管理者ガイド

Sun™ ONE Directory Proxy Server

Version 5.2

817-4654-10
2003 年 6 月

Copyright © 2003 Sun Microsystems, Inc. Some preexisting portions Copyright © 2001 Netscape Communications Corporation. Copyright © 1996-1998 Critical Angle Inc. Copyright © 1998-2001 Innosoft International, Inc. All rights reserved.

Sun 、Sun Microsystems 、Sun のロゴマークは、米国およびその他の国における米国 Sun Microsystems, Inc. (以下、米国 Sun Microsystems 社とします) の商標もしくは登録商標です。Netscape および Netscape の N のロゴマークは、米国およびその他の国における Netscape Communications Corporation 社の登録商標です。その他の Netscape のロゴマーク、製品名、およびサービス名もまた、米国の Netscape Communications Corporation の商標であり、その他の国においても登録されている可能性があります。

Sun ONE Directory Proxy Server 製品の一部はミシガン大学、カリフォルニア大学バークレイ校、およびハーバード大学にそれぞれ著作権があるソフトウェアに由来しています。特に事前の書面による許可なしにここで言及されている製品もしくは文書に由来する製品を推薦または宣伝するためにこれらの大学の名称を使用することはできません。

Sun ONE Directory Proxy Server の一部の著作権は The Internet Society (1997) にあります。

Federal Acquisitions: Commercial Software-Government Users Subject to Standard License Terms and Conditions

本書で説明されている製品は著作権法により保護されており、その使用、複製、頒布および逆コンパイルを制限するライセンスのもとにおいて頒布されます。Sun | Netscape Alliance および Sun のライセンサーの書面による事前の許可なく、本製品および関連する文書のいかなる部分も、いかなる方法によっても複製することが禁じられます。

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ないものとします。

目 次

図目次

本書について

この管理者ガイドでは、Sun™ Open Net Environment (Sun ONE) Directory Proxy Server のさまざまな配備例を紹介し、設定と管理の方法について説明します。

ここでは次の項目について説明します。

本書の対象読者

『Directory Proxy Server 管理者ガイド』は、1 つまたは複数のサーバーを設定、操作する管理者を対象に記述されています。本書は、ユーザーが次の背景知識を持つことを前提としています。

- インターネットと LDAP に関する一般的な理解
- Sun ONE Directory Server 5.x とその管理に関する一般的な理解。ディレクトリデータを読み取り、それを変更できる能力が必要です。

本書の内容

本書は、次の 3 つの部に分かれています。

- 第 1 部「Sun ONE Directory Proxy Server の概要」
- 第 2 部「コンソールベースの管理」
- 第 3 部「付録」

表記上の規則

このマニュアルで使用している表記上の規則について説明します。

モノスペース（固定スペースフォント）: コンピュータの画面に表示されるテキストおよび入力するテキストに使用します。また、ファイル名、機能および例にも使用します。

注	「注」、「注意」は、重要な情報です。必ずこれらの情報を読んでから、作業を続けてください。

大なり記号 (>) は、連続するメニュー選択項目を分けるために使用します。たとえば、「オブジェクト」> 「新規」> 「ユーザー」は、「オブジェクト」メニューのプルダウンメニューを開き、マウスをドラッグして「新規」を強調表示し、「新規」のサブメニューから「ユーザー」を選択することを意味します。

このマニュアルでは、次の形式でパスを示します。

`<server-root>/dps-<hostname>/...`

この `<server-root>` はデフォルトのインストールディレクトリで、`<hostname>` は Directory Proxy Server をインストールしたホストマシンの名前です。たとえば、インストールディレクトリが `/usr/sunone/servers` で、マシンのホスト名が `testmachine` の場合、実際のパスは次のようになります。

`/usr/sunone/servers/dps-testmachine/. . .`

このマニュアルでは、すべてのパスを UNIX 形式で記述しています。Windows ベースのディレクトリサーバーを使用している場合は、本書の UNIX ファイルパスを Windows のファイルパスに読み替えてください。

関連情報

このマニュアルのほかに、Directory Proxy Server には次のマニュアルセットが用意されています。

- 『Sun ONE Directory Proxy Server リリースノート』: このリリースノートには、Directory Proxy Server のリリース時に明らかになっている重要な情報が記載されています。新機能と機能拡張、既知の問題、その他の最新情報がとりあげられます。このマニュアルを読んでから、Directory Proxy Server の使用を始めてください。
- 『Sun ONE Directory Proxy Server インストールガイド』: このマニュアルには、Directory Proxy Server のインストール手順、および要件と調整に関する情報が記載されています。

Sun ONE に関するその他の有用な情報は、次の Web サイトから入手できます。

- 製品のオンラインマニュアル : `http://docs.sun.com`
- 製品サポートおよび状況 : `http://www.sun.com/service/support/software/`
- Sun Enterprise Service for Solaris のパッチとサポート : `http://www.sun.com/service/`
- 開発者向けの情報 : `http://www.sun.com/developers/`
- サポートおよびトレーニングの情報 : `http://www.sun.com/supportraining`
- 製品のデータシート : `http://www.sun.com/software/`

ユーザー補助機能

Java™ Foundation Classes (JFC) に基づいて、Sun ONE Directory Proxy Server コンソールでは、障害をもつユーザーのための支援ソフトウェアおよび技術をサポートしています。この節では、Sun ONE Directory Proxy Server コンソールの補助機能、および使いやすいように改善された、マニュアルセットの箇所について説明します。

コンソールの補助機能

次に示す補助機能の多くは、JFC/Swing! コンポーネントを利用して自動的に提供されます。

分かりやすい名前および説明

すべてのオブジェクトには、分かりやすい名前 (オブジェクトの使用目的を簡単に示したもの) が付いています。名前を使用して、補助機能はオブジェクトをユーザーに表示します。分かりやすい説明では、オブジェクトについてのより詳細な情報が提供されます。

カスタマイズ可能なフォント

テキストペイン、メニュー、ラベル、および情報メッセージのフォントスタイルおよびサイズをカスタマイズできます。

カラーコードを使用して情報伝達は行われますが、それが唯一の方法ではありません。

GUI の動的レイアウト

動的レイアウトを使用して、Directory Server のウィンドウサイズおよび位置を指定できます。また、その指定をユーザー設定として確定できます。

キーボードで操作できるコンポーネント

この補助機能は、マウスを使用するのが困難なユーザーに対応しています。Tab キーを押すと、入力フォーカスが、あるコンポーネントから別のコンポーネントに移動し、Shift キーを押しながら Tab キーを押すと、フォーカスは反対方向に移動します。矢印キーを使用すると、マウスを使用しないでツリーをナビゲートできます。

フォーカスはプログラムで検出されるため、支援ソフトウェアでフォーカスやフォーカスの変更を追跡することができます。

テキスト以外の要素と同等のテキスト要素

プログラム要素が画像で示されている場合、その情報はテキストでも提供されます。

同等のコマンド行インタフェース

コンソールのほとんどの機能は、コマンド行からも実行できます。コマンド行インタフェースについて、詳しい説明を表示させることができます。

マニュアルの補助機能

Sun ONE Directory Proxy Server 5.2 のマニュアルセットは、PDF と HTML 形式の両方で入手できます。ここでは、HTML 形式のマニュアルの補助機能について説明します。

テキスト以外の要素と同等のテキスト要素

補助的なテキストラベルは、リンクあるいはグラフィックに割り当てられます。グラフィックを説明するテキストは周辺テキスト、または別のファイルで提供されます。

補助技術で解釈可能なテーブル

すべてのテーブルには、説明的なヘッダーが含まれています。テーブルの内容については、周辺テキストでも簡潔に説明されています。

第 1 部

Sun ONE Directory Proxy Server の概要

第 1 章「Sun ONE Directory Proxy Server の概要」

第 2 章「Sun ONE Directory Proxy Server の配備例」

第 1 章

Sun ONE Directory Proxy Server の概要

この章では、Sun ONE Directory Proxy Server の概要について説明します。この章は、次の節から構成されています。

概要

Sun ONE Directory Proxy Server は、電子商取引ソリューションで使用されるミッションクリティカルなディレクトリサービスの重要なコンポーネントです。Directory Proxy Server は、強化されたディレクトリアクセス制御、スキーマ互換性、およびアプリケーション層のロードバランスとフェイルオーバーによる高い可用性を提供する、LDAP アプリケーション層プロトコルゲートウェイです。

機能の面から見ると、Directory Proxy Server は LDAP クライアントと LDAP ディレクトリサービスの間に置かれる「LDAP アクセスルータ」です。LDAP クライアントからの要求を、Directory Proxy Server の設定に定義されている規則に基づいてフィルタリングし、LDAP ディレクトリサーバーに転送することができます。ディレクトリサーバーからの結果は、フィルタリングされ、クライアントに戻されます。この処理には、Directory Proxy Server の設定に定義されている規則が適用されます。このプロセスは、LDAP クライアントには完全に透過的です。LDAP クライアントは、通常の LDAP ディレクトリサーバーに接続するように Directory Proxy Server に接続します。

Directory Proxy Server は、高い可用性、セキュリティ、クライアント互換性機能を、エクストラネットとイントラネットの両方のディレクトリインフラストラクチャに提供するユニークな製品です。主な機能は次のとおりです。

- 自動的なロードバランス
- 透過的なサーバーフェイルオーバーとフェイルバック

- 自動的なリフェラル実行
- エクストラネットおよびイントラネットのアクセス制御グループ
- セキュリティ保護されたクライアントおよびサーバーの認証
- クエリと応答のダイナミックなフィルタリング
- ダイナミックなスキーママッピング
- ディレクトリベースまたはファイルベースの設定
- 設定可能なログ記録

Directory Proxy Server は新しいまたは既存の LDAP ディレクトリインフラストラクチャと共存し、その機能を補完します。また、企業のエクストラネットおよびイントラネットにすでに配備されているディレクトリ対応アプリケーションとシームレスに統合できます。このため、既存のディレクトリインフラストラクチャ投資を活用するように配備することができます。Directory Proxy Server は、あらゆる LDAP 互換ディレクトリサーバーと相互動作します。Directory Proxy Server は、LDAP に対応準拠する、ネイティブ LDAP ディレクトリ、LDAP 対応 X.500 ディレクトリ、または LDAP 対応リレーショナルデータベースなどすべてのディレクトリで使用できます。

Directory Proxy Server は LDAPv3 インターネット仕様を実装しますが、すでに配備され、LDAPv2 を使用するディレクトリ対応クライアントアプリケーションとの互換性を維持するために、機能が少なく、古い LDAPv2 仕様もサポートします。Directory Proxy Server は、UNIX および Windows プラットフォームで独立したシステムサーバープロセスとして実行されます。サーバーはマルチスレッド化され、数千の LDAP クライアント要求を処理すると同時に、各要求にアクセス制御規則とプロトコルフィルタリング規則を適用できます。

Directory Proxy Server は、組織が非公開ディレクトリ情報を未認証のアクセスから保護し、公開情報の安全なパブリッシングを行う上で役立ちます。Directory Proxy Server を使用することで、LDAP ディレクトリに対する詳細なアクセス制御ポリシーを設定できます。たとえば、ディレクトリ情報ツリー (DIT) の特定部分に対して特定の操作を実行できるユーザーを制御することができます。また、Web トローラやロボットが情報収集のためによく実行する特定種類の操作を許可しないように Directory Proxy Server を設定することもできます。

Web プロキシサーバーとは異なり、Directory Proxy Server は逆プロキシモードで動作します。ファイアウォール内のクライアントからは、インターネット上の任意のサーバーに対して順方向に接続しません。また、検索結果もキャッシュしません。その主な理由は、データにアクセス制御を適用する問題です。現時点では、この動作はアクセス制御が管理される LDAP ディレクトリサーバーだけで行われています。Directory Proxy Server は、ディレクトリサーバーのアクセス制御には一切関与しません。

Directory Proxy Server の機能セット

Directory Proxy Server の機能セットには、高い可用性、ロードバランス、フェイルオーバー、ファイアウォールのようなセキュリティ、クライアントとサーバーの互換性など、独特な機能が含まれます。

高い可用性

Directory Proxy Server は、レプリケートされている LDAP ディレクトリサーバー間で、自動的なロードバランスと、自動的なフェイルオーバーおよびフェイルバックを行うことで、配備したディレクトリの高い可用性を実現します。エクストラネット環境やイントラネット環境では多くの場合、ミッションクリティカルなディレクトリ対応クライアントとアプリケーションからディレクトリデータに、1 日 24 時間、週に 7 日アクセスできることが必要になります。Directory Proxy Server は、認識しているすべてのディレクトリサーバーの接続状態情報を維持し、設定されているディレクトリサーバー間で LDAP 処理の比例ロードバランスを動的に実行できます。1 つまたは複数のサーバーが使用不能になった場合、その負荷は残りのサーバーに比例配分されます。ディレクトリサーバーがオンライン状態に戻ると、負荷は動的かつ比例的に割り当て直されます。

たとえば、ディレクトリサーバー A が LDAP クライアントロードの 40%、サーバー B が 20%、サーバー C が 20%、サーバー D が 20% を受け持つように設定されていると仮定します。ディレクトリサーバー B が使用不能になると、Directory Proxy Server はサーバー A がサーバー C、D の 2 倍の負荷を受け持つように設定されていることを認識し、サーバー B が受け持つ 20% 分の負荷を比例配分し、A が 50%、C が 25%、D が 25% を受け持つように変更します。ディレクトリサーバー B が復帰すると、Directory Proxy Server はそれを検出し、4 つのサーバー全体で負荷を元の設定割合に戻します。

ネットワーク層 IP ロードバランスデバイスは、LDAP プロトコル層にアクセスできません。しかし、Directory Proxy Server はロードバランスをアクセス制御、クエリフィルタリング、クエリルーティングと統合し、アプリケーション層アクセス制御と LDAP ルーティングの決定をインテリジェントに行うことができます。

ロードバランス

222 ページの「ids-proxy-sch-LoadBalanceProperty オブジェクトクラス」で説明するロードバランスプロパティ、または第 7 章「プロパティオブジェクトの定義と管理」で説明するロードバランスプロパティを使用して、Directory Proxy Server にロードバランスを設定する必要があります。Directory Proxy Server が通信できるバックエンドディレクトリサーバーには、合計クライアントロードの何パーセントを受け持つかがそれぞれに設定されます。Directory Proxy Server は、この設定に定義されている負荷条件に合わせて、各バックエンドサーバーにクライアントクエリを自動的に配分します。サーバーが使用不能になると、Directory Proxy Server はこのサーバーの受け持ち負荷を、残りのサーバーのそれぞれの受け持ち負荷の割合に基づいて再配分します。すべてのバックエンド LDAP サーバーが使用不能になると、Directory Proxy Server はクライアントからのクエリを拒否するようになります。

Directory Proxy Server のロードバランスはセッションベースで行われます。つまり、クライアントからのクエリを担当させるサーバーを選択する決定機能は、クライアントセッションごとに、特にクライアントセッションの開始時に適用されます。そのセッションの以後のすべてのクライアントクエリは、セッションの開始時に選択されたサーバーに向けられます。

Directory Proxy Server がロードバランスを行えるバックエンド LDAP サーバーの数は、いくつかの条件によって変わります。この条件には、Directory Proxy Server が稼動するホストのサイズ、利用できるネットワーク帯域幅、Directory Proxy Server が受信するクエリミックス、クライアントセッションの時間的な長さ、Directory Proxy Server の設定が含まれます。一般に、ほとんどのセッションの存続時間が短く、クエリがコンピュータ集約型である場合は、Directory Proxy Server がサポートできるサーバーの数は少なくなります。コンピュータ集約型のクエリは、106 ページの「属性名変更プロパティ」で説明する属性名変更機能が使用される場合のように、メッセージ全体の検査を必要とします。

Directory Proxy Server は監視プロセスを使用して、バックエンドサーバーを診断します。対象には、SSL を通じてだけ通信するバックエンドサーバーも含まれます。ロードバランスを使用する場合は、この機能は自動的に有効になります。Directory Proxy Server は、それぞれのバックエンドディレクトリサーバーに対して 10 秒おきに Root DSE の匿名検索を実行します。いずれかが使用不能になったり、応答を返さない場合、サーバーセットのロードバランスのために Directory Proxy Server はそのサーバーをセットから外します。使用可能な状態に戻ると、このサーバーはセットに戻されます。

フェイルオーバー

サーバーが使用不能になったことを Directory Proxy Server が検出するのは、接続試行時に接続拒否が返された場合と、タイムアウトが生じた場合です。どちらもセッションの初期段階で発生し、そのセッションのための処理はまだ行われていないため、Directory Proxy Server は透過的に使用可能な別のサーバーがあれば、そのサーバーにフェイルオーバーします。接続試行時にタイムアウトが生じた場合は、クライアントは応答の取得まで長く待たされる可能性があります。Directory Proxy Server とバックエンドサーバーとの間の接続が急に失われた場合、Directory Proxy Server は進行中のすべての処理について、影響を受けるクライアントに LDAP_BUSY エラーを返します。続いて、Directory Proxy Server はそのクライアントセッションを別のディレクトリサーバーにフェイルオーバーします。

Directory Proxy Server がディレクトリ配備のシングルポイント障害となることがないように、少なくとも 2 つの Directory Proxy Server を使用し、その前段に IP 関連装置を構成することをお勧めします。

セキュリティ

Directory Proxy Server には柔軟な外部ディレクトリアクセス制御機能が用意されており、ディレクトリサーバーによる基本的なアクセス制御を強化することができます。アクセス制御メカニズムでは、特定のユーザーやユーザーコミュニティに特定のアクセスグループを関連付けることができ、このアクセスグループには、管理者が定義したセキュリティ制限とクエリフィルタが適用されます。管理者は、LDAP 認証情報、IP アドレス、ドメイン名などの条件に基づいてエントリへのアクセスを制御できます。

Directory Proxy Server が提供する重要なセキュリティ機能に、LDAP クライアントと LDAP ディレクトリサーバーの間で確立されている接続の数による保護があります。並行して実行されているクライアント処理の数、1 回の接続でクライアントが要求できる処理の数、特定のクライアントグループの接続数など、数多くの指標を監視するように Directory Proxy Server を設定することで、LDAP ディレクトリサーバーを接続攻撃から保護することができます。また、無効になったクライアントをタイムアウトにすることもできます。

Directory Proxy Server では、特定の指標にしきい値を設定することもできます。Directory Proxy Server はこれらの指標を監視し、その値がしきい値を超えていないことを確認します。Directory Proxy Server は、ディレクトリのトローリングやサービス拒否攻撃の可能性を制限するために、特定のホストから開かれている接続の数、特定のセッションで実行された処理の数などのいくつかの指標を維持します。これらのパラメータの設定については、65 ページの「システム設定インスタンスの作成」を参照してください。

Directory Proxy Server は、(cn=A*) や (cn>A) などの特定種類の汎用フィルタを禁止することによってもトローリングを制限しています。フィルタのフィルタリングを設定する方法については、第 6 章「グループの作成と管理」を参照してください。

Directory Proxy Server では、認証されたクライアントはディレクトリサービスへのアクセス制御を変更できます。これにより、認証されたクライアントがセキュリティ保護されたネットワークの外にある場合でも、ディレクトリ情報に対して強力なアクセス権を持つことができます。

Directory Proxy Server は、SSL (Secure Socket Layer) 転送プロトコルによるデータの保護に対応しています。たとえば、保護されたネットワークの外からディレクトリサービスにアクセスするすべてのクライアントに対して、SSL セッションの確立を要求するように Directory Proxy Server を設定することができます。SSL の設定については、155 ページの「セキュリティの設定」の「Directory Proxy Server」を参照してください。

これらの機能は、近年一般化してきた「サービス拒否攻撃」や「洪水攻撃」の防止に役立ちます。Directory Proxy Server は、しきい値の超過を検出すると、ディレクトリサーバーへの接続を拒否するようになり、ディレクトリサーバーを攻撃や過大な集中アクセスから保護します。

クライアントとサーバーの互換性

Directory Proxy Server は、LDAP 識別名 (DN) とグループアクセス権 (認証の証明情報に基づくモバイルユーザーの識別を含む) に基づいてクエリのルーティングを決定します。Directory Proxy Server は、ディレクトリサービスの高度な分散とスケーラビリティをサポートするために、LDAP リフェラルを自動的に実行します。このリフェラルには、ディレクトリサーバーから返されたリフェラルも含まれます。リフェラルの自動実行は、ディレクトリサーバーのセットにディレクトリ情報を物理的に分散させる必要があり、その分散されたディレクトリがユーザーからは 1 つの論理ディレクトリに見えるような大規模なディレクトリ配備で大きな利点となります。Directory Proxy Server は、分散されたディレクトリデータを論理的に統合する機能を提供することで、このような配備例に対応し、これによってスケーラブルな分散ディレクトリサービスをサポートします。

Directory Proxy Server は、LDAPv2 または LDAPv3 に準拠するあらゆるクライアントアプリケーションをサポートします。これは、スキーマの書き替えにより、ディレクトリサーバーのスキーマと常に一致するとは限らない固定スキーマを持つクライアントアプリケーションに対応することで実現されています。たとえば、Microsoft Outlook™ 電子メールクライアントには、Microsoft が定義した属性がディレクトリサーバーに実装されることを前提とした固定スキーマがあり、これは、企業のより一般的なスキーマ要件と一致しない可能性があります。スキーマ書き替え機能により、ディレクトリシステムの管理者は企業の汎用スキーマを実装し、そのスキーマの特定の要素を、機能が限定されているクライアントアプリケーションで必要とされる属性

タイプのセットにダイナミックにマッピングすることができます。それ以外の面では、Directory Proxy Server はスキーマを重用しません。多くの標準で定義されているあらゆる属性タイプやオブジェクトクラスだけでなく、RFC1274、X.520、X.521、LIPS、PKIX、inetOrgPerson、DEN など、業界で提唱されている特別なスキーマ定義の属性タイプとオブジェクトクラスも受け付けます。

