<br><br>ENOTSUP デバイスの上限または下限が無効です。 |
| 関連項目 | list_devices(1), free(3C), m_label_free(3TSOL), attributes(5)                                                                                                                                   |

『Solaris Trusted Extensions 開発ガイド』の「プリンタのラベル範囲に対するラベル要求の検査」

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 名前   | getpathbylabel - ゾーンのパス名を返す                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 形式   | <pre>cc [flags...] file... -ltsol #include &lt;tsol/label.h&gt;  char *getpathbylabel(const char *path, char *resolved_path, size_t bufsize,                     const m_label_t *sl);</pre>                                                                                                                                                                                                                                                                                                                                                    |
| 機能説明 | <p>getpathbylabel() は、ゾーンパス名中のすべてのシンボリックリンクを展開し、「./」および「../」への参照、余分な「/」文字を解決した上で <i>resolved_path</i> で指定されたバッファ内に保存します。 <i>bufsize</i> 引数には、このバッファのサイズをバイト単位で指定します。表示されるパスには、シンボリックリンクコンポーネントも、「./」や「../」も含まれません。この関数は、大域ゾーンからだけ呼び出すことができます。</p> <p>ゾーンパス名は、機密ラベル <i>sl</i> に対する相対位置を示します。存在しないゾーン名に対する機密ラベルを指定するには、指定された機密レベルがプロセス機密レベルより優位にあるか下位にあるかに応じて、プロセスは、PRIV_FILE_UPGRADE_SL または PRIV_FILE_DOWNGRADE_SL 特権を表明する必要があります。</p>                                                                                                           |
| 戻り値  | getpathbylabel() は、成功時に <i>resolved_path</i> へのポインタを返します。失敗時には NULL を返し、 <i>errno</i> を設定してエラーを示します。                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| エラー  | <p>EACCES <i>path</i> のパス接頭辞の構成要素に対する検索権限が拒否されています。</p> <p>EFAULT <i>resolved_path</i> は、プロセスの割り当てられたアドレス空間の外、または <i>bufsize</i> バイトを超えて展開されます。</p> <p>ELOOP <i>path</i> を変換するときに検出されたシンボリックリンクの数が多すぎます。</p> <p>EINVAL <i>path</i> または <i>resolved_path</i> が NULL でした。現在のゾーンが大域ゾーンではないか、<i>sl</i> が無効です。</p> <p>EIO ファイルシステムに対する読み取りまたは書き込みで I/O エラーが発生しました。</p> <p>ENOENT 指定されたファイルが存在しません。</p> <p>ENAMETOOLONG パス引数の長さが PATH_MAX を超えています。パス名コンポーネントの長さが NAME_MAX を超えています (sysconf(3C) を参照)、_POSIX_NO_TRUNC が有効になっています (pathconf(2) を参照)。</p> |
| 属性   | 次の属性については、attributes(5) を参照してください。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

---

| 属性タイプ       | 属性値      |
|-------------|----------|
| 使用条件        | SUNWcslr |
| MT レベル      | MT-安全    |
| インタフェースの安定性 | 安定       |

**関連項目** [readlink\(2\)](#), [getzonerootbyid\(3TSOL\)](#), [attributes\(5\)](#), [labels\(5\)](#)

**警告** `getpathbylabel()` は、`readlink(2)` システムコールを間接的に呼び出すので、ファイルシステム資源にアクセス不能なためにシステムがハングアップする可能性が継承されます。

名前 getlabel - プロセスラベルの取得

形式 `cc [flag...] file... -ltsol [library...]`  
`#include <tsol/label.h>`  
`int getlabel(m_label_t *label_p);`

機能説明 getlabel() は、呼び出し元プロセスの機密ラベルを取得します。

戻り値 getlabel() は、次の値を返します。

- 0 成功の場合。
- 1 失敗の場合。errno を設定してエラーを示します。label\_p は変更されません。

エラー 次の条件が当てはまる場合、getlabel() は失敗し、label\_p は有効な機密ラベルを参照しません。

EFAULT label\_p が、無効なアドレスを指しています。

属性 次の属性については、attributes(5) を参照してください。

| 属性タイプ       | 属性値     |
|-------------|---------|
| 使用条件        | SUNWtsu |
| MT レベル      | MT-安全   |
| インタフェースの安定性 | 安定      |

関連項目 [ucred\\_getlabel\(3C\)](#), [m\\_label\\_alloc\(3TSOL\)](#), [m\\_label\\_free\(3TSOL\)](#), [attributes\(5\)](#)

『Solaris Trusted Extensions 開発ガイド』の「プロセスラベルの取得」

注意事項 この関数が返すシステムプロセスの値は、ucred\_getlabel(3C) の返す値とは異なります。

名前 getuserrange - ユーザーのラベル範囲の取得

形式 `cc [flags...] file... -ltsol`

```
#include <tsol/label.h>
```

```
m_range_t *getuserrange(const char *username);
```

機能説明 `getuserrange()` 関数は、`username` のラベル範囲を返します。範囲の下限は、ユーザーがマルチレベルデスクトップにログインするときの初期ワークスペースラベルとして使用されます。上限、または認可上限は、ユーザーがラベル付けされたワークスペースに割り当てることができるラベルの上限として使用します。

ユーザーのラベル範囲のデフォルト値については、[label\\_encodings\(4\)](#) を参照してください。個別のユーザーについてデフォルト値を無効にする値については、[user\\_attr\(4\)](#) を参照してください。

戻り値 `getuserrange()` 関数は、メモリー割り当てが失敗すると `NULL` を返します。それ以外の場合、この関数は、次に示すように、呼び出し元が解放する必要のある構造を返します。

```
m_range_t *range;
...
m_label_free(range->lower_bound);
m_label_free(range->upper_bound);
free(range);
```

エラー `getuserrange()` 関数が失敗するのは、次の場合です。

**ENOMEM** システムの物理的制限を超過したために、`size` バイトのメモリーを割り当てることができません。

属性 次の属性については、[attributes\(5\)](#) を参照してください。

| 属性タイプ       | 属性値          |
|-------------|--------------|
| 使用条件        | SUNWcslr     |
| MT レベル      | MT-安全        |
| インタフェースの安定性 | 後述の「注意事項」を参照 |

関連項目 [free\(3C\)](#), [m\\_label\\_free\(3TSOL\)](#), [label\\_encodings\(4\)](#), [user\\_attr\(4\)](#), [attributes\(5\)](#)

注意事項 [label\\_encodings\(4\)](#) の米国国防情報局 (DIA) MAC ポリシーを実装しているシステムでは、この関数の安定性は「安定」です。Trusted Extensions の将来のリリースにその他のポリシーが存在する可能性はありますが、それらは将来のリリースでは旧式とされるか、[label\\_encodings\(4\)](#) の補完的役割になる可能性があります

名前 `getzonelabelbyid, getzonelabelbyname, getzoneidbylabel` – ゾーンとラベル間のマッピング

形式 `cc [flags...] file... -ltsol`

```
#include <tsol/label.h>

m_label_t *getzonelabelbyid(zoneid_t zoneid);
m_label_t *getzonelabelbyname(const char *zonename);
zoneid_t *getzoneidbylabel(const m_label_t *label);
```

機能説明 `getzonelabelbyid()` 関数は、`zoneid` の必須アクセス制御 (MAC) ラベルを返します。

`getzonelabelbyname()` 関数は、`zonename` という名前のゾーンの MAC ラベルを返します。

`getzoneidbylabel()` 関数は、`label` という名前のラベルを持つゾーンのゾーン ID を返します。

これらのすべての関数で、指定されたゾーンの状態が `ZONE_IS_READY` であることが最低限必要です。呼び出し元プロセスのゾーンが指定されたゾーンのラベルに対して優位にあるか、呼び出し元プロセスが大域ゾーン内に存在する必要があります。

戻り値 成功時に、`getzonelabelbyid()` および `getzonelabelbyname()` 関数は、これらの関数内部で割り当てられている機密ラベルへのポインタを返します。記憶領域を解放するには、`m_label_free(3TSOL)` を使用します。ゾーンが存在しない場合は、`NULL` が返されます。

成功時に、`getzoneidbylabel()` 関数は一致するラベルを持つゾーン ID を返します。一致するゾーンが存在しない場合、この関数は `-1` を返します。

属性 次の属性については、`attributes(5)` を参照してください。

| 属性タイプ       | 属性値      |
|-------------|----------|
| 使用条件        | SUNWcslr |
| MT レベル      | 安全       |
| インタフェースの安定性 | 安定       |

エラー `getzonelabelbyid()` 関数と `getzonelabelbyname()` 関数は、次の場合に失敗します。

`ENOENT` 指定されたゾーンが存在しません。

`getzonelabelbyid()` 関数は、次の場合に失敗します。

`ENOENT` 指定されたラベルに対応するゾーンが存在しません。

関連項目      Intro(2), getzonenamebyid(3C), getzoneidbyname(3C), [m\\_label\\_free\(3TSOL\)](#),  
attributes(5), [labels\(5\)](#)

名前 getzoneroobid, getzoneroobylabel, getzoneroobbyname – ゾーンのリートパス名とラベル間のマッピング

形式 `cc [flags...] file... -ltsol`

```
#include <tsol/label.h>

char *getzoneroobid(zoneid_t zoneid);
char *getzoneroobylabel(const m_label_t *label);
char *getzoneroobbyname(const char *zonename);
```

機能説明 getzoneroobid() 関数は、*zoneid* のリートパス名を返します。

getzoneroobylabel() 関数は、ラベルが *label* であるゾーンのリートパス名を返します。

getzoneroobbyname() 関数は、*zonename* のリートパス名を返します。

これらのどの関数の場合でも、指定されたゾーンの状態が `ZONE_IS_READY` であることが最低限必要です。呼び出し元プロセスのゾーンが指定されたゾーンのリートパス名に対して優位にあるか、呼び出し元プロセスが大域ゾーン内に存在する必要があります。返されるパス名は、呼び出し元のゾーンのリートパスとの相対位置を示します。

戻り値 成功時に、`getzoneroobid()`、`getzoneroobylabel()`、および `getzoneroobbyname()` 関数は、これらの関数内部で割り当てられているパス名へのポインタを返します。記憶領域の解放には、`free(3C)` を使用します。失敗時に、これらの関数は `NULL` を返して、エラーを示す `errno` を設定します。

エラー `EINVAL` *zoneid* が無効であるか、ゾーンが見つからないか、またはゾーンの準備ができていません。

`EFAULT` 無効な引数。ポインタの位置が無効です。

`ENOMEM` パス名を割り当てることができません。

`ENOENT` ゾーンが存在しません。

属性 次の属性については、`attributes(5)` を参照してください。

| 属性タイプ       | 属性値      |
|-------------|----------|
| 使用条件        | SUNWcslr |
| MT レベル      | 安全       |
| インタフェースの安定性 | 安定       |

関連項目 `Intro(2)`, `free(3C)`, `getzonenamebyid(3C)`, `attributes(5)`, `labels(5)`

|            |                                                                                                                                                                                                                                                 |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 名前         | hextob, htobsl, htobclear – 16 進文字列のバイナリラベルへの変換                                                                                                                                                                                                 |
| 形式         | <pre>cc [flag...] file... -ltsol [library...] #include &lt;tsol/label.h&gt;  int htobsl(const char *s, m_label_t *label); int htobclear(const char *s, m_label_t *clearance);</pre>                                                             |
| インタフェースレベル | htobsl() および htobclear() 関数は、廃止または互換性がなくなる可能性があります。代わりに、 <a href="#">str_to_label(3TSOL)</a> 関数を使用してください。                                                                                                                                       |
| 機能説明       | <p>これらの関数は、内部ラベル値の 16 進文字列表現をバイナリラベルに変換します。</p> <p>htobsl() は、次の形式の 16 進文字列をバイナリ機密ラベルに変換します。<br/> <i>0xsensitivity_label_hexadecimal_value</i></p> <p>htobclear() は、次の形式の 16 進文字列をバイナリ認可上限に変換します。<br/> <i>0xclearance_hexadecimal_value</i></p> |
| 戻り値        | これらの関数は、変換が成功した場合はゼロ以外の値を、成功しなかった場合はゼロを返します。                                                                                                                                                                                                    |
| 属性         | 次の属性については、 <a href="#">attributes(5)</a> を参照してください。                                                                                                                                                                                             |

| 属性タイプ  | 属性値                |
|--------|--------------------|
| 使用条件   | SUNWtsu            |
| 安定性レベル | 廃止または互換性がなくなる可能性あり |
| MT レベル | MT-安全              |

|      |                                                                                                 |
|------|-------------------------------------------------------------------------------------------------|
| 関連項目 | <a href="#">str_to_label(3TSOL)</a> , <a href="#">attributes(5)</a> , <a href="#">labels(5)</a> |
| 注意事項 | これらの関数は旧式であり、移植を容易にする目的で維持されています。これらは、将来の Solaris Trusted Extensions リリースでは削除される可能性があります。       |

名前 labelbuilder, tsol\_lbuild\_create, tsol\_lbuild\_get, tsol\_lbuild\_set, tsol\_lbuild\_destroy – 有効なラベルまたは認可上限を対話形式で構築するための Motif ベースのユーザーインタフェースの作成

形式 `cc [flag...] file... -ltsol -lDtTsol [library...]`

```
#include <Dt/ModLabel.h>
```

```
ModLabelData *tsol_lbuild_create(Widget widget void (*event_handler)() ok_callback
 lbuild_attributes extended_operation, ..., NULL);
```

```
void *tsol_lbuild_get(ModLabelData *data, lbuild_attributes extended_operation);
```

```
void tsol_lbuild_set(ModLabelData *data lbuild_attributes extended_operation, ...,
 NULL);
```

```
void tsol_lbuild_destroy(ModLabelData *data);
```

## 機能説明

ラベルビルダーのユーザーインタフェースは、エンドユーザーに情報の入力を求めるプロンプトを表示し、アプリケーションを実行しているシステム上の [label\\_encodings\(4\)](#) ファイルの指定に基づいて、ユーザー入力から有効な機密ラベルまたは認可上限を生成します。エンドユーザーは、テキスト値を入力するか、対話形式でオプションを選択することによって、ラベルまたは認可上限を構築できます。

アプリケーション固有の機能は、OK プッシュボタンのコールバックで実行されます。このコールバックは `tsol_lbuild_create()` 呼び出しに引き渡され、OK プッシュボタンウィジェットに対応付けられます。

オプションの選択時、ラベルビルダーでは、実行可能ファイルが有効なセットの中に `PRIV_SYS_TRANS_LABEL` 特権を持つ場合を除いて、ワークスペースの機密ラベルより下位の格付け (と関連コンパートメントおよびマーキング) だけが表示されます。

エンドユーザーがラベルを昇格または降格する承認を持たない場合、ユーザーが構築したラベルがユーザーの認可範囲を超える場合は、OK プッシュボタンとリセットプッシュボタンは灰色表示になっています。これらの制限を無効にする特権はありません。

`tsol_lbuild_create()` は、グラフィカルユーザーインタフェースを作成し、ユーザーインタフェースについての情報を含む `ModLabelData*` タイプのポインタ変数を返します。この情報は、`tsol_lbuild_create()` 入力パラメータリストに引き渡される値、指定されていない情報のデフォルト値、ラベルビルダーがユーザーインタフェースを作成するのに使用するウィジェットについての情報の組み合わせです。ウィジェット情報を除くすべての情報には `tsol_lbuild_get()` ルーチンと `tsol_lbuild_set()` ルーチンでアクセスします。

ウィジェット情報には、`ModLabelData` 構造体の次のフィールドを参照すると、直接アクセスできます。

`lbuild_dialog`     ラベルビルダーダイアログボックス。

|                                         |                                                             |
|-----------------------------------------|-------------------------------------------------------------|
| ok                                      | OK プッシュボタン。                                                 |
| cancel                                  | 取消しプッシュボタン。                                                 |
| reset                                   | リセットプッシュボタン。                                                |
| help                                    | ヘルププッシュボタン。                                                 |
| tsol_lbuild_create() パラメータリストは次の値をとります。 |                                                             |
| widget                                  | ダイアログボックスを作成するウィジェット。どの Motif ウィジェットも引き渡せます。                |
| ok_callback                             | ダイアログボックス上に OK プッシュボタンの動作を実装するコールバック機能。                     |
| ..., NULL                               | 拡張操作と値の組み合わせから成る NULL で終わるリスト。ラベルビルダーダイアログボックスの特性と動作を定義します。 |

tsol\_lbuild\_destroy() は、tsol\_lbuild\_create() が返す ModLabelData 構造体を破棄します。

tsol\_lbuild\_get() と tsol\_lbuild\_set() は、tsol\_lbuild\_create() が返す ModLabelData 構造体に格納されている情報にアクセスします。

次の拡張操作は、tsol\_lbuild\_create() に引き渡すとユーザーインタフェースを構築でき、tsol\_lbuild\_get() に引き渡すとユーザーインタフェースについての情報を検出でき、tsol\_lbuild\_set() に引き渡すとユーザーインタフェースの情報を変更できます。tsol\_lbuild\_get() に対してはすべての拡張操作が有効ですが、\*WORK\* 操作はエンドユーザーからの入力によって設定されるため tsol\_lbuild\_set() または tsol\_lbuild\_create() に対しては有効ではありません。これらの例外事項については「機能説明」で解説します。

|                  |                                                                            |
|------------------|----------------------------------------------------------------------------|
| LBUILD_MODE      | 機密ラベルまたは認可上限のどちらを構築するためのユーザーインタフェースを作成するかを指定します。デフォルト値は LBUILD_MODE_SL です。 |
|                  | LBUILD_MODE_SL      機密ラベルを構築します。                                           |
|                  | LBUILD_MODE_CLR     認可上限を構築します。                                            |
| LBUILD_VALUE_SL  | 開始機密ラベル。デフォルト値は ADMIN_LOW で、モードが LBUILD_MODE_SL のときに使用されます。                |
| LBUILD_VALUE_CLR | 開始認可上限。デフォルト値は ADMIN_LOW で、モードが LBUILD_MODE_CLR のときに使用されます。                |
| LBUILD_USERFIELD | ラベルビルダーダイアログボックスの一番上に表示される文字列プロンプト。デフォルト値は NULL です。                        |

|                    |                                                                                                                                                                                                      |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LBUILD_SHOW        | <p>ラベルビルダーダイアログボックスの表示と非表示を切り替えます。デフォルト値は FALSE です。</p> <p>TRUE      ラベルビルダーダイアログボックスを表示します。</p> <p>FALSE     ラベルビルダーダイアログボックスを非表示にします。</p>                                                          |
| LBUILD_TITLE       | <p>ラベルビルダーダイアログボックスの一番上に表示される文字列タイトル。デフォルト値は NULL です。</p>                                                                                                                                            |
| LBUILD_WORK_SL     | <p>tsol_lbuild_set()、tsol_lbuild_create() に対しては有効ではありません。エンドユーザーが構築中の機密ラベル。更新プッシュボタンを選択するか、対話形式でオプションを選択すると、値はエンドユーザーの入力値に更新されません。</p>                                                               |
| LBUILD_WORK_CLR    | <p>tsol_lbuild_set()、tsol_lbuild_create() に対しては有効ではありません。エンドユーザーが構築中の認可上限。更新プッシュボタンを選択するか、対話形式でオプションを選択すると、値はエンドユーザーの入力値に更新されません。</p>                                                                |
| LBUILD_X           | <p>画面の左上角を基準として、ラベルビルダーダイアログボックスの左上角の X 位置 (ピクセル数)。ラベルビルダーダイアログボックスは、デフォルトで、画面の中央に配置されます。</p>                                                                                                        |
| LBUILD_Y           | <p>画面の左上角を基準として、ラベルビルダーダイアログボックスの左上角の Y 位置 (ピクセル数)。ラベルビルダーダイアログボックスは、デフォルトで、画面の中央に配置されます。</p>                                                                                                        |
| LBUILD_LOWER_BOUND | <p>ラベルまたは認可上限を対話形式で構築する際、ユーザーが使用できるラジオボタンとして最下位の格付け (と関連するコンパートメントおよびマーキング)。この値はユーザーの最下位ラベルです。</p>                                                                                                   |
| LBUILD_UPPER_BOUND | <p>ラベルまたは認可上限を対話形式で構築する際、ユーザーが使用できるラジオボタンとして最上位の格付け (と関連するコンパートメントおよびマーキング)。指定する値はユーザーの認可範囲内とします。値が指定されない場合、値はユーザーのワークスペース機密ラベルとなります。また、実行可能ファイルに PRIV_SYS_TRANS_LABEL 特権がある場合、値はユーザーの認可上限になります。</p> |

|                      |                                                                                                                                                     |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| LBUILD_CHECK_AR      | ユーザーが構築し「更新後のラベル」フィールドに入力されたラベルが、ユーザーの認可範囲内にあるかどうかをチェックします。値1のときはチェックが行われ、値0のときはチェックが行われません。チェックを実行するように指定したとき、ラベルが範囲外であれば、エンドユーザーにエラーメッセージが表示されます。 |
| LBUILD_VIEW          | 内部または外部のラベル表現を使用します。デフォルト値はLBUILD_VIEW_EXTERNALです。                                                                                                  |
| LBUILD_VIEW_INTERNAL | システム内の最上位ラベルと最下位ラベル、ADMIN_HIGHとADMIN_LOWの内部名を使用します。                                                                                                 |
| LBUILD_VIEW_EXTERNAL | ADMIN_LOWラベルを次に高いラベルに昇格し、ADMIN_HIGHラベルを次に低いラベルに降格します。                                                                                               |