第 2 章

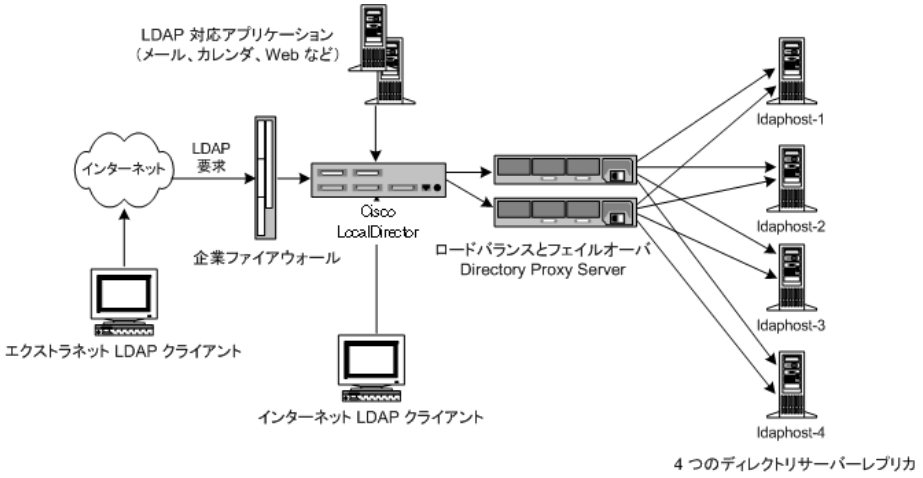
Sun ONE Directory Proxy Server の配備例

利用しているコンピュータ環境に応じて、Sun ONE Directory Proxy Server をさまざまな方法で配備することができます。この章では、次のような代表的な配備について説明します。

高い可用性の社内構成

図 2-1 は、LDAP インフラストラクチャを社内だけで使用するように配備した構成を示しています。この企業の LDAP サービスにアクセスするには、外部ネットワークは必要ありません。社内の LDAP サービスに対するファイアウォールの外部からのアクセスを拒否するように、企業ファイアウォールが配備されています。内部で発生するすべてのクライアント LDAP 要求は、(高可用性のために) Cisco LocalDirector を経由して Directory Proxy Server に入ります。Cisco LocalDirector は、クライアントが少なくとも 1 つの Directory Proxy Server にアクセスできるようにするための IP パケットスイッチの一例に過ぎません。Sun ONE Directory Proxy Server を実行しているホスト以外からは、誰もディレクトリサーバーに直接アクセスできません。この制限は、ディレクトリサーバーと Directory Proxy Server を実行しているホストをファイアウォールによって保護することで行われています。

図 2-1　高い可用性の社内構成



分散型の LDAP ディレクトリインフラストラクチャ

次に、分散型の LDAP ディレクトリインフラストラクチャで Directory Proxy Server が果たす役割について説明します。

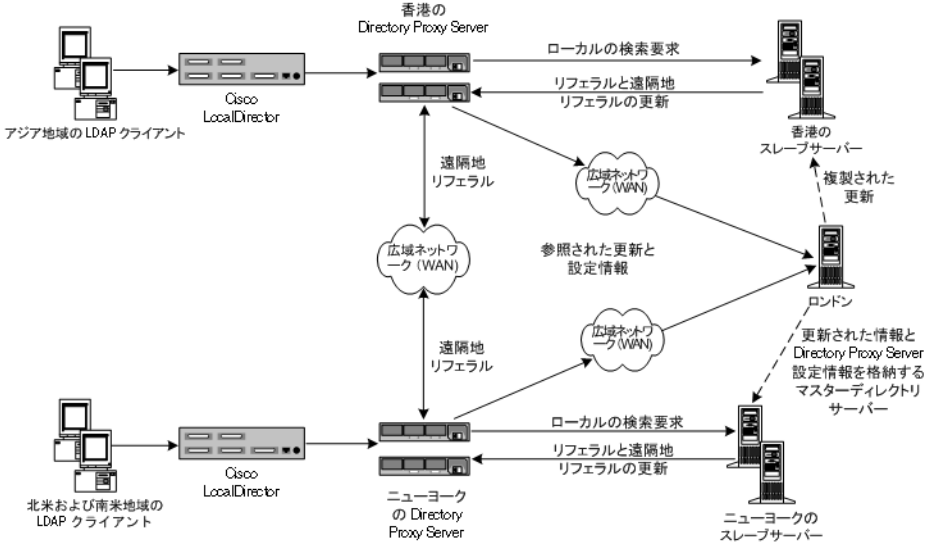
- 事例の背景
- 配備例
- LDAP 要求の流れ

事例の背景

図 2-2 は、ロンドンに本社があり、ロンドン、ニューヨーク、香港にデータセンターを持つ大手金融機関の構成を示しています。現在、従業員が利用するデータのほとんどは、ロンドンにある旧式の RDBMS リポジトリに格納されています。この金融機関のクライアントコミュニティからこのデータへのすべてのアクセスは、広域ネットワーク (WAN) を経由します。この金融機関は、この集中型のモデルのスケーラビリティとパフォーマンスに不満を感じており、分散型のデータモデルに移行することを決断しました。また、同時に LDAP ディレクトリインフラストラクチャの配備も決定しました。問題となっているデータは「ミッションクリティカル」であるとされており、高い可用性と耐障害性を持つインフラストラクチャに配備する必要があります。

クライアントアプリケーションプロファイルを分析することで、ある地域別クライアントコミュニティによるデータへのアクセスの 95% は、そのコミュニティ自体に対するものであることが判明しました。これは、データが顧客ベースであるためです。アジアのクライアントが北米の顧客データにアクセスすることはほとんどありません。ただし、皆無ではありません。また、クライアントは顧客情報を随時更新する必要があります。

図 2-2　分散型の LDAP ディレクトリインフラストラクチャ



配備例

プロファイルの 95% がローカルデータアクセスであることから、この金融機関は LDAP ディレクトリインフラストラクチャを地域別に分散することにしました。複数のディレクトリコンシューマサーバーが各地域 (香港、ニューヨーク、ロンドン) に配備されます (この図にはロンドンのコンシューマサーバーは含まれません)。これらのコンシューマサーバーは、その地域の顧客データを保持するように設定されています。ヨーロッパと中東の顧客データはロンドンのコンシューマサーバーに格納され、北米と南米の顧客データはニューヨークのコンシューマサーバーに格納されます。アジアと太平洋地域の顧客データは香港のコンシューマサーバーに保持されます。この配備では、ローカルクライアントコミュニティが必要とするデータの大部分はそのコミュニティで保持されます。クライアント要求がローカルに処理されることになるため、集中型モデルと比較してパフォーマンスが大きく向上します。ネットワークのオーバーヘッドが減り、ローカルディレクトリサーバーが効率的にディレクトリイン

フラストラクチャをパーティション分割します。これにより、ディレクトリサーバーのパフォーマンスとスケーラビリティは向上します。コンシューマディレクトリサーバーの各セットは、クライアントが更新要求を送信した場合、またはクライアントがいずれかの場所に格納されているデータに対する検索要求を送信した場合にリフェラルを返すように設定されています。

LDAP 要求の流れ

クライアントからの LDAP 要求は、Cisco LocalDirector 経由で Sun ONE Directory Proxy Server に送信されます。この Cisco LocalDirector は、クライアントが少なくとも 1 つの Directory Proxy Server にアクセスできるようにするための IP パケットスイッチの一例に過ぎません。ローカル配備された Directory Proxy Server は、まず、すべての要求をローカル顧客データを保持するローカルディレクトリサーバーの配列にルーティングします。Directory Proxy Server のインスタンスは、配列に含まれるディレクトリサーバー間で負荷をバランスするように設定されており、フェイルオーバーとフェイルバックは自動的に行われます。ローカル顧客情報に対するクライアント検索要求は、ローカルディレクトリ内で処理が完了し、適切な応答が Directory Proxy Server 経由でクライアントに返されます。地域が異なる顧客の情報に対するクライアント検索要求は、Directory Proxy Server にリフェラルを返すことで、初期段階はローカルディレクトリサーバー内で完了します。

このリフェラルには、別地域に分散している Directory Proxy Server の適切なインスタンスをポイントする LDAP URL が含まれます。ローカル Directory Proxy Server は、ローカルクライアントの代わりにリフェラルを処理し、遠隔地の Directory Proxy Server の適切なインスタンスに対して検索要求を送信します。遠隔地の Directory Proxy Server は、検索要求を遠隔地のディレクトリサーバーに送信し、適切な応答を受信します。この応答は、遠隔地とローカルの Directory Proxy Server を経由してローカルクライアントに返されます。

ローカル Directory Proxy Server が受信する更新要求も、ローカルディレクトリサーバーがリフェラルを返すことで、その初期段階は内部的に完了します。この場合も、Directory Proxy Server がローカルクライアントの代わりにリフェラルを実行しますが、更新要求の場合は、ロンドンにあるサプライヤディレクトリサーバーが送信先となります。このサプライヤディレクトリは、サプライヤデータベースに更新を適用し、応答をローカル Directory Proxy Server 経由でローカルクライアントに返します。その後、サプライヤディレクトリサーバーは適切なコンシューマディレクトリサーバーに更新を伝達します。

すべての Sun ONE Directory Proxy Server は、起動時にそれぞれの設定情報をサプライヤディレクトリサーバーから検索するように設定されています。これにより、Directory Proxy Server の複数のインスタンスを分散しても、それぞれの設定を集中管理することができます。

集中型の LDAP ディレクトリインフラストラクチャ

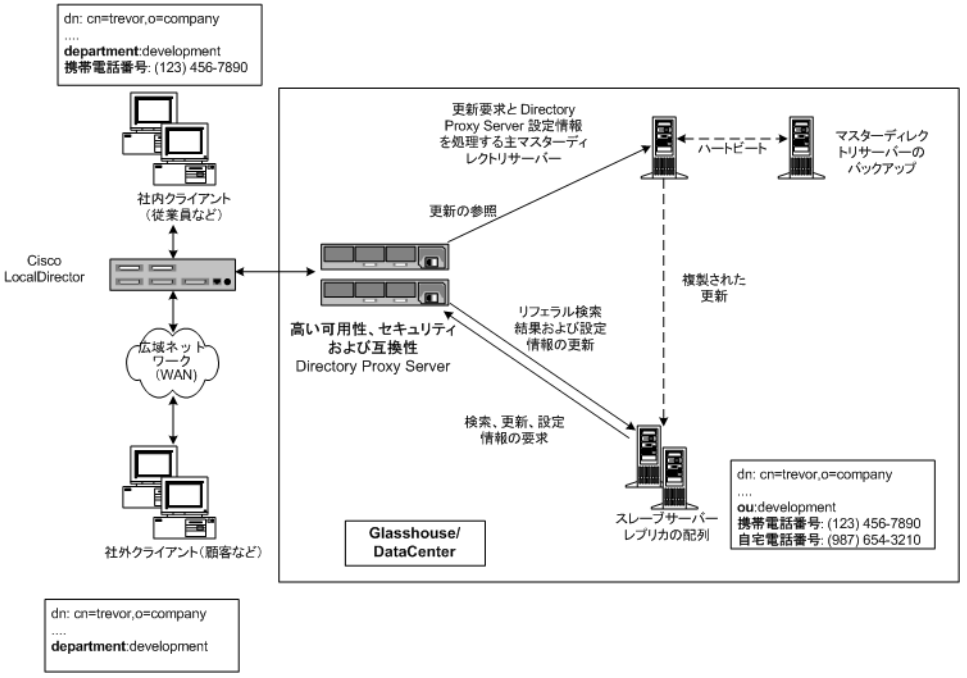
次に、集中型の LDAP ディレクトリインフラストラクチャで Directory Proxy Server が果たす役割について説明します。

- 事例の背景
- 配備例
- LDAP 要求の流れ

事例の背景

図 2-3 は、顧客と従業員が世界各地に分散している大規模な多国籍企業での配備例を示しています。この企業は企業電子電話帳を配備することで、紙媒体の電話帳を製作するコストを削減し、企業情報の精度を向上させ、環境資源を節約することを目指しています。電話帳情報は、適切なアクセス制御によって制限することで、顧客と従業員の両方に公開する必要があります。また、顧客と従業員が世界のさまざまなタイムゾーンに分散しており、1 日 24 時間、週に 7 日利用できる必要があるため、この電話帳はミッションクリティカルとして位置付けられています。

図 2-3　集中型の LDAP ディレクトリインフラストラクチャ



配備例

この企業は、電子電話帳を配備するために集中型の LDAP ディレクトリインフラストラクチャを配備することにしました。集中型の配備を選択したのは、この電子電話帳に登録される情報が、従業員に関する情報だけであるためです。これは顧客データベースではありませんが、配備の目的は、顧客が情報にアクセスできるようにすることにあります。予想されるディレクトリデータベースのサイズ (200,000 エントリ以下) では、スケーラビリティとパフォーマンスのどちらにも問題が生じることはないと予想され、より複雑な分散型の配備モデルは必要ないと判断されました。

高い可用性が要求されるため、単一のサプライヤディレクトリサーバーから複数のコンシューマディレクトリサーバーレプリカにデータを伝達する配備が選択されました。単一のサプライヤディレクトリサーバーがシングルポイント障害になるのを避けるため、この企業はバックアップのサプライヤディレクトリサーバーも配備しました。

Sun ONE Directory Proxy Server が配備されたのは、次の 3 つの理由からです。まず、すべての LDAP クライアントとディレクトリサーバーレプリカの配列の間で、ロードバランスと自動フェイルオーバーおよびフェイルバックを行うためです。次に、外部クライアントと内部クライアントを識別してそれぞれに適切なアクセス制御を設定す

るためです。最後に、電子電話帳を利用する LDAP クライアントとディレクトリサーバー自体との間で互換性を維持するためです。LDAP クライアントは、カスタム構築された電子電話帳アプリケーション以外にも、多数の市販 LDAP 対応アプリケーションを使用しており、これらのアプリケーションではスキーマ要件が固定されています。これらのスキーマ要件は、企業が設計したディレクトリスキーマと常に一致するとは限りません。このため、一部の基本的なスキーマ属性のマッピングが必要となります。さらに、クライアントが使用する LDAP 対応アプリケーションのすべてがディレクトリサーバーから受け取るリフェラルを正しく処理できるわけではありません。Sun ONE Directory Proxy Server は、クライアントの代わりにこれらのリフェラルを実行するように設定されました。

LDAP 要求の流れ

社内クライアント、社外クライアントを問わず、また、それが検索要求であるか、更新要求であるかを問わず、すべてのクライアント要求は、Cisco LocalDirector 経由で Directory Proxy Server のインスタンスに送信されます。この Cisco LocalDirector は、クライアントが少なくとも 1 つの Directory Proxy Server にアクセスできるようにするための IP パケットスイッチの一例に過ぎません。シングルポイント障害が発生しないように、Directory Proxy Server の複数のインスタンスが配備されています。Directory Proxy Server のインスタンスは、配列に含まれるすべてのコンシューマディレクトリの間で、クライアントから受け取ったすべての要求の負荷をバランスさせます。また、Directory Proxy Server はコンシューマサーバーの障害を検出し、配列内で利用可能なコンシューマサーバーにフェイルオーバーします。

コンシューマサーバーは読み取り専用のレプリカなので、クライアントから更新要求を受け取った場合は LDAP リフェラルを返すように設定されています。このリフェラルには、サプライヤディレクトリサーバーをポイントする LDAP URL が含まれます。ディレクトリサーバーがリフェラルを返すと、Directory Proxy Server はそれを認識し、クライアントに代わってそのリフェラルを実行します。Directory Proxy Server はサプライヤディレクトリサーバーにバインドし、更新要求を送信します。このサプライヤディレクトリは、サプライヤデータベースに更新を適用し、Directory Proxy Server 経由でクライアントに応答を返します。その後、サプライヤディレクトリサーバーは適切なコンシューマディレクトリサーバーに更新を伝達します。

クライアントから送信された検索要求は、Directory Proxy Server 経由でコンシューマディレクトリサーバーレプリカの配列にルーティングされます。Sun ONE Directory Proxy Server は、検索要求をディレクトリサーバーに送信する前に、これらの要求を「検査」し、特定のクライアントグループに設定されているアクセス制御規則とセキュリティ規則に違反する要求をフィルタリングして、必要なマッピングを行うように設定することができます。また、ディレクトリサーバーから返される検索結果を「検査」し、適切なフィルタリングとマッピングを行うように Directory Proxy Server を設定することもできます。図 2-3 の例では、社内と社外の両方のクライアントが「Trevor」

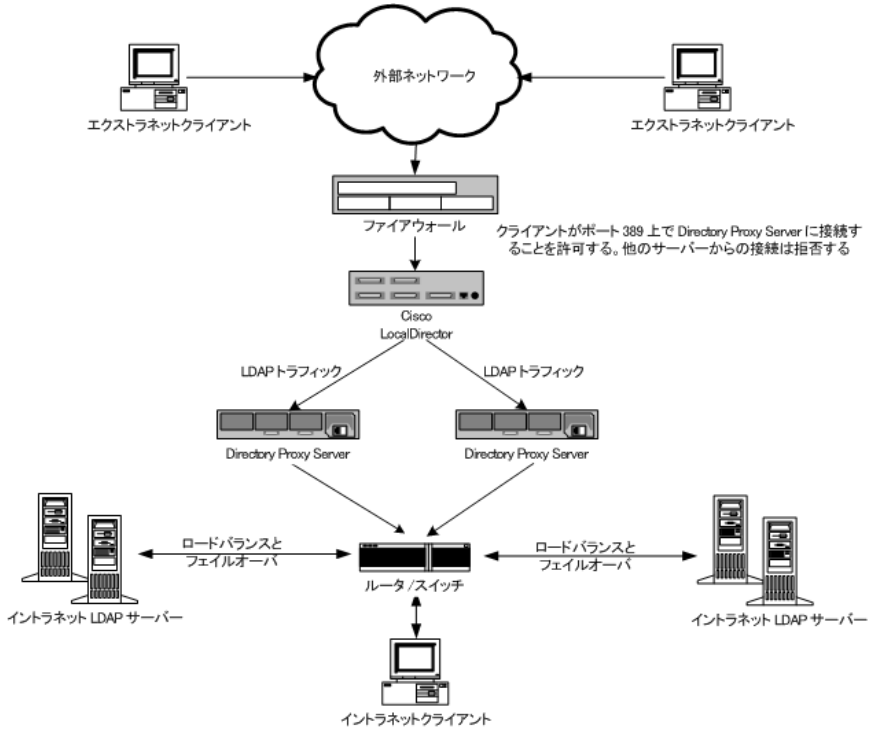
に属するエントリの検索を要求しています。これらの要求は、Directory Proxy Server ではクライアントの種類に関係なく、同じように扱われます。ディレクトリサーバーは要求を正常に実行し、「Trevor」のエントリを Directory Proxy Server に返します。Directory Proxy Server は、要求の送信元が社内クライアントであるか社外クライアントであるかに応じて、検索結果に異なる処理を行うように設定されています。外部クライアントの場合は、エントリに含まれる携帯電話の番号と自宅の電話番号のフィールドは、顧客向けではないデータとしてフィルタリングされます。また、「ou: development」という属性と値のペアが、「department: development」にマッピングされることに注意してください。これは、クライアントがディレクトリへのアクセスに使用するアプリケーションの 1 つが (たとえば、Outlook、Outlook Express)、企業ディレクトリサーバーに配備されているスキーマ要素と一致しない固定スキーマ要素を持っているためです。社内クライアントの場合は、携帯電話の番号は重要なデータ要素として従業員間で共有されますが、自宅の電話番号は共有されないことになっています。このため、社内クライアントからの要求に対しては、Directory Proxy Server は自宅の電話番号だけをフィルタリングし、携帯電話の番号をクライアントに公開します。ここでも ou 属性が department 属性にマッピングされていることに注意してください。

すべての Sun ONE Directory Proxy Server は、起動時にサプライヤディレクトリサーバー内の設定を検索するように設定されています。これにより、複数の Directory Proxy Server の設定を 1 つのディレクトリから集中的に管理できます。

1 つのファイアウォールを使用した Directory Proxy Server の配備

企業のファイアウォールを図 2-4 のように構成し、LDAP クライアントだけが Directory Proxy Server が稼動するマシンとポートにアクセスできるように制限する必要があります。通常は、LDAP クライアントは TCP ポート 389 に接続します。これにより、未認証でアクセスしようとするクライアントから Directory Proxy Server を実行するホストが保護されます。また、ルータスイッチを使用して、Proxy Server を実行するホストを専用 LAN に設置することで、ネットワークを不要なトラフィックで満たすなどによるサービス拒否攻撃から社内ネットワークを保護することができます。ファイアウォールは、LDAP ディレクトリサーバーが「隠れて」いるマシンとポートに対する LDAP アクセスを拒否するように設定する必要があります。これにより、LDAP ディレクトリデータベースが保護されます。

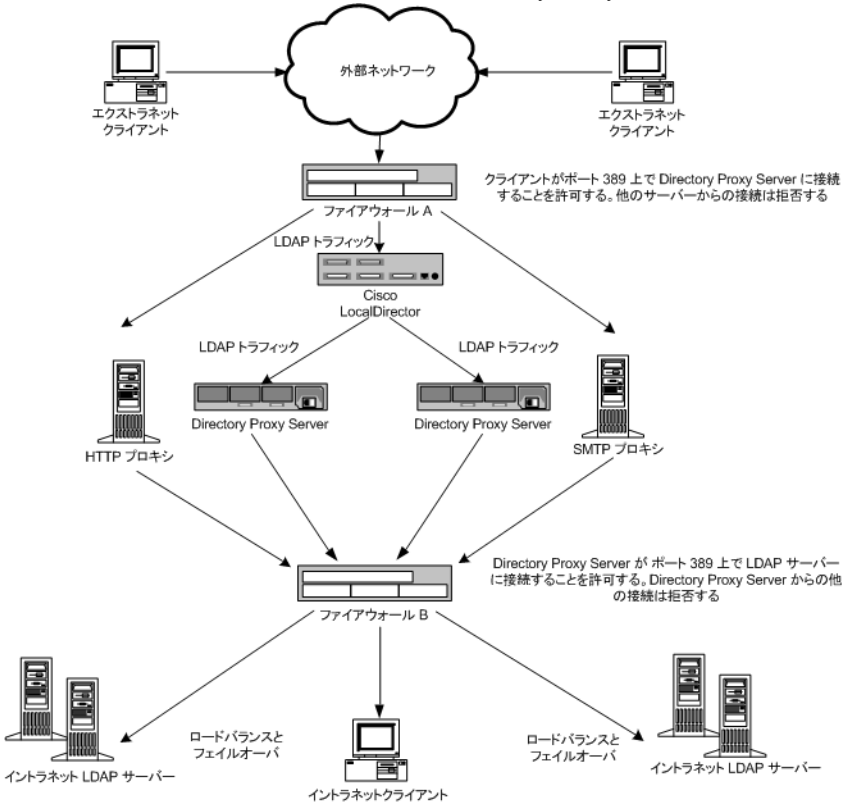
図 2-4　1 つのファイアウォールによる Directory Proxy Server の設定



2 つのファイアウォールによる Directory Proxy Server の配備

図 2-5 の構成には、図 2-4 の構成のすべての利点のほかに、いくつかのセキュリティが追加されています。2 つのファイアウォールを設置することで、「プロキシ」の周囲に制御可能なゾーンができ、サイト管理者が、外部ネットワークからのトラフィックを制限できるようになります。また、いずれかの「プロキシ」が危険にさらされても、そこから社内ネットワークのその他のマシンを直接攻撃することができなくなります。ファイアウォール A は、宛先 IP アドレスが、TCP または UDP プロトコルを処理するプロキシのアドレスである場合にだけ受信パケットを受け付けるように設定します。ファイアウォール B は、アクセス先のサーバーがプロキシマシンに適している場合にだけ、そのプロキシからのパケットを受け付けるように設定します。

図 2-5 2 つのファイアウォールによる Directory Proxy Server の設定



第 2 部

コンソールベースの管理

第 3 章「Directory Proxy Server コンソールの紹介」

第 4 章「Directory Proxy Server の起動、再起動、停止」

第 5 章「システム設定インスタンスの作成」

第 6 章「グループの作成と管理」

第 7 章「プロパティオブジェクトの定義と管理」

第 8 章「イベントオブジェクトの作成と管理」

第 9 章「アクションオブジェクトの作成と管理」

第 10 章「ログの設定と監視」

第 11 章「セキュリティの設定」

第 3 章

Directory Proxy Server コンソールの紹介

Sun ONE Directory Proxy Server をインストールしたら、まず、配備されているディレクトリで機能するように設定し、次にアクティビティを詳しく監視します。Directory Proxy Server の管理では、サーバーの起動、停止、再起動、グループの作成、特定のイベントを識別し適切な処理を実行するためのサーバーの設定、設定の変更、定期的なサーバー保守タスクの実行、ログの監視など、サーバーに関連するタスクを実行します。

サーバーに関連するタスクを迅速かつ簡単に行えるように、Directory Proxy Server には Directory Proxy Server コンソールおよび Directory Proxy Server 設定エディタコンソール という GUI ベースの管理ツールが用意されています。どちらのツールにもコンソールからアクセスできます。この章では、Sun ONE と Directory Proxy Server のコンソールについて、その概要を説明します。

この章で説明する項目は、次のとおりです。

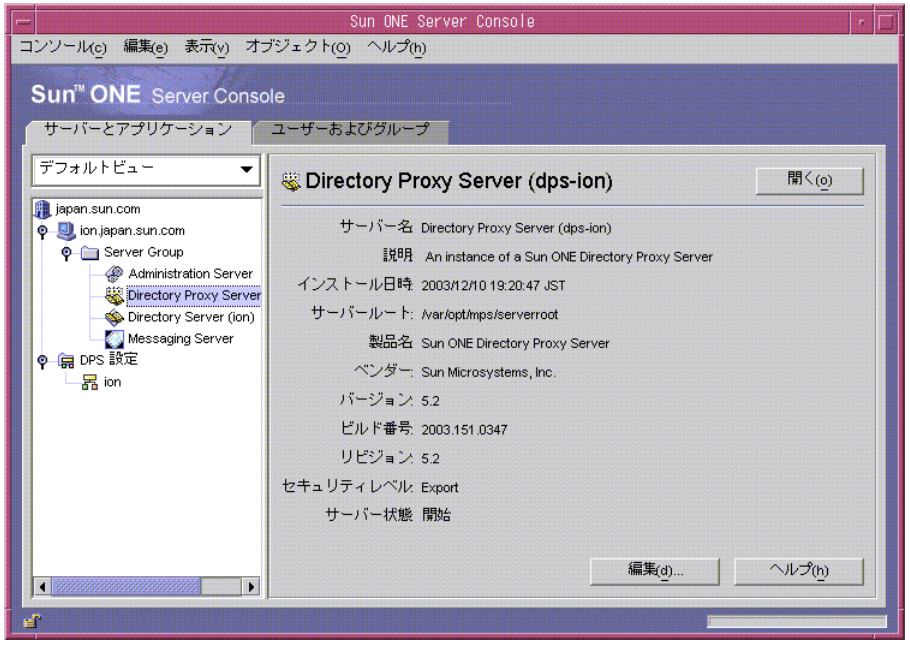
注 Sun ONE コンソールを使用して、さまざまなネットワークリソースを管理することができます。ただし、この章では Directory Proxy Server の管理機能を中心に、Sun ONE コンソールの使用方法を説明しています。Sun ONE コンソールの詳細については、Directory Proxy Server のマニュアルセットに含まれる『Managing Servers with Sun ONE Console』を参照してください。また、`http://docs.sun.com/` からこのマニュアルをダウンロードすることもできます。

Sun ONE コンソールについて

Sun ONE コンソールは、スタンドアロン型の Java アプリケーションで、組織の設定ディレクトリに登録されているすべてのネットワークリソースを管理するための GUI ベースのフロントエンドとして機能します。この統合型管理インタフェースにより、ネットワーク上にインストールされている Sun ONE バージョン 5.0 サーバーのすべてのインスタンスへのアクセスポイントが提供され、ネットワーク管理を簡略化できます。同様に、ユーザーディレクトリに対する統合型管理インタフェースとしても機能するので、ユーザーとグループの基本的な管理も簡略化できます。

図 3-1 は、Sun ONE コンソールの「サーバーとアプリケーション」タブで Directory Proxy Server インスタンスを選択したところです。

図 3-1 Sun ONE コンソールの「サーバーとアプリケーション」タブ



サーバーとアプリケーションタブ

Sun ONE コンソールの特定のインスタンスで管理できるネットワークの限界は、設定情報が同じ設定ディレクトリに格納されているリソースセットによって決定します。つまり、Sun ONE コンソールからは、最大セットのホストとサーバーを監視できます。設定ディレクトリを管理するスーパーアドミニストレータは、設定ディレクトリに登録されているすべてのネットワークリソースにアクセス権を設定できます。このため、スーパーアドミニストレータが設定するアクセス権によっては、Sun ONE コンソールを使用する管理者が実際に表示できるホストとサーバーの数は少なくなります。

「サーバーとアプリケーション」タブには、特定の設定ディレクトリに登録されているすべてのサーバーが表示され、管理対象のすべてのサーバーソフトウェアとリソースを統合的に表示できます。管理対象は、スーパーアドミニストレータが設定したアクセス権によって決定されます。

この表示では、1 回の操作で任意のサーバーグループまたは複数のサーバーに対して処理を実行できます。言い換えれば、「サーバーとアプリケーション」タブを使用して、1 つのサーバー、あるいは 1 つのマシンの複数のポートにインストールされている複数のサーバーを管理することができます。また、サーバーインスタンスエントリ (SIE) に対応するアイコンをダブルクリックすることで、そのサーバーのサーバーコンソール (管理インタフェース) にアクセスできます。

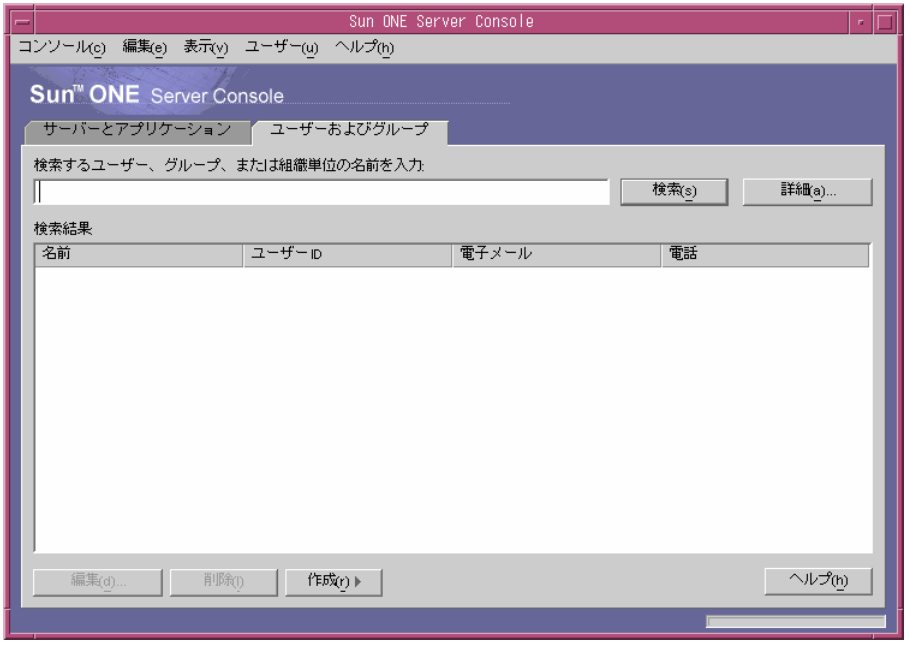
「サーバーとアプリケーション」タブでは、Directory Proxy Server に固有のさまざまな処理を行えます。

- Directory Proxy Server コンソールを起動する
- Directory Proxy Server 設定エディタコンソールを起動する (この結果、Directory Proxy Server グループが設定できる)
- Directory Proxy Server のアクセス権を設定する
- 管理サーバーコンソールを起動する (この結果、Directory Proxy Server を管理する管理サーバーインスタンスが設定できる)

ユーザーおよびグループタブ

図 3-2 の「ユーザーおよびグループ」タブでは、ユーザーアカウント、グループリスト、個々のユーザーおよびグループのアクセス制御情報を管理します。Sun ONE コンソールフレームワークに登録されているすべてのアプリケーションは、ユーザーディレクトリ内のコアユーザーおよびグループの情報を共有します。ユーザーディレクトリは、通常は社内全体のユーザーデータを格納するグローバルディレクトリです。

図 3-2　Sun ONE コンソールの「ユーザーおよびグループ」タブ



このタブでは、ユーザーとグループに関連する次のような処理を実行できます。

- ユーザーディレクトリ内のユーザーとグループの情報を追加、修正、削除する
- ユーザーディレクトリから、特定のユーザーやグループを検索する

Sun ONE 管理サーバー

Sun ONE 管理サーバーは Web ベースの (HTTP) サーバーで、Directory Proxy Server を含むすべての Sun ONE サーバーを Sun ONE コンソールから設定できます。これらのサーバーを設定するには、事前に管理サーバー (および設定ディレクトリ) が稼動している必要があります。管理サーバーはすべての Sun ONE サーバーに含まれ、サーバーグループに最初のサーバーをインストールするときにインストールされます。サーバーグループには、サーバールートディレクトリにインストールされるサーバーと、管理サーバーの 1 つのインスタンスによって管理されるサーバーが含まれます。

管理サーバーには、Sun ONE コンソールのログイン画面に URL を入力してアクセスします。45 ページの「手順 1: Sun ONE コンソールにログインする」を参照してください。この URL は、Directory Proxy Server のインストール時に指定したコンピュータホスト名とポート番号に基づいています。この URL の形式は、`http://<machine_name>.<your_domain>.<domain>:<port>` です。

管理サーバーにアクセスしようとすると、設定ディレクトリに対する認証のために、ユーザー ID とパスワードの入力が常に求められます。これは、Directory Proxy Server (またはサーバーグループ内の最初のサーバー) と管理サーバーをコンピュータにインストールするときに指定した、管理者のユーザー名とパスワードです。管理サーバーが稼動すると、Sun ONE コンソールを使用して、Directory Proxy Server を含むそのグループのすべてのサーバーを管理できるようになります。

管理サーバーの詳細については、『Managing Servers with Sun ONE Console』を参照してください。Directory Proxy Server のインストールに含まれるこのマニュアルのオンラインバージョンを探すときは、`<server-root>/manual/en/admin/ag/contents.htm` ファイルを開きます。

次のサイトでは、このマニュアルの最新バージョンを入手できます。

`http://docs.Sun ONE.com/docs/manuals/console.html`

管理サーバーの起動

Directory Proxy Server のインストールプログラムは、インストール時に Directory Proxy Server の監視用に指定した管理サーバーのインスタンスを自動的に起動します。Directory Proxy Server のインストール後に管理サーバを停止した場合は、Directory Proxy Server コンソールから Directory Proxy Server の管理を始める前に管理サーバーを再起動する必要があります。

管理サーバーは、コマンド行または Windows の「サービス」パネルから起動できます。

- コマンド行から管理サーバーを起動するには

  プロンプトに `<server-root>/start-admin` を入力します。

- Windows システムでは、管理サーバーはサービスとして稼動します。Windows の「サービス」パネルを使用して、サービスを直接開始できます。

説明した方法ではすべて、インストール時に指定したポート番号で管理サーバーが起動されます。サーバーが起動すると、Sun ONE コンソールを使用して Directory Proxy Server にアクセスできるようになります。

管理サーバーの停止

管理サーバーを使用していないときは、セキュリティの面からも停止しておくことが望ましいと考えられます。設定が他者によって変更されてしまう機会を最小化することができます。管理サーバーは、Sun ONE コンソール、コマンド行、Windows の「サービス」パネルから停止できます。

- Sun ONE コンソールから管理サーバーを停止するには

  a. Sun ONE コンソールにログインします (45 ページの「手順 1: Sun ONE コンソールにログインする」を参照)。

  b. 「サーバーとアプリケーション」タブで停止する管理サーバーインスタンスを探し、対応するエントリをダブルクリックします。

     管理サーバーコンソールが表示されます。

  c. 「タスク」タブで「Server を停止」をクリックします。

- コマンド行から管理サーバーを停止するには

  プロンプトに `<server-root>/stop-admin` を入力します。

- Windows システムでは、管理サーバーはサービスとして稼動しています。Windows の「サービス」パネルを使用して、サービスを直接停止できます。

Directory Proxy Server コンソールへのアクセス

Directory Proxy Server コンソールから Directory Proxy Server の管理作業を行うには、まず、コンソールを開く必要があります。

- 手順 1: Sun ONE コンソールにログインする
- 手順 2: 適切な Directory Proxy Server コンソールを開く

手順 1: Sun ONE コンソールにログインする

Sun ONE コンソールを起動して使用するには、対応する設定ディレクトリと管理サーバーが稼動している必要があります。サーバーが稼動していない場合は、コマンド行から起動します。コマンド行からのサーバーの起動については、43 ページの「管理サーバーの起動」を参照してください。設定ディレクトリの起動については、Sun ONE Directory Server のマニュアルを参照してください。

Sun ONE コンソールを起動すると、ログインウィンドウが表示されます。設定ディレクトリに対する認証のため、管理者 ID とパスワード、アクセス権を持つサーバーグループの管理サーバーの URL とそのポート番号を入力する必要があります。Sun ONE コンソールを使用するには、ネットワーク上の少なくとも 1 つのサーバーグループにアクセスする権限が必要です。

1. 適切なオプションを使用して Sun ONE コンソールアプリケーションを起動します。
   - UNIX マシンでのローカルアクセスでは、コマンド行に `<server-root>/start-console` と入力します。
   - Windows 環境でのローカルアクセスでは、デスクトップ上の Sun ONE コンソールのアイコンをダブルクリックします。このアイコンは、Sun ONE サーバーを初めてインストールした時点で作成されます。

   Sun ONE コンソールのログインウィンドウが表示されます。

2. 設定ディレクトリに対する認証を受けます。

   ユーザー ID: 管理サーバーのインストール時に指定した管理者 ID を入力します。管理サーバーは、最初の Sun ONE サーバーのインストール時、または Directory Proxy Server のインストール時にインストールされているはずです。

   パスワード : Directory Proxy Server のインストール中に、管理サーバーのインストール時に指定した管理者パスワードを入力します。

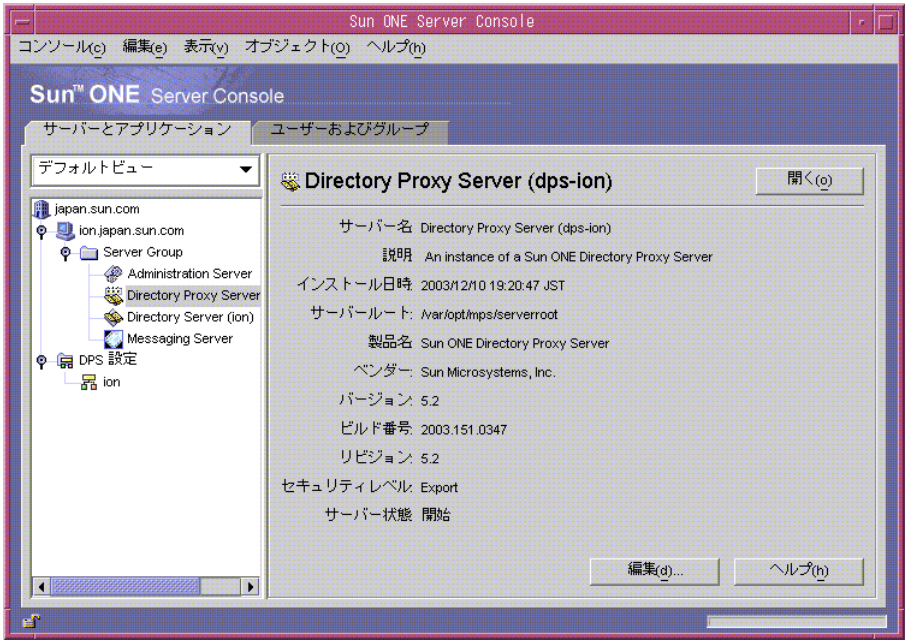
管理 URL: ここには、管理サーバーの URL が表示されているはずです。表示されていない場合、または適切な管理サーバー以外の URL が表示される場合は、ここに URL を入力します。この URL は、Directory Proxy Server のインストール時に指定したコンピュータホスト名と管理サーバーポート番号に基づいています。次の形式で指定します。

```
http://<machine_name>.<your_domain>.<domain>:<port_number>
```

たとえば、ドメイン名が sun で、管理サーバーをインストールしたホスト名が myHost、指定したポート番号が 12345 であれば、URL は `http://myHost.sun.com:12345` となります。

3. 「了解」をクリックします。

   管理対象のすべてのサーバーとリソースを示す Sun ONE コンソールが表示されます。



手順 2: 適切な Directory Proxy Server コンソールを開く

Sun ONE コンソールには、Directory Proxy Server の 2 つのエントリが表示されていることがわかります。1 つは Directory Proxy Server インスタンスノードのエントリで、もう 1 つは Directory Proxy Server Configurations ノードのエントリです。Directory Proxy Server インスタンスノードは Directory Proxy Server のサーバーインスタンスに対応し、Directory Proxy Server Configurations ノードは複数の Directory Proxy Server インスタンスが共有する設定に対応します。

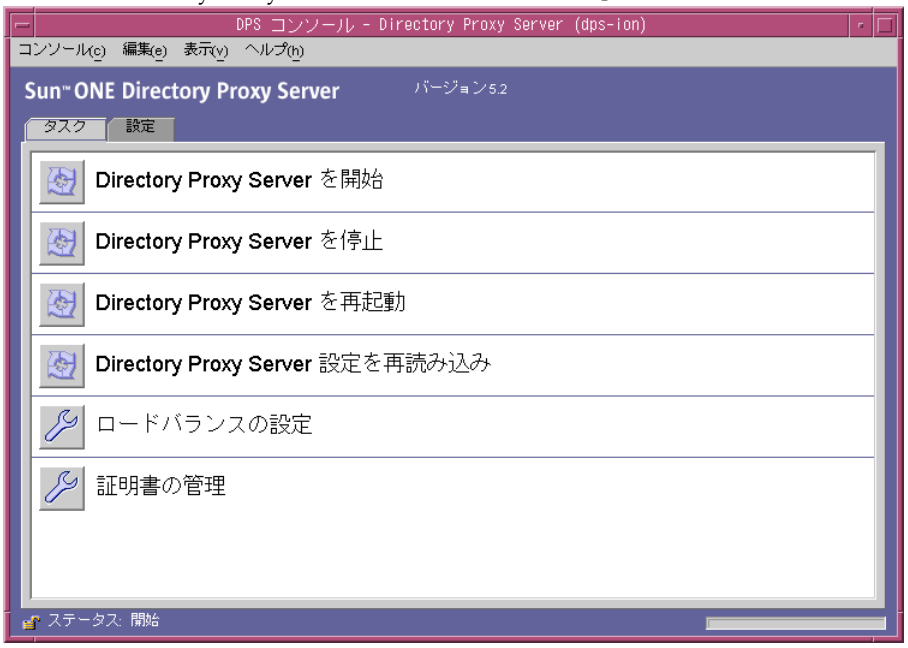
各ノードは、GUI ベースの管理インタフェースに関連付けられています。

- Directory Proxy Server コンソール : この管理インタフェースでは、Directory Proxy Server インスタンスを作成、設定、管理できます。たとえば、起動、停止、設定、ログの監視などの操作が可能です。Directory Proxy Server コンソールを使用して、サーバーにローカルまたはリモートアクセスすることができます。Directory Proxy Server コンソールを使用して作成および設定した Directory Proxy Server インスタンスは、その設定を使用するすべての Directory Proxy Server インスタンスに適用されます。
- Directory Proxy Server 設定エディタコンソール : Directory Proxy Server の複数のインスタンスがロジックとシステム設定を共有できます。Directory Proxy Server インスタンスが設定情報を共有する機能によって、複数の Directory Proxy Server の管理が簡略化されます。Directory Proxy Server 設定エディタコンソールは、複数の Directory Proxy Server を設定、管理するための管理インタフェースです。このインタフェースからの編集内容は、その設定を使用するすべての Directory Proxy Server インスタンスに適用されます。

Directory Proxy Server コンソールの起動

Sun ONE コンソールにログインすると、Directory Proxy Server コンソールを起動できるようになります。Sun ONE コンソールのナビゲーションツリーで、Directory Proxy Server インスタンスが属するサーバーグループのホスト名を展開し、サーバーグループノードを展開します。次に、適切な Directory Proxy Server インスタンスに対応するエントリを選択し、「開く」をクリックします。Directory Proxy Server コンソールが図 3-3 のように表示されます。