## 戻り値

tsol\_lbuild\_get() は、値を取得できなかった場合、-1を返します。

tsol\_lbuild\_create() ルーチンは、tsol\_lbuild\_create() 入力パラメータリストに指定される情報を含むModLabelDataタイプの変数、指定されていない情報のデフォルト値、ラベルビルダーがユーザーインタフェースを作成するのに使用するウィジェットに関する情報を返します。

## 使用例

例1 ラベルビルダーを作成する

```
(ModLabelData *)lbldata = tsol_lbuild_create(widget0, callback_function,
 LBUILD_MODE, LBUILD_MODE_SL,
 LBUILD_TITLE, "Setting Sensitivity Label",
 LBUILD_VIEW, LBUILD_VIEW_INTERNAL,
 LBUILD_X, 200,
 LBUILD_Y, 200,
 LBUILD_USERFIELD, "Pathname:",
 LBUILD_SHOW, FALSE,
 NULL);
```

例2 モードを問い合わせ、ラベルビルダーを表示する

次の例は、tsol\_lbuild\_get() ルーチンを呼び出して使用中のモードを問い合わせ、tsol\_lbuild\_set() ルーチンを呼び出してラベルビルダーダイアログボックスが表示されるようにします。

```
mode = (int)tsol_lbuild_get(lbldata, LBUILD_MODE);
tsol_lbuild_set(lbldata, LBUILD_SHOW, TRUE, NULL);
```

## 例3 ModLabelData 変数を破棄する

次の例は、`tsol_lbuild_create()` を呼び出したときに返される `ModLabelData` 変数を破棄します。

```
tsol_lbuild_destroy(lbldata);
```

## ファイル

```
/usr/dt/include/Dt/ModLabel.h
```

ラベルビルダー機能用ヘッダーファイル

```
/etc/security/tsol/label_encodings
```

ラベルエンコーディングファイルには、このシステムの定義済みラベルに対する格付け名、語句、制約、および値が含まれます。

## 属性

次の属性については、`attributes(5)` を参照してください。

| 属性タイプ  | 属性値     |
|--------|---------|
| 使用条件   | SUNWtsu |
| MT レベル | MT-安全   |

## 関連項目

[label\\_encodings\(4\)](#), [attributes\(5\)](#)

『Solaris Trusted Extensions 開発ガイド』の第7章「ラベルビルダー API」

|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 名前             | labelclipping, Xbsltos, Xbcleartos – バイナリラベルの変換および指定された幅への編集 (クリッピング)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 形式             | <pre>cc [flag...] file... -ltsol -lDtTsol [library...] #include &lt;Dt/label_clipping.h&gt;  XmString Xbsltos(Display *display, const m_label_t *senslabel, Dimension width,                const XmFontList fontlist, const int flags);  XmString Xbcleartos(Display *display, const m_label_t *clearance,                    Dimension width, const XmFontList fontlist, const int flags);</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| インタフェース<br>レベル | ラベルクリッピング関数 Xbsltos() および Xbcleartos() は、廃止または互換性がなくなる可能性があります。代わりに <a href="#">label_to_str(3TSOL)</a> 関数を使用してください。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 機能説明           | <p>現在のプロセスの機密ラベルより優位にあるラベルや認可上限を変換するには、呼び出し元プロセスの、有効な特権セットの中に PRIV_SYS_TRANS_LABEL が存在する必要があります。</p> <p><i>display</i> X Window System 表示への接続を制御する構造体。</p> <p><i>senslabel</i> 変換される機密ラベル。</p> <p><i>clearance</i> 変換される認可上限。</p> <p><i>width</i> 変換されたラベルまたは認可上限の幅 (ピクセル数)。指定された幅がフルラベルより短い場合、ラベルはクリッピングされ、クリッピングした文字があることが矢印で示されます。この例では、文字は TS&lt;- の右側でクリッピングされています。クリッピングされたことを示すインジケータについては、<a href="#">sbltos(3TSOL)</a> のマニュアルページを参照してください。指定された幅が表示幅 (<i>display</i>) に等しい場合は、ラベルは表示幅の半分の幅で折り返されます。このとき、ラベルの長さは切り捨てられません。</p> <p><i>fontlist</i> フォントと文字セットのリスト。各フォントは文字セット 1 つと関連付けられています。</p> <p><i>flags</i> フラグの値は、<a href="#">label_encodings(4)</a> ファイルの中のどの語句を変換に使用するかを示しています。次のフラグ値の説明については、<a href="#">bltos(3TSOL)</a> マニュアルページを参照してください。LONG_WORDS、SHORT_WORDS、LONG_CLASSIFICATION、SHORT_CLASSIFICATION、ALL_ENTRIES、ACCESS_RELATED、VIEW_EXTERNAL、VIEW_INTERNAL、NO_CLASSIFICATION。BRACKETED は、Xbsltos() でのみ使用できる補足フラグです。次のように、機密ラベルは角括弧で囲まれます。[C]。</p> |
| 戻り値            | これらのインタフェースは、文字コード形式の変換済み機密ラベルまたは認可上限を表す複合文字列を返します。複合文字列に使用する言語とフォントは、 <i>fontlist</i> に指定され、 <i>width</i> にクリップされます。これらのインタフェースは、ラベルまたは認可上限が <a href="#">label_encodings(4)</a> ファイルに定義される有効かつ必須のタイプでない場                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

合、またはプロセスの機密ラベルより下位でなく、PRIV\_SYS\_TRANS\_LABEL 特権が表明されていない場合には、NULL を返します。

## ファイル

`/usr/dt/include/Dt/label_clipping.h`  
ラベルクリッピング用ヘッダファイル

`/etc/security/tsol/label_encodings`  
ラベルエンコーディングファイルには、このシステムの定義済みラベルに対する格付け名、語句、制約、および値が含まれます。

## 使用例

例1 許可上限を変換およびクリップする

この例では、フォントリストである `label_encodings(4)` ファイルに指定されている `long word` を使って認可上限をテキストに変換し、変換した認可上限を 72 ピクセル幅にクリップします。

```
xmstr = Xbcleartos(XtDisplay(topLevel),
&clearance, 72, fontlist, LONG_WORDS
```

## 属性

次の属性については、`attributes(5)` を参照してください。

| 属性タイプ  | 属性値     |
|--------|---------|
| 使用条件   | SUNWtsu |
| MT レベル | MT-安全   |

## 関連項目

`bltos(3TSOL)`, `label_to_str(3TSOL)`, `label_encodings(4)`, `attributes(5)`

フォントリストの作成および構造については、`XmStringDraw(3)` および `FontList(3)` を参照してください。

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |         |                                         |            |                                                                           |         |                                        |                    |                                                                                                   |               |                                                                       |                 |                                                                                  |                  |                                                                           |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|-----------------------------------------|------------|---------------------------------------------------------------------------|---------|----------------------------------------|--------------------|---------------------------------------------------------------------------------------------------|---------------|-----------------------------------------------------------------------|-----------------|----------------------------------------------------------------------------------|------------------|---------------------------------------------------------------------------|
| 名前                 | label_to_str - ラベルの、人間が読める文字列への変換                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |         |                                         |            |                                                                           |         |                                        |                    |                                                                                                   |               |                                                                       |                 |                                                                                  |                  |                                                                           |
| 形式                 | <pre>cc [flag...] file... -ltsol [library...] #include &lt;tsol/label.h&gt;  int label_to_str(const m_label_t *label, char **string,                 const m_label_str_t conversion_type, uint_t flags);</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |         |                                         |            |                                                                           |         |                                        |                    |                                                                                                   |               |                                                                       |                 |                                                                                  |                  |                                                                           |
| 機能説明               | <p>label_to_str() は、さまざまな必須ラベルタイプを人間が読める文字列に変換する単純な関数です。</p> <p>label は、変換対象の必須ラベルです。string は、変換された文字列を含む label_to_str() により割り当てられるメモリを指し示します。free(3C) を呼び出して割り当てられたメモリを解放するのは、呼び出し元の役割です。</p> <p>呼び出し元のプロセスは、生成される人間の読み取り可能な文字列への必須読み取りアクセス権を保持する必要があります。または、呼び出し元のプロセスが sys_trans_label 特権を保持する必要があります。</p> <p>conversion_type パラメータは、ラベル変換のタイプを制御します。次のように、すべての変換タイプが、すべてのラベルタイプに有効なわけではありません。</p> <table border="0"> <tr> <td style="vertical-align: top;">M_LABEL</td> <td>label を、そのタイプに基づいて、人間が読み取り可能な文字列に変換します。</td> </tr> <tr> <td style="vertical-align: top;">M_INTERNAL</td> <td>label を、公開オブジェクトに安全に格納できる内部テキスト表現に変換します。内部変換したあとで構文解析することで、同じ値に戻すことができます。</td> </tr> <tr> <td style="vertical-align: top;">M_COLOR</td> <td>管理者がラベルと関連付けたカラー名を表す文字列に、label を変換します。</td> </tr> <tr> <td style="vertical-align: top;">PRINTER_TOP_BOTTOM</td> <td>label を、米国国防情報局 (DIA) エンコーディング印刷出力スキーマ内のバナーページとトレーラーページの上部および下部ラベルとしての使用に適した、人間が読み取り可能な文字列に変換します。</td> </tr> <tr> <td style="vertical-align: top;">PRINTER_LABEL</td> <td>label を、DIA エンコーディング印刷スキーマ内のバナーページ降格警告としての使用に適した、人間が読み取り可能な文字列に変換します。</td> </tr> <tr> <td style="vertical-align: top;">PRINTER_CAVEATS</td> <td>label を、DIA エンコーディング印刷スキーマ内のバナーページの caveats セクションとしての使用に適した、人間が読み取り可能な文字列に変換します。</td> </tr> <tr> <td style="vertical-align: top;">PRINTER_CHANNELS</td> <td>label を、DIA エンコーディング印刷スキーマ内のバナーページの処理チャンネルとしての使用に適した、人間が読み取り可能な文字列に変換します。</td> </tr> </table> <p>flags パラメータは、ラベル変換を実行する際のヒントを提供します。</p> | M_LABEL | label を、そのタイプに基づいて、人間が読み取り可能な文字列に変換します。 | M_INTERNAL | label を、公開オブジェクトに安全に格納できる内部テキスト表現に変換します。内部変換したあとで構文解析することで、同じ値に戻すことができます。 | M_COLOR | 管理者がラベルと関連付けたカラー名を表す文字列に、label を変換します。 | PRINTER_TOP_BOTTOM | label を、米国国防情報局 (DIA) エンコーディング印刷出力スキーマ内のバナーページとトレーラーページの上部および下部ラベルとしての使用に適した、人間が読み取り可能な文字列に変換します。 | PRINTER_LABEL | label を、DIA エンコーディング印刷スキーマ内のバナーページ降格警告としての使用に適した、人間が読み取り可能な文字列に変換します。 | PRINTER_CAVEATS | label を、DIA エンコーディング印刷スキーマ内のバナーページの caveats セクションとしての使用に適した、人間が読み取り可能な文字列に変換します。 | PRINTER_CHANNELS | label を、DIA エンコーディング印刷スキーマ内のバナーページの処理チャンネルとしての使用に適した、人間が読み取り可能な文字列に変換します。 |
| M_LABEL            | label を、そのタイプに基づいて、人間が読み取り可能な文字列に変換します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |         |                                         |            |                                                                           |         |                                        |                    |                                                                                                   |               |                                                                       |                 |                                                                                  |                  |                                                                           |
| M_INTERNAL         | label を、公開オブジェクトに安全に格納できる内部テキスト表現に変換します。内部変換したあとで構文解析することで、同じ値に戻すことができます。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |         |                                         |            |                                                                           |         |                                        |                    |                                                                                                   |               |                                                                       |                 |                                                                                  |                  |                                                                           |
| M_COLOR            | 管理者がラベルと関連付けたカラー名を表す文字列に、label を変換します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |         |                                         |            |                                                                           |         |                                        |                    |                                                                                                   |               |                                                                       |                 |                                                                                  |                  |                                                                           |
| PRINTER_TOP_BOTTOM | label を、米国国防情報局 (DIA) エンコーディング印刷出力スキーマ内のバナーページとトレーラーページの上部および下部ラベルとしての使用に適した、人間が読み取り可能な文字列に変換します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |         |                                         |            |                                                                           |         |                                        |                    |                                                                                                   |               |                                                                       |                 |                                                                                  |                  |                                                                           |
| PRINTER_LABEL      | label を、DIA エンコーディング印刷スキーマ内のバナーページ降格警告としての使用に適した、人間が読み取り可能な文字列に変換します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |         |                                         |            |                                                                           |         |                                        |                    |                                                                                                   |               |                                                                       |                 |                                                                                  |                  |                                                                           |
| PRINTER_CAVEATS    | label を、DIA エンコーディング印刷スキーマ内のバナーページの caveats セクションとしての使用に適した、人間が読み取り可能な文字列に変換します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |         |                                         |            |                                                                           |         |                                        |                    |                                                                                                   |               |                                                                       |                 |                                                                                  |                  |                                                                           |
| PRINTER_CHANNELS   | label を、DIA エンコーディング印刷スキーマ内のバナーページの処理チャンネルとしての使用に適した、人間が読み取り可能な文字列に変換します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |         |                                         |            |                                                                           |         |                                        |                    |                                                                                                   |               |                                                                       |                 |                                                                                  |                  |                                                                           |

DEF\_NAMES デフォルト名が優先されます。  
 SHORT\_NAMES 短形式名が定義されている箇所では、短形式名が優先されます。  
 LONG\_NAMES 長形式名が優先されます。

戻り値 label\_to\_str() は、成功時にはゼロ (0) を返します。それ以外の場合には、-1 が返されます。また、エラーを示す `errno` が設定されて、文字列ポインターが NULL に設定されます。

エラー 次の場合に、label\_to\_str() 関数は失敗します。

EINVAL パラメータが無効です。  
 ENOTSUP システムがラベル変換をサポートしません。  
 ENOMEM システムの物理的制限を超過したために、size バイトのメモリーを割り当てることができません。

属性 次の属性については、attributes(5) を参照してください。

| 属性タイプ       | 属性値                 |
|-------------|---------------------|
| 使用条件        | SUNWtsu             |
| MT レベル      | MT-安全               |
| インタフェースの安定性 | 後述の「注意事項」および「警告」を参照 |

関連項目 free(3C), [str\\_to\\_label\(3TSOL\)](#), [label\\_encodings\(4\)](#), [attributes\(5\)](#), [labels\(5\)](#)

『Solaris Trusted Extensions 開発ガイド』の「label\_to\_str 関数の使用」

注意事項 label\_to\_str() は「安定」です。DIA エンコーディングスキーマ関連の変換タイプは「標準」です。「標準」については、[label\\_encodings\(4\)](#) を参照してください。返される文字列は「未定義」であり、固有の `label_encodings` ファイルに依存しています。変換タイプ `INTERNAL` は「不安定」ですが、[str\\_to\\_label\(3TSOL\)](#) への入力として常に使用可能です。

警告 これらの変換の多くは、DIA ラベルエンコーディングスキーマに依存しています。このため、その他のラベルスキーマでは有効ではない場合があります。

名前 m\_label, m\_label\_alloc, m\_label\_dup, m\_label\_free – m\_label 関数

形式 cc [*flag...*] *file...* -ltsol [*library...*]

```
#include <tsol/label.h>
```

```
m_label_t *m_label_alloc(const m_label_type_t label_type);
```

```
int m_label_dup(m_label_t **dst, const m_label_t *src);
```

```
void m_label_free(m_label_t *label);
```

機能説明 m\_label\_alloc() 関数は、新規ラベル用の資源を割り当てます。label\_type は、新たに割り当てられたラベルのタイプを定義します。ラベルタイプを次に示します。

MAC\_LABEL 必須アクセス制御 (MAC) ラベル。

USER\_CLEAR ユーザーの認可上限。

m\_label\_dup() 関数は、新規 dst ラベル用の資源を割り当てます。この関数は、src ラベルの正確なコピーである、割り当てられたラベルへのポインタを返します。呼び出し元は、m\_label\_free() を呼び出して、割り当てられた資源を解放します。

m\_label\_free() 関数は、以前に割り当てられたラベルに関連付けられている資源を解放します。

戻り値 成功時に、m\_label\_alloc() 関数は、新たに割り当てられたラベルへのポインタを返します。それ以外の場合、m\_label\_alloc() は NULL を返し、エラーを示す errno を設定します。

成功時に、m\_label\_dup() 関数はゼロ (0) を返します。それ以外の場合、-1 が返され、エラーを示す errno が設定されます。

エラー EINVAL 無効なパラメータです。

ENOMEM システムの物理的制限を超過したために、size バイトのメモリーを割り当てることができません。

属性 次の属性については、attributes(5) を参照してください。

| 属性タイプ       | 属性値 |
|-------------|-----|
| MT レベル      | 安全  |
| インタフェースの安定性 | 安定  |