図 3-3　Directory Proxy Server コンソールの「タスク」タブ

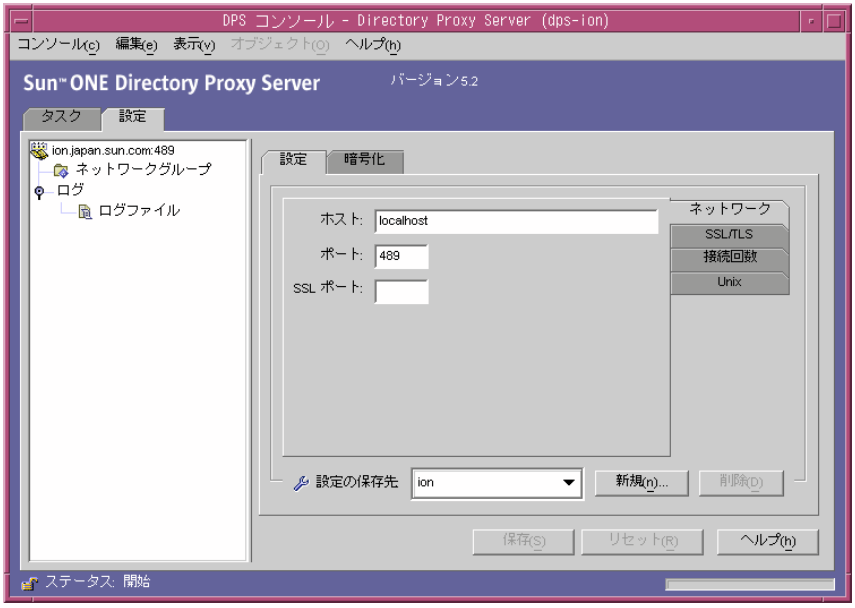


Directory Proxy Server コンソールには、「タスク」タブと「設定」タブがあり、それぞれが特定の管理領域を受け持ちます。

「タスク」タブでは、サーバーの起動、停止、再起動、再読み込み、各種 LDAP ディレクトリ間での負荷の分散とバランス、証明書の管理など、各サーバーインスタンスに共通する作業を実行できます。Directory Proxy Server の起動、停止、再起動の詳細については、第 4 章「Directory Proxy Server の起動、再起動、停止」を参照してください。ロードバランスの詳細については、第 7 章「プロパティオブジェクトの定義と管理」を参照してください。証明書管理の詳細については、第 11 章「セキュリティの設定」を参照してください。

「設定」タブ (図 3-4) を使用して、特定のインスタンスの設定を表示したり変更したりできます。

図 3-4　Directory Proxy Server コンソールの「設定」タブ内の「設定」タブ



「設定」タブと「暗号化」タブは、Directory Proxy Server の特定のインスタンスの設定に関連します。

「設定」タブ (図 3-4) では、次のパラメータを設定することができます。

ネットワーク : この Directory Proxy Server インスタンスのホスト名、ポート、および SSL ポートを表示します。

SSL/TLS: 現在選択されている設定を表示します。Directory Proxy Server は、この設定から SSL 証明書をサーバーに送信したり、SSL 証明書をクライアントに要求したりします。また、クライアントと Directory Proxy Server の間、および Directory Proxy Server とバックエンドサーバーの間の通信に使用する SSL/TLS バージョンも識別します。

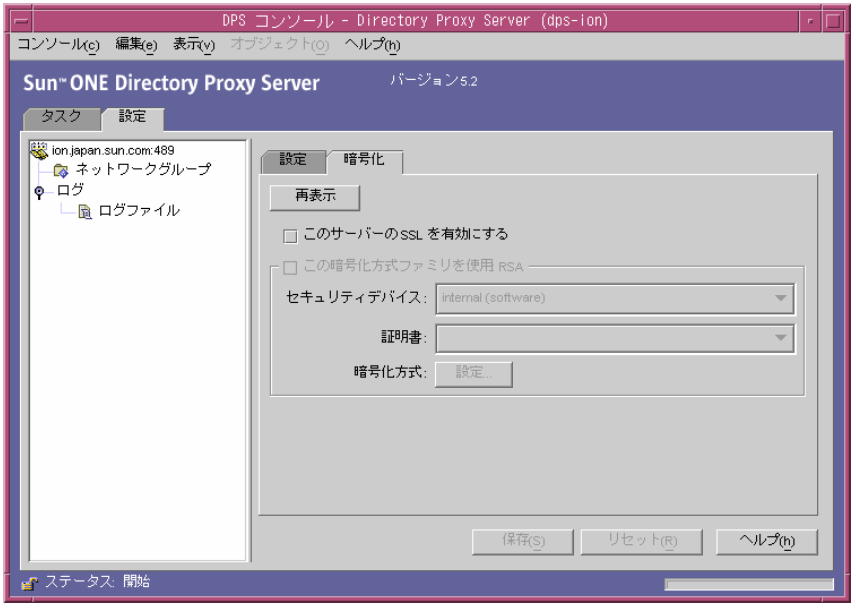
接続回数 : Directory Proxy Server の接続バックログの値を表示します。この値により、最大接続数を指定したり、接続プールのタイムアウト値を設定したりできます。

UNIX: この Directory Proxy Server インスタンスの UNIX のユーザー ID と実行時のディレクトリを表示します。

設定の保存先 : リストボックスに現在表示されている編集セッションに対して Directory Proxy Server 名の値を指定できます。Directory Proxy Server の設定を新たに作成することも、既存の設定を削除することもできます。

「設定」タブの「暗号化」タブ (図 3-5) では、暗号化の設定を表示、変更することができます。

図 3-5　Directory Proxy Server コンソールの「設定」タブ内の「暗号化」タブ



「暗号化」タブでは、次のパラメータを設定することができます。

再表示：画面に表示されている現在の値を更新し、新たに追加された証明書を確認できます。

このサーバーの SSL を有効にする：この Directory Proxy Server インスタンスで SSL による暗号化を有効にします。

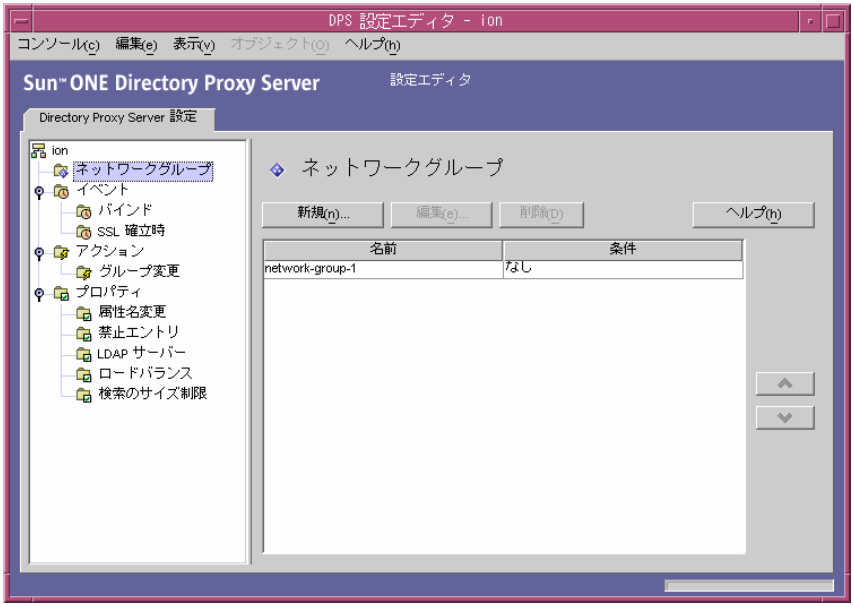
この暗号化方式ファミリを使用：RSA: この Directory Proxy Server インスタンスのセキュリティデバイス、証明書、暗号化方式を設定できます。

システムの暗号化設定に関する詳細は、65 ページの「システム設定インスタンスの作成」を参照してください。

Directory Proxy Server 設定エディタコンソールの起動

Sun ONE コンソールにログインすると、Directory Proxy Server 設定エディタコンソールを起動できるようになります。コンソールのナビゲーションツリーで Directory Proxy Server Configurations ノードを展開し、エントリを選択して「開く」をクリックします。Directory Proxy Server 設定エディタコンソール (図 3-6) が表示されます。

図 3-6　Directory Proxy Server 設定エディタコンソール



左側のナビゲーションツリーには、各 Directory Proxy Server の基本設定オブジェクトのノードがあります。主ノードの 1 つを展開すると、オブジェクトのサブタイプごとにツリーノードが表示されます。ツリーノードをクリックすると、選択したツリーノードに表示されるすべての現行オブジェクトタイプを含むテーブルが右側に表示されます。オブジェクトテーブルはその順番が重要で (ネットワークグループがその例)、1 組の上下ボタンによって個々のオブジェクトの優先順位を変更できます。

表 3-1 は、ナビゲーションツリーに表示される設定オブジェクトの種類を示しています。

表 3-1　Directory Proxy Server コンソールの設定オブジェクト

設定オブジェクトの種類	内容
ネットワークグループ	ネットワークグループの各オブジェクトは、特定のクライアントコミュニティを識別し、そのグループに適合するクライアントに適用する制限を指定します。 詳細は、第 6 章「グループの作成と管理」を参照してください。

表 3-1　Directory Proxy Server コンソールの設定オブジェクト (続き)

設定オブジェクトの種類	内容
イベント	イベントオブジェクトは、事前に定義した状態のときに発生する条件を指定します。条件はある特定のイベントに関連付けることができ、そのイベントに対して条件が満たされると、Directory Proxy Server によって特定の処理が実行されます。 詳細は、第 8 章「イベントオブジェクトの作成と管理」を参照してください。
アクション	アクションは、イベントが発生したときに実行する処理を指定します。詳細は、第 9 章「アクションオブジェクトの作成と管理」を参照してください。
プロパティ	プロパティは、そのクライアントのより詳細な制限を指定します。各グループオブジェクトには、プロパティオブジェクトによって定義された 1 組のプロパティを含めることができます。 詳細は、第 7 章「プロパティオブジェクトの定義と管理」を参照してください。

第 4 章

Directory Proxy Server の起動、再起動、停止

この章では、Sun ONE Directory Proxy Server を起動、停止、再起動する方法と、現在の状態を調べる方法について説明します。

この章で説明する項目は、次のとおりです。

- Directory Proxy Server の起動と停止 (53 ページ)
- Directory Proxy Server の再起動 (57 ページ)
- Directory Proxy Server のシステム状態の確認 (60 ページ)

注 Directory Proxy Server コンソールをを使用できるのは、Directory Server (および、その設定ディレクトリ) が適切であり、管理サーバーが起動している場合に限ります。管理サーバーは、Directory Proxy Server のインストール時に指定したポートで起動してください。セキュリティ上の危険を最小限にするため、Sun ONE コンソールの使用を終了したときは、管理サーバーを停止してください。管理サーバーの起動と停止の方法については、43 ページの「Sun ONE 管理サーバー」を参照してください。

Directory Proxy Server の起動と停止

Directory Proxy Server はインストールされると稼動を続け、要求を待機して受け付けます。また、UNIX デーモンプロセスか Windows サービスとして実行され、通常はシステムの起動時に開始されます。

Directory Proxy Server は次に示す複数の方法で起動したり停止したりできます。

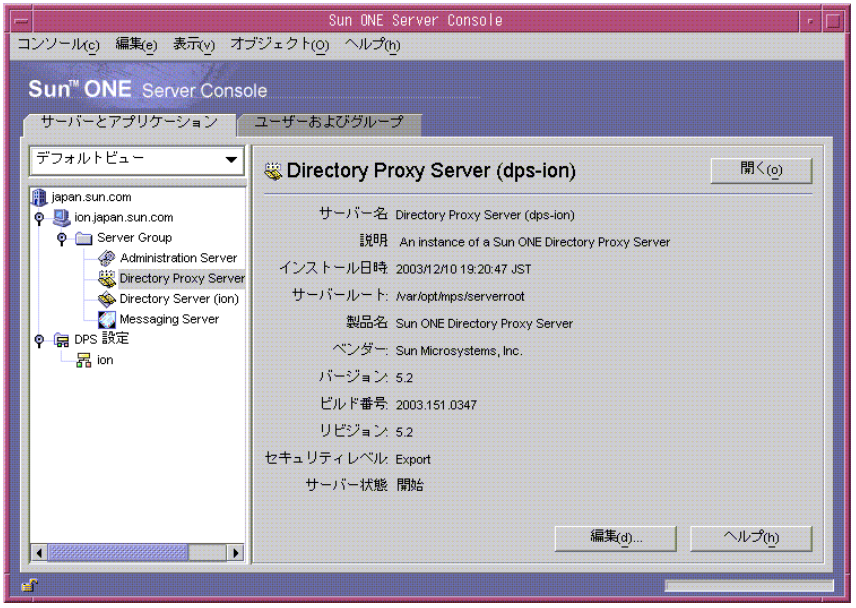
- Sun ONE コンソールからローカルまたはリモートで
- コマンド行からローカルのみで
- Windows システムでは、Windows の「サービス」パネルから

Directory Proxy Server を停止すると、そのすべてのコンポーネントが完全に停止され、サーバーを再起動するまでサービスは中断されます。ホストマシンがクラッシュしたりオフラインになった場合は、サーバーは停止して処理中の要求は失われます。サービスを復元するには、サーバーを起動し直す必要があります。

Sun ONE コンソールからの Directory Proxy Server の起動と停止

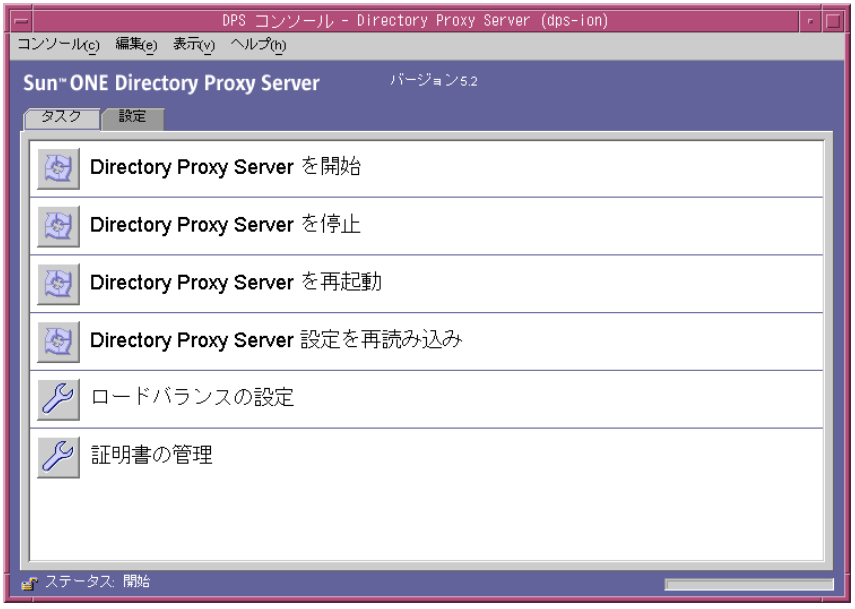
ローカルホストまたはリモートホストにインストールされている Directory Proxy Server を Sun ONE コンソールから起動したり停止したりできます。Directory Proxy Server を起動または停止するには、次の手順を実行します。

1. Sun ONE コンソールにログインします (45 ページの「手順 1: Sun ONE コンソールにログインする」を参照)。
2. 「サーバーとアプリケーション」タブで、ホスト名を展開し、起動または停止する Directory Proxy Server インスタンスが含まれるサーバーグループを展開します。
3. ナビゲーションツリーで、起動または停止する Directory Proxy Server インスタンスを探し、対応するエントリを選択して「開く」をクリックします。



Directory Proxy Server コンソールが表示されます。

4. 「タスク」タブで、サーバーを起動する場合は「Directory Proxy Server を開始」、停止する場合は「Directory Proxy Server を停止」をクリックします。



コマンド行からの Directory Proxy Server の起動と停止

コマンド行から Directory Proxy Server を起動するには、次の手順を実行します。

1. サーバーへのターミナルウィンドウを開きます。
2. UNIX システムでは、サーバーが 1024 未満のポートで稼動している場合は、`root` としてログインします。それ以外の場合は、`root` またはサーバーのユーザーアカウントでログインします。(デフォルトでは、Directory Proxy Server が `root` によって実行されている場合、ユーザー ID は `nobody` に変更されます。)
3. コマンド行プロンプトで、次のいずれかの行を入力します。

   Directory Proxy Server を起動する場合 :
   `<server-root>/dps-<hostname>/start-dps[.exe]`

   Directory Proxy Server を停止する場合 :
   `<server-root>/dps-<hostname>/stop-dps[.exe]`

<server-root> は、Directory Proxy Server のバイナリが格納されているディレクトリです。このディレクトリを最初に指定するのは、インストール時です。

<hostname> は、Directory Proxy Server のインスタンスがインストールされているホストの名前です。

.exe は、ファイル拡張子です。これは、このユーティリティを Windows システムで実行する場合にだけ必要です。

注 Directory Proxy Server がすでに稼動している場合は、起動コマンドは失敗します。stop-dps コマンドを実行してサーバーを停止してから start-dps コマンドを実行してください。

Windows のサービスパネルからの Directory Proxy Server の起動と停止

Directory Proxy Server を Windows システムにインストールした場合は、Windows の「サービス」パネルからサーバーをサービスとして起動したり停止したりできます。Directory Proxy Server サービスには、Sun ONE Directory Proxy Server という名前が付けられています。

Windows の「サービス」パネルから Directory Proxy Server を起動または停止するには、次の手順を実行します。

1. デスクトップで、「スタート」>「設定」>「コントロールパネル」を選択します。
2. 表示される「コントロールパネル」で「サービス」をダブルクリックします。
3. サービスのリストをスクロールして Directory Proxy Server インスタンスに対応するサービスを探します。
4. サービスを起動するには、Directory Proxy Server インスタンスを選択してから「開始」をクリックします。サービスを停止するには、Directory Proxy Server インスタンスを選択し、「停止」をクリックします。

Directory Proxy Server の再起動

Directory Proxy Server の設定を変更するたびに、設定ディレクトリにその変更内容を保存する必要があります。設定を変更した場合は常に、その変更を保存したあと Directory Proxy Server を起動し直す必要があります。再起動が必要になると、コンソールにメッセージが表示されます。

Directory Proxy Server を再起動すると、設定ファイルが再読み込みされ、それ以後の接続に新しい設定が適用されます。すでに確立されているクライアント接続では、クライアントが接続を終了するまで古い設定が適用されます。再起動機能は、UNIX プラットフォームだけで使用できます。Windows 環境では、Directory Proxy Server を再起動する場合、Directory Proxy Server を停止してから起動し直すことになります。

Directory Proxy Server は、次の 2 つの方法で再起動できます。

- Directory Proxy Server コンソールからローカルまたはリモートで
- コマンド行からローカルのみで

コマンド行からの Directory Proxy Server の再起動

コマンド行からの Directory Proxy Server を再起動するには、次の手順を実行します。

1. サーバーへのターミナルウィンドウを開きます。
2. UNIX システムでは、`root`、またはサーバーを起動したユーザーアカウントでログインします。
3. コマンド行プロンプトで、次の行を入力します。

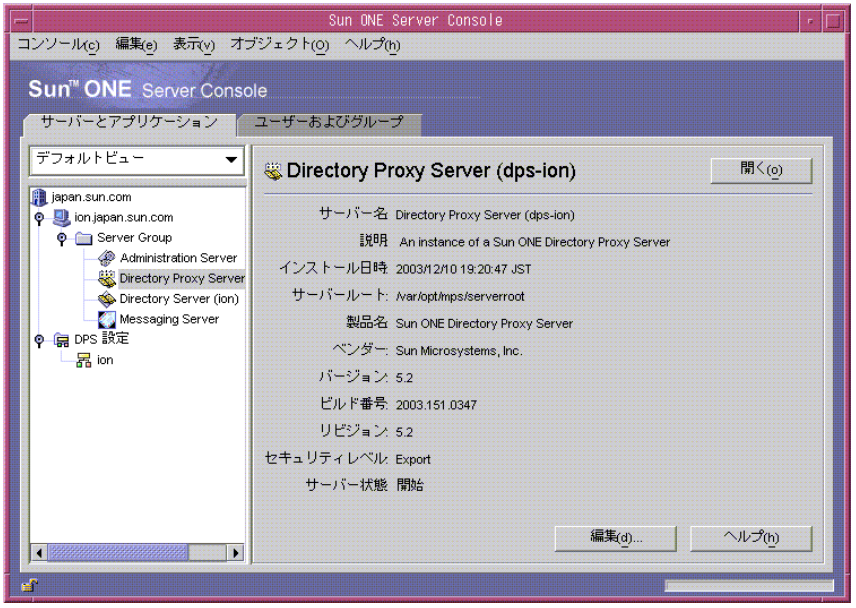
   ```
   <server-root>/dps-<hostname>/restart-dps[.exe]
   ```

UNIX プラットフォームの Sun ONE コンソールからの Directory Proxy Server の再読み込み

UNIX プラットフォームでは Directory Proxy Server コンソールを使用して、ローカルまたはリモートホストにインストールされている Directory Proxy Server の設定を再度読み込むことができます。UNIX プラットフォームでは、Directory Proxy Server の設定変更後、Directory Proxy Server の設定を読み込み直すと変更が適用されます。Windows プラットフォームで設定を読み込み直すには、Directory Proxy Server を再起動する必要があります。

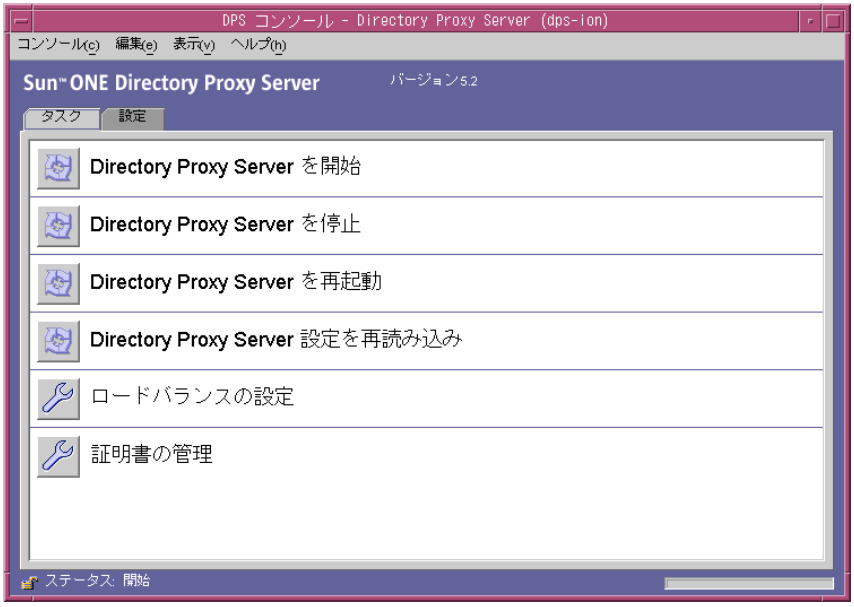
Directory Proxy Server コンソールから Directory Proxy Server を再度読み込むには、次の手順を実行します。

1. Directory Proxy Server コンソールが表示されていない場合は、Sun ONE コンソールにログインします (45 ページの「手順 1: Sun ONE コンソールにログインする」を参照)。
2. 「サーバーとアプリケーション」タブで、ホスト名を展開し、読み込み直す Directory Proxy Server インスタンスが含まれるサーバーグループを展開します。
3. ナビゲーションツリーで、読み込み直す Directory Proxy Server インスタンスを探し、対応するエントリを選択して「開く」をクリックします。



Directory Proxy Server コンソールが表示されます。

4. 「タスク」タブで「Directory Proxy Server 設定を再読み込み」をクリックし、サーバーを読み込み直します。



Directory Proxy Server のシステム状態の確認

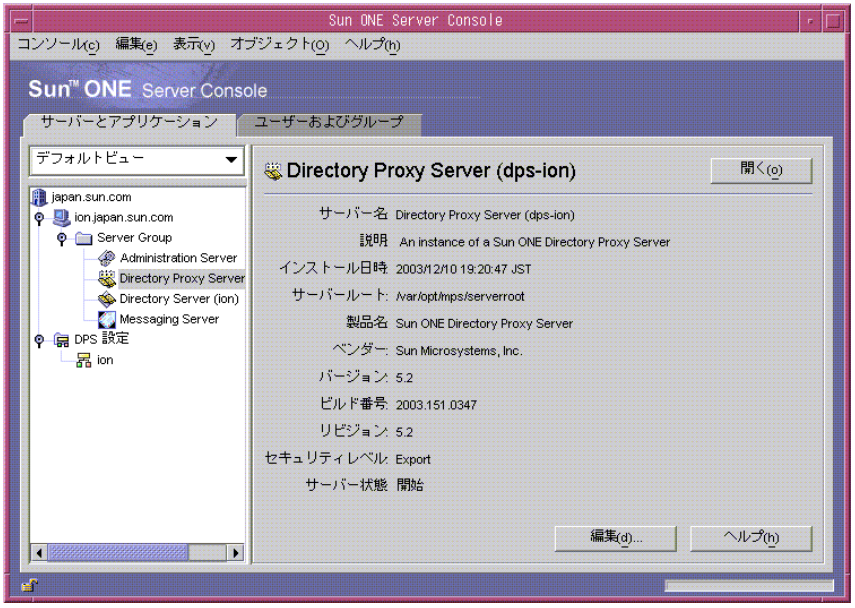
Directory Proxy Server の特定のインスタンスが稼動しているか、停止しているかを、次の 2 つの方法で確認することができます。

- Sun ONE コンソールからローカルまたはリモートで
- コマンド行からローカルのみで

Sun ONE コンソールからの Directory Proxy Server の状態確認

Sun ONE コンソールを使用して、Directory Proxy Server の特定のインスタンスが稼動しているかどうかを確認することができます。

1. Sun ONE コンソールにログインします (45 ページの「手順 1: Sun ONE コンソールにログインする」を参照)。
2. 「サーバーとアプリケーション」タブで、確認する Directory Proxy Server インスタンスに対応するエントリを選択します。



3. 右のペインで「サーバー状態」の表示を確認します。

選択した Directory Proxy Server インスタンスが稼動していれば、「開始」と表示されます。それ以外の場合は、「警告」、「停止」、または「不明」と表示されます。SIE 名が斜体で表示される場合も、サーバーが停止状態にあることを意味します。

コマンド行からの Directory Proxy Server の状態確認

Directory Proxy Server の特定のインスタンスの稼動状態をコマンド行から確認するには、次の手順を実行します。

1. サーバーへのターミナルウィンドウを開きます。
2. UNIX システムでは、root、またはサーバーを起動したユーザーアカウントでログインします。
3. コマンド行プロンプトで、次の行を入力します。

```
<server-root>/dps-<hostname>/status-dps[.exe]
```

コマンド行からの Directory Proxy Server の起動と停止

Directory Proxy Server プログラムは UNIX デーモンプロセスまたは Windows サービスとして実行され、通常はシステムの起動時に起動されます。

Directory Proxy Server の起動プログラムは、プラットフォームの種類に関係なく次の場所に格納されます。

```
<server-root>/dps-<hostname>/start-dps
```

起動用の設定ファイルは、次の場所に格納されます。

```
<server-root>/dps-<hostname>/etc/tailor.txt
```

Directory Proxy Server は、次の場所にあるスクリプトを使用して起動したり停止したりできます。

```
<server-root>/dps-<hostname>
```

Windows 環境で Directory Proxy Server を起動したり停止したりするには、Windows のサービスマネージャを使用する必要があります。Windows 以外のプラットフォームでは、Directory Proxy Server は、有効なユーザー ID が実際のユーザー ID と同じ場合にだけ、クラッシュの発生時に コアイメージを生成します。このため、Directory Proxy Server にコアを生成させるには、オブジェクトクラス

ids-proxy-sch-GlobalConfiguration の ids-proxy-con-userid 属性を、Directory Proxy Server プロセスを開始したユーザーと同じに設定する必要があります。デフォルトでは、Directory Proxy Server が root によって実行されている場合、ユーザー ID は nobody に変更されます。

サポートされているフラグ

表 4-1 は、起動と停止のスクリプトでサポートされているフラグとその説明を示しています。

表 4-1 起動および停止スクリプトがサポートするフラグ

フラグ	説明
-d	このフラグが指定されている場合、Directory Proxy Server が一度に処理する着信接続は 1 つだけとなり、より詳細な内部追跡情報がログファイルに記録されます。通常の操作では、このフラグは使用しないでください。Directory Proxy Server が制御ターミナルからデーモンを切り離すことができなくなります。
-D	このフラグを指定すると、Directory Proxy Server はより詳細な追跡情報をログファイルに記録します。Directory Proxy Server は複数のクライアント接続を処理することができ、デーモンとして稼動を続けます。-d と -D は、互いに排他的に扱う必要があります。
-t <startup configuration file>	別の起動用設定ファイルを指定するときは、このオプションを使用します。設定ファイルのパスは、絶対パスとして指定する必要があります。
-s	このオプションを指定すると、Directory Proxy Server は LOG_DAEMON 機能を使用して、内部ログメッセージを syslogd に出力します。Windows 環境ではこのフラグは無視されます。環境変数 dps_ROOT が定義されていない場合は、この設定がデフォルトとなります。
-M	このフラグを指定すると、Directory Proxy Server は別のプロセスを実行してそれ自体を監視します。Directory Proxy Server の状態に問題がある場合、監視プロセスは 30 秒の待機時間後に Directory Proxy Server を再起動します。Windows 環境ではこのフラグは使用できません。

表 4-1　起動および停止スクリプトがサポートするフラグ (続き)

フラグ	説明
-r	レジストリパスのハードコードの最後に値を追加するときは、このフラグを使用します。生成されるレジストリパスにより、Directory Proxy Server サービスは、ルート名またはインスタンスルート名などの設定情報などを参照します。Windows システムでは、ホストにインストールできる Directory Proxy Server のインスタンスは 1 つだけです。
-v	Directory Proxy Server のバージョン情報を出力するときは、このフラグを使用します。Windows 環境では、このフラグはコマンド行だけで使用する必要があります。

Directory Proxy Server の再起動

UNIX プラットフォームでは、Directory Proxy Server に SIGHUP 信号を送信することで、設定の再読み込みを行うことができます。設定の再読み込みが正常に完了すると、Directory Proxy Server はそれ以後の接続に新しい設定を適用します。すでに確立されているクライアント接続では、クライアントが接続を終了するまで古い設定が適用されます。

設定の再読み込みを Directory Proxy Server に命令するには、<server-root>/dps-<hostname> にある hup-dps コマンドを使用します。

HUP 信号機能を使用しても、一部の属性値は変更できません。次の設定パラメータの変更を適用するには、Directory Proxy Server の停止と起動が必要となります。次の属性が対象となります。

```
ids-proxy-con-listen-port
ids-proxy-con-listen-host
ids-proxy-con-ldaps-port
ids-proxy-con-foreground
ids-proxy-con-listen-backlog
ids-proxy-con-ssl-cert
ids-proxy-con-ssl-key
```

また、この機能を使用してログプロパティ ids-proxy-sch-LogProperty を変更することもできません。

restart-dps コマンドは、プラットフォームの種類に関係なく <server-root>/dps-<hostname> にあります。再起動コマンドを実行しても、同じディレクトリにある stop-dps コマンドと start-dps コマンドが続けて呼び出されるだけです。

第 5 章

システム設定インスタンスの作成

システムパラメータは、Sun ONE Directory Proxy Server の機能の動作に影響します。この章では、システム設定を指定して保存する方法について説明します。

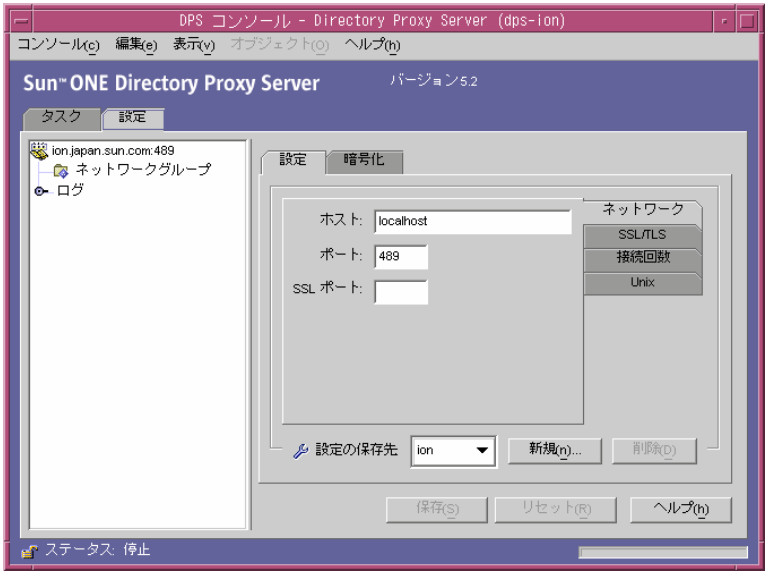
この章は、次の節から構成されています。

システム設定インスタンスの作成

ここでは、Directory Proxy Server インスタンスのシステム関連パラメータの設定方法について説明します。システム設定用のオブジェクトを作成するには、次の手順を実行します。

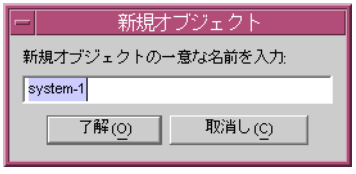
1. Directory Proxy Server コンソールにアクセスします。45 ページの「Directory Proxy Server コンソールへのアクセス」を参照してください。
2. ナビゲーションツリーで、適切な Directory Proxy Server インスタンスを選択し、「開く」をクリックします。

   Directory Proxy Server コンソールの「設定」タブを選択します。



3. 「新規」をクリックします。

   「新規オブジェクト」ウィンドウが表示されます。



4. 入力フィールドにシステム設定の名前を入力します。この名前には、一意の英数文字列を指定する必要があります。「了解」をクリックします。

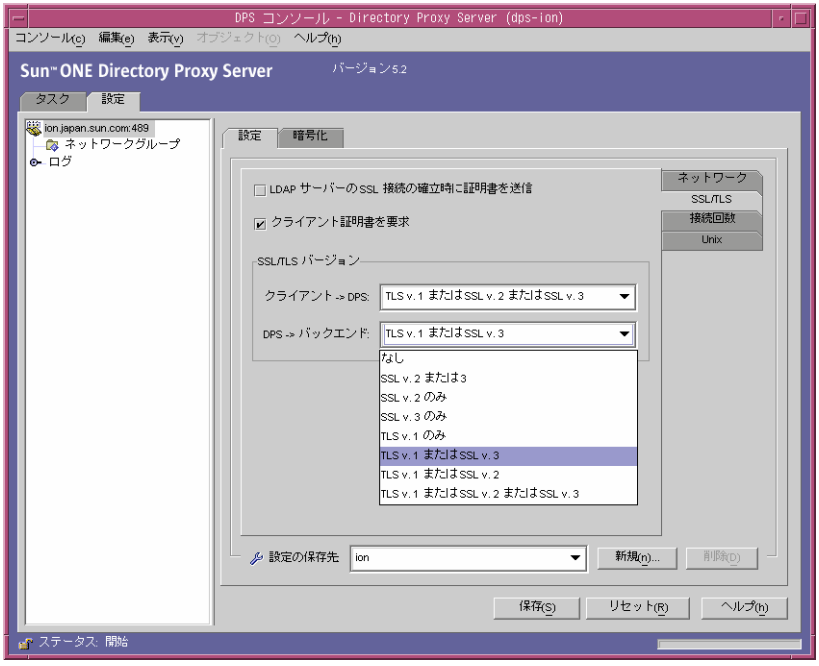
5. 「ネットワーク」タブで、システムの一般設定を指定します。

   ホスト：Directory Proxy Server が接続を待機するホストインタフェースの名前を入力します。この属性は、Directory Proxy Server を実行しているホスト上にネットワークインタフェースが複数存在する場合にだけ必要となります。デフォルトでは、ホスト名は「localhost」に設定されます。つまり、Directory Proxy Server は利用可能なすべてのネットワークインタフェースの接続を待機します。「localhost」を指定すると、システムプロパティの共有が許可されます。

ポート : Directory Proxy Server が着信接続を待機するポートの番号を入力します。このフィールドに指定できる値は、1 ～ 65535 です。デフォルトでは、この値は 389 (LDAP 用) に設定されます。この番号には、同じホストで動作している他の LDAP サーバーが使用しているポート番号は指定できません。UNIX プラットフォームでは、1024 未満のポート番号で待機する場合に、サーバーをルートとして起動する必要があります。

SSL ポート : Directory Proxy Server が LDAPS (SSL 経由の LDAP) 接続を待機するポートの番号を入力します。デフォルトでは、Directory Proxy Server は LDAPS クライアントからの接続を待機しません。この値は、636 などの値を指定して、この標準以外の機能を使ってクライアントからの LDAPS 接続を有効にするために必要です。この値は、ホストの値と同じにはできません。このオプションでは、「暗号化」タブにある TLS/SSL 設定も必要です。

6. 「SSL/TLS」タブをクリックします。



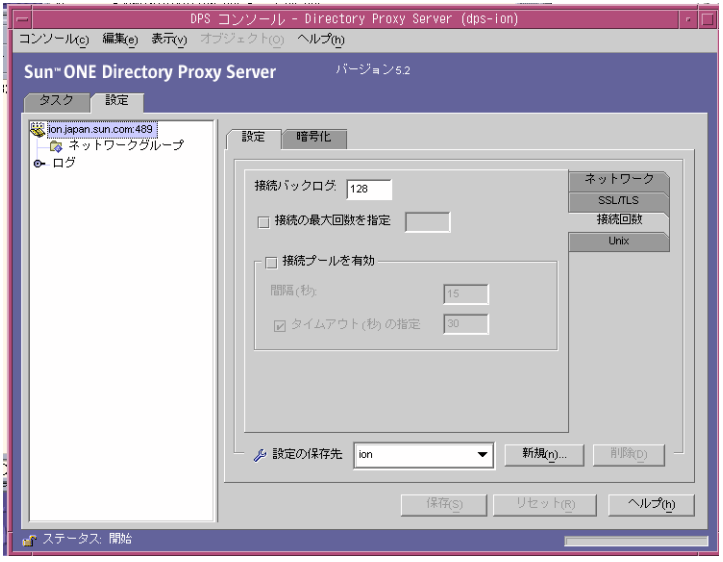
ここには、Directory Proxy Server が SSL 証明書をサーバーに送信したり、SSL 証明書をクライアントに要求するときに適用されるデフォルトの設定が表示されます。次のエントリを選択します。

LDAP サーバーの SSL 接続の確立時に証明書を送信 : TLS 接続を行うときに、Directory Proxy Server がその証明書をバックエンドの LDAP ディレクトリサーバーに送信する場合は、この設定を有効にします。デフォルトでは、この設定は無効になっています。

クライアント証明書を要求：SSL セッションを確立するすべてのクライアントに証明書チェーンを送信するよう Directory Proxy Server が要求するように指定する場合は、この設定を有効にします。証明書チェーンが送信されない場合、Directory Proxy Server は接続を閉じます。このオプションは、Directory Proxy Server とバックエンドサーバーとの SSL セッションには影響しません。デフォルトでは、この設定は無効になっています。

SSL/TLS バージョン：「クライアント -> DPS」と「DPS -> バックエンド」の隣のドロップダウンウィンドウで、それぞれの適切な SSL/TLS バージョンを選択します。システムで SSL が有効化されている場合は、バージョンを指定する必要があります。

7. 「接続回数」タブをクリックし、Directory Proxy Server が接続をどのように維持するかを指定します。



ここには、Directory Proxy Server の接続バックログの値が表示されます。この値により、最大接続数を指定したり、接続プールのタイムアウト値を設定したりできます。次のエントリを選択します。

接続バックログ：待機中のソケットのキューに入っている未処理の接続の最大数を示す、0 (ゼロ) よりも大きい値を入力します。デフォルトは 128 です。最大値は、基盤となるオペレーティングシステムの設定によって異なります。

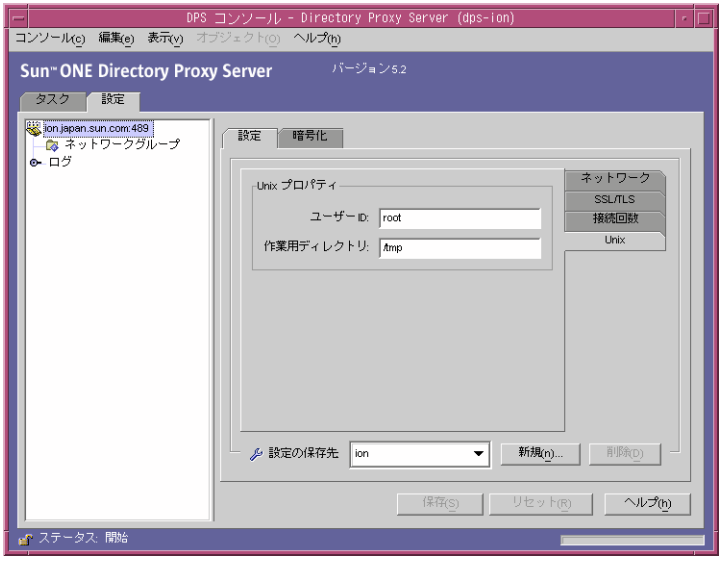
接続の最大回数を指定：このオプションを選択し、Directory Proxy Server が受け入れるクライアントの同時接続の最大数を示す値 (0 より大きい値) を入力します。同時接続の数を無制限にする場合は、このオプションを選択しません。

接続プールを有効：Directory Proxy Server がディレクトリサーバーに事前接続するために使用する接続プールモジュールを有効にします。デフォルトでは、この設定は無効になっています。接続プールを有効にすると、Directory Proxy Server はバックエンドの LDAP サーバーへの既存の接続を再使用しようとします。バックエンドサーバーが広域ネットワーク (WAN : Wide Area Network) 上にある場合は、このオプションに切り替えると、パフォーマンスが大幅に向上する可能性があります。次の値を入力してください。

間隔：今後の活動状況を予測するために Directory Proxy Server が着信要求を収集する間隔を示す秒数 (1 以上) を入力します。デフォルトは 15 です。

タイムアウトの指定：このオプションを選択し、LDAP サーバーへのアイドル状態の接続が切断されるまでの時間を示す秒数 (0 以上) を入力します。このチェックボックスをオフにすると、タイムアウトは適用されません。デフォルトは 30 です。この値は、バックエンドの LDAP サーバーのアイドル状態の接続のタイムアウト値より小さくする必要があります。

8. 「UNIX」タブをクリックします。

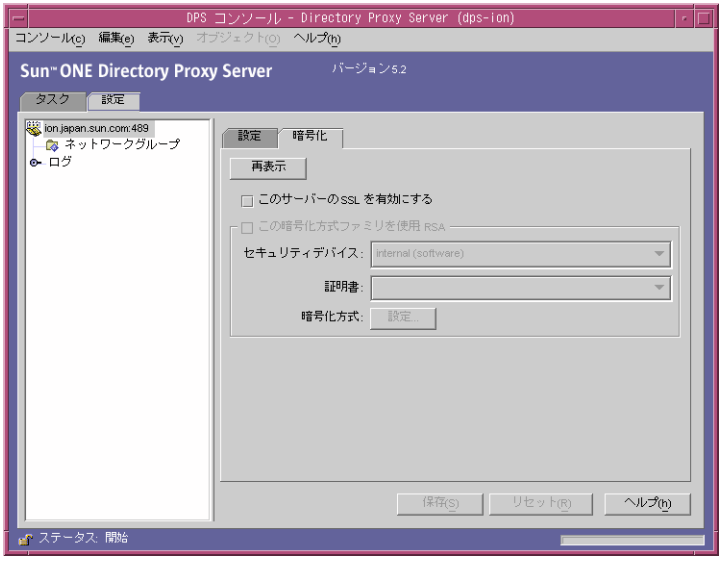


ここには、UNIX 環境だけの Directory Proxy Server 関連属性が表示されます。

ユーザー ID：Directory Proxy Server を実行するユーザー ID を入力します。Directory Proxy Server が *root* として動作していた場合は、ユーザー ID がここで指定した値に変更されます。デフォルトでは、*nobody* に切り替わります。このオプションは、Windows 環境には適用されません。