関連項目 label\_to\_str(3TSOL), str\_to\_label(3TSOL), label\_encodings(4), attributes(5), labels(5)

『Solaris Trusted Extensions 開発ガイド』の「ラベル付けされている環境で印刷サービスが実行されているか否かの判別」

名前 sbltos, sbsltos, sbclearantos – バイナリラベルを標準的な文字形式のラベルに変換する

形式 `cc [flag...] file... -ltsol [library...]`

```
#include <tsol/label.h>
```

```
char *sbsltos(const m_label_t *label, const int len);
```

```
char *sbclearantos(const m_label_t *clearance, const int len);
```

インタフェース レベル sbsltos() および sbclearantos() 関数は、廃止または互換性がなくなる可能性があります。代わりに `label_to_str(3TSOL)` 関数を使用してください。

機能説明 呼び出し元プロセスは、現在のプロセスの機密ラベルより優位にあるラベルについてラベル変換を実行するには、有効な特権セットの中に `PRIV_SYS_TRANS_LABEL` を保持している必要があります。

これらの関数は、バイナリラベルを標準的な文字列に変換し、文字列は `len` に指定される印刷可能な文字数にクリッピングされます。変換された文字列の文字数が `len` より長い場合は、クリッピングが必要です。クリップとは、指定された文字数より2文字少なくなるまでラベルを右方向に切り捨てることです。機密ラベルと認可上限にはクリッピングされたことを示すインジケータ「<-」が追加されます。文字形式のラベルの先頭には格付け名が指定され、ラベルの残りの部分を構成する語句のリストとの間は単一の空白文字で区切られます。バイナリラベルは正しい定義済みタイプを持ち、プロセスの機密ラベルより下位である必要があります。`len` が0 (ゼロ) のときは、クリッピングしないで文字列全体を返します。

`sbsltos()` は、バイナリ機密ラベルを `Word` の長形式と格付け名の短形式を使うクリップ文字列に変換します。`len` が最短文字数である3文字より短い場合は、変換は失敗します。

`sbclearantos()` は、バイナリ認可上限を `Word` の長形式と格付け名の短形式を使うクリップ文字列に変換します。`len` が最短文字数である3文字より短い場合は、変換は失敗します。認可上限の変換結果は、機密ラベルの変換結果と同じでないことがあります。これらの関数は、`label_encodings` ファイルの別々のテーブルを使用します。各テーブルの `Word` と制約条件は異なっている場合があります。

戻り値 これらのルーチンは、変換結果を含む静的に割り当てられた文字列へのポインタを返します。何らかの原因で変換に失敗した場合は、`(char *)0` を返します。

## 使用例

`sbsltos()` 次のような機密ラベルの場合、

```
UN TOP/MIDDLE/LOWER DRAWER
```

10文字にクリッピングすると次のようになります。

```
UN TOP/M<-
```

`sbclearantos()` 次のような認可上限の場合、

UN TOP/MIDDLE/LOWER DRAWER

10 文字にクリッピングすると次のようになります。

UN TOP/M<-

#### プロセス属性

VIEW\_EXTERNAL または VIEW\_INTERNAL フラグが指定されないと、ADMIN\_LOW ラベルと ADMIN\_HIGH ラベルの変換は、ラベル表示プロセス属性のフラグによって制御されます。ラベル表示プロセス属性のフラグが定義されていない場合は、label\_encodings ファイルに設定されているラベル表示によって変換が制御されます。値 External は、ADMIN\_LOW ラベルと ADMIN\_HIGH ラベルが label\_encodings ファイルに定義されている最下位ラベルと最上位ラベルに割り当てられるように指定します。値 Internal は、ADMIN\_LOW ラベルと ADMIN\_HIGH ラベルが label\_encodings ファイルに指定されている admin low name 文字列と admin high name 文字列に変換されるように指定します。このような名前が指定されていない場合は、文字列「ADMIN\_LOW」と「ADMIN\_HIGH」が使用されます。

#### ファイル

/etc/security/tsol/label\_encodings

ラベルエンコーディングファイルには、このシステムの定義済みラベルに対する格付け名、語句、制約、および値が含まれます。

#### 属性

次の属性については、attributes(5) を参照してください。

| 属性タイプ  | 属性値                |
|--------|--------------------|
| 使用条件   | SUNWtsu            |
| 安定性    | 廃止または互換性がなくなる可能性あり |
| MT レベル | 危険                 |

#### 関連項目

[label\\_to\\_str\(3TSOL\)](#), [attributes\(5\)](#), [labels\(5\)](#)

#### 注意事項

これらの関数は旧式であり、移植を容易にする目的で維持されています。これらは、将来の Solaris Trusted Extensions リリースでは削除される可能性があります。

#### 警告

これらの関数はすべて、静的に割り当てられた文字列記憶領域を共有しています。MT-安全ではありません。これらの関数を呼び出すたびに、文字列は新しく変換された文字列で上書きされます。

名前 setlabel – 対応する機密ラベルを持つゾーンへのファイルの移動

形式 `cc [flag...] file... -ltsol [library...]`

```
#include <tsol/label.h>
```

```
int setlabel(const char *path, const m_label_t *label_p);
```

## 機能説明

*path* により指定されたファイルは、*label\_p* に対応するゾーンのルートディレクトリを基準とする新しいパス名に移動することで、再度ラベル付けされます。移動元および移動先のファイルシステムが、基盤をなす同一のファイルシステムからループバックマウントされている場合、ファイルの名前が変更されます。それ以外の場合、ファイルはコピーされて、移動元のディレクトリから削除されます。

この関数により、次のポリシーチェックが実行されます。

- *label\_p* の機密レベルが既存の機密レベルに等しい場合、ファイルは移動されません。
- 対応するディレクトリが移動先のゾーン内に存在しない場合、またはディレクトリは存在するが、*label\_p* 以外のラベルが設定されている場合、ファイルは移動されません。また、移動先ディレクトリにファイルが既に存在する場合も、ファイルは移動されません。
- 既存のファイルの機密ラベルが呼び出し元プロセスのラベルと等価でなく、呼び出し元が大域ゾーン内にない場合、ファイルは移動されません。呼び出し元が大域ゾーン内に存在する場合、既存のファイルラベルは、ラベル付けされたゾーン (ADMIN\_LOW または ADMIN\_HIGH 以外) に存在する必要があります。
- 呼び出し元のプロセスが移動元と移動先の両方のディレクトリに書き込みアクセス権を持たない場合、呼び出し元プロセスは有効な特権セット内に PRIV\_FILE\_DAC\_WRITE を保持している必要があります。
- *label\_p* の機密ラベルが、既存の機密ラベルへの読み取り専用アクセス権を提供する場合 (昇格)、ユーザーは `solaris.label.file.upgrade` 承認を保持している必要があります。また、現在のゾーンがラベル付けされたゾーンである場合は、ゾーンの設定時に PRIV\_FILE\_UPGRADE\_SL 特権が割り当てられている必要があります。
- *label\_p* の機密ラベルが既存の機密ラベルへのアクセスを提供しない場合 (降格)、呼び出し元のユーザーは `solaris.label.file.downgrade` 承認を保持している必要があります。また、現在のゾーンがラベル付けされたゾーンである場合は、ゾーンの設定時に PRIV\_FILE\_DOWNGRADE\_SL 特権が割り当てられている必要があります。
- 呼び出し元のプロセスが大域ゾーン内に存在せず、ユーザーが `solaris.label.range` 承認を保持しない場合、*label\_p* はユーザーのラベル範囲内およびシステム認可範囲内に存在する必要があります。
- 既存のファイルが使用中の (トランキルでない) 場合、ファイルは移動されません。この使用中かどうかのチェックでは、競合状態もリモートファイルアクセスも検査されません。

シェルスクリプト `/etc/security/tsol/relabel` をカスタマイズすることで、追加ポリシー制約を実装できます。このファイルのコメントを参照してください。

## 戻り値

`setlabel()` は、次の値を返します。

- 0 成功の場合。
- 1 失敗の場合。 `errno` を設定してエラーを示します。

## エラー

これらの条件のいずれかが当てはまる場合、`setlabel()` は失敗します。ファイルは変更されません。

- EACCES** *path* のパス接頭辞の構成要素に対する検索権限が拒否されています。
- 呼び出し元のプロセスは、パスの最終構成要素への必須書き込みアクセス権を保持しません。パスの最終構成要素の機密ラベルは、呼び出し元プロセスの機密ラベルより優位ではなく、呼び出し元プロセスは有効な権限セット内に `PRIV_FILE_MAC_WRITE` を保持しないためです。
- EBUSY** *path* の最終構成要素へのオープンファイル記述子の参照が存在します。
- ECONNREFUSED** ラベルデーモンへの接続を確立できませんでした。
- EEXIST** 同名のファイルが移動先のディレクトリに存在します。
- EINVAL** ラベルデーモンが不正なパラメータを受け取りました。
- EISDIR** 既存のファイルは、ディレクトリです。
- ELOOP** *path* を変換するときに検出されたシンボリックリンクの数が多すぎます。
- EMLINK** 既存のファイルは、別のファイルにハードリンクされています。
- ENAMETOOLONG** パス引数の長さが `PATH_MAX` を超えています。
- ENOENT** *path* で参照されているファイルが存在しません。
- EROFS** ファイルシステムは読み取り専用であるか、そのラベルが `ADMIN_LOW` または `ADMIN_HIGH` です。

## 属性

次の属性については、`attributes(5)` を参照してください。

| 属性タイプ  | 属性値      |
|--------|----------|
| 使用条件   | SUNWcslr |
| MT レベル | MT-安全    |

| 属性タイプ       | 属性値 |
|-------------|-----|
| インタフェースの安定性 | 安定  |

## 関連項目

attributes(5)

『Solaris Trusted Extensions 開発ガイド』の「ファイル機密ラベルの設定」

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                        |                                                                                                                                                                                                          |                            |                                                                                                                      |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|----------------------------------------------------------------------------------------------------------------------|
| 名前                         | stobl, stobsl, stobclear – 文字形式のラベルのバイナリラベルへの変換                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                        |                                                                                                                                                                                                          |                            |                                                                                                                      |
| 形式                         | <pre>cc [flag...] file... -ltsol [library...] #include &lt;tsol/label.h&gt;  int stobsl(const char *string, m_label_t *label, const int flags, int *error); int stobclear(const char *string, m_label_t *clearance, const int flags,               int *error);</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                        |                                                                                                                                                                                                          |                            |                                                                                                                      |
| インタフェース<br>レベル             | stobl() および stobclear() 関数は、廃止または互換性がなくなる可能性があります。代わりに、 <a href="#">str_to_label(3TSOL)</a> 関数を使用してください。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                        |                                                                                                                                                                                                          |                            |                                                                                                                      |
| 機能説明                       | <p>呼び出しプロセスは、プロセスの機密ラベルより優位にある文字形式のラベルについてラベル変換を実行するには、有効な特権セット内に <code>PRIV_SYS_TRANS_LABEL</code> を保持する必要があります。</p> <p><code>stobl</code> 関数は、文字形式のラベルをバイナリラベルに変換します。また、その既存の値を基準に、既存のバイナリラベルを増分または減分して新しいバイナリラベルを生成し、既存のバイナリラベルを変更します。</p> <p>入力する文字形式のラベル文字列の汎用形式は次のとおりです。</p> <pre>[ + ] classification name [ [ +   - ] word ...</pre> <p>語の前後のスペースは無視されます。フィールド間はスペース、「/」(スラッシュ)、または「,」(カンマ)で区切ります。大文字と小文字は区別されません。<code>string</code> の先頭が + または - の場合、<code>string</code> は既存のラベルを変更したものと解釈されます。<code>string</code> の先頭が格付け名で、そのあとに + または - が続く場合は、新しい格付けが使用され、古いラベルの残りの部分は保管されて、<code>string</code> に指定されるように変更されます。+ は、<code>Word</code> を追加して既存のラベルを変更することを示します。- は、<code>Word</code> を削除して既存のラベルを変更することを示します。結果として生成されるバイナリラベル <code>label</code> の中では、<code>string</code> 中のエラーが最大限訂正されています。</p> <p><code>stobl</code> 関数は、文字列の先頭が <code>0x</code> で、<code>flags</code> の中に <code>NEW_LABEL</code>、<code>NO_CORRECTION</code> のいずれかが指定されているときは、16進ラベル表現もバイナリラベルに変換します(<a href="#">hextob(3TSOL)</a> を参照)。</p> <p><code>flags</code> は次の値をとります。</p> <table border="0"> <tr> <td style="vertical-align: top;"><code>NEW_LABEL</code></td> <td><code>label</code> の内容が使用されておらず、関連タイプのラベルとしてフォーマットされています。また、<code>ADMIN_LOW</code> であると仮定して変更を行います。<code>NEW_LABEL</code> が存在しない場合、プロセスの機密ラベルより下位にある正しいタイプの定義済みラベルとして、<code>label</code> の妥当性が検査されます。</td> </tr> <tr> <td style="vertical-align: top;"><code>NO_CORRECTION</code></td> <td>文字形式のラベル <code>string</code> 中にエラーがあっても、訂正は行われません。<code>string</code> は完全で、<code>label_encodings</code> ファイルで必要とされ</td> </tr> </table> | <code>NEW_LABEL</code> | <code>label</code> の内容が使用されておらず、関連タイプのラベルとしてフォーマットされています。また、 <code>ADMIN_LOW</code> であると仮定して変更を行います。 <code>NEW_LABEL</code> が存在しない場合、プロセスの機密ラベルより下位にある正しいタイプの定義済みラベルとして、 <code>label</code> の妥当性が検査されます。 | <code>NO_CORRECTION</code> | 文字形式のラベル <code>string</code> 中にエラーがあっても、訂正は行われません。 <code>string</code> は完全で、 <code>label_encodings</code> ファイルで必要とされ |
| <code>NEW_LABEL</code>     | <code>label</code> の内容が使用されておらず、関連タイプのラベルとしてフォーマットされています。また、 <code>ADMIN_LOW</code> であると仮定して変更を行います。 <code>NEW_LABEL</code> が存在しない場合、プロセスの機密ラベルより下位にある正しいタイプの定義済みラベルとして、 <code>label</code> の妥当性が検査されます。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                        |                                                                                                                                                                                                          |                            |                                                                                                                      |
| <code>NO_CORRECTION</code> | 文字形式のラベル <code>string</code> 中にエラーがあっても、訂正は行われません。 <code>string</code> は完全で、 <code>label_encodings</code> ファイルで必要とされ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                        |                                                                                                                                                                                                          |                            |                                                                                                                      |

るすべてのラベルコンポーネントを含んでいなくてはなりません。NO\_CORRECTION フラグには、NEW\_LABEL フラグも含まれます。

0 (ゼロ) デフォルトのアクションが実行されます。

error は、関数が不成功の場合にのみ設定される戻りパラメータです。

stobsl() は、文字形式の機密ラベルをバイナリ機密ラベルに変換し、戻りパラメータ *label* の中に結果を格納します。

*flags* は、NEW\_LABEL、NO\_CORRECTION、または 0 (ゼロ) になります。NO\_CORRECTION が指定されている場合を除けば、ラベルは、最下位の格付けと *label\_encodings* ファイルに指定される初期のコンパートメントセットより優位になり、*label\_encodings* ファイルで必要とされるが *string* 内には存在しない他のラベルコンポーネントを含むように訂正されます。

stobclear() は、文字形式の認可上限文字列をバイナリ認可上限に変換し、結果を戻りパラメータ *clearance* の中に格納します。

*flags* は、NEW\_LABEL、NO\_CORRECTION、または 0 (ゼロ) になります。NO\_CORRECTION が指定されている場合を除けば、ラベルは、最下位の格付けと *label\_encodings* ファイルに指定される初期のコンポーネントセットより優位になり、*label\_encodings* ファイルで必要とされるが *string* 内には存在しない他のラベルコンポーネントを含むように訂正されます。認可上限の変換結果は、機密ラベルの変換結果と同じにならないことがあります。これらの関数は、*label\_encodings* ファイルの異なるテーブルを使用します。各テーブルの Word と制約条件は異なっている場合があります。

戻り値 これらの関数は次の値を返します。

- 1 変換が成功し、有効なバイナリラベルが返された場合。
- 0 エラーが発生した場合。error は、エラーのタイプを示します。

エラー これらの関数がゼロを返す場合は、error には次のいずれかの値が含まれます。

- 1 *label\_encodings* ファイルにアクセスできませんでした。
- 0 ラベル *label* がこの変換に有効でなく、NEW\_LABEL または NO\_CORRECTION フラグが指定されていないか、ラベル *label* がプロセスの *sensitivity label* より下位でなく、プロセスが有効な特権セットの中に PRIV\_SYS\_TRANS\_LABEL を持っていないか。
- >0 文字形式のラベル *string* にエラーがあります。error は、どこで変換エラーが発生したかを示す *string* への索引で、1 を基準にしています。

ファイル

/etc/security/tsol/*label\_encodings*

ラベルエンコーディングファイルには、このシステムの定義済みラベルに対する格付け名、語句、制約、および値が含まれます。

属性 次の属性については、`attributes(5)` を参照してください。

| 属性タイプ  | 属性値                |
|--------|--------------------|
| 使用条件   | SUNWtsu            |
| 安定性レベル | 廃止または互換性がなくなる可能性あり |
| MT レベル | MT-安全              |

関連項目 [blcompare\(3TSOL\)](#), [hextob\(3TSOL\)](#), [str\\_to\\_label\(3TSOL\)](#), [attributes\(5\)](#)

注意事項 これらの関数は旧式であり、移植を容易にする目的で維持されています。Solaris Trusted Extensions の将来のリリースでは、これらの関数が削除される可能性があります。

`label_encodings` ファイルに定義される `ADMIN_LOW name` 文字列と `ADMIN_HIGH name` 文字列に加えて、文字列「`ADMIN_LOW`」と「`ADMIN_HIGH`」は常に文字形式のラベルとして受け入れられ、それぞれ、適切な `ADMIN_LOW` ラベルと `ADMIN_HIGH` ラベルに変換されます。

既存の `ADMIN_LOW` ラベルの変更は、`NEW_LABEL` を指定したのと同じように働き、ラベルは `label_encodings` ファイルに指定される最下位ラベルで開始するように強制されます。

既存の `ADMIN_HIGH` ラベルの変更は、定義済みの最上位の格付けと `label_encodings` ファイルに指定される定義済みのすべてのコンパートメントを表すラベル変更の試みとして処理されます。

`NO_CORRECTION` フラグは、文字形式のラベルが完全かつ正確でなくてはならないときに使用されるので、バイナリ形式への(バイナリ形式からの)変換の結果、同等な文字形式のラベルが生成されます。

名前 str\_to\_label – 人間が読み取り可能な文字列からラベルへの構文解析

形式 cc [*flag...*] *file...* -ltsol [*library...*]

```
#include <tsol/label.h>
```

```
int str_to_label(const char *string, m_label_t **label,
 const m_label_type_t label_type, uint_t flags, int *error);
```

## 機能説明

str\_to\_label() は、人間が読み取り可能な文字列を構文解析して、要求されたタイプのラベルにする単純な関数です。

*string* は、構文解析する文字列です。*string* が M\_INTERNAL タイプの label\_to\_str() 変換の結果である場合、*flags* は無視され、以前に構文解析されたラベルがすべて置換されます。

\**label* が NULL の場合、str\_to\_label() は *label* に資源を割り当て、*string* を構文解析する前に要求された *label\_type* にラベルを初期化します。

\**label* が NULL でない場合、ラベルは以前に構文解析されたラベルの結果である必須ラベルへのポインタになり、*label\_type* は無視されます。タイプを反映する操作の場合、構文解析に使用されるタイプは *label* から派生します。

*flags* が L\_MODIFY\_EXISTING である場合、構文解析された文字列を使ってこのラベルを変更できます。

*flags* が L\_NO\_CORRECTION である場合、以前に構文解析されたラベルが置換されず。構文解析アルゴリズムは、欠落した要素を文字列から推測して、有効なラベルを作成しようとはしません。

*flags* が L\_DEFAULT の場合は、以前に構文解析されたラベルが置換され、構文解析アルゴリズムによって、*string* の要素から有効なラベルを導き出すための最大限の動作が試みられます。

呼び出し元は、m\_label\_free() 関数を呼び出して、割り当てられた資源を解放します。*label\_type* は、新たに割り当てられたラベルのタイプを定義します。ラベルタイプを次に示します。

MAC\_LABEL 文字列は、必須アクセス制御 (MAC) ラベルとして変換されます。

USER\_CLEAR 文字列は、ユーザーにアクセスが許可されるラベルのもっとも低い上限を表すラベルとして変換されます。

*error* が NULL の場合、EINVAL の追加エラー情報は返しません。呼び出し元プロセスは、*label* および人間が読み取ることのできる *string* への必須読み取りアクセス権を保持する必要があります。または、呼び出し元プロセスは、sys\_trans\_label 特権を保持している必要があります。

マニフェスト定数 ADMIN\_HIGH および ADMIN\_LOW は、Trusted Extensions ポリシーの admin\_high および admin\_low ラベル値に対応する、人間が読み取り可能な文字列です。labels(5) を参照してください。

**戻り値** 成功時に、`str_to_label()` 関数はゼロ (0) を返します。それ以外の場合は、-1 が返され、エラーを示す `errno` が設定されます。また、`error` が `EINVAL` の追加情報を提供します。それ以外の場合、`error` は、文字列構文解析が失敗したポイントへのゼロから始まるインデックスになります。

**エラー** 次の場合に、`str_to_label()` 関数は失敗します。

**EINVAL** 無効なパラメータ。 `M_BAD_STRING` は、`string` を構文解析できなかったことを示します。 `M_BAD_LABEL` は、渡されたラベルでエラーが発生したことを示します。

**ENOTSUP** システムがラベル変換をサポートしません。

**ENOMEM** システムの物理的制限を超過したために、`size` バイトのメモリーを割り当てることができません。

**属性** 次の属性については、`attributes(5)` を参照してください。

| 属性タイプ       | 属性値                 |
|-------------|---------------------|
| MT レベル      | MT-安全               |
| インタフェースの安定性 | 後述の「注意事項」および「警告」を参照 |

**関連項目** [label\\_to\\_str\(3TSOL\)](#), [m\\_label\(3TSOL\)](#), [label\\_encodings\(4\)](#), [attributes\(5\)](#), [labels\(5\)](#)

『Solaris Trusted Extensions 開発ガイド』の「プリンタのラベル範囲に対するラベル要求の検査」

**注意事項** `str_to_label()` は「安定」です。米国国防情報局 (DIA) のエンコーディングスキーマに関連する構文解析タイプは、「標準」です。「標準」は、[label\\_encodings\(4\)](#) に指定されています。

**警告** 構文解析規則の多くは、DIA ラベルエンコーディングスキーマに依存しています。このため、その他のラベルスキーマでは規則が有効でない場合があります。

名前 `tsol_getrhtype` – トラストドネットワークのホストタイプの取得

形式 `cc [flag...] file... -ltsnet [library...]`

```
#include <libtsnet.h>
```

```
tsol_host_type_t tsol_getrhtype(char *hostname);
```

機能説明 `tsol_getrhtype()` 関数はカーネルレベルのネットワーク情報を照会して、指定された *hostname* に関連付けられているホストタイプを識別します。*hostname* には、通常のホスト名、IP アドレス、またはネットワークワイルドカードアドレスを指定できます。

戻り値 返される値は、型定義 `tsol_host_type_t` に定義されている列挙型の 1 つになります。現在のところ、これらの型には `UNLABELED` および `SUN_CIPSO` があります。

属性 次の属性については、`attributes(5)` を参照してください。

| 属性タイプ  | 属性値     |
|--------|---------|
| 使用条件   | SUNWcsl |
| MT レベル | MT-安全   |

ファイル `/etc/security/tsol/tnrhdb` トラストドネットワーク遠隔ホストデータベース

関連項目 [tnrhdb\(4\)](#), [attributes\(5\)](#)

『Solaris Trusted Extensions 開発ガイド』の「遠隔ホストタイプの取得」

参照

Xライブラリ拡張

名前 XTSOLgetClientAttributes - クライアントに関連付けられたすべてのラベル属性の取得

形式 

```
#include <X11/extensions/Xtsol.h>

Status XTSOLgetClientAttributes(display, windowid, clientattr);

Display *display;
XID windowid;
XTsolClientAttributes *clientattrp;
```

機能説明 XTSOLgetClientAttributes() は、クライアントに関連付けられたすべてのラベル属性を 1 回の呼び出しで取得する場合に使用します。この属性には、プロセス ID、ユーザー ID、IP アドレス、監査フラグ、およびセッション ID が含まれます。

パラメータ *display* Display 構造体へのポインタを指定します。これは、XOpenDisplay() から返されます。

*windowid* X クライアントのウィンドウ ID を指定します。

*clientattrp* クライアントは、XTsolClientAttributes 構造体へのポインタを提供する必要があります。

属性 次の属性については、attributes(5) を参照してください。

| 属性タイプ  | 属性値      |
|--------|----------|
| 使用条件   | SUNWxwts |
| MT レベル | MT-危険    |

戻り値 なし

エラー BadAccess 特権がありません。

BadValue 有効なクライアントではありません。

関連項目 [XTSOLgetPropAttributes\(3XTSOL\)](#), [XTSOLgetResAttributes\(3XTSOL\)](#)

|       |                                                                                                                                                                                                                                                                   |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 名前    | XTSOLgetPropAttributes – ウィンドウのプロパティに関連付けられたラベル属性の取得                                                                                                                                                                                                              |
| 形式    | <pre>#include &lt;X11/extensions/Xtsol.h&gt;  Status XTSOLgetPropAttributes(<i>display</i>, <i>window</i>, <i>property</i>, <i>propattrp</i>);  Display *<i>display</i>; Window <i>window</i>; Atom <i>property</i>; XTSOLPropAttributes *<i>propattrp</i>;</pre> |
| 機能説明  | クライアントには、PRIV_WIN_DAC_READ および PRIV_WIN_MAC_READ 特権が必要です。XTSOLgetPropAttributes() は、ウィンドウのプロパティに関連付けられたラベル属性を 1 回の呼び出しで取得する場合に使用します。この属性には、UID および機密ラベルが含まれます。                                                                                                    |
| パラメータ | <p><i>display</i>     Display 構造体へのポインタを指定します。これは、XOpenDisplay() から返されます。</p> <p><i>window</i>     ウィンドウシステムオブジェクトの ID を指定します。</p> <p><i>property</i>     プロパティアトムを指定します。</p> <p><i>propattrp</i>     クライアントは、XTSOLPropAttributes へのポインタを提供する必要があります。</p>         |
| 属性    | 次の属性については、attributes(5) を参照してください。                                                                                                                                                                                                                                |

| 属性タイプ  | 属性値      |
|--------|----------|
| 使用条件   | SUNWxwts |
| MT レベル | MT-危険    |

|      |                                                                                                                                                                        |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 戻り値  | なし                                                                                                                                                                     |
| エラー  | <p>BadAccess     特権がありません。</p> <p>BadWindow     有効なウィンドウではありません。</p> <p>BadAtom     有効なアトムではありません。</p>                                                                 |
| 関連項目 | <p><a href="#">XTSOLgetClientAttributes(3XTSOL)</a>, <a href="#">XTSOLgetResAttributes(3XTSOL)</a></p> <p>『Solaris Trusted Extensions 開発ガイド』の「ウィンドウの多インスタンス化情報の設定」</p> |

名前 XTSOLgetPropLabel - ウィンドウのプロパティーに関連付けられたラベルの取得  
形式

```
#include <X11/extensions/Xtsol.h>
```

```
Status XTSOLgetPropLabel(display, window, property, sl);
```

```
Display *display;
Window window;
Atom property;
m_label_t *sl;
```

機能説明 クライアントには、PRIV\_WIN\_DAC\_READ および PRIV\_WIN\_MAC\_READ 特権が必要です。XTSOLgetPropLabel() は、ウィンドウのプロパティーに関連付けられた機密ラベルの取得に使用されます。

パラメータ

*display* Display 構造体へのポインタを指定します。これは、XOpenDisplay() から返されます。

*window* 取得するプロパティーのラベルを保持するウィンドウの ID を指定します。

*property* プロパティーアトムを指定します。

*sl* 指定したプロパティーの現在のラベルである機密ラベルを返します。

属性 次の属性については、attributes(5) を参照してください。

| 属性タイプ  | 属性値      |
|--------|----------|
| 使用条件   | SUNWxwts |
| MT レベル | MT-危険    |

戻り値 なし

エラー

BadAccess 特権がありません。

BadWindow 有効なウィンドウではありません。

BadAtom 有効なアトムではありません。

関連項目 [XTSOLgetPropAttributes\(3XTSOL\)](#), [XTSOLsetPropLabel\(3XTSOL\)](#)

『Solaris Trusted Extensions 開発ガイド』の「ウィンドウの多インスタンス化情報の設定」

|       |                                                                                                                                                                                                                                                                                                                                          |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 名前    | XTSOLgetPropUID – ウィンドウのプロパティーに関連付けられた UID の取得                                                                                                                                                                                                                                                                                           |
| 形式    | <pre>#include &lt;X11/extensions/Xtsol.h&gt;  Status XTSOLgetPropUID (display, window, property, uidp); Display *display; Window window; Atom property; uid_t *uidp;</pre>                                                                                                                                                               |
| 機能説明  | クライアントには、PRIV_WIN_DAC_READ および PRIV_WIN_MAC_READ 特権が必要です。XTSOLgetPropUID() は、ウィンドウのプロパティーの所有権を取得します。クライアントは、これを使用して、それ自体が作成したのではないオブジェクトの所有権を取得できます。                                                                                                                                                                                     |
| パラメータ | <p><i>display</i>    Display 構造体へのポインタを指定します。これは、XOpenDisplay() から返されます。</p> <p><i>window</i>    取得するプロパティーの UID を保持するウィンドウの ID を指定します。</p> <p><i>property</i>    プロパティーアトムを指定します。</p> <p><i>uidp</i>    指定したプロパティーの現在の UID である UID を返します。クライアントは、uid_t タイプの記憶領域を提供し、この記憶領域のアドレスを関数の引数として渡す必要があります。クライアントは、uid_t へのポインタを提供する必要があります。</p> |
| 属性    | 次の属性については、attributes(5) を参照してください。                                                                                                                                                                                                                                                                                                       |

| 属性タイプ  | 属性値      |
|--------|----------|
| 使用条件   | SUNWxwts |
| MT レベル | MT-危険    |

|      |                                                                                                                                                                |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 戻り値  | なし                                                                                                                                                             |
| エラー  | <p>BadAccess    特権がありません。</p> <p>BadWindow    有効なウィンドウではありません。</p> <p>BadAtom    有効なアトムではありません。</p>                                                            |
| 関連項目 | <p><a href="#">XTSOLgetPropAttributes(3XTSOL)</a>, <a href="#">XTSOLsetPropUID(3XTSOL)</a></p> <p>『Solaris Trusted Extensions 開発ガイド』の「ウィンドウの多インスタンス化情報の設定」</p> |

**名前** XTSOLgetResAttributes – ウィンドウまたはピクセルマップに関連付けられたすべてのラベル属性の取得

**形式**

```
#include <X11/extensions/Xtsol.h>

Status XTSOLgetResAttributes(display, object, type, winattrp);

Display *display;
XID object;
ResourceType type;
XTSOLResAttributes *winattrp;
```

**機能説明** クライアントには、PRIV\_WIN\_DAC\_READ および PRIV\_WIN\_MAC\_READ 特権が必要です。XTSOLgetResAttributes() は、関連付けられたすべてのラベル属性を1回の呼び出しで取得する場合に使用します。この属性には、UID、機密ラベル、およびワークステーション所有者が含まれます。

**パラメータ**

*display* Display 構造体へのポインタを指定します。これは、XOpenDisplay() から返されます。

*object* ウィンドウシステムオブジェクトの ID を指定します。指定可能なウィンドウシステムオブジェクトは、ウィンドウとピクセルマップです。

*type* アクセスしようとしている資源のタイプを指定します。指定可能な値は IsWindow および IsPixmap です。

*winattrp* クライアントは、XTSOLResAttributes へのポインタを提供する必要があります。

**属性** 次の属性については、attributes(5) を参照してください。

| 属性タイプ  | 属性値      |
|--------|----------|
| 使用条件   | SUNWxwts |
| MT レベル | MT-危険    |

**戻り値** なし

**エラー**

BadAccess 特権がありません。

BadWindow 有効なウィンドウではありません。

BadPixmap 有効なピクセルマップではありません。

BadValue 有効なタイプではありません。

**関連項目** [XTSOLgetClientAttributes\(3XTSOL\)](#), [XTSOLgetPropAttributes\(3XTSOL\)](#)

## 『Solaris Trusted Extensions 開発ガイド』の「ウィンドウ属性の取得」

名前 XTSOLgetResLabel – ウィンドウ、ピクセルマップ、またはカラーマップに関連付けられたラベルの取得

形式 

```
#include <X11/extensions/Xtsol.h>

Status XTSOLgetResLabel(display, object, type, sl);

Display *display;
XID object;
ResourceType type;
m_label_t *sl;
```

機能説明 クライアントには、PRIV\_WIN\_DAC\_READ および PRIV\_WIN\_MAC\_READ 特権が必要です。XTSOLgetResLabel() は、ウィンドウ、ピクセルマップ、またはカラーマップに関連付けられたラベルを取得する場合に使用します。

パラメータ *display* Display 構造体へのポインタを指定します。これは、XOpenDisplay() から返されます。

*object* 取得するラベルを持つウィンドウシステムオブジェクトの ID を指定します。指定可能なウィンドウシステムオブジェクトは、ウィンドウ、ピクセルマップ、およびカラーマップです。

*type* アクセスしようとしている資源のタイプを指定します。指定可能な値は、IsWindow、IsPixmap、または IsColormap です。

*sl* 指定したオブジェクトの現在のラベルである機密ラベルを返します。

属性 次の属性については、attributes(5) を参照してください。

| 属性タイプ  | 属性値      |
|--------|----------|
| 使用条件   | SUNWxwts |
| MT レベル | MT-危険    |

戻り値 なし

エラー BadAccess 特権がありません。

BadPixmap 有効なピクセルマップではありません。

BadValue 有効なタイプではありません。

関連項目 [XTSOLgetClientAttributes\(3XTSOL\)](#), [XTSOLsetResLabel\(3XTSOL\)](#)

『Solaris Trusted Extensions 開発ガイド』の「ウィンドウラベルの取得」

|       |                                                                                                                                                                                                                                                                                                                                                    |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 名前    | XTSOLgetResUID – ウィンドウやピクセルマップに関連付けられた UID の取得                                                                                                                                                                                                                                                                                                     |
| 形式    | <pre>#include &lt;X11/extensions/Xtsol.h&gt;  Status XTSOLgetResUID(<i>display</i>, <i>object</i>, <i>type</i>, <i>uidp</i>);  Display *<i>display</i>; XID <i>object</i>; ResourceType <i>type</i>; uid_t *<i>uidp</i>;</pre>                                                                                                                     |
| 機能説明  | <p>クライアントには、PRIV_WIN_DAC_READ および PRIV_WIN_MAC_READ 特権が必要です。</p> <p>XTSOLgetResUID() は、ウィンドウシステムオブジェクトの所有権を取得します。クライアントは、これを使用して、それ自体が作成したのではないオブジェクトの所有権を取得できます。</p>                                                                                                                                                                              |
| パラメータ | <p><i>display</i> Display 構造体へのポインタを指定します。これは、XOpenDisplay() から返されます。</p> <p><i>object</i> 取得する UID を持つウィンドウシステムオブジェクトの ID を指定します。指定可能なウィンドウシステムオブジェクトは、ウィンドウまたはピクセルマップです。</p> <p><i>type</i> アクセスしようとしている資源のタイプを指定します。指定可能な値は IsWindow および IsPixmap です。</p> <p><i>uidp</i> 指定したオブジェクトの現在の UID である UID を返します。クライアントは、uid_t へのポインタを提供する必要があります。</p> |
| 属性    | 次の属性については、attributes(5) を参照してください。                                                                                                                                                                                                                                                                                                                 |

| 属性タイプ  | 属性値      |
|--------|----------|
| 使用条件   | SUNWxwts |
| MT レベル | MT-危険    |

戻り値 なし

|     |           |                    |
|-----|-----------|--------------------|
| エラー | BadAccess | 特権がありません。          |
|     | BadWindow | 有効なウィンドウではありません。   |
|     | BadPixmap | 有効なピクセルマップではありません。 |
|     | BadValue  | 有効なタイプではありません。     |

関連項目 [XTSOLgetClientAttributes\(3XTSOL\)](#), [XTSOLgetResAttributes\(3XTSOL\)](#), [XTSOLgetResLabel\(3XTSOL\)](#)

『Solaris Trusted Extensions 開発ガイド』の「ウィンドウユーザー ID の取得」

名前 XTSOLgetSSHeight – 画面ストライプの高さの取得

形式 `#include <X11/extensions/Xtsol.h>`

```
Status XTSOLgetSSHeight(display, screen_num, newheight);
```

```
Display *display;
int screen_num;
int *newheight;
```

機能説明 XTSOLgetSSHeight() は、画面の下部にある、トラステッド画面ストライプの高さを取得します。現在のところ、画面のストライプが表示されるのはデフォルト画面だけです。クライアントは、トラステッドパスポセス属性を保持する必要があります。

パラメータ *display* Display 構造体へのポインタを指定します。これは、XOpenDisplay() から返されます。

*screen\_num* 画面の番号を指定します。

*newheight* ストライプの高さが返される記憶領域を指定します (高さの単位はピクセル)。

属性 次の属性については、attributes(5) を参照してください。

| 属性タイプ  | 属性値      |
|--------|----------|
| 使用条件   | SUNWxwts |
| MT レベル | MT-危険    |

戻り値 なし

エラー BadAccess 特権がありません。

BadValue 有効な *screen\_num* または *newheight* ではありません。

関連項目 [XTSOLsetSSHeight\(3XTSOL\)](#)

『Solaris Trusted Extensions 開発ガイド』の「スクリーンストライプの高さへのアクセスと設定」

名前 XTSOLgetWorkstationOwner – ワークステーションの所有権の取得

形式 `#include <X11/extensions/Xtsol.h>`

```
Status XTSOLgetWorkstationOwner(display, uidp);
```

```
Display *display;
uid_t *uidp;
```