作業用ディレクトリ: Directory Proxy Server の実行元のディレクトリを入力します。Directory Proxy Server は起動時に、実行時のディレクトリをこの属性値として指定したディレクトリに変更します。デフォルトは `/tmp` です。この属性は、Windows 以外のプラットフォームだけで有効です。

9. 「暗号化」タブを選択し、SSL が有効な通信を Directory Proxy Server に設定します。サーバーの SSL 通信の設定については、「セキュリティの設定」を参照してください。



「暗号化」タブでは、次のパラメータを設定することができます。

再表示: このオプションをクリックすると、現在の画面の値が更新されます。新しく作成した証明書を確認する場合は、画面を最新の状態に更新します。

このサーバーの SSL を有効にする: Directory Proxy Server がセキュリティ保護された接続を介して待機するのに必要な SSL/TLS 情報を有効にする場合は、このボックスを選択します。SSL ポートを指定した場合は、設定を保存するためにこの設定を有効にする必要があります。

この暗号化方式ファミリを使用: **RSA**: この Directory Proxy Server インスタンスに対して「セキュリティデバイス」、「証明書」、および「暗号化方式」を設定する場合は、このボックスを選択します。

セキュリティデバイス: 利用可能なオプションから選択する場合は、ドロップダウンウィンドウをクリックします。デフォルトは「内部 (ソフトウェア)」です。

証明書：利用可能なオプションから選択する場合は、ドロップダウンウィンドウをクリックします。

暗号化方式：SSL 2.0、SSL 3.0、および TLS の各暗号化方式を設定する場合は、「設定」を選択します。「SSL 2.0」、「SSL 3.0」、および「TLS」の各タブを押し、それぞれに必要な暗号化方式の横のボックスを選択します。

10. 「保存」をクリックして、オブジェクトを保存します。

    Directory Proxy Server の設定が変更され、この設定が適用されるサーバーを再起動するように促すメッセージが表示されます。この時点では、まだサーバーを再起動しません。再起動は、すべての設定変更が完了してから行えます。

11. 必要なすべての追加オブジェクトについて、手順 3 から手順 10 を繰り返します。

12. サーバーを再起動します。57 ページの「Directory Proxy Server の再起動」を参照してください。

注

「設定」タブで「ホスト」、「ポート」、「SSL ポート」の各フィールドを変更した場合は、Directory Proxy Server を停止し、起動し直す必要があります。

Directory Proxy Server を起動、停止する方法については、53 ページの「Directory Proxy Server の起動と停止」を参照してください。

設定の保存

Directory Proxy Server の設定をダウンロードし、LDIF ファイルとして保存するには、`dpsconfig2ldif` というユーティリティを使用します。このユーティリティは、次の場所にあります。

```
<Install Root>/bin/dps_utilities/dpsconfig2ldif
```

このユーティリティでは、2 つの引数を指定する必要があります。

引数 :	意味
-t *filename*	*filename* は、起動用設定ファイルへのパスです。これは、通常は etc ディレクトリ内の tailor.txt ファイルです。
-o *filename*	設定の出力先ファイル名を指定します。

第 6 章

グループの作成と管理

LDAP クライアントは LDAP ディレクトリからのサービスを要求する場合、Sun ONE Directory Proxy Server に接続します。Sun ONE Directory Proxy Server では、クライアントプロファイルからクライアントのアクセス権を特定し、クライアントがディレクトリからサービスを要求できるかどうかを決定します。次に、設定されている制限を適用し、要求を適切なディレクトリに転送します。この章では、Directory Proxy Server 設定エディタコンソールを使用して、クライアントを識別して制限を適用できるように Directory Proxy Server を設定する方法について説明します。

この章で説明する項目は、次のとおりです。

グループの概要

Directory Proxy Server のしくみを理解するには、Directory Proxy Server ネットワークグループを理解することが重要です。ネットワークグループは、Directory Proxy Server が LDAP クライアントを識別する方法と、そのグループと一致するクライアントに対して Directory Proxy Server がどの制限を適用するかを決定します。Directory Proxy Server グループを使用して LDAP クライアントからのディレクトリアクセスを効率的に制御するには、このグループの詳細を理解することが重要です。

ネットワークグループは、次の項目の識別に使用されます。

- クライアント
- クライアントからの要求を Directory Proxy Server が転送する先の LDAP ディレクトリのセット

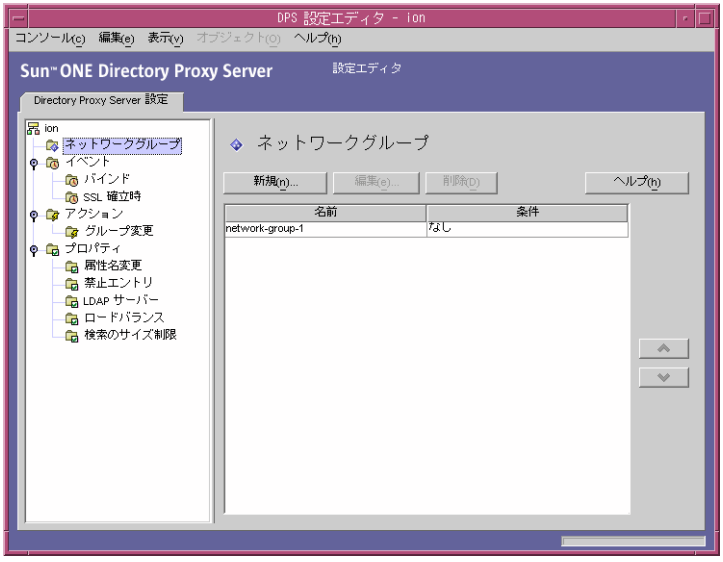
- クライアントがディレクトリセットとのやり取りで実行できる処理のセット
- クライアントがディレクトリセットとのやり取りでアクセスできるデータ
  Directory Proxy Server では、特定のエントリを非表示にしたりディレクトリ内の属性名を変更したりできるため、クライアントで表示できるディレクトリ内のデータを効率的に制御できます。

Directory Proxy Server は、接続の発信元属性をグループの条件と比較することで、そのクライアントがどのグループに属するか (クライアントのグループメンバーシップ) を決定します。サーバーは、降順の優先度 (高いものから低いものへ) で、現在設定されているグループを調べます。接続の発信元属性と最初に一致するネットワークグループ条件が接続に適用されます。このため、一般的な条件と具体的な条件を分けてグループを作成し、最も詳細かつ具体的なグループから最も一般的な汎用グループの順で優先順位を付けることが重要です。

クライアントに適合するグループが見つからない場合、クライアントの要求は拒否され、接続は閉じられます。このため、Directory Proxy Server の設定には少なくとも 1 つのグループエントリが必要です。

グループの優先度は、Directory Proxy Server 設定エディタコンソールの「ネットワークグループ」ウィンドウ (図 6-1 を参照) で、グループを配置することで指定されます。このウィンドウでは、リストの一番下にあるグループは上の方にあるグループよりも優先順位が低くなります。同じ重要度を持つグループを、同じ順序として定義することはできません。

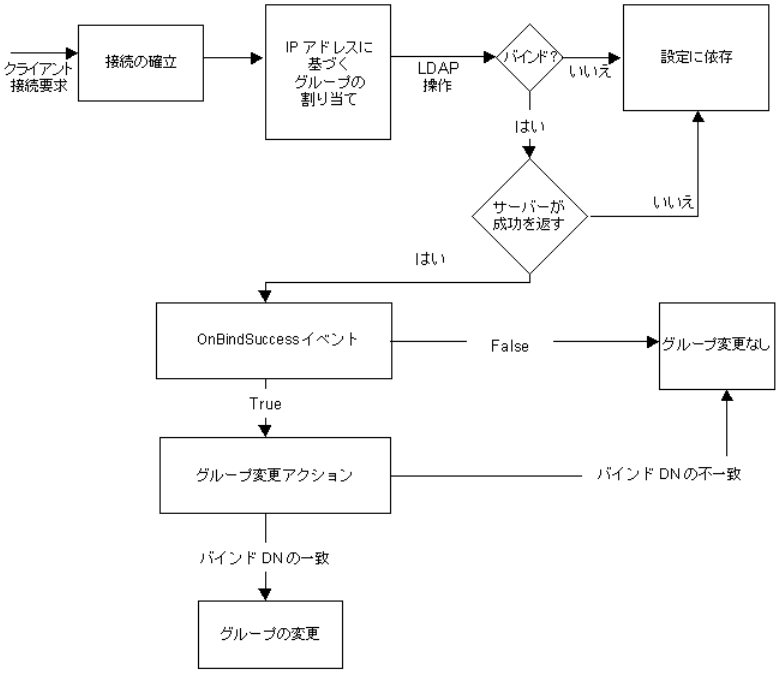
図 6-1 Directory Proxy Server 設定エディタコンソールの「ネットワークグループ」ウィンドウ



クライアントが属するグループは、最初は接続元のネットワークアドレス (たとえば、IP アドレス、ドメイン名、または両方) に基づいて決定されます。クライアントは、バインドが正常に行われた後でこのグループを変更することができます。詳細は、第 8 章「イベントオブジェクトの作成と管理」を参照してください。クライアントがグループのメンバーシップを獲得することは、そのグループのすべてのプロパティがそのクライアントに適用されることを意味します。

図 6-2 は、クライアントからのクエリに応じて Directory Proxy Server がグループを決定する方法を示しています。

図 6-2 グループメンバーシップを特定するための Directory Proxy Server の意思決定ツリー



グループのネットワーク条件には、次の項目を指定できます。

- ホストの IP アドレスまたはネットワークマスク
  - 単一 IP アドレス (たとえば、`129.153.129.14`)
  - IP quad/match ビット (たとえば、`129.153.129.0/24`)
  - IP quad/match クァッド (たとえば、`129.153.129.0/255.255.255.128`)
- ホストのドメイン名
  - 完全名 (たとえば、`box.eng.sun.com`)

- サフィックス名 (たとえば、.eng.sun.com)

クライアントの識別にドメイン名サフィックスの規則を使用する場合、DNS クエリに対して完全修飾名を返すように DNS を設定する必要があります。短縮名が返された場合は機能しません。

- 特別な規則
  - ALL (これは「catch-all」グループで使用されます。)
  - 0.0.0.0 (これは、たとえばバインド時に変更する場合にだけクライアントが使用するグループのように、最初のメンバーシップを考慮に入れないグループで使用されます。)

Directory Proxy Server がグループを特定する方法についてさらに詳しく理解するために、表 6-1 のサンプルグループのリストを参照してください。ここには、具体的なネットワーク条件から一般的な条件の降順で、優先度順に 5 つのグループが示されています。

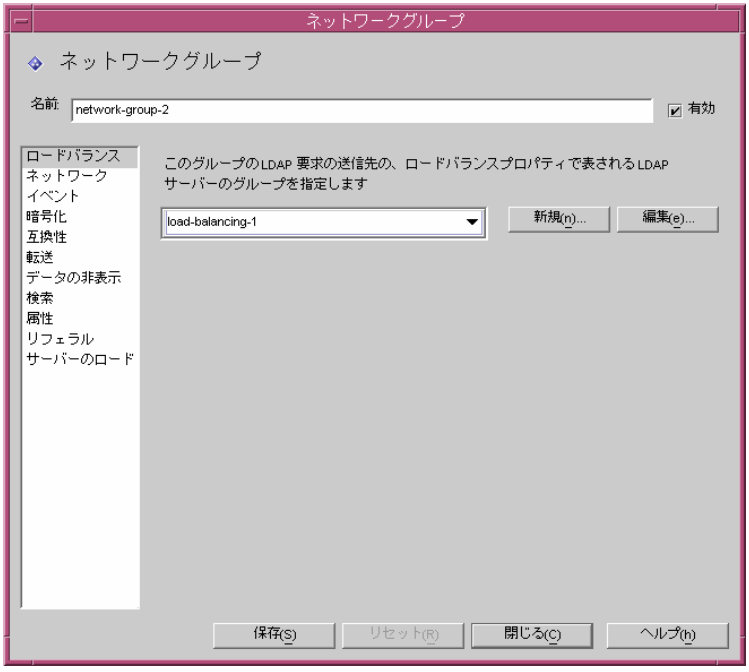
表 6-1 サンプルグループ

優先度	グループ名	ネットワーク条件
5	Admin-machine	129.153.129.72
4	IT-management-subnet	129.153.120.0/24
3	Operations	.ops.sun.com
2	Catch-all	ALL
1	Trusted	0.0.0.0

LDAP クライアントが LDAP ディレクトリからのサービスを要求すると、Directory Proxy Server は、その要求が 129.153.129.72 という IP アドレスから送信されているかどうかを確認します。送信元が異なる場合、Directory Proxy Server は要求が 129.153.129.0/24 と一致するかどうかを確認します。一致しない場合、Directory Proxy Server は要求の送信元が .ops.sun.com であるかどうかを確認します。送信元が異なる場合、Directory Proxy Server は接続を catch-all グループに入れ、意思決定ツリーの次の段階に進みます (図 6-2 を参照)。

図 6-3 は、グループを作成するための Directory Proxy Server 設定エディタコンソールのインタフェースを示しています。

図 6-3　Directory Proxy Server のネットワークグループの定義



ネットワークグループを作成するときに、条件を組み合わせて指定することができます。表 6-2 を参照してください。

表 6-2　ネットワークグループに適用できる条件

条件	説明
ロードバランス	ロードバランスプロパティによって指定される、このグループによる LDAP 要求の転送先となる LDAP サーバーのグループを指定できます。詳細は、119 ページの「ロードバランスプロパティ」を参照してください。
ネットワーク	要求が適切なグループにソートまたはフィルタリングされるように、クライアントの接続詳細とその他のネットワーク条件を指定できます。
イベント	グループに属するクライアントが、バインド後に指定のディレクトリに効率的にグループ変更できるように、グループにイベントを指定できます。イベントの既存オブジェクトのリストが表示されます。詳細は、79 ページの「グループの作成」を参照してください。
暗号化	グループに暗号化条件 (たとえば、クライアントが SSL セッションを要求できるかどうか) を指定できます。

表 6-2　ネットワークグループに適用できる条件 (続き)

条件	説明
互換性	LDAPv2 仕様 (RFC 1777) では、クライアントが 1 つのセッションで複数回バインドすることはできません。しかし、この機能を必要としているクライアントもあります。このようなクライアントとの相互動作のために、このオプションを設定できます。
転送	バインド、比較、その他の LDAP 要求をサーバーに渡す条件を指定できます。
データの非表示	ディレクトリに含まれるエントリのどのサブツリー、エントリ、または属性をグループで非表示にするかを指定できます。禁止エントリプロパティの既存オブジェクトのリストが表示されます。詳細は、110 ページの「禁止エントリプロパティ」を参照してください。
検索	グループの検索対象範囲とサイズ制限を指定できます。検索のサイズ制限プロパティのオブジェクトがリスト表示されます。詳細は、124 ページの「検索のサイズ制限プロパティ」を参照してください。
属性	ある特定の種類の検索操作や比較操作が LDAP サーバーに転送されないようにするための規則を指定できます。属性名変更プロパティの既存オブジェクトのリストが表示されます。詳細は、106 ページの「属性名変更プロパティ」を参照してください。
リフェラル	サーバーから返されるリフェラルをグループがどのように処理するかを、転送、実行、破棄から指定できます。LDAPv3 を実装しないクライアントは、転送されたリフェラルを認識できないので注意してください。この設定は、検索の継続リフェラルを除き、すべてのリフェラルに適用されます。
サーバーのロード	グループへの接続の合計数、1 接続あたりの並行および合計処理数、1 IP アドレスあたりの並行処理数など、詳細を指定できます。

グループの作成

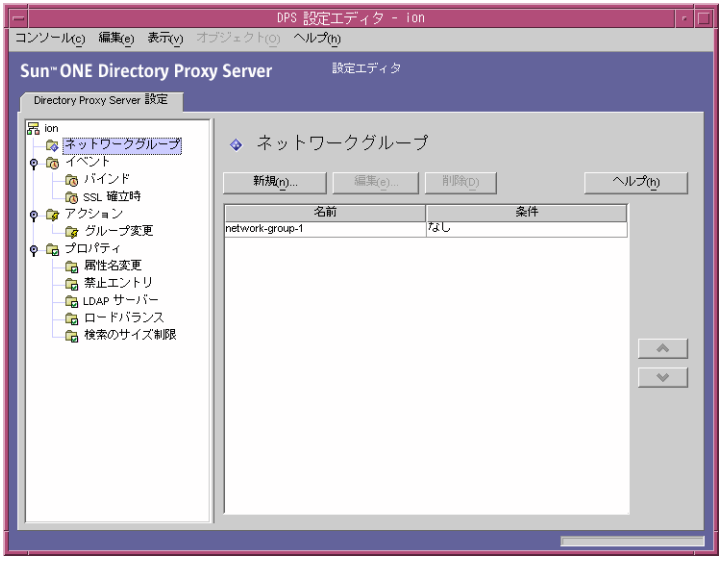
ここでは、Directory Proxy Server 設定エディタコンソールを使用してグループを作成する方法について説明します。グループを作成する前に 73 ページの「グループの概要」を参照し、Directory Proxy Server グループの重要性を理解してください。必要なグループを作成して優先度を設定したら、設定をテストしてグループがクライアント要求を適切にフィルタリングすることを確認してください。

ネットワークグループを作成するときには、さまざまな条件を指定できます。次に示す手順では、ユーザーインタフェースに表示される順で、すべての条件について説明します。適切な条件を選んでグループに設定してください。

Directory Proxy Server のネットワークグループを作成するには、次の手順を実行します。

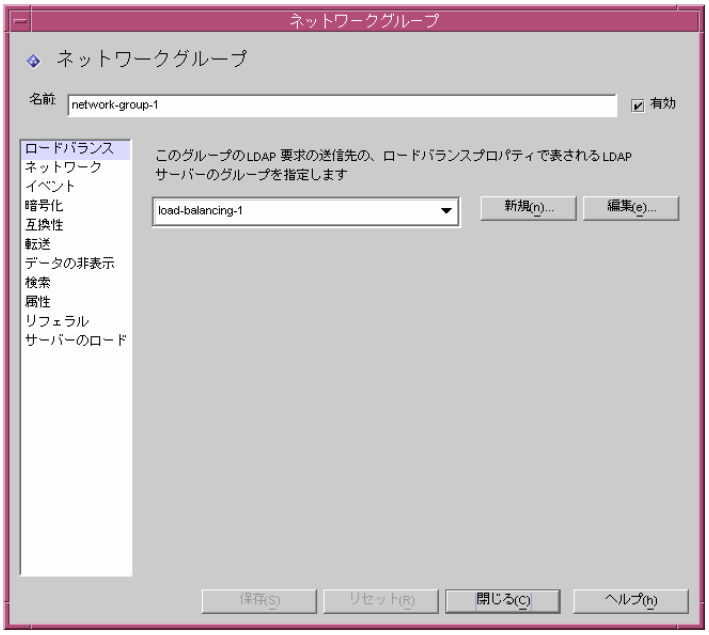
1. Directory Proxy Server 設定エディタコンソールにアクセスします。45 ページの「Directory Proxy Server コンソールへのアクセス」を参照してください。
2. ナビゲーションツリーで、Network Groups を選択します。

   右側のペインには既存のグループがリスト表示されます。



3. 「新規」をクリックします。

   「ネットワークグループ」ウィンドウが表示されます。



4. 「名前」フィールドには、グループ名を入力します。この名前には、一意の英数文字列を指定する必要があります。

5. 「有効」オプションが選択されていることを確認してください。デフォルトでは「有効」が選択されています。Directory Proxy Server の設定に含まれるグループに対しては、このオプションを選択する必要があります。設定に含まれるグループを無効にする場合は、このオプションの選択を解除します。

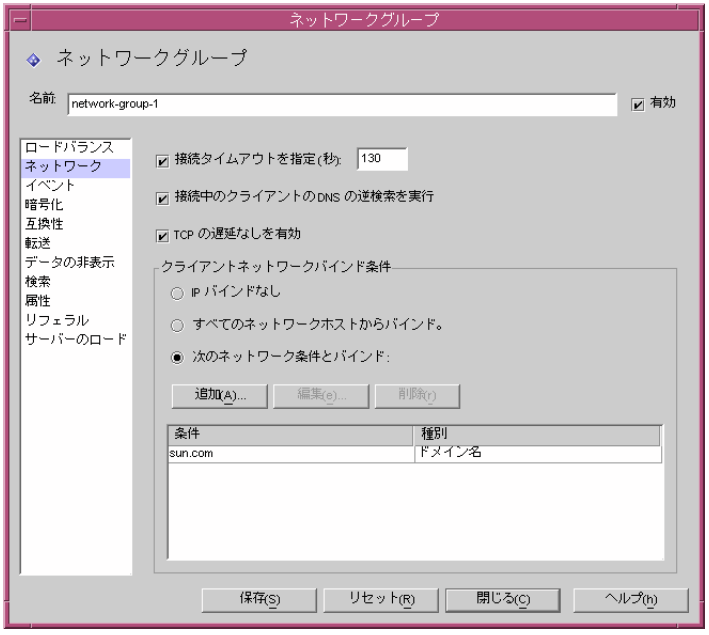
6. 必要であれば、ドロップダウンメニューから「ロードバランス」プロパティを指定します。このプロパティによって、LDAP 要求の転送先である LDAP サーバーのグループが識別され、LDAP サーバーは、ロードバランスプロパティを使ってクライアントからの要求を処理できます。関連するドロップダウンリストには、ロードバランスプロパティの既存のオブジェクトが表示されます。119 ページの「ロードバランスプロパティ」を参照してください。該当するオブジェクトを選択します。デフォルトでは、オブジェクトは選択されていません (< なし >)。オブジェクトがない場合は、「新規」ボタンをクリックして、オブジェクトをその場で作成することができます。

   新規 : 新しいロードバランスプロパティを作成するためのダイアログを表示します。

   編集 : 既存のロードバランスプロパティを編集するためのダイアログを表示します。

7. グループのネットワーク条件を指定して、要求をソートまたはフィルタリングするときは、左のフレームで「ネットワーク」を選択します。次に示す画面要素の説明を参照して、次のように適切なネットワーク値を指定します。