機能説明 XTSOLgetWorkstationOwner() は、ワークステーションの所有権の取得に使用します。

パラメータ *display* Display 構造体へのポインタを指定します。これは、XOpenDisplay() から返されます。

*uidp* 指定された Display ワークステーションサーバーの現在の UID である UID を返します。クライアントは、uid\_t へのポインタを提供する必要があります。

属性 次の属性については、attributes(5) を参照してください。

| 属性タイプ  | 属性値      |
|--------|----------|
| 使用条件   | SUNWxwts |
| MT レベル | MT-危険    |

戻り値 なし

エラー BadAccess 特権がありません。

関連項目 [XTSOLsetWorkstationOwner\(3XTSOL\)](#)

『Solaris Trusted Extensions 開発ガイド』の「X ウィンドウサーバーワークステーション所有者 ID の取得」

|       |                                                                                                                                                                     |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 名前    | XTSOLIsWindowTrusted – ウィンドウがトラステッドクライアントにより作成されたものかどうかのテスト                                                                                                         |
| 形式    | <pre>#include &lt;X11/extensions/Xtsol.h&gt;  Bool XTSOLIsWindowTrusted(<i>display</i>, <i>window</i>);  Display *<i>display</i>; Window <i>window</i>;</pre>       |
| 機能説明  | XTSOLIsWindowTrusted() は、 <i>window</i> がトラステッドクライアントにより作成されるかどうかをテストします。トラステッドクライアントにより作成される <i>window</i> は、特殊なビットが有効に設定されています。クライアントには、この操作を実行するための特権は一切必要ありません。 |
| パラメータ | <p><i>display</i>    Display 構造体へのポインタを指定します。これは、XOpenDisplay() から返されます。</p> <p><i>window</i>    テストするウィンドウの ID を指定します。</p>                                         |
| 属性    | 次の属性については、attributes(5) を参照してください。                                                                                                                                  |

| 属性タイプ  | 属性値      |
|--------|----------|
| 使用条件   | SUNWxwts |
| MT レベル | MT-危険    |

|     |                                       |
|-----|---------------------------------------|
| 戻り値 | True    ウィンドウがトラステッドクライアントにより作成される場合。 |
| エラー | BadWindow    有効なウィンドウではありません。         |

名前 XTSOLMakeTPWindow – このウィンドウをトラステッドパスウィンドウにする

形式 `#include <X11/extensions/Xtsol.h>`  
`Status XTSOLMakeTPWindow(display, w);`

`Display *display;`  
`Window w;`

機能説明 XTSOLMakeTPWindow() は、ウィンドウをトラステッドパスウィンドウにする場合に使用します。トラステッドパスウィンドウは、常にほかのウィンドウより前面に配置されます。クライアントは、トラステッドパスプロセス属性セットを保持する必要があります。

パラメータ *display* Display 構造体へのポインタを指定します。これは、XOpenDisplay() から返されます。

*w* ウィンドウの ID を指定します。

属性 次の属性については、attributes(5) を参照してください。

| 属性タイプ  | 属性値      |
|--------|----------|
| 使用条件   | SUNWxwts |
| MT レベル | MT-危険    |

戻り値 なし

エラー BadAccess 特権がありません。  
BadWindow 有効なウィンドウではありません。  
BadValue 有効なタイプではありません。

名前 XTSOLsetPolyInstInfo – 多インスタンス化情報の設定

形式 

```
#include <X11/extensions/Xtsol.h>

Status XTSOLsetPolyInstInfo(display, sl, uidp, enabled);

Display *display;
m_label_t sl;
uid_t *uidp;
int enabled;
```

機能説明 XTSOLsetPolyInstInfo() は、プロパティ資源を取得するための多インスタンス化情報を設定します。デフォルトでは、クライアントが多インスタンス化されたプロパティのプロパティデータを要求する場合、返されるデータは要求元クライアントの SL および UID に対応します。特定の *sl* および *uid* を持つプロパティに関連付けられたプロパティデータを取得する場合、クライアントはこの呼び出しを使って、*enabled* フラグを TRUE に設定し、SL および UID を指定します。また、クライアントは、プロパティ値を取得したあとで、*enabled* フラグを FALSE に戻します。クライアントは、PRIV\_WIN\_MAC\_WRITE および PRIV\_WIN\_DAC\_WRITE 特権を保持する必要があります。

パラメータ *display* Display 構造体へのポインタを指定します。これは、XOpenDisplay() から返されます。

*sl* 機密ラベルを指定します。

*uidp* UID へのポインタを指定します。

*enabled* クライアントが、取得したプロパティ情報を設定できるかどうかを指定します。

属性 次の属性については、attributes(5) を参照してください。

| 属性タイプ  | 属性値      |
|--------|----------|
| 使用条件   | SUNWxwts |
| MT レベル | MT-危険    |

戻り値 なし

エラー BadAccess 特権がありません。

BadValue *display* または *sl* が有効ではありません。

関連項目 『Solaris Trusted Extensions 開発ガイド』の「ウィンドウの多インスタンス化情報の設定」

名前 XTSOLsetPropLabel – ウィンドウのプロパティーに関連付けられたラベルの設定

形式

```
#include <X11/extensions/Xtsol.h>

Status XTSOLsetPropLabel(*display, window, property, *sl);

Display *display;
Window window;
Atom property;
m_label_t *sl;
```

機能説明 XTSOLsetPropLabel() は、ウィンドウのプロパティーに関連付けられている機密ラベルの変更に使用されます。クライアントは、PRIV\_WIN\_DAC\_WRITE、PRIV\_WIN\_MAC\_WRITE、および PRIV\_WIN\_UPGRADE\_SL 特権を保持する必要があります。

パラメータ

*display* Display 構造体へのポインタを指定します。これは、XOpenDisplay() から返されます。

*window* 変更するプロパティーのラベルを保持するウィンドウの ID を指定します。

*property* プロパティーアトムを指定します。

*sl* 機密ラベルへのポインタを指定します。

属性 次の属性については、attributes(5) を参照してください。

| 属性タイプ  | 属性値      |
|--------|----------|
| 使用条件   | SUNWxwts |
| MT レベル | MT-危険    |

戻り値 なし

エラー

BadAccess 特権がありません。

BadWindow 有効なウィンドウではありません。

BadAtom 有効なアトムではありません。

BadValue 有効な *sl* ではありません。

関連項目 [XTSOLgetPropAttributes\(3XTSOL\)](#), [XTSOLgetPropLabel\(3XTSOL\)](#)

|       |                                                                                                                                                                                                                                        |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 名前    | XTSOLsetPropUID - ウィンドウのプロパティーに関連付けられた UID の設定                                                                                                                                                                                         |
| 形式    | <pre>#include &lt;X11/extensions/Xtsol.h&gt;  Status XTSOLsetPropUID(<i>display</i>, <i>window</i>, <i>property</i>, <i>uidp</i>);  Display *<i>display</i>; Window <i>window</i>; Atom <i>property</i>; uid_t *<i>uidp</i>;</pre>     |
| 機能説明  | XTSOLsetPropUID() は、ウィンドウのプロパティーの所有権を変更します。これは、別のクライアントが、それ自体が作成したのではないウィンドウのプロパティーを変更することを可能にします。クライアントは、PRIV_WIN_DAC_WRITE および PRIV_WIN_MAC_WRITE 特権を保持する必要があります。                                                                    |
| パラメータ | <p><i>display</i>    Display 構造体へのポインタを指定します。これは、XOpenDisplay() から返されます。</p> <p><i>window</i>    変更するプロパティーの UID を持つウィンドウの ID を指定します。</p> <p><i>property</i>    プロパティーアトムを指定します。</p> <p><i>uidp</i>    UID を含む uid_t へのポインタを指定します。</p> |
| 属性    | 次の属性については、attributes(5) を参照してください。                                                                                                                                                                                                     |

| 属性タイプ  | 属性値      |
|--------|----------|
| 使用条件   | SUNWxwts |
| MT レベル | MT-危険    |

|      |                                                                                                     |
|------|-----------------------------------------------------------------------------------------------------|
| 戻り値  | なし                                                                                                  |
| エラー  | <p>BadAccess    特権がありません。</p> <p>BadWindow    有効なウィンドウではありません。</p> <p>BadAtom    有効なアトムではありません。</p> |
| 関連項目 | <a href="#">XTSOLgetPropAttributes(3XTSOL)</a> , <a href="#">XTSOLgetPropUID(3XTSOL)</a>            |

名前 XTSOLsetResLabel – ウィンドウまたはピクセルマップに関連付けられたラベルの設定

形式 `#include <X11/extensions/Xtsol.h>`

`Status XTSOLsetResLabel(display, object, type, sl);`

```
Display *display;
XID object;
ResourceType type;
m_label_t *sl;
```

機能説明 クライアントは、PRIV\_WIN\_DAC\_WRITE、PRIV\_WIN\_MAC\_WRITE、PRIV\_WIN\_UPGRADE\_SL、および PRIV\_WIN\_DOWNGRADE\_SL 特権を保持する必要があります。

XTSOLsetResLabel() は、ウィンドウまたはピクセルマップに関連付けられたラベルを変更する場合に使用します。

パラメータ

*display* Display 構造体へのポインタを指定します。これは、XOpenDisplay() から返されます。

*object* 変更するラベルを持つウィンドウシステムオブジェクトの ID を指定します。指定可能なウィンドウシステムオブジェクトは、ウィンドウおよびピクセルマップです。

*type* アクセスしようとしている資源のタイプを指定します。指定可能な値は IsWindow および IsPixmap です。

*sl* 機密ラベルへのポインタを指定します。

属性 次の属性については、attributes(5) を参照してください。

| 属性タイプ  | 属性値      |
|--------|----------|
| 使用条件   | SUNWxwts |
| MT レベル | MT-危険    |

戻り値 なし

エラー

BadAccess 特権がありません。

BadPixmap 有効なピクセルマップではありません。

BadValue *type* または *sl* が有効ではありません。

関連項目 [XTSOLgetResAttributes\(3XTSOL\)](#), [XTSOLgetResLabel\(3XTSOL\)](#)

『Solaris Trusted Extensions 開発ガイド』の「ウィンドウラベルの設定」

|       |                                                                                                                                                                                                                                                                                                                                     |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 名前    | XTSOLsetResUID - ウィンドウ、ピクセルマップ、またはカラーマップに関連付けられた UID の設定                                                                                                                                                                                                                                                                            |
| 形式    | <pre>#include &lt;X11/extensions/Xtsol.h&gt;  Status XTSOLsetResUID(<i>display</i>, <i>object</i>, <i>type</i>, <i>uidp</i>);  Display *<i>display</i>; XID <i>object</i>; ResourceType <i>type</i>; uid_t *<i>uidp</i>;</pre>                                                                                                      |
| 機能説明  | クライアントは、PRIV_WIN_DAC_WRITE および PRIV_WIN_MAC_WRITE 特権を保持する必要があります。XTSOLsetResUID() は、ウィンドウシステムオブジェクトの所有権を変更します。これにより、クライアントは、オブジェクトを作成してからその所有権を変更できます。新しい所有者は、このオブジェクトを、それ自体が作成したオブジェクトであるかのように変更できます。                                                                                                                              |
| パラメータ | <p><i>display</i>    Display 構造体へのポインタを指定します。これは、XOpenDisplay() から返されます。</p> <p><i>object</i>     変更する UID を持つウィンドウシステムオブジェクトの ID を指定します。指定可能なウィンドウシステムオブジェクトは、ウィンドウとピクセルマップです。</p> <p><i>type</i>       アクセスしようとしている資源のタイプを指定します。指定可能な値は、次のとおりです。IsWindow および IsPixmap</p> <p><i>uidp</i>       UID を含む uid_t 構造体へのポインタを指定します。</p> |
| 属性    | 次の属性については、attributes(5) を参照してください。                                                                                                                                                                                                                                                                                                  |

| 属性タイプ  | 属性値      |
|--------|----------|
| 使用条件   | SUNWxwts |
| MT レベル | MT-危険    |

|     |                                                                                                                                              |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------|
| 戻り値 | なし                                                                                                                                           |
| エラー | <p>BadAccess    特権がありません。</p> <p>BadWindow    有効なウィンドウではありません。</p> <p>BadPixmap    有効なピクセルマップではありません。</p> <p>BadValue     有効なタイプではありません。</p> |

関連項目    [XTSOLgetResUID\(3XTSOL\)](#)

名前 XTSOLsetSessionHI – セッション最上位機密ラベルをウィンドウサーバーに設定する  
形式

```
#include <X11/extensions/Xtsol.h>
```

```
Status XTSOLsetSessionHI(display, sl);
```

```
Display *display;
m_label_t *sl;
```

機能説明 XTSOLsetSessionHI() Trusted Extensions ウィンドウシステムの TCB コンポーネントである `logintool` によりセッション最上位機密ラベルが設定されると、`Xsun` は、セッション最上位ラベルよりも高い機密ラベルで稼働中のクライアントからの接続要求を拒否します。クライアントは、`PRIV_WIN_CONFIG` 特権を保持する必要があります。

パラメータ *display* Display 構造体へのポインタを指定します。これは、`XOpenDisplay()` から返されます。  
*sl* セッション最上位ラベルとして使用する機密ラベルへのポインタを指定します。

属性 次の属性については、`attributes(5)` を参照してください。

| 属性タイプ  | 属性値      |
|--------|----------|
| 使用条件   | SUNWxwts |
| MT レベル | MT-危険    |

戻り値 なし

エラー BadAccess 特権がありません。

関連項目 [XTSOLsetSessionLO\(3XTSOL\)](#)

『Solaris Trusted Extensions 開発ガイド』の「Xウィンドウサーバーの認可上限と最下位ラベルの設定」

|       |                                                                                                                                                                                                                                                              |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 名前    | XTSOLsetSessionLO - セッション最下位機密ラベルをウィンドウサーバーに設定する                                                                                                                                                                                                             |
| 形式    | <pre>#include &lt;X11/extensions/Xtsol.h&gt;  Status XTSOLsetSessionLO(<i>display</i>, <i>sl</i>);  Display *<i>display</i>; m_label_t *<i>sl</i>;</pre>                                                                                                     |
| 機能説明  | XTSOLsetSessionLO() は、セッション最下位機密ラベルを設定します。Trusted Extensions ウィンドウシステムの TCB コンポーネントである <code>logintool</code> によりセッション最下位ラベルが設定されると、 <code>Xsun</code> は、セッション最下位ラベルよりも低い機密ラベルで稼働するクライアントからの接続要求を拒否します。クライアントは、 <code>PRIV_WIN_CONFIG</code> 特権を保持する必要があります。 |
| パラメータ | <p><i>display</i>    Display 構造体へのポインタを指定します。これは、<code>XOpenDisplay()</code> から返されます。</p> <p><i>sl</i>            セッション最下位ラベルとして使用する機密ラベルへのポインタを指定します。</p>                                                                                                   |
| 属性    | 次の属性については、 <code>attributes(5)</code> を参照してください。                                                                                                                                                                                                             |

| 属性タイプ  | 属性値      |
|--------|----------|
| 使用条件   | SUNWxwts |
| MT レベル | MT-危険    |

|      |                                                                                                                        |
|------|------------------------------------------------------------------------------------------------------------------------|
| 戻り値  | なし                                                                                                                     |
| エラー  | BadAccess    特権がありません。                                                                                                 |
| 関連項目 | <p><a href="#">XTSOLsetSessionHI(3XTSOL)</a></p> <p>『Solaris Trusted Extensions 開発ガイド』の「Xウィンドウサーバーの認可上限と最下位ラベルの設定」</p> |

名前 XTSOLsetSSHeight – 画面ストライプの高さの設定

形式 `#include <X11/extensions/Xtsol.h>`

```
Status XTSOLsetSSHeight(display, screen_num, newheight);
```

```
Display *display;
int screen_num;
int newheight;
```

機能説明 XTSOLsetSSHeight() は、画面の下部にある、トラステッド画面ストライプの高さを設定します。現在のところ、画面のストライプが表示されるのはデフォルト画面だけです。クライアントは、トラステッドパスポセス属性を保持する必要があります。

パラメータ *display* Display 構造体へのポインタを指定します。これは、XOpenDisplay から返されます。

*screen\_num* 画面の番号を指定します。

*newheight* ストライプの高さをピクセルで指定します。

属性 次の属性については、attributes(5) を参照してください。

| 属性タイプ  | 属性値      |
|--------|----------|
| 使用条件   | SUNWxwts |
| MT レベル | MT-危険    |

戻り値 なし

エラー BadAccess 特権がありません。

BadValue 有効な *screen\_num* または *newheight* ではありません。

関連項目 [XTSOLgetSSHeight\(3XTSOL\)](#)

『Solaris Trusted Extensions 開発ガイド』の「スクリーンストライプの高さへのアクセスと設定」

名前 XTSOLsetWorkstationOwner – ワークステーションの所有権の設定

形式 

```
#include <X11/extensions/Xtsol.h>

Status XTSOLsetWorkstationOwner(display, uidp);

Display *display;
uid_t *uidp;
XTSOLClientAttributes *clientattrp;
```

機能説明 XTSOLsetWorkstationOwner() は、Solaris Trusted Extensions の `logintool` により、ワークステーションサーバーの所有者として識別されるユーザー ID の割り当てに使用されます。このユーザー ID で稼働しているクライアントは、キーボードマッピング、マウスマッピング、および修飾子マッピングなどのサーバーのデバイスオブジェクトを設定できます。このクライアントは、トラステッドパスプロセス属性を保持する必要があります。

パラメータ *display* Display 構造体へのポインタを指定します。これは、`XOpenDisplay()` から返されます。

*uidp* UID を含む `uid_t` 構造体へのポインタを指定します。

属性 次の属性については、`attributes(5)` を参照してください。

| 属性タイプ  | 属性値      |
|--------|----------|
| 使用条件   | SUNWxwts |
| MT レベル | MT-危険    |

戻り値 なし

エラー BadAccess 特権がありません。

関連項目 [XTSOLgetWorkstationOwner\(3XTSOL\)](#)

『Solaris Trusted Extensions 開発ガイド』の「ワークステーション所有者 ID へのアクセスと設定」



参照  
ファイル形式

名前 label\_encodings – ラベルエンコーディングファイル

形式 /etc/security/tsol/label\_encodings

インタフェース  
レベル このファイルは、米国国防情報局 (DIA) の必須アクセス制御 (MAC) ポリシーの一部です。このファイルは、Solaris Trusted Extensions ソフトウェアの将来のリリース向けに作成されるその他の必須ポリシーには適用されない可能性があります。

label\_encodings ファイルの一部は標準と見なされており、米国国防情報局 (DIA) ドキュメント DDS-2600-6216-93、『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』(1993年9月)の制御下にあります。この標準の中で INFORMATION LABELS: および NAME INFORMATION LABELS: のセクションに言及した箇所は、廃止または互換性がなくなる可能性があります。ただし、INFORMATION LABELS: セクションは存在する必要がある、かつ構文的にも正しいものである必要があります。これは、無視されます。NAME INFORMATION LABELS: セクションの使用は、任意です。存在する場合、これは無視されますが、構文的に正しいものである必要があります。

オプションの LOCAL DEFINITIONS: セクション内の、次に示す値は旧式です。これらの値は、旧式の `bltos(3TSOL)` 関数にのみ有効である場合があるため、`label_to_str(3TSOL)` 置換関数には認識されない可能性があります。

```
ADMIN LOW NAME=
ADMIN HIGH NAME=
DEFAULT LABEL VIEW IS EXTERNAL
DEFAULT LABEL VIEW IS INTERNAL
DEFAULT FLAGS=
FORCED FLAGS=
CLASSIFICATION NAME=
COMPARTMENTS NAME=
```

機能説明 label\_encodings ファイルは、人間が読み取り可能なラベルから内部形式への変換、内部形式から人間が読み取り可能な正規形式への変換、および印刷出力用バナーページの作成に使用されるセキュリティーラベルの標準エンコーディングファイルです。Solaris Trusted Extensions システムでは、label\_encodings ファイルは、ラベル `admin_high` で保護されています。セキュリティー管理者は、アプリケーションマネージャーの「システム管理」フォルダ内にある「エンコーディングの検査」操作を使って、このファイルを編集および検査するようにしてください。

拡張機能説明 Solaris Trusted Extensions システムでは、『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』に記載されているラベルエンコーディングファイルの必須セクションに加えて、オプションのローカル拡張機能も使用できます。これらの拡張機能は、文字コード形式のカラー名と機密ラベル間のさまざまな変換オプションおよび関連付けを提供します。これらの拡張機能は、文字コード形式のカラー名と機密ラベル間のさまざまな変換オプションおよび関連付けを提供します。

オプションのローカル拡張機能セクションは、LOCAL DEFINITIONS: キーワードで始まり、次に示す順序付けのない文がゼロ個以上続きます。

DEFAULT USER SENSITIVITY LABEL= *sensitivity label*

管理データベース内にユーザーに関する定義が存在しない場合、このオプションで指定された機密ラベルが、ユーザーの最下位機密ラベルとして使用されます。デフォルト値は、ラベルエンコーディングファイルの ACCREDITATION RANGE: セクション内の MINIMUM SENSITIVITY LABEL= 値です。

DEFAULT USER CLEARANCE= *clearance*

管理データベース内にユーザーに関する定義が存在しない場合、このオプションで指定された認可上限が、ユーザーの認可上限として使用されます。デフォルト値は、ラベルエンコーディングファイルの ACCREDITATION RANGE: セクション内の MINIMUM CLEARANCE= 値です。

LOCAL DEFINITIONS: セクションの最終部分では、さまざまな語句、機密ラベル、または格付けに関連付けられる文字コード形式のカラー名が定義されます。このセクションでは、`str_to_label(3TSOL)` 関数がサポートされます。これには、COLOR NAMES: キーワードと、それに続いて色からラベルへの割り当てがゼロ個以上含まれます。各文は、次に示す2つの構文のいずれかが含まれます。

```
word= word value; color= color value;
```

```
label= label value; color= color value;
```

*color value* は、語句 *word value*、機密ラベル *label value*、または格付け *label value* と関連付けられる文字コード形式のカラー名です。

ラベルの文字コード形式のカラー名 *color value* は、ラベルを構成する COLOR NAMES: セクション内のエントリの順序により決定されます。ラベルに、このセクションで指定されている語句 *word value* が含まれる場合、ラベルの *color value* は、指定された最初の *word value* に関連付けられた値になります。指定された語句 *word value* がラベルに含まれない場合、*color value* は、*label value* と正確に一致する値に関連付けられた値になります。正確に一致するものがない場合、*color value* は、ラベルの格付けと一致する格付けを持つ、最初に指定された *label value* に関連付けられた値になります。

## 使用例

例1 LOCAL DEFINITIONS: セクションの例

```
LOCAL DEFINITIONS:
```

```
DEFAULT USER SENSITIVITY LABEL= C A;
DEFAULT USER CLEARANCE LABEL= S ABLE;
```

```
COLOR NAMES:
```

```
label= Admin_Low; color= Pale Blue;
label= unclassified; color= light grey;
```

例1 LOCAL DEFINITIONS: セクションの例 (続き)

```
word= Project A; color= bright blue;
label= c; color= sea foam green;
label= secret; color= #ff0000; * Hexadecimal RGB value
word= Hotel; color= Lavender;
word= KeLO; color= red;
label= TS; color= khaki;
label= TS Elephant; color= yellow;
label= Admin_High; color= shocking pink;
```

属性 次の属性については、attributes(5)を参照してください。

| 属性タイプ  | 属性値                    |
|--------|------------------------|
| 使用条件   | SUNWtsr                |
| 安定性レベル | 混在。前述の「インタフェースレベル」を参照。 |

ファイル

/etc/security/tsol/label\_encodings

ラベルエンコーディングファイルには、このシステムの定義済みラベルに対する格付け名、語句、制約、および値が含まれます。これは、ラベル admin\_high で保護されています。

診断

次に示す診断メッセージは、『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』の「付録 A」に記載された診断メッセージへの追加情報です。

Can't allocate NNN bytes for color names table.

システムは、COLOR NAMES: セクションの処理に必要なメモリーを動的に割り当てることができません。

Can't allocate NNN bytes for color table entry.

システムは、Color Table エントリの処理に必要なメモリーを動的に割り当てることができません。

Can't allocate NNN bytes for color word entry.

システムは、Color Word エントリの処理に必要なメモリーを動的に割り当てることができません。

Can't allocate NNN bytes for DEFAULT USER CLEARANCE.

システムは、DEFAULT USER CLEARANCE の処理に必要なメモリーを動的に割り当てることができません。

Can't allocate NNN bytes for DEFAULT USER SENSITIVITY LABEL.

システムは、DEFAULT USER SENSITIVITY LABEL の処理に必要なメモリーを動的に割り当てることができません。

DEFAULT USER CLEARANCE= XXX is not in canonical form. Is YYY what is intended?  
 このエラーは、指定された認可上限が理解されてはいるが、正規の形式ではない場合に発生します。この追加の正規化チェックにより、認可上限の指定でエラーが生成されないことが保証されます。

DEFAULT USER SENSITIVITY LABEL= XXX is not in canonical form. Is YYY what is intended?  
 このエラーは、指定された機密ラベルが理解されてはいるが、正規の形式ではない場合に発生します。この追加の正規化チェックにより、機密ラベルの指定でエラーが生成されないことが保証されます。

Duplicate DEFAULT USER CLEARANCE= ignored.  
 複数の DEFAULT USER CLEARANCE= オプションが検出されました。最初のオプション以外は、すべて無視されます。

Duplicate DEFAULT USER SENSITIVITY LABEL= ignored.  
 複数の DEFAULT USER SENSITIVITY LABEL= オプションが検出されました。最初のオプション以外は、すべて無視されます。

End of File not found where expected. Found instead: XXX.  
 ラベルエンコーディングファイルの終端が期待される位置に、表記の無関係なテキストが検出されました。

End of File or LOCAL DEFINITIONS: not found. Found instead: XXX.  
 LOCAL DEFINITIONS: セクションまたはラベルエンコーディングファイルの終端が期待される位置に、表記の無関係なテキストが検出されました。

Found color XXX without associated label.  
 カラー xxx が検出されましたが、これに関連付けられたラベルや語句が存在しません。

Invalid color label XXX.  
 ラベル xxx を構文解析できません。

Invalid DEFAULT USER CLEARANCE XXX.  
 DEFAULT USER CLEARANCE xxx を構文解析できません。

Invalid DEFAULT USER SENSITIVITY LABEL XXX.  
 DEFAULT USER SENSITIVITY LABEL xxx を構文解析できません。

Label preceding XXX did not have a color specification.  
 ラベルまたは語句が検出されましたが、一致するカラー名が存在しません。

Word XXX not found as a valid Sensitivity Label word.  
 語句 xxx は、機密ラベル用の有効な語句として検出されませんでした。

## 関連項目

[chk\\_encodings\(1M\)](#), [label\\_to\\_str\(3TSOL\)](#), [str\\_to\\_label\(3TSOL\)](#), [attributes\(5\)](#), [labels\(5\)](#)

『Solaris Trusted Extensions ラベルの管理』

米国防情報局 (DIA) ドキュメント DDS-2600-6216-93、『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』(1993年9月)

## 警告

ラベルエンコーディングファイルの作成および変更は、『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』の概念だけではなく、ローカルのラベル付け要件の詳細も完全に理解している場合にのみ行うようにしてください。

次の警告が、『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』から表現を変えて表示されます。

Solaris Trusted Extensions システムにロードして実行しているラベルエンコーディングファイルを変更する場合には、特別に注意を払ってください。ラベルエンコーディングファイルを使ってシステムが実行されると、多数のオブジェクトが、ロードされたラベルエンコーディングファイルに合わせて適切に形成された機密ラベルを使ってラベル付けされます。そのあとでラベルエンコーディングファイルが変更されると、既存のラベルが適正なものでなくなってしまう可能性があります。語句に関連付けられたビットパターンを変更すると、その語句を含むラベルを持つ既存のオブジェクトが無効なラベルを持つことになる可能性があります。その語句に関連付けられた最下位の格付けを引き上げるか、最上位の格付けを引き下げると、その語句を含むラベルを持つ既存のオブジェクトが適正でなくなる可能性があります。

すでに使用されている現在のエンコーディングファイルへの変更は、新たな格付けや語句の追加、既存の語句の名前変更、ローカル拡張機能の変更だけに限定するようにしてください。『コンパートメントモードワークステーションのラベル作成: エンコード形式』に説明されているように、ラベルエンコーディングファイルの初回作成時に、あとでラベルエンコーディングファイルを拡張して新しい反転語句を組み込むことができるように、余分の反転ビットを予約しておくことは重要です。追加された反転語句が予約された反転ビットを使用しない場合、システムの既存のオブジェクトはすべて、新規反転語句を含むラベルを誤って保持するようになります。

## 注意事項

このファイルは、DIA MAC ポリシーに対してのみ有効です。このファイルの一部は旧式であり、移植を容易にする目的で維持されています。旧式の部分は、将来の Solaris Trusted Extensions リリースで削除される可能性があります。

ラベルエンコーディングファイルを定義するには、次の3つの手順を実行します。最初に、表示される人間が読み取り可能なラベルセットが識別および理解される必要があります。このセットの定義には、人間が読み取り可能なラベルで使用される格付けおよびその他の語句、語句間の関係、各語句の使用に関連付けられた格付け制限、および必須アクセス制御とラベル付けシステム出力内の語句の意図された使用方法を示すリストが含まれます。次に、この定義は、整数、ビットパターン、および論理関係文の内部形式と関連付けられます。最後に、ラベルエンコーディングファイルが作成されます。『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』ドキュメントでは、最初の手順は実行済みと想定して、2番目と3番目の手順が記述されています。

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 名前   | sel_config - コピー、カット、ペースト、およびドラッグ&ドロップ操作時の選択規則                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 形式   | /usr/dt/config/sel_config                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 機能説明 | <p>sel_config ファイルは、ユーザーがラベルの異なるウィンドウ間でデータ転送を行う際の、Trusted Extensions を使って設定されたシステムの動作を指定します。転送操作には、カット&amp;ペースト、コピー&amp;ペースト、およびドラッグ&amp;ドロップが含まれます。このファイルには、自動確認と自動応答という2つのエントリが含まれます。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 自動確認 | <p>このタイプのエントリでは、確認ウィンドウ (選択確認) を表示するかどうかを指定します。各エントリの形式は、次のようになります。</p> <p><i>relationship: confirmation</i></p> <p><i>relationship</i> は、選択したデータの転送元および転送先ウィンドウのラベルを比較した結果を示します。次の3つの値を指定できます。</p> <p><i>upgradesl</i>            転送元ウィンドウのラベルは、転送先ウィンドウのラベルより小さいことを示します。</p> <p><i>downgradesl</i>        転送元ウィンドウのラベルが、転送先ウィンドウのラベルより大きいことを示します。</p> <p><i>disjointsl</i>           転送元ウィンドウのラベルと転送先ウィンドウのラベルが無関係であることを示します。一方のラベルが他方より優位であるということはありません。</p> <p><i>confirmation</i> は、自動確認を実行するかどうかを指定します。次に指定できる値を示します。</p> <p><i>n</i>    手動確認を使用します。選択確認ウィンドウが表示されます。これはデフォルトです。</p> <p><i>y</i>    自動確認を使用します。選択確認ウィンドウは表示されません。</p> |
| 自動応答 | <p>ユーザーが1つの操作を実行すると、転送元ウィンドウと転送先ウィンドウ間で複数の情報フローが実行されます。自動応答のエントリセットを設定することにより、ユーザーに求められる確認の数を減らすことができます。</p> <p>次の形式のエントリが1つ存在する必要があります。</p> <p><i>autoreply: value</i></p> <p><i>value</i> が <i>y</i> (yes の略) の場合、セットの残りのエントリが選択データの属性 (実際の内容ではなく) として使用され、確認を求めずに操作が完了します。<i>value</i> が <i>n</i> (no の略) の場合、残りのエントリは無視されます。</p>                                                                                                                                                                                                                                                                                                        |

コンファーマウィンドウに表示されるすべての *type* フィールドで、デフォルトを指定できます。次に、デフォルトのエントリ例を示します。

```
replytype: TARGETS
replytype: Pixel Sets
replytype: LENGTH
replytype: Type Of Monitor
```

TARGETS エントリを使用すると、転送元ウィンドウでサポートされるターゲットアトムが返されます。ドラッグ&ドロップ操作時のアニメーションに、Pixel Sets および Type Of Monitor エントリが使用されます。LENGTH エントリは、選択内のバイト数を指定します。

属性 次の属性については、`attributes(5)` を参照してください。

| 属性タイプ | 属性値     |
|-------|---------|
| 使用条件  | SUNWtsu |

関連項目 `attributes(5)`

『Solaris Trusted Extensions 管理の手順』の「データのセキュリティーレベルを変更する際の規則」

|      |                                                                                                                                                                                                                             |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 名前   | tnrhdb - トラステッドネットワーク遠隔ホストデータベース                                                                                                                                                                                            |
| 形式   | /etc/security/tsol/tnrhdb                                                                                                                                                                                                   |
| 機能説明 | tnrhdb データベースは、分散システム内の各ホスト (ローカルホストを含む) で使用する遠隔ホストテンプレートを指定します。tnrhdb は <a href="#">tnrhtp(4)</a> データベースと協調動作するため、管理者は各ホストのセキュリティーおよびネットワーク認可属性を確立できます。ホストの IP アドレスを tnrhdb データベース内のエン트리と一致させることができない場合、そのホストとの通信は許可されません。 |

トラステッドネットワークソフトウェアは、ネットワークの「一致するビットの最長接頭辞」機構を使用してホストの tnrhdb エントリを検索します。このソフトウェアは、最初にホスト固有のエントリを検索します。一致するエントリを検出できない場合、このソフトウェアは、一致するビットパターンのもっとも長い接頭辞を持つエントリから検索を開始します。

注-この機構では、システムのサブネットアドレスの実際の数値またはその他のサブネット情報 ([netmasks\(4\)](#) ファイルから取得可能な情報など) は考慮されません。

IPv4 ワイルドカードエン트리 (IPv4 アドレス `0.0.0.0`) は、「一致するビットの最長接頭辞」機構を使用して 0 の接頭辞長を持つため、任意の IPv4 アドレスに一致させることが可能です。

tnrhdb 内の各エントリ行は次の形式になります。 *IP-address:template*。

*IP-address* このフィールドは、[tnrhtp\(4\)](#) データベースで定義された *template* により指定されたセキュリティープロパティーを持つホストまたはネットワークの IP アドレスです。

エントリは、`10.100.100.201` や `fe80\:\:9\:20ff\:fea0\:21f7` の形式のホストアドレスにできます。または、IPv4 または IPv6 サブネットアドレスをエントリにすることもできます。

IPv4 サブネットのエントリは、明示的な接頭辞長を持つサブネットアドレス形式 (`10.100.128.0/17`)、または接頭辞長を示すゼロオクテットを末尾に持つサブネットアドレス形式 (`10.100.0.0`) にできます。

IPv6 サブネットエントリは、接頭辞長を持つサブネットアドレス形式 (`fe80\:\:/10`) にできます。tnrhdb エントリ内でのバックスラッシュの使用方法については、「注意事項」を参照してください。

示された接頭辞長形式を使って IPv4 サブネットエントリを指定する場合、末尾のゼロオクテットが 4、3、2、または 1 であれば、実際の接頭辞長はそれぞれ値 0、8、16、または 24 になります。末尾のオクテットにゼロ以外の値を持つエントリは、ホストアドレスとして解釈され、接頭辞長が 32 であることを意味します。IPv4 エントリの例については、「使用例」を参照してください。

*template* この値は、tnrhtp データベース内の有効なテンプレート名である必要があります。セキュリティ属性の詳細は、[tnrhtp\(4\)](#) を参照してください。

複数の IP アドレスで、1つのテンプレートを使用可能です。ネットワークが稼働中にこのデータベースが変更された場合、[tnctl\(1M\)](#) を使って遠隔ホストエントリを更新するまで、変更は有効になりません。管理者は、ネットワークの稼働中に新規エントリの追加および既存エントリの変更を行えます。*template* フィールドに、空白文字を含めることはできません。

tnrhdb データベースを変更するたびに、管理者は [tnchkdb\(1M\)](#) を実行して構文を検査するようにしてください。ネットワークの稼働中にこのデータベースが変更された場合、[tnctl\(1M\)](#) によりカーネルが更新されるまで、変更は有効になりません。

## 使用例

### 例1 IPv4エントリの例

| IPv4 Entry   | Host Address<br>or Wildcard? | Implied Prefix<br>Length |
|--------------|------------------------------|--------------------------|
| 0.0.0.0      | Wildcard                     | 0                        |
| 10.0.0.0     | Wildcard                     | 8                        |
| 10.100.0.0   | Wildcard                     | 16                       |
| 10.0.100.0   | Wildcard                     | 24                       |
| 10.0.100.100 | Host Address                 | 32                       |

### 例2 tnrhdb ファイルの例

次の例で使用するテンプレートは、tnrhtp 内で定義されたあとで、tnrhdb ファイル内で使用されます。この例では、テンプレート *cipso* を使用するホスト、テンプレート *public* を使用するホスト、およびテンプレート *needtoknow* を使用するホストを示します。2つのサブネットが存在します。一方のサブネットではテンプレート *internal* を使用し、他方のサブネットではテンプレート *secret* を使用します。ほかのすべてのホストは、IPv4 ホストおよび IPv6 ホスト用のワイルドカードエントリで指定されたテンプレート *default-template* を使用します。

```
#
Assume that templates default-template, cipso, public,
internal, needtoknow, and secret are defined in the
tnrhtp database.
#
the first two entries are addresses of the IPv4 and
IPv6 loopback interfaces
127.0.0.1:cipso
\:\:1:cipso
10.0.0.1:cipso
```

## 例2 tnrhdb ファイルの例 (続き)

```

192.168.120.6:public
192.168.120.0:internal
192.168.120.7:needtoknow
192.168.121.0:secret
0.0.0.0:default-template
0\:\:0/0:default-template
fe80\:\:a00\:\:20ff\:\:fea0\:\:21f7:cipso