- 接続タイムアウトを指定します。デフォルトでは、値は指定されていません。つまり、接続タイムアウトは設定されていません。
- 接続中のクライアントの DNS の逆検索を有効にします。
- TCP の遅延なしを有効にします。
- クライアントネットワークバインド条件を定義します。



画面要素の説明は、次のとおりです。

接続タイムアウトを指定: クライアントをアクティブでない状態にしておける時間を指定する場合は、このボックスを選択します。この時間が経過すると、Directory Proxy Server はクライアントへの接続を閉じることができます。この値は、秒単位で指定し、通常は 120 以上です。デフォルトでは、値は指定されていません。つまり、接続タイムアウトは設定されていません。TCP キープアライブが有効になっていない場合は、切断されたクライアント接続によって Directory Proxy Server の処理が滞らないように、この属性を指定する必要があります。

接続中のクライアントの DNS の逆検索を実行：この設定は、デフォルトで有効です。DNS の逆検索を無効にすると、Directory Proxy Server は接続するクライアントのドメイン名を検索するために DNS の逆検索を実行しません。また、DNS の逆検索を無効にすると、Directory Proxy Server のパフォーマンスが大幅に向上する場合があります。「クライアントネットワークバインド条件」の値にドメイン名またはドメイン名サフィックスを使用した場合は、「DNS の逆検索」を無効にしないでください。無効にすると、Directory Proxy Server が正しく機能しません。クエリを検索できるように、ホストの完全名を返すように DNS を設定する必要があります。

TCP の遅延なしを有効：この設定は、デフォルトで有効です。このオプションを無効にすると、Directory Proxy Server はサーバーとこのグループに分類されるクライアントとの接続用の Nagle アルゴリズムを無効にします。「TCP の遅延なしを有効」は、Directory Proxy Server とクライアントとのネットワークの帯域幅が小さい場合にだけ無効にしてください。ただし、無効にすると、パフォーマンスが大幅に低下することがあります。

クライアントネットワークバインド条件：このセクションは、このネットワークグループでバインドできるクライアントを指定する場合に使用します。

IP バインドなし：クライアントがグループへのバインド時にだけ切り替えるときは、このオプションを選択します。このオプションは、デフォルトで選択されています。クライアントが、バインド時に切り替える場合にだけこのグループを使用する場合は、このオプションを選択しません。

すべてのネットワークホストからバインド：すべてのホストがこのネットワークグループにバインドできるようにするときは、このオプションを選択します。

次のネットワーク条件とバインド：ネットワークグループと適合させるホストのドメイン名と IP アドレスを指定するときは、このオプションを選択します。選択した場合、バインドするホストのドメイン名または IP アドレスをグループに指定する必要があります。

追加：ネットワーク条件を追加するためのダイアログを表示します。「ドメイン名」、「IP アドレス」、「IP アドレスとビット」、「IP アドレスと quad」という 4 つのオプションがあります。

編集：ネットワーク条件を編集するためのダイアログを表示します。

削除：ネットワーク条件を削除するためのダイアログを表示します。

ドメイン名のダイアログ：ネットワークグループにバインドできるクライアントのドメイン名サフィックスまたは完全ドメイン名を指定します (`foo.sun.com` など)。Directory Proxy Server は、デフォルトでドメインサフィックスを想定していないため、完全なドメイン名を指定する必要があります。先頭にピリオドが付いたドメイン名サフィックス (`.sun.com` など) を指定すると、そのサフィックスで終わるドメイン名を持つすべてのホストが適合します。

また、クライアントの識別にドメイン名サフィックスの規則を使用する場合、DNS クエリに対して完全修飾名を返すように DNS を設定する必要があります。短縮名が返された場合は機能しません。

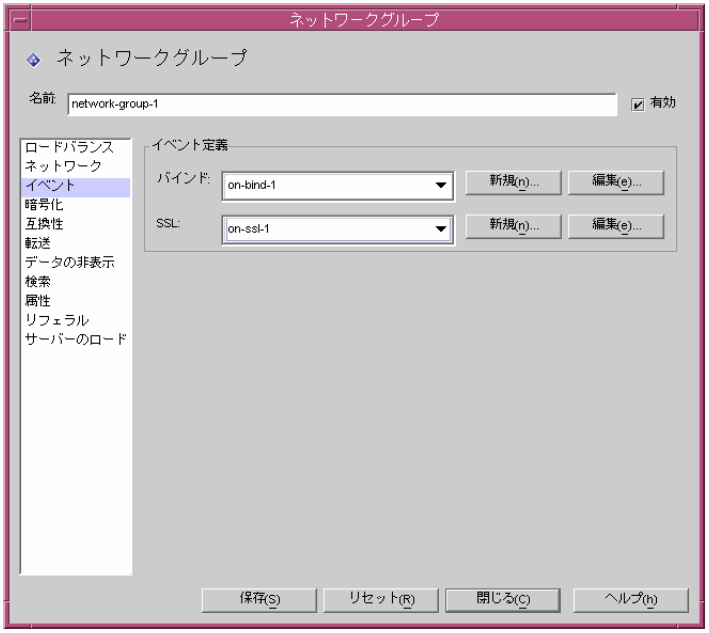
IP アドレス : 1 つの IP アドレスを、10 進数をドットで区切った形式で指定します (`198.214.11.1` など)。

IP アドレスとビット : IP ネットワークマスクを、`<network number>/<mask bits>` という形式で指定します (`198.241.11.0/24` など)。前半部分はネットワーク番号を示し、後半部分は適合に必要なネットワーク番号のビット数を示します。

IP アドレスと quad : IP ネットワークマスクを、IP アドレスとドットで区切られた 10 進数の 4 つの値のペアで指定します (`198.241.11.0/255.255.255.128` など)。前半部分はネットワーク番号を示し、後半部分は適合に必要なネットワーク番号のビット数を示します。たとえば、`198.214.11.0/255.255.255.128` は IP アドレス `198.214.11.63` を持つホストに適合しますが、IP アドレス `198.214.11.191` を持つホストには適合しません。

ドメイン名またはドメイン名サフィックスを使用する場合は、「接続中のクライアントの DNS の逆検索を実行」を有効にする必要があります。

8. グループにイベント駆動型のアクション (クライアントを別のグループに変更する、など) を関連付けるときは、左のフレームで「イベント」を選択し、右のフレームに適切な値を指定します。



画面要素の説明は、次のとおりです。

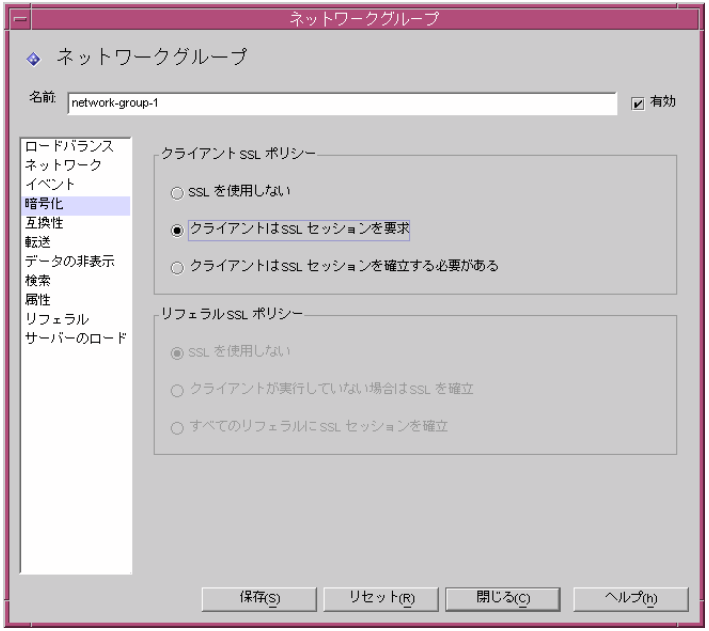
バインド：ドロップダウンリストには、OnBindSuccess イベントの既存のオブジェクトが表示されます。130 ページの「OnBindSucess イベントオブジェクトの作成」を参照してください。クライアントがバインド操作を正常に完了したときに実行されるオブジェクトの名前を選択します。デフォルトでは、オブジェクトは選択されていません (< なし >)。オブジェクトがない場合は、「新規」ボタンをクリックして、オブジェクトをその場で作成することができます。

SSL：ドロップダウンリストには、SSL 確立時イベントの既存のオブジェクトが表示されます。133 ページの「SSL 確立時イベントオブジェクトの作成」を参照してください。クライアントが SSL セッションを正常に確立したときに実行されるオブジェクトの名前を選択します。オブジェクトがない場合は、「新規」ボタンをクリックして、オブジェクトをその場で作成することができます。

編集：イベントの動作を編集するためのダイアログボックスを表示します。

新規：新しいイベントを作成するためのダイアログボックスを表示します。

9. グループに暗号化条件 (クライアントが SSL セッションを要求できるかどうか、など) を指定するときは、左のフレームで「暗号化」を選択し、右のフレームに適切な値を指定します。



画面要素の説明は、次のとおりです。

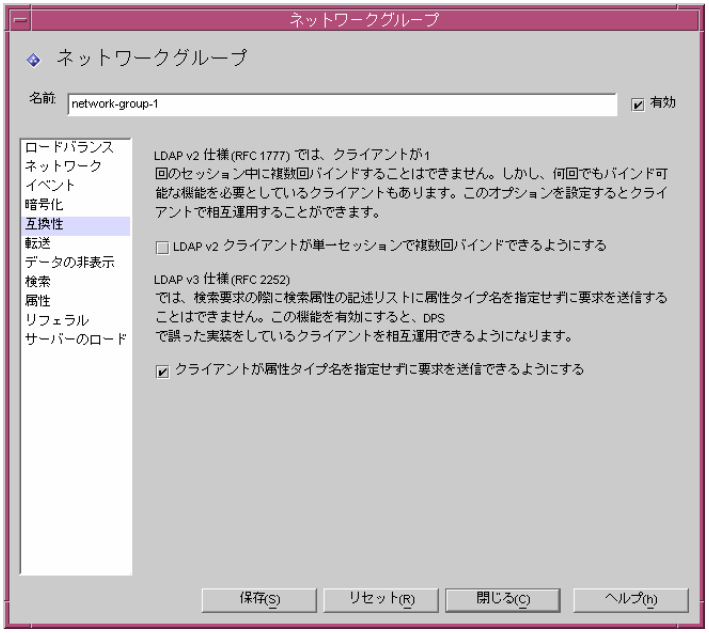
クライアント SSL ポリシー：クライアントの SSL ポリシーを設定します。

- **SSL を使用しない** : SSL 暗号化を使用しない場合は、このオプションを選択します。
- **クライアントは SSL セッションを要求** : グループ内のクライアントが SSL を要求する SSL セッションを確立する場合は、このオプションを選択します。
- **クライアントは SSL セッションを確立する必要がある** : グループ内のクライアントが、操作を実行する前に、SSL セッションを確立する必要がある場合は、このオプションを選択します。

リフェラル SSL ポリシー : リフェラルを実行している間の SSL ポリシーを設定します。

- **SSL を使用しない** : SSL 暗号化を使用しない場合は、このオプションを選択します。
- **クライアントが実行してない場合は SSL を確立** : このオプションを有効にすると、クライアントが Directory Proxy Server により SSL セッションをすでに確立している場合にのみ、Directory Proxy Server はそのグループのクライアントに対して SSL を開始します。
- **すべてのリフェラルに SSL セッションを確立** : リフェラルに対してこのオプションを有効にすると、オペレーションの転送前に Directory Proxy Server が SSL セッションを開始します。

10. グループに互換性条件 (クライアントが 1 回のセッションで複数回バインドできるようにする、など) を指定するときは、左のフレームで「互換性」を選択し、右のフレームに適切な値を指定します。



画面要素の説明は、次のとおりです。

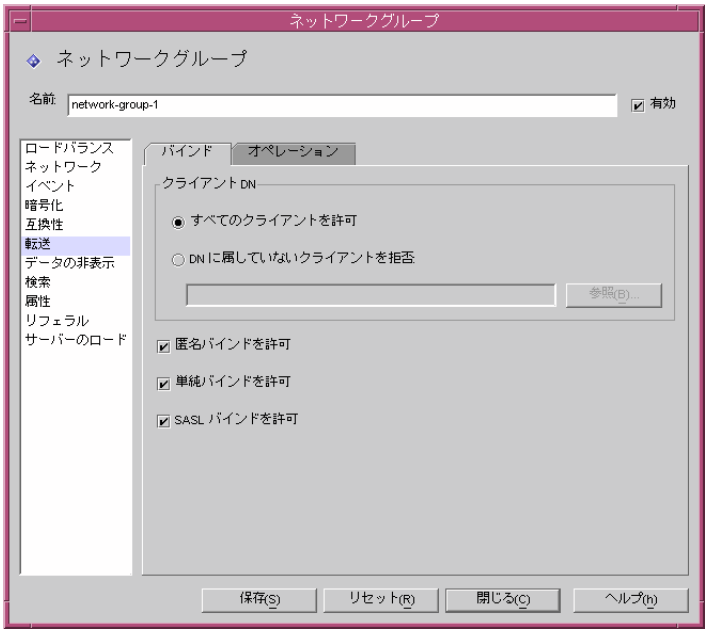
LDAPv2 クライアントが単一セッションで複数回バインドできるようにする: LDAPv2 仕様 (RFC 1777) では、クライアントが 1 つのセッションで複数回バインドすることはできません。しかし、この機能を必要としているクライアントもあります。属性要求リストで 1 つまたは複数の属性を NULL として指定した検索要求をクライアントが送信できるようにグループを設定するときは、このオプションを選択します。この互換性機能を使用することで、Directory Proxy Server は誤った実装が行われている一部の Java ベースクライアントと相互動作できるようになります。属性要求リスト内の NULL という属性名は、LDAP プロトコルに違反しています。デフォルトでは、このオプションは TRUE に設定されています。

クライアントが属性タイプ名を指定せずに要求を送信できるようにする: クライアントの属性タイプ名が識別されない場合でも、クライアントが要求を送信できるようにグループを設定するときは、このオプションを選択します。

11. グループの要求転送条件を指定するときは、左のフレームで「転送」を選択し、右のフレームに適切な値を指定します。

    Directory Proxy Server は、クライアントからの接続を受け入れグループを割り当てると、クライアントが LDAP 操作を送信するまで待機します。Directory Proxy Server は、「クライアント DN」、「匿名バインドを許可」、「単純バインドを許可」、および「SASL バインドを許可」を使用して、バインド要求をサーバーに渡すか、バインド要求を拒否してクライアントの接続を閉じるかを判断します。

クライアントのバインドが有効かどうかのテストに合格すると、Directory Proxy Server はそのバインド要求をサーバーに転送します。サーバーがバインドを受け入れると、接続が確立されます。ただし、クライアントが LDAPv2 を使用していた場合、サーバーがバインド要求に対してエラー表示を返すと、Directory Proxy Server はそのエラー表示をクライアントに転送してクライアントへの接続を閉じます。



「バインド」タブの要素の説明は、次のとおりです。

すべてのクライアントを許可 : デフォルトでは、このオプションが選択されています。すべてのクライアントによるアクセスが許可されます。

DN に付属していないクライアントを拒否 : グループに識別名 (DN) を確認させるときは、このオプションを選択します。指定した DN に属さない識別名がバインドに指定されていないクライアントは、拒否されます。DN を作成するために LDAP ディレクトリを参照するときは「参照」ボタンをクリックします。

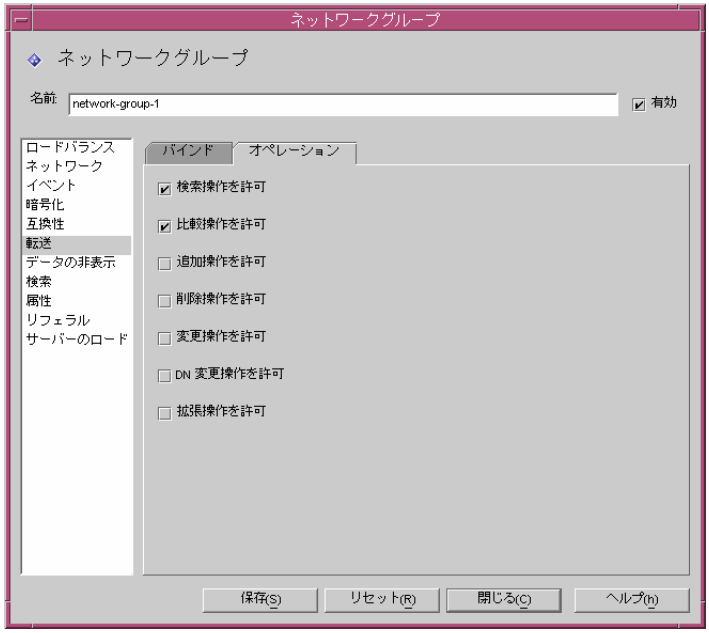
匿名バインドを許可 : デフォルトではこのオプションが有効です。クライアントがパスワードを提供しなかった場合でもバインドを許可します。匿名バインドを禁止するときは、このオプションを無効にします。

単純バインドを許可 : デフォルトではこのオプションが有効です。クライアントはパスワードをクリアテキストで指定できます。クリアテキストのパスワードによって認証されたバインド要求を禁止する場合は、このオプションを無効にします。

SASL バインドを許可：デフォルトではこのオプションが有効で、SASL バインドが許可されます。SASL 認証を禁止するときは、このオプションを無効にします。

12. 「オペレーション」タブを選択し、どの操作を転送するかを指定します。

    デフォルトでは、Directory Proxy Server は検索要求と比較要求を転送します。また、Directory Proxy Server はバインド解除要求を認識し、LDAP サーバーへの接続を閉じます。



「オペレーション」タブの要素の説明は、次のとおりです。

検索操作を許可：この設定は、デフォルトで有効です。Directory Proxy Server が検索要求をサーバーに転送しないようにするときは、このオプションを無効にします。

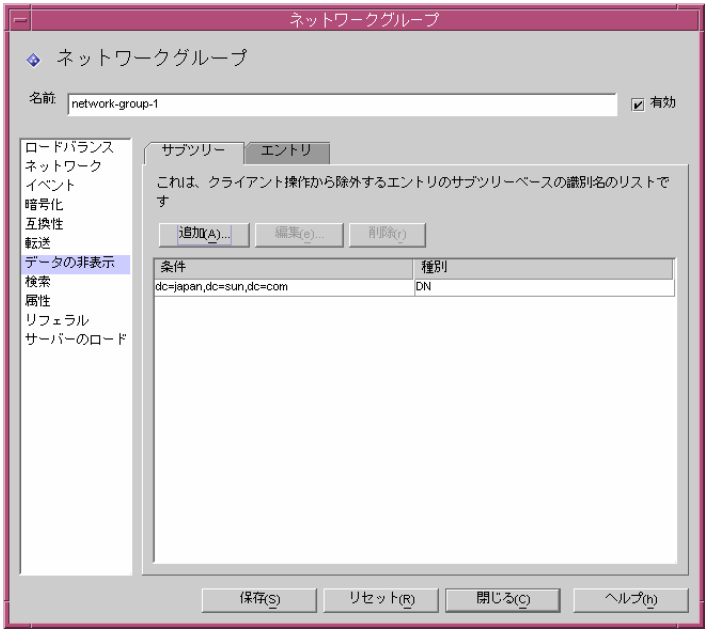
比較操作を許可：この設定は、デフォルトで有効です。Directory Proxy Server が比較要求をサーバーに転送しないようにするときは、このオプションを無効にします。

追加、削除、変更、DN 変更、拡張操作を許可：デフォルトでは、Directory Proxy Server は追加操作、変更操作、削除操作、DN 変更操作、拡張操作の各要求を転送しません。これらの操作を転送できるようにする場合は、該当する操作を有効にします。

クライアントが TLS 開始操作のネゴシエーションを行えるようにする場合は、「拡張操作を許可」を有効にする必要があります。

13. グループのデータ非表示条件を指定するときは、左のフレームで「データの非表示」を選択し、右のフレームに適切な値を指定します。

    ディレクトリツリーのどの部分を非表示にするかを指定するときは「サブツリー」タブを使用し、非表示にするエントリまたは属性を指定するときは「エントリ」タブを使用します。



「サブツリー」タブの要素の説明は、次のとおりです。

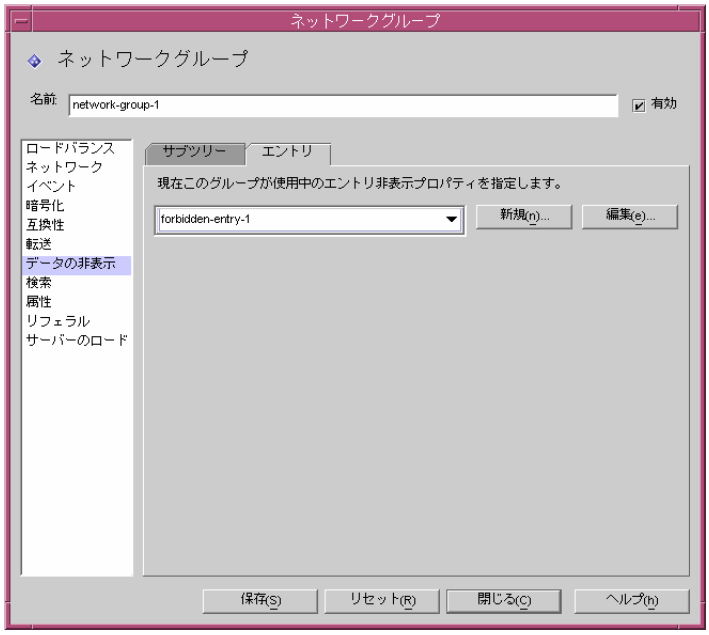
除外するエントリのサブツリー：禁止されたサブツリーと同じ位置か、その下にあるエントリを要求する操作は、不正アクセスエラーで拒否されます。検索フィルタに適合しても、禁止されたサブツリー内のエントリは除外されます。ただし、このオプションによって、結果の一部として返されるエントリから、サブツリーの下にある値を含む DN 構文の属性が削除されることはありません。