```

## 属性

次の属性については、attributes(5)を参照してください。

| 属性タイプ | 属性値       |
|-------|-----------|
| 使用条件  | SUNWtsg   |
| 安定性   | プロジェクト非公開 |

## ファイル

/etc/security/tsol/tnrhdb トラストッドネットワーク遠隔ホストデータベース

## 関連項目

smtnrhdb(1M), hosts(4), ipnodes(4), netmasks(4), tnchddb(1M), tnctl(1M), tnd(1M),  
tninfo(1M), tnrhpt(4), tnzonecfg(4), attributes(5)

『Solaris Trusted Extensions 管理の手順』の第12章「トラストッドネットワーク」

## 警告

ネットワークの稼働中にテンプレートを変更すると、不特定数のホストのセキュリティ表示が変更される可能性があります。

## 注意事項

コロン(:)は、データベース区切り文字です。コロンをデータフィールドの一部に使用する場合は、fe80\:\:a00\:\:20ff\:\:fea0\:\:21f7のように、バックスラッシュ(\)を使ってエスケープする必要があります。

管理者が、Trusted Extensions ソフトウェアを実行するホストごとに1つのtnrhdb エントリを作成する一方、同一のセキュリティ属性を持つラベル付けされていないすべてのホストに適用できるサブネット単位のエントリを作成したい場合があります。この場合、管理者は、異なるセキュリティ属性セットを割り当てる必要のあるホストごとにエントリを個別に作成できます。

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 名前   | tnrhtp – トラストドネットワーク遠隔ホストテンプレート                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 形式   | /etc/security/tsol/tnrhtp                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 機能説明 | <p>テンプレートの tnrhtp データベースは、分散システム内の各ホスト (ローカルホストとネットワークを含む) に認可属性とセキュリティー属性を割り当てる際、利便性を向上させる目的で管理者により指定されます。</p> <p>tnrhtp は、<a href="#">tnrhdb(4)</a> と協調動作します。tnrhdb 内の IP アドレスを割り当てることのできるのは、tnrhtp データベース内で定義されているテンプレートに対してだけです。tnrhtp データベースを変更するたびに、管理者は <a href="#">tnchkdb(1M)</a> を実行して構文を検査するようにしてください。</p> <p>テンプレートデータベース内の各エントリは、1 つの長い行として入力されます。エントリ内のフィールドは、セミコロン (;) で区切られます。</p> <p><i>template_name:attr</i></p> <p>行の先頭のポンド記号 (#) はコメント行であることを示し、コメント行は無視されます。</p> <p><i>template_name</i><br/> 定義中のテンプレートに名前を付ける文字列です。この文字列では、大文字と小文字が区別されます。文字列の最初の 31 文字だけが読み取られて、解釈されます。<i>template_name</i> には、フィールド区切り文字、改行文字、およびコメント文字を除く出力可能な任意の文字を使用できます。</p> <p><i>attr</i><br/> セミコロン (;) で区切られた <i>key=value</i> ペアのリストで、各ペアにはテンプレートの属性が記述されます。none 以外の値が設定されていない場合でも、その旨が示されていない限り、すべてのキーは必須です。現在のところ、次のキーがシステムにより解釈されます。</p> <p><i>host_type</i>            定義済みの 2 つの値 <i>unlabeled</i>、<i>cipso</i> のいずれかをとりま<br/> す。ホストタイプ <i>cipso</i> は、パケットのラベル付けに CIPSO<br/> (Common IP Security Options - Tag Type 1 のみ) を使用するホス<br/> ト用です。</p> <p><i>def_label</i>            これらの属性をサポートしない遠隔ホストからの着信データ<br/> に適用するデフォルト属性を定義します。このキーは、ホス<br/> トタイプ <i>unlabeled</i> に対してのみ有効です。</p> <p><i>doi</i>                    解釈ドメイン。ホストタイプ <i>unlabeled</i> の場合、これは<br/> <i>def_label</i> 用の解釈ドメインです。</p> <p>解釈ドメインは、セキュリティー属性の外部または内部表現<br/> と、そのネットワーク表現との間の変換に適用される規則<br/> セットを定義します。設定に Trusted Extensions ソフトウェア<br/> を使用する複数のシステムが同一の解釈ドメインを保持する</p> |

場合、これらは規則セットを共有します。ホストタイプ `unlabeled` の場合、これらのシステムは、同じ解釈ドメインを保持するラベル付けされていないテンプレートに割り当てられるデフォルト属性についても同一の解釈を共有します。

`min_sl`、`max_sl`

このテンプレートを使用する遠隔ホストに対して、ラベル認可範囲を指定します。管理ラベル `ADMIN_LOW` および `ADMIN_HIGH` を除くすべてのラベルは、短縮化された 16 進数形式で指定されます。

ゲートウェイシステムの場合、`min_sl` および `max_sl` は、ラベル付けされたパケットを転送する際のデフォルト範囲を定義します。通常、経路のラベル範囲は、`route(1M)` サブコマンドで `-secattr` オプションを使って設定します。ルートのラベル範囲が未指定の場合、`tnrhtp` データベースの `min_sl` から `max_sl` の範囲が使用されます。

`sl_set`

このテンプレートを使用する遠隔ホストに許可されるセキュリティレベルセットを指定します。ゲートウェイシステムの場合、`sl_set` 内のラベルは、ラベル付けされたパケットの転送に使用されます。`sl_set` の指定は任意です。セット内のラベルの最大数は 4 です。

ネットワークの稼働中に `tnrhtp` データベースが変更された場合、`tnctl(1M)` を使ってテンプレートのエントリが更新されるまで、変更は有効になりません。それ以外の場合は、トラステッドネットワークデーモン `tnd(1M)` による次回のポーリング時に、変更が有効になります。管理者は、ネットワークの稼働中に新規テンプレートの追加、および既存のテンプレートの属性変更を実行できます。

## 使用例

例1 ラベル付けされていないホストエントリ

この例では、マニュアルページを見やすくするために継続文字 (`\`) を使用しています。ただし、データベースファイル内では、各エントリは 1 行で記述する必要があります。バックスラッシュは使用できません。

```
Sample ADMIN_LOW template entry for machines or networks.
Note that the doi field is required.
#
admin_low:host_type=unlabeled;\
def_label=ADMIN_LOW;\
min_sl=ADMIN_LOW;\
max_sl=ADMIN_HIGH;\
doi=1;
```

ラベル付けされていないホストとの通信に使用するラベルが `ADMIN_LOW` でないかぎり、上記のテンプレートは使用しないでください。ラベルエンコーディングファイ

例1 ラベル付けされていないホストエントリ (続き)

ル内のエントリと一致するテンプレートを使用してください。次の例は、サンプルの `label_encodings` ファイル内のエントリに一致します。

```
Sample PUBLIC template entry
based on the sample label_encodings file.
#
public:host_type=unlabeled;\
def_label=0x0002-08-08;\
min_sl=ADMIN_LOW;\
max_sl=ADMIN_HIGH;\
doi=1;
```

例2 CIPSO ホストエントリ

```
Labeled host template
#
hl_allzones:host_type=cipso;\
min_sl=ADMIN_LOW;\
max_sl=ADMIN_HIGH;\
doi=1;
```

属性 次の属性については、`attributes(5)` を参照してください。

| 属性タイプ | 属性値       |
|-------|-----------|
| 使用条件  | SUNWtsg   |
| 安定性   | プロジェクト非公開 |

ファイル `/etc/security/tsol/tnrntp`    トラストドネットワーク遠隔ホストテンプレート

関連項目 `route(1M)`, `smtnrntp(1M)`, `tnchkdb(1M)`, `tnctl(1M)`, `tnd(1M)`, `tninfo(1M)`, `tnrhdb(4)`, `attributes(5)`

『Solaris Trusted Extensions 管理の手順』の「Trusted Extensions のネットワークセキュリティ属性」

警告 ネットワークの稼働中にテンプレートを変更すると、不特定数のホストのセキュリティ表示が変更される可能性があります。

ラベル付けされていないホストから Solaris Trusted Extensions ネットワークへの接続を許可することには、セキュリティ上の危険が伴います。ネットワークの残りの部分の危険化を避けるため、管理者がラベル付けされていないホストのために分散システムが危険化することがないことを確信しているという意味で、この種のホストを「信頼する」必要があります。また、これらのホストを物理的に保護して、承認されている個人だけがアクセスするよう制限することも必要です。ラベル付けさ

---

れていないホストが物理的に改ざんされる危険がないことを保証できない場合、そのホストおよび類似のホストをネットワークの別個のブランチに隔離するようにしてください。

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 名前   | tnzonecfg – トラストドネットワークゾーン構成データベース                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 形式   | /etc/security/tsol/tnzonecfg                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 機能説明 | <p>tnzonecfg データベースは、ローカルホスト用の Solaris Trusted Extensions ゾーン構成エントリのリストです。このデータベースでは、ゾーン名を使ってインデックスが作成されます。各構成エントリでは、ゾーンのラベル、マルチレベルポート (MLP)、およびゾーン作成用のその他のゾーン関連情報を指定します。</p> <p>ゾーン構成データベース内の各エントリは、5つのフィールドで構成されます。各エントリは、各フィールドがコロン(:)で区切られた1つの長い行になっています。</p> <pre>zone-name:label:network-policy:zone-mlp-list:shared-mlp-list global:ADMIN_LOW:1:6000-6003/tcp:6000-6003/tcp</pre> <p>行の先頭のポンド記号(#)はコメント行であることを示し、コメント行は無視されます。</p> <p><i>zone-name</i>            ゾーンの名前。この名前は、ゾーンの構成時に使用されます。ゾーン名の制限については、zonecfg(1M)の -z zonename オプションを参照してください。</p> <p><i>label</i>                ゾーンのラベル。ゾーンの起動時に、このフィールドを使ってゾーンがラベル付けされます。ラベルには、短縮化された16進数形式、またはテキスト形式を使用できます。ラベルは、label_encodings ファイル内で定義されます。各ゾーンのラベルは一意でなければなりません。</p> <p><i>network-policy</i>      すべての非トランスポートトラフィックを処理するためのポリシー。正確なゾーンラベルが必須であるか、ラベル範囲の一致が許可される場合に、このフィールドを使って非MLPトラフィック用のポリシーが決定されます。値0は、受信パケットに対してゾーンラベルが厳密に一致することを示します。このフィールドが1に設定されている場合、受信側のホストは、ホストの認可範囲内でパケットを受信します。</p> <p>                      大域ゾーンの <i>network-policy</i> フィールドが1に設定されている場合、大域ゾーンのIPアドレス上で受信するICMPパケットは、大域ゾーンの <i>tnrhtp</i> エントリのラベル範囲に基づいて受け入れられます。ゾーンに対してこのフィールドが0に設定されている場合、ゾーンはラベルの異なるホストからのICMPエコー要求に回答しません。</p> <p><i>zone-mlp-list</i>        ゾーンに所属するIPアドレス上にある、そのゾーンのマルチレベルポート構成エントリ。<i>zone-mlp-list</i> は、セミコロンで区切られたMLP構成エントリのリストです。各MLP構成エントリは、</p> |

*port/protocol* または *port-range/protocol* で指定されます。たとえば、6001-6003/tcp は、tcp ポート 6001、6002、および 6003 がすべて MLP であることを意味します。

MLP は、大域ゾーンと非大域ゾーンの両方でマルチレベルサービスを提供するために使用されます。非大域ゾーンで MLP を使用する方法を示す例として、2つのラベル付きゾーン *internal* および *public* を設定する場合を考えましょう。*internal* ゾーンは、会社のネットワークにアクセスできます。*public* ゾーンは公開されたインターネットにアクセスできますが、会社の内部ネットワークにはアクセスできません。ブラウズを安全に行うため、*internal* ゾーン内のユーザーがインターネットをブラウズする場合、*internal* ゾーンのブラウザは URL を *public* ゾーンに転送します。その後、Web コンテンツが *public* ゾーンの Web ブラウザに表示されます。このため、*public* ゾーン内へのダウンロードが原因で Web ブラウザが危険化する場合でも、会社の内部ネットワークが影響を受けることはありません。この設定を行うために、*public* ゾーン内の tcp ポート 8080 は MLP (8080/tcp) になります。また、*public* ゾーンの *tnrhttp* テンプレートが PUBLIC から INTERNAL のラベル範囲を保持するようにします。

#### *shared-mlp-list*

共有 IP アドレスのマルチレベルポート構成エントリです。*shared-mlp-list* は、セミコロンで区切られた MLP 構成エントリのリストです。各 MLP 構成エントリの指定には、*port/protocol* の形式を使用します。ほかのゾーンは共有インタフェース上にあるこの *port/protocol* にはアクセスできません。2つ以上のゾーンで *shared-mlp-list* フィールドに同じ *port/protocol* を指定すると構成エラーとなります。

共有 IP アドレスを使用すると、特に大量のゾーンを構成する場合に、システムで必要とされる IP アドレスの総数を減らすことができます。ネットワークトラフィックが共有インタフェース上の、ゾーンの *shared-mlp-list* で指定されているポートで受信された場合、ほかのゾーンがそのトラフィックを受信することはできません。

*tnzonecfg* データベースを変更するごとに、管理者はあとで *tnchkdb(1M)* を実行して構文を検査するようにしてください。ネットワークの稼働中にこのデータベースが変更された場合、*tnctl(1M)* によりカーネルが更新されるまで、変更は有効になりません。

## 使用例

### 例1 ゾーン構成エントリの例

各ゾーンエントリは、データベースファイル内で1行で記述されます。

## 例1 ゾーン構成エントリの例 (続き)

この例では、4つの非大域ゾーン `public`、`internal`、`needtoknow`、および `restricted` が存在します。大域ゾーンと `public` ゾーンだけが MLP を保持します。

大域エントリ内の `zone-mlp-list` 値 `111/tcp;111/udp;2049/tcp;6000-6003/tcp` は、これらのポートを大域ゾーン専用の MLP として指定します。`shared-mlp-list` 値の `6000-6003/tcp` は、これらのポートを共有 IP アドレス (ラベル付けされたゾーン) 用の MLP として指定します。`network-policy` が 1 であるため、大域ゾーンだけが、自分自身とは異なるラベルを持つホストからの着信パケットを受け入れます。

`public` エントリ内の `network-policy` 値 0 は、受信を `public` 非トランスポートトラフィックだけに制限します。`zone-mlp-list` 値の `8080/tcp` は、`public` ゾーンの Web ブラウザポートを MLP にします。

その他のゾーン内の `8080 tcp` ポートは、単一レベルのポートであるため、リストには含められません。同様に、ラベル付けされた各ゾーンは単一レベルの `111` ポート、`2049` ポートなどを保持します。

```
#
Sample global zone configuration file
#
Multilevel Port (MLP) specification:
#
MLP PURPOSE
--- -
111 Port Mapper
2049 NFSv4 server
6000-6003 Multilevel Desktop
#
global:ADMIN_LOW:1:111/tcp;111/udp;2049/tcp;6000-6003/tcp;6000-6003/tcp
public:PUBLIC:0:8080/tcp:
internal:0x0004-08-48:0::
needtoknow:0x0004-08-68:0::
restricted:0x0004-08-78:0::
```

属性 次の属性については、`attributes(5)` を参照してください。

| 属性タイプ | 属性値       |
|-------|-----------|
| 使用条件  | SUNWtsg   |
| 安定性   | プロジェクト非公開 |

ファイル `/etc/security/tsol/tnzonecfg`      トラストドネットワークゾーン構成データベース

## 関連項目

[smtzonecfg\(1M\)](#), [tnchkdb\(1M\)](#), [tnctl\(1M\)](#), [tnd\(1M\)](#), [tninfo\(1M\)](#), [zonecfg\(1M\)](#),  
[label\\_encodings\(4\)](#), [tnrhdb\(4\)](#), [tnrhtp\(4\)](#), [attributes\(5\)](#)

『Solaris Trusted Extensions 管理の手順』の「Solaris 管理コンソールツール」

名前 TrustedExtensionsPolicy – Trusted Extensions X サーバー拡張用構成ファイル

形式 /usr/X11/lib/X11/xserver/TrustedExtensionsPolicy

/usr/openwin/server/etc/TrustedExtensionsPolicy

機能説明 TrustedExtensionsPolicy は、Trusted Extensions X サーバー拡張 (SUN\_TSOL) 用の構成ファイルです。SUN\_TSOL を使用すると、セキュリティーポリシーを施行できます。これは、必須アクセス制御 (MAC) および任意アクセス制御 (DAC) に基づいています。

TrustedExtensionsPolicy ファイル内の空白行およびコメントは無視されます。コメントの先頭には、ポンド記号 (#) が付けられます。このファイルの形式を次に示します。

*keyword*{*space*|*tab*}*value*

ここで、*keyword* には次のいずれかを指定できます。

**atom** このアトムに ADMIN\_LOW のラベルを付けて、XGetAtomName(3X11) が成功するようにします。

**property** このプロパティを一度インスタンス化します。デフォルトは、プロパティの多インスタンス化です。

**selection** この選択を多インスタンス化します。デフォルトでは、選択内容を一度インスタンス化します。

**extension** この拡張機能を無効にします。

**privilege** このウィンドウ特権を、すべてのクライアントで暗黙的に許可します。

使用可能なキーワード値については、Xorg X サーバーの /usr/X11/lib/X11/xserver/TrustedExtensionsPolicy ファイルを参照してください。Xsun については、/usr/openwin/server/etc/TrustedExtensionsPolicy ファイルを参照してください。

属性 次の属性については、attributes(5) を参照してください。

| 属性タイプ | 属性値      |
|-------|----------|
| 使用条件  | SUNWxwts |

使用例 TrustedExtensionsPolicy ファイル内の次のエントリにより、Dtpad プログラムが多インスタンス化されます。

```
selection Dtpad
```

このエントリが存在しないか、コメントアウトされている場合、Dtpad プログラムは1回インスタンス化されます。

同様に、次のエントリにより WM\_ICON\_SIZE プロパティが1回インスタンス化されます。

property WM\_ICON\_SIZE

エントリが欠落しているか、コメントアウトされている場合、WM\_ICON\_SIZE プロパティが多インスタンス化されます。

#### ファイル

/usr/X11/lib/X11/xserver/TrustedExtensionsPolicy  
Trusted Extensions X サーバー拡張用の構成ファイル

#### 関連項目

XGetAtomName(3X11), attributes(5)



参照

標準、環境、マクロ

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 名前            | labels – Solaris Trusted Extensions ラベル属性                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 機能説明          | ラベルは、必須ポリシーの決定で使用される属性です。ラベルは、すべてのサブジェクト (通常はプロセス) およびサブジェクトへとアクセス可能なオブジェクト (通常はファイルのようにデータを保持するもの) に、明示的または暗黙的に関連付けられます。デフォルトの Trusted Extensions 必須ポリシーラベルは、サイトのセキュリティ管理者により、 <code>label_encodings(4)</code> 内で定義されます。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 必須ポリシー        | <p>Solaris Trusted Extensions の有効期間中に、さまざまな必須ポリシーを提供できません。</p> <p>Trusted Extensions のデフォルト必須ポリシーは必須アクセス制御 (MAC) ポリシー (Lattice の Bell-LaPadula Model の必須ポリシー、Simple Security Property、および * -Property (Star Property) と同等) で、制限された上位書き込みを持ちます。デフォルト必須ポリシーは、Non-Inteference の Goguen and Mesegeur モデルとも同等です。</p> <p>この MAC ポリシーの場合、2つのラベル <code>admin_low</code> および <code>admin_high</code> が常に定義されます。サイトのセキュリティ管理者は、<code>label_encodings(4)</code> 内でその他のラベルすべてを定義します。<code>admin_low</code> は、ユーザーが読み取り (表示) 可能な通常の Trusted Extensions オブジェクトすべてと関連付けられます。<code>admin_high</code> は、その他の Trusted Extensions オブジェクトすべてと関連付けられます。<code>admin_high</code> オブジェクトへの MAC 読み取り (表示) アクセス権を保持するのは、管理ユーザーだけです。また、<code>admin_low</code> オブジェクトや <code>admin_high</code> オブジェクトへの MAC 書き込み (変更) アクセス権を保持するのも管理ユーザーだけです。</p> |
| 人間が読み取り可能なラベル | ユーザーは、ラベルを文字列として対話的に処理します。グラフィカルユーザーインタフェースおよびコマンド行インタフェースには、 <code>label_encodings(4)</code> の定義に従って文字列が表示されます。人間が読み取り可能なラベルは、それが表現するラベルで格付けされます。このため、ラベル A の文字列を読み取り可能 (表示可能、人間が読み取り可能な文字列と不透明な <code>m_label_t</code> 間の相互変換が可能)なのは、そのラベルへの読み取り (表示) アクセスを許可するラベルを持つサブジェクトだけです。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 内部テキストラベル     | 公開アクセス可能な ( <code>admin_low</code> ) ネームサービスデータベースにラベルを格納する場合には、格付けされていない内部テキスト形式が使用されます。このテキスト形式は、この形式のラベルを作成した Trusted Extensions ソフトウェアリリースで提供されるインタフェース以外のインタフェースでの使用は意図されていません。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| ラベルとアプリケーション  | アプリケーションは、ラベルとの対話処理を行う際に、ラベルが不透明な ( <code>m_label_t</code> ) 構造体であると見なします。これら不透明な構造体のセマンティクスは、文字列から <code>m_label_t</code> への変換で定義されます。変換は、 <code>label_encodings(4)</code> 内で定義されます。さまざまなアプリケーションプログラミングインタフェース (API) が、文字列と <code>m_label_t</code> 構造体間の変換を行います。さまざま API が、サブジェクト関連のラベルからオブジェクト関連のラベルへのアクセスをテストします。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 属性            | 次の属性については、 <code>attributes(5)</code> を参照してください。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| 属性タイプ       | 属性値          |
|-------------|--------------|
| インタフェースの安定性 | 後述の「注意事項」を参照 |

## 関連項目

`chk_encodings(1M)`, `blcompare(3TSOL)`, `label_to_str(3TSOL)`, `m_label_alloc(3TSOL)`, `m_label_dup(3TSOL)`, `m_label_free(3TSOL)`, `str_to_label(3TSOL)`, `label_encodings(4)`, `attributes(5)`

Bell, D. E., and LaPadula, L. J. Secure Computer Systems: Unified Exposition and Multics Interpretation, MTR-2997 Rev. 2, MITRE Corp., Bedford Mass., March 1976. NTIS AD-A023 588/7.

Goguen, J. A., and Meseguer, J.: Security Policies and Security Models, Proceedings 1982 Symposium on Security and Privacy, IEEE Computer Society Press, 1982, p 11-20.

Goguen, J. A., and Meseguer, J.: Unwinding and Interference Control, Proceedings 1984 Symposium on Security and Privacy, IEEE Computer Society Press, 1984, p 75-86.

『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』

## 注意事項

ラベル実装の安定性は、`label_encodings(4)` の米国国防情報局 (DIA) MAC ポリシーを実装するシステムでは「安定」です。Trusted Extensions の将来のリリースでは、ほかのポリシーが存在する可能性があります。その時点では、`label_encodings` は旧式になっているか、ほかのポリシーにより `label_encodings` が補完されている可能性があります。

内部テキストラベルはインタフェースではないため、Trusted Extensions のいずれかのリリースで変更される可能性があります。これらは、同一の Trusted Extensions ソフトウェアリリース上で入力および生成を行う場合だけを想定しています。

Trusted Solaris 8 アプリケーションでの移植性を高めるために、不透明な構造体名 `blabel_t`、`blevel_t`、および `bclear_t` が、`m_label_t` と等価なものとして定義されています。これらのタイプは、`m_label_t` と同様に、不透明なポインタとして移植する必要があります。さまざまな Trusted Solaris 8 ラベルインタフェースに対して、同じ作業を行う必要があります。これらの Trusted Solaris 8 構造体およびインタフェースは「旧式」であり、Trusted Extensions の将来のリリースでは削除される可能性があります。

- 名前** pam\_tsol\_account – Trusted Extensions 用 PAM アカウント管理モジュール
- 形式** /usr/lib/security/pam\_tsol\_account.so.1
- 機能説明** PAM 用の Solaris Trusted Extensions サービスモジュール  
/usr/lib/security/pam\_tsol\_account.so.1 は、ラベルに関連したアカウント制限を検査します。pam\_tsol\_account.so.1 モジュールは、必要な機能をオンデマンドで提供する、動的にロード可能な共有オブジェクトです。パスは、PAM 構成ファイルで指定されます。
- pam\_tsol\_account.so.1 には、アカウント管理を実行するための関数 pam\_sm\_acct\_mgmt() が含まれます。この関数は、ユーザーに許可されるラベル範囲を検査します。許可されるラベル範囲のデフォルトは、label\_encodings(4) ファイル内に設定されています。これらのデフォルトは、user\_attr(4) データベース内のエントリで上書きできます。
- デフォルトでは、このモジュールは、大域ゾーンに接続する遠隔ホストが CIPSO ホストタイプであることが必要です。このポリシーを無効にするには、次に示すように、pam.conf(4) のエントリのオプションとして allow\_unlabeled キーワードを追加します。
- ```
other account required pam_tsol_account allow_unlabeled
```
- オプション** このモジュールに渡すことができるオプションを、次に示します。
- allow_unlabeled** ラベル付けされていないテンプレートタイプのホストからのリモート接続を許可します。tnrhttp(4) を参照してください。
- debug** デバッグ情報を LOG_DEBUG レベルで提供します。syslog(3C) を参照してください。
- 戻り値** 次の値が返されます。
- PAM_SUCCESS** アカウントは、今回およびこのラベルでの使用で有効です。
- PAM_PERM_DENIED** 現在のプロセスラベルがユーザーのラベル範囲外にある、プロセスのラベル情報を使用できない、遠隔ホストタイプが無効である、のいずれかです。
- Other values** 通常の PAM 操作と一致するエラーコードを返します。エラー関連の戻り値の詳細は、pam(3PAM) のマニュアルページを参照してください。
- 属性** 次の属性については、attributes(5) を参照してください。

属性タイプ	属性値
インタフェースの安定性	開発中

属性タイプ	属性値
MT レベル	例外付き MT-安全

関連項目

keylogin(1), syslog(3C), libpam(3LIB), pam(3PAM), pam_sm_acct_mgmt(3PAM), pam_start(3PAM), [label_encodings\(4\)](#), pam.conf(4), [tnrhtp\(4\)](#), user_attr(4), attributes(5)

『Solaris のシステム管理 (セキュリティサービス)』の第 16 章「PAM の使用」

注意事項

libpam(3LIB) のインタフェースは、マルチスレッドアプリケーション内部の各スレッドが独自の PAM ハンドルを使用する場合にのみ、「MT-安全」です。

索引

数字・記号

- 2つのラベルのうちの高い方の下限,
 blminimum, 59
- 2つのラベルのうち低いほうの上限,
 blmaximum, 59
- 2つのラベルの上限と下限, 59

C

- .copy_files, 51

E

- /etc/security/tsol ファイル
 - tnrhdb, 129
 - tnrhtp, 132
 - tnzonecfg, 136
 - ラベルエンコーディング, 122

L

- .link_files, 51

S

- SMF サービス
 - tnctl, 44
 - tnd, 47

Solaris 管理コンソール

- tnrhdb データベースの管理, 29
- tnrhtp データベースの管理, 33
- tnzonecfg データベースの管理, 37
- SUN_TSOL, 140

T

- tnrhdb, 遠隔ホストタイプの取得, 96
- tnrhdb 内のエントリの管理, smtnrhdb, 29
- tnrhdb の管理, smtnrhdb, 29
- tnrhtp データベース内のエントリの管理,
 smtnrhtp, 33
- tnrhtp の管理, smtnrhtp, 33
- tnzonecfg データベース内のエントリの管理,
 smttnzonecfg, 37
- tnzonecfg の管理, smttnzonecfg, 37
- Trusted Extensions X サーバー拡張, 140
- Trusted Extensions X サーバー拡張用構成ファイル,
 TrustedExtensionsPolicy, 140
- Trusted Extensions ネットワークパラメータの構成,
 tnctl, 44
- Trusted Extensions のアカウント管理, 146

U

- /usr/openwin/server/etc/TrustedExtensionsPolicy, 140
- /usr/X11/lib/X11/xserver/TrustedExtensionsPolicy, 140

い
以前に割り当てられたラベルに関連付けられている資源の解放, 85

う
ウィンドウがトラステッドクライアントにより作成されたものかどうかのテスト,
XTSOLIsWindowTrusted, 109
ウィンドウのプロパティーに関連付けられたUIDの取得, XTSOLgetPropUID, 101
ウィンドウのプロパティーに関連付けられたUIDの設定, XTSOLsetPropUID, 113
ウィンドウのプロパティーに関連付けられたラベル属性の取得, XTSOLgetPropAttributes, 99
ウィンドウのプロパティーに関連付けられたラベルの取得, XTSOLgetPropLabel, 100
ウィンドウのプロパティーに関連付けられたラベルの設定, XTSOLsetPropLabel, 112
ウィンドウ、ピクセルマップ、またはカラーマップに関連付けられたUIDの設定,
XTSOLsetResUID, 115
ウィンドウ、ピクセルマップ、またはカラーマップに関連付けられたラベルの取得,
XTSOLgetResLabel, 104
ウィンドウまたはピクセルマップに関連付けられたすべてのラベル属性の取得,
XTSOLgetResAttributes, 102
ウィンドウまたはピクセルマップに関連付けられたラベルの設定, XTSOLsetResLabel, 114
ウィンドウやピクセルマップに関連付けられたUIDの取得, XTSOLgetResUID, 105

え
遠隔管理, dtappsession, 14
遠隔ホストタイプの取得, tsol_getrhtype, 96

か
画面ストライプの高さの取得,
XTSOLgetSSHheight, 107

画面ストライプの高さの設定,
XTSOLsetSSHheight, 118

く
クライアントに関連付けられたすべてのラベル属性の取得, XTSOLgetClientAttributes, 98

こ
このウィンドウをトラステッドパスウィンドウにする, XTSOLMakeTPWindow, 110
コピー、カット、ペースト、およびドラッグ&ドロップ操作時の選択規則, sel_config ファイル, 127

し
新規アプリケーションマネージャーセッションの起動, 14
新規ターゲットラベル用の資源の割り当て, 85
新規ラベル用の資源の割り当て, 85

せ
セッション最下位機密ラベルの設定,
XTSOLsetSessionLO, 117
セッション最上位機密ラベルをウィンドウユーザーに設定する, XTSOLsetSessionHI, 116

そ
ゾーン
getpathbylabel, 68
getzoneidbylabel, 72
getzonelabelbyid, 72
getzonelabelbyname, 72
getzonepath, 17
getzonerootbyid, 74
getzonerootbylabel, 74

ゾーン (続き)

- getzonerootbyname, 74
- tnzonecfg, 136
- ゾーン構成データベース, 136
- ゾーンとラベル間のマッピング
 - getzoneidbylabel, 72
 - getzonelabelbyid, 72
 - getzonelabelbyname, 72
- ゾーンのパス名, 68
- ゾーンのパス名を返す, getpathbylabel, 68
- ゾーンのルートパス名とラベル間のマッピング
 - getzonerootbyid, 74
 - getzonerootbylabel, 74
 - getzonerootbyname, 74

た

- 対応する機密ラベルを持つゾーンへのファイルの移動, 19
- 多インスタンス化情報の設定,
 - XTSOLsetPolyInstInfo, 111

て

データベース

- Solaris 管理コンソールからの tnrhdb の管理, 29
- Solaris 管理コンソールからの tnrhtp の管理, 33
- Solaris 管理コンソールからの tnzonecfg の管理, 37
- tnrhdb, 129
- tnrhtp, 132
- tnzonecfg, 136
- トラステッドネットワークデータベースからの遠隔ホストタイプの取得, 96
- トラステッドネットワークデータベースの構成, 44
- ネットワークデータベースのファイル構文の検査, 42
- ラベルエンコーディング, 122

デバイス

- デバイス割り当て機構からのエントリの削除, 28
- デバイス割り当て機構への追加, 22

- デバイス割り当て機構へのエントリの追加,
 - add_allocatable, 22

と

- トラステッドネットワーク遠隔ホストデータベース, tnrhdb, 129
- トラステッドネットワーク遠隔ホストテンプレート, tnrhtp, 132
- トラステッドネットワーク情報の取得,
 - tsol_getrhtype, 96
- トラステッドネットワークゾーン構成データベース, tnzonecfg, 136
- トラステッドネットワークデータベース, 「ネットワークデータベース」を参照
- トラステッドネットワークデータベースのファイル構文の検査, tnchkdb, 42
- トラステッドネットワークデーモン, tnd, 47

な

- 内部テキストラベルの人間が読める形式への変換, hextoalabel, 27

に

- 人間が読めるラベルの内部テキスト形式への変換, atohexlabel, 25

ね

ネットワークコマンド

- smtnrhdb, 29
- smtnrhtp, 33
- データベースの構文の検査, 42
- トラステッドネットワークデータベースの構成, 44
- ネットワーク情報の出力, 49
- ネットワークデータベースの初期化, 47
- ネットワーク情報
 - tninfo, 49

ネットワーク情報 (続き)

トラステッドネットワークデータベースからの
遠隔ホストタイプの取得, 96

ネットワークデータベース

Solaris 管理コンソールからの tnrhdb の管理, 29

Solaris 管理コンソールからの tnrhttp の管理, 33

tnrhdb, 129

tnrhttp, 132

遠隔ホストタイプの取得, 96

カーネルの初期化, 47

構文の検査, 42

情報の出力, 49

トラステッドネットワークの構成, 44

ネットワークデータベースの初期化, tnd, 47

は

廃止または互換性がなくなる可能性がある関数

bcleartoh, 65

bcleartoh_r, 65

bcleartos, 62

bltcolor, 60

bltcolor_r, 60

bsltoh, 65

bsltoh_r, 65

bsltos, 62

h_alloc, 65

h_free, 65

htobclear, 75

htobsl, 75

sbcleartos, 86

sbsltos, 86

stobclear, 91

stobsl, 91

Xbcleartos, 81

Xbsltos, 81

ふ

ファイル

.copy_files, 51

.link_files, 51

pam_tsol_account, 146

ファイル (続き)

tnrhdb, 129

tnrhttp, 132

tnzonecfg, 136

TrustedExtensionsPolicy, 140

ラベルエンコーディング, 122

ラベルモデルの説明, 144

ファイルの機密ラベル

fgetlabel, 54

getlabel, 54

ファイルの機密ラベルの設定, setlabel, 88

ファイルの機密ラベルの変更, setlabel, 88

ファイルラベル

fgetlabel, 54

getlabel, 16, 54

setlabel, 88

setlabel, 19

ファイルラベルの変更, setlabel, 19

プロセスラベル

getplabel, 70

plabel, 18

ほ

ホームディレクトリファイルのコピー,

updatehome, 51

ホームディレクトリファイルのリンク,

updatehome, 51

も

文字列からラベルへの構文解析, str_to_label, 94

文字列からラベルへの変換, str_to_label, 94

文字列へのラベルの変換, label_to_str, 83

ゆ

ユーザーインタフェース, 76

ユーザーのラベル範囲の取得, 71

ら

ラベル

2つのラベルの上限と下限, 59
 Solaris Trusted Extensions のモデル, 144
 インタフェース, 76
 エンコーディングファイル, 122
 説明, 144
 内部テキスト形式への変換, 25
 人間が読める形式への変換, 27
 表示, 76
 ファイルラベルの取得, 16, 54
 ファイルラベルの設定, 19, 88
 プロセスラベルの取得, 18
 ホームディレクトリファイルの別ラベルへのコピー, 51
 ホームディレクトリファイルの別ラベルへのリンク, 51
 文字列からの構文解析, 94
 文字列への変換, 83
 ユーザーインタフェース, 76
 ラベルエンコーディングファイルの構文の検査, 26
 ラベルの構築, 76
 ラベルの比較, 58
 ラベルビルダー, 76
 ラベルインタフェース, ラベルビルダー, 76
 ラベルエンコーディングファイルの構文の検査, `chk_encodings`, 26
 ラベルが同等かどうかの比較, 58
 ラベルがラベル範囲内にあるかどうかの判定, 58
 ラベルの完全な優位性の比較, 58
 ラベルの優位性の比較, 58
 ラベルのユーザーインタフェースの作成, `tsol_lbuild_create`, 76
 ラベルのユーザーインタフェースの取得, `tsol_lbuild_get`, 76
 ラベルのユーザーインタフェースの破棄, `tsol_lbuild_destroy`, 76
 ラベルのユーザーインタフェースの変更, `tsol_lbuild_set`, 76
 ラベル範囲
 `blcompare`, 58
 `getdevicerange`, 67
 `getuserrange`, 71

ラベル表示, ラベルビルダー, 76

ラベルビルダー

`tsol_lbuild_create`, 76
`tsol_lbuild_destroy`, 76
`tsol_lbuild_get`, 76
`tsol_lbuild_set`, 76
 ラベルファイル, 144
 ラベルマッピング
 `getzoneidbylabel`, 72
 `getzonelabelbyid`, 72
 `getzonelabelbyname`, 72
 `getzonerootbyid`, 74
 `getzonerootbylabel`, 74
 `getzonerootbyname`, 74
 `label_to_str`, 83
 `str_to_label`, 94
 ラベルモデル, 144
 ラベルライブラリ
 `bldominates`, 58
 `blequal`, 58
 `blinrange`, 58
 `blmaximum`, 59
 `blminimum`, 59
 `blstrictdom`, 58
 `getdevicerange`, 67
 `getpathbylabel`, 68
 `getplabel`, 70
 `getuserrange`, 71
 `getzoneidbylabel`, 72
 `getzonelabelbyid`, 72
 `getzonelabelbyname`, 72
 `getzonerootbyid`, 74
 `getzonerootbylabel`, 74
 `getzonerootbyname`, 74
 `label_to_str`, 83
 `m_label_alloc`, 85
 `m_label_dup`, 85
 `m_label_free`, 85
 `setflabel`, 88
 `str_to_label`, 94
 `tsol_lbuild_create`, 76
 `tsol_lbuild_destroy`, 76
 `tsol_lbuild_get`, 76
 `tsol_lbuild_set`, 76

わ

ワークステーションの所有権の取得,
XTSOLgetWorkstationOwner, 108
ワークステーションの所有権の設定,
XTSOLsetWorkstationOwner, 119