追加：除外されるエントリのサブツリーのベースのリストに識別名を追加するためのダイアログボックスを表示します。デフォルトでは、ネットワークグループに識別名が存在しない場合は、ディレクトリ内のすべてのエントリにアクセスできます。リスト内のエントリには dn 構文があります。

編集：識別名を編集するためのダイアログボックスを表示します。

削除：識別名をリストから削除します。

14. 「エントリ」タブを選択し、非表示にするエントリまたは属性を指定します。



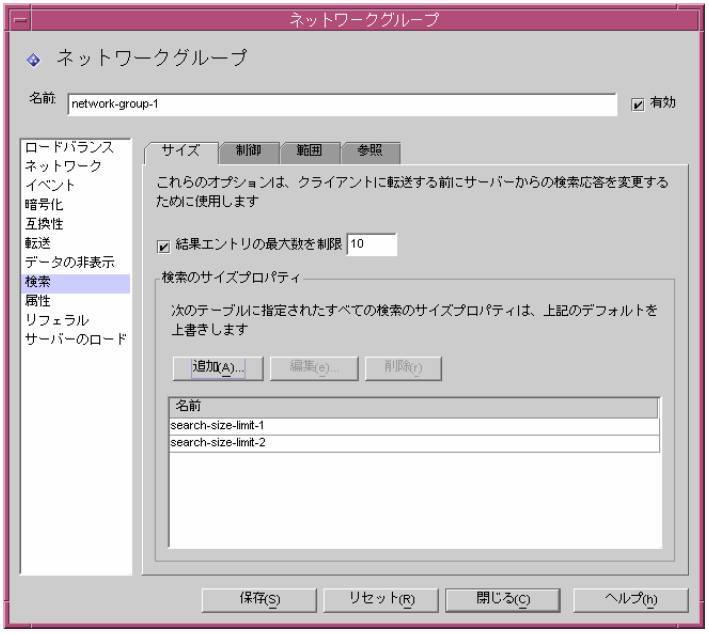
「エントリ」タブの要素の説明は、次のとおりです。

現在このグループが使用中のエントリ非表示プロパティを指定します：ドロップダウンリストには、禁止エントリプロパティの既存のオブジェクトが表示されます。110 ページの「禁止エントリプロパティ」を参照してください。オブジェクト名を選択します。デフォルトでは、オブジェクトは選択されていません (< なし >)。オブジェクトがない場合は、「新規」ボタンをクリックして、オブジェクトをその場で作成することができます。

新規：新しい禁止エントリプロパティを作成するためのダイアログを表示します。

編集：既存の禁止エントリプロパティを編集するためのダイアログを表示します。

15. グループの検索属性を指定するときは、左のフレームで「検索」を選択し、右のフレームに適切な値を指定します。



「サイズ」タブの要素の説明は、次のとおりです。

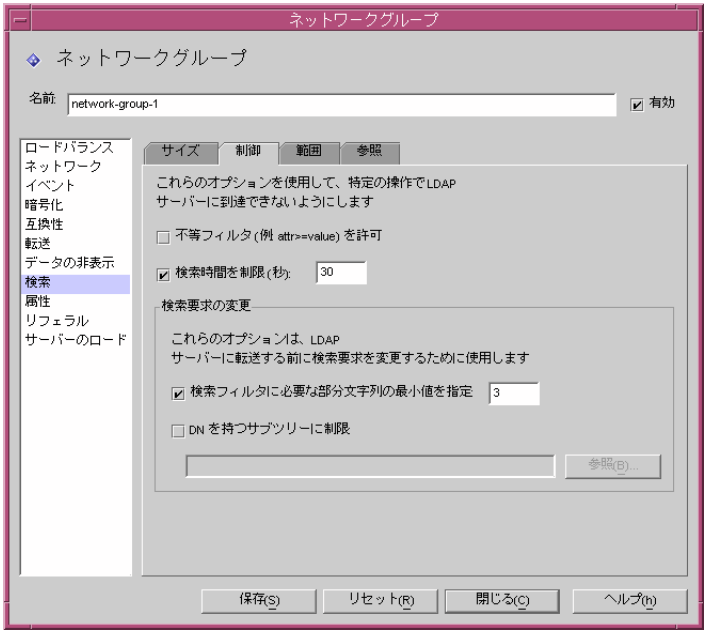
結果エントリの最大数を制限：1 回の検索操作で一度にクライアントから返すことができる結果エントリの最大数を指定するときは、このオプションを有効にします。0 (ゼロ) よりも大きい任意の数値を指定できます。検索されたエントリの数が指定された値に達すると、`administrativeLimitExceeded` エラーがクライアントに通知され、以降のエントリは破棄されます。デフォルトでは、このプロパティは無効で、エントリは破棄されません。

追加：検索のサイズ制限プロパティを追加するためのダイアログを表示します。詳細は、124 ページの「検索のサイズ制限プロパティ」を参照してください。

編集：検索のサイズ制限プロパティを編集するためのダイアログを表示します。

削除：検索のサイズ制限プロパティを削除するためのダイアログを表示します。(この処理では、確認メッセージを表示することなくグループからプロパティが削除されます。)

16. 「制御」タブを選択し、検索フィルタの制御条件を指定します。



「制御」タブの要素の説明は、次のとおりです。

不等フィルタを許可：この設定は、デフォルトで有効です。このオプションは、クライアントが不等フィルタ (`attr>=value`) および (`attr<=value`) を含む検索を要求できるかどうかを指定します。ネットワークグループが不等値検索の実行を許可しない場合は、このオプションを無効にします。

検索時間を制限：検索操作の最大制限時間 (秒) を指定するには、このオプションを有効にし、ネットワークグループに対して値 (秒数) を入力します。クライアントがこのオプションで指定した値よりも大きい制限時間を指定した場合は、このネットワークグループに指定した値はクライアントの要求よりも優先されます。このオプションはデフォルトで無効になっているため、クライアントは任意の制限時間 (無制限を含む) を設定できます。

検索フィルタに必要な部分文字列の最小値を指定：検索フィルタに指定するために必要な部分文字列の最小文字数を指定する場合は、このオプションを有効にして、値を入力します。この値には、1 よりも大きい数値を指定します。このオプションが無効になっている場合は、デフォルトで検索フィルタに任意の長さの部分文字列を指定できます。Web ロボットで実行できる検索の種類を制限する場合は、ネットワークグループ内でこのオプションを有効にする必要があります。たとえば、値に 2 を指定すると、(`cn=A*`) のような検索は行われません。

注 この属性は presence フィルタ (attrname=*) には影響しません。特定の presence フィルタを使用できないようにするには、禁止比較設定を使用します。

DN を持つサブツリーに制限 : このオプションを有効にして、すべての操作に対してサブツリーのベースを指定します。このオプションには、dn 構文を指定します。このオプションを無効にすると、最低ベースに対する制限がなくなります。

対象となるエントリが最低ベースのエントリと同じ位置か、それよりも下位にある操作は、このオプションの影響を受けません。対象となるエントリが最低ベースのエントリよりも上位にある操作がサブツリー検索である場合は、対象エントリを最低ベースに変更するために、サーバーに送信する前にクエリーが書き換えられます。対象となるエントリが最低ベースか、それよりも上位にある場合、要求は拒否され、オブジェクトエラーは発生しません。

たとえば、「DN を持つサブツリーに制限」を次のように設定します。

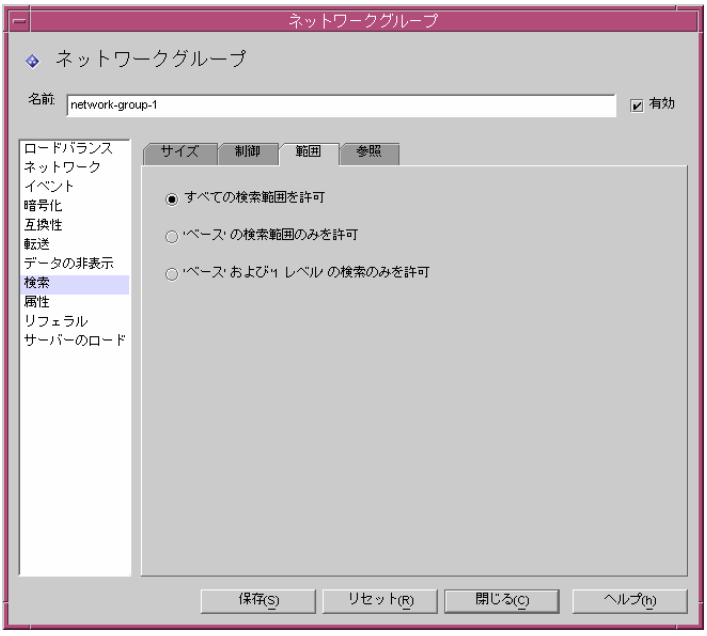
`o=sun、st=California、c=US`

`st=California、c=US` のサブツリー検索を受信すると、サーバーが次のサブツリー検索を実行するように検索が書き換えられます。

`o=sun、st=California、c=US`

参照 : 有効な DN の作成に役立つダイアログを表示します。

17. 「範囲」タブを選択して、検索対象範囲 (クライアントが検索要求に指定できる範囲) を指定します。



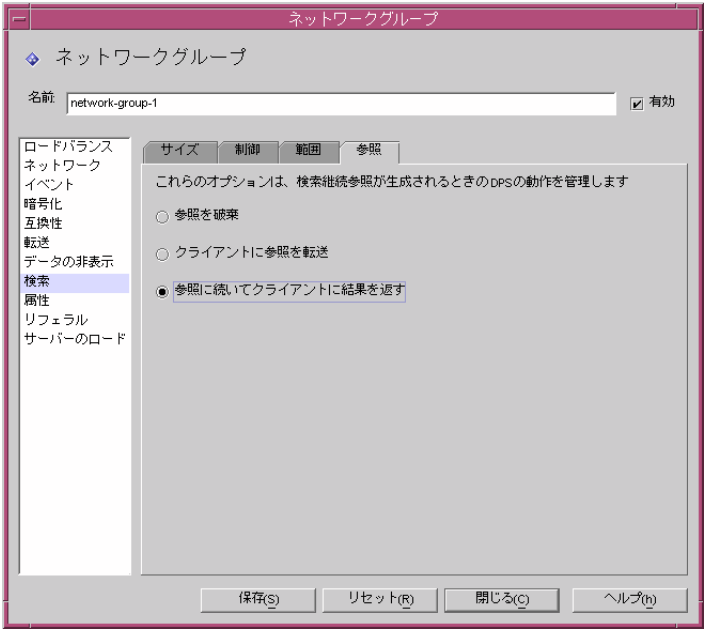
「範囲」タブの要素の説明は、次のとおりです。

すべての検索範囲を許可：デフォルトでは、このオプションは有効で、クライアントはすべての検索範囲を指定できます。

' ベース ' の検索範囲のみを許可：ベース検索のみを指定できるようにするには、このオプションを有効にします。

' ベース ' および '1 レベル ' の検索のみを許可：ベース検索と 1 レベル検索のみを指定できるようにするには、このオプションを有効にします。

18. 「参照」タブを選択し、検索時に検索の継続参照が生成された場合の処理を指定します。



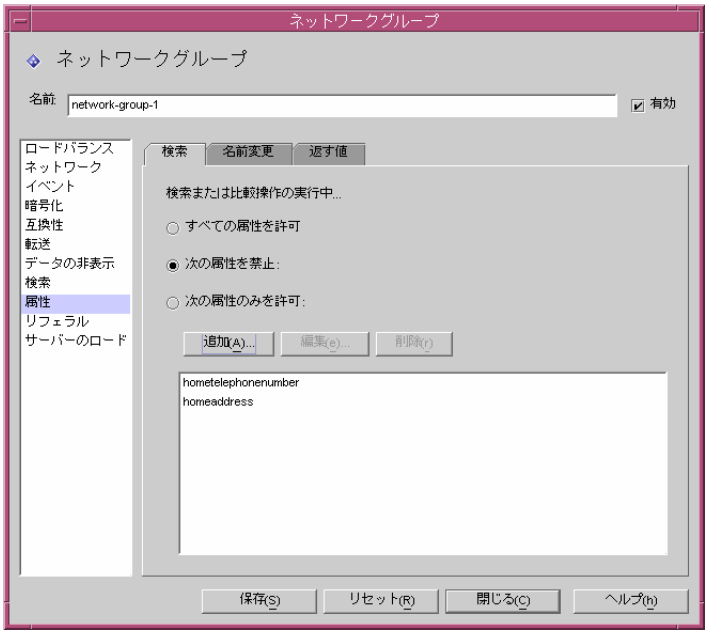
「参照」タブの要素の説明は、次のとおりです。

参照を破棄：デフォルトでは、このオプションは有効で、検索時に生成される参照は破棄されます。

クライアントに参照を転送：検索の継続参照を転送する場合にのみこのオプションを有効にします。

参照に続いてクライアントに結果を返す：検索の継続参照を実行して、その結果を返す場合は、このオプションを有効にします。検索の継続リフェラルは特殊なリフェラルであり、照会した元のディレクトリサーバーによって照会の一部が満たされていますが、そのディレクトリサーバーにはその照会を満たす他のデータを持つ別のディレクトリサーバーへの参照があります。このオプションを使用すると、ネーミングコンテキストが別の LDAP サーバーによって使用されるディレクトリ情報ツリーの一部を非表示にすることができます。また、このオプションを有効にすると、クライアントはこのサーバーが動作しているネットワークアドレスやポートを確認できなくなります。

19. グループの属性条件を指定するときは、左のフレームで「属性」を選択し、右のフレームに適切な値を指定します。



「検索」タブの要素の説明は、次のとおりです。

このタブは、ある特定の種類の検索操作や比較操作が LDAP サーバーに達しないようにするために使用します。クライアントの要求がこの制限に当てはまる場合、Directory Proxy Server は不正アクセスエラーをクライアントに返します。

すべての属性を許可：このオプションはデフォルトで有効になっているため、検索フィルタや比較にすべての属性を使用できます。

次の属性を禁止：検索フィルタや比較要求にクライアントが使用できない属性の名前を指定するには、このオプションを有効にします。

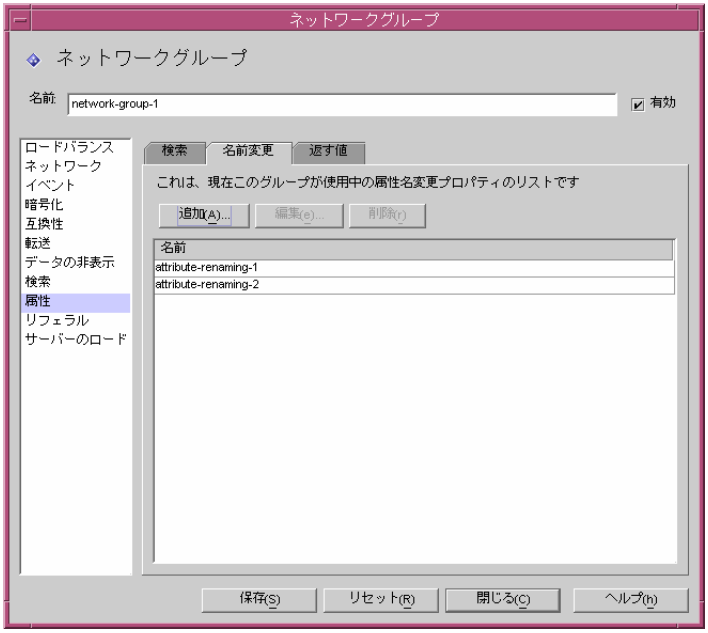
次の属性のみを許可：検索フィルタや比較要求に使用できる属性の名前を指定するには、このオプションを有効にします。ネットワークグループのテーブル内に属性値が 1 つ以上ある場合、比較要求がこれらのどの属性値とも適合しなければ、Directory Proxy Server によって要求が拒否されます。ネットワークグループのテーブル内に属性値が 1 つもない場合、属性がどの属性とも一致しなければ、クライアントはその属性を使用することができます。たとえば、cn、dn、mail の各属性だけをクライアントで検索できるようにする場合は、これらの属性をテーブルに追加します。

追加：属性をテーブルに追加できるダイアログボックスを表示します。これらの属性を使用不可にするか、使用可能にするかを指定する必要があります。

編集：選択されているテーブル内の属性を編集するためのダイアログボックスを表示します。

削除：属性をテーブルから削除します。

20. 「名前変更」タブを選択し、属性名の変更規則を指定します。



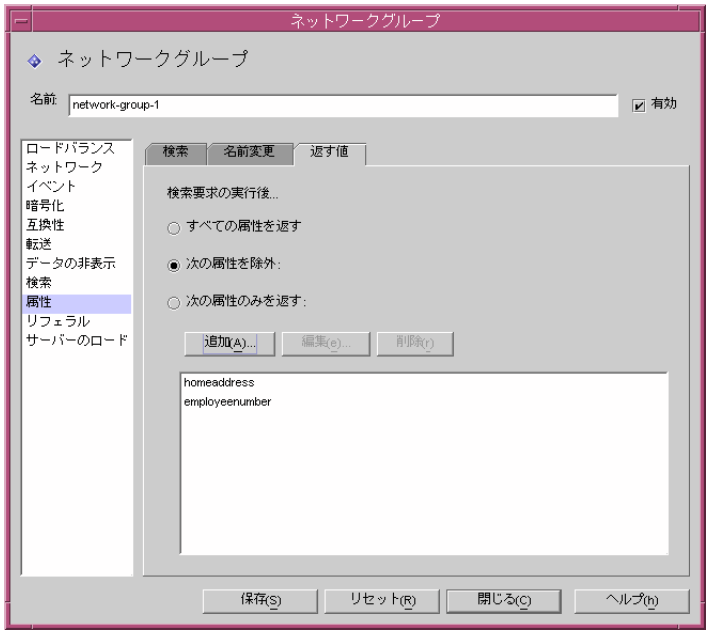
「名前変更」タブの要素の説明は、次のとおりです。

追加：1 つ以上の既存の属性の名前変更プロパティを、このネットワークグループで使用される次のテーブルに追加するためのダイアログボックスを表示します。(106 ページの「属性名変更プロパティ」を参照してください。)

編集：選択された属性の名前変更プロパティを編集するためのダイアログボックスを表示します。

削除：属性の名前変更プロパティをテーブルから削除します。

21. 「返す値」タブを選択し、サーバーが返す検索結果がクライアントに転送される前に、それに適用する制限を指定します。



「返す値」タブの要素の説明は、次のとおりです。

すべての属性を返す：デフォルトではこのオプションが有効で、すべての属性が返されます。

次の属性を除外：検索結果のエントリから除外する属性の名前を指定する場合は、このオプションを有効にします。

次の属性のみを返す：検索結果から返すことができる属性 (存在する場合) の名前を指定する場合は、このオプションを有効にします。

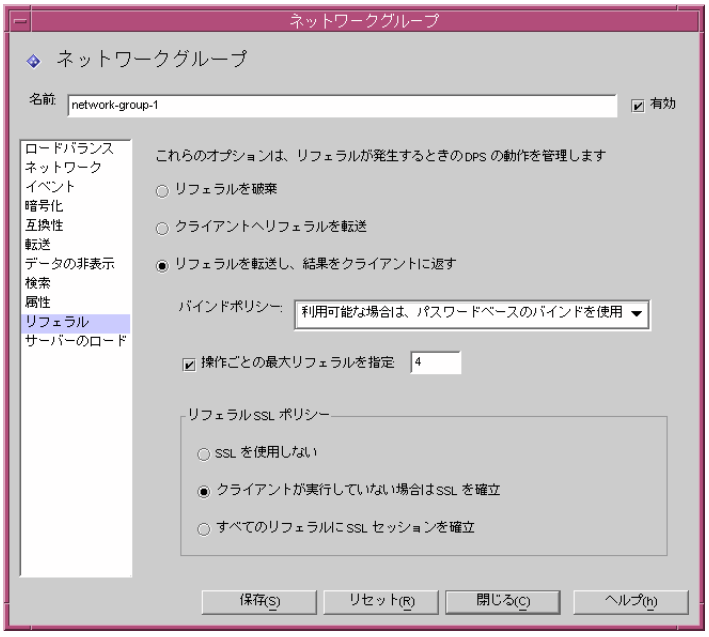
検索結果の一部として返される属性が「次の属性のみを返す」テーブルに指定されていない場合、これらの属性は返されません。テーブルが空で、「次の属性を除外」テーブルに指定されていない場合は、これらの属性は返されます。

追加：属性をテーブルに追加できるダイアログボックスを表示します。これらの属性を使用不可にするか、使用可能にするかを上のオプションで指定する必要があります。

編集：選択されているテーブル内の属性を編集するためのダイアログボックスを表示します。

削除：属性をテーブルから削除します。

22. グループのリフェラルを指定するときは (たとえば、サーバーから返されるリフェラルをグループが転送、実行、または破棄する、など)、左のフレームで「リフェラル」を選択し、右のフレームに適切な値を指定します。



画面要素の説明は、次のとおりです。

リフェラルを破棄：ネットワークグループがサーバーによって返されたすべてのリフェラルを破棄する場合は、このオプションを有効にします。

クライアントへリフェラルを転送：デフォルトではこのオプションが有効で、サーバーによって返されたリフェラルを転送します。

リフェラルを転送し、結果をクライアントに返す：ネットワークグループがサーバーによって返されたリフェラルを実行し、結果をクライアントに返す場合は、このオプションを有効にします。

バインドポリシー：このオプションは、リフェラルが実行されるときのバインドポリシーを制御します。

Directory Proxy Server は、SASL メカニズムを使ってバインドされたクライアントに対してバインドを再実行できないので注意してください。このため、「パスワードベースのバインドを要求」が指定され、クライアントが SASL メカニズムでバインドされている場合、リフェラル操作は拒否されます。

常に匿名でバインド：ネットワークグループに接続しているクライアントのリフェラルを実行するときに、Directory Proxy Server が常に匿名でバインドするように指定するときは、このオプションを選択します。

利用可能な場合は、パスワードベースのバインドを使用：クライアントがパスワードベースのバインドを使用している場合、ネットワークグループが単純なバインドを使用する必要があるときは、このオプションを選択します。このオプションを選択しない場合は、匿名でバインドします。このオプションはデフォルトで選択されています。

パスワードベースのバインドを要求：クライアントがパスワードベースのバインドを使用しない場合に、ネットワークグループが参照された操作を拒否する必要があるときは、このオプションを選択します。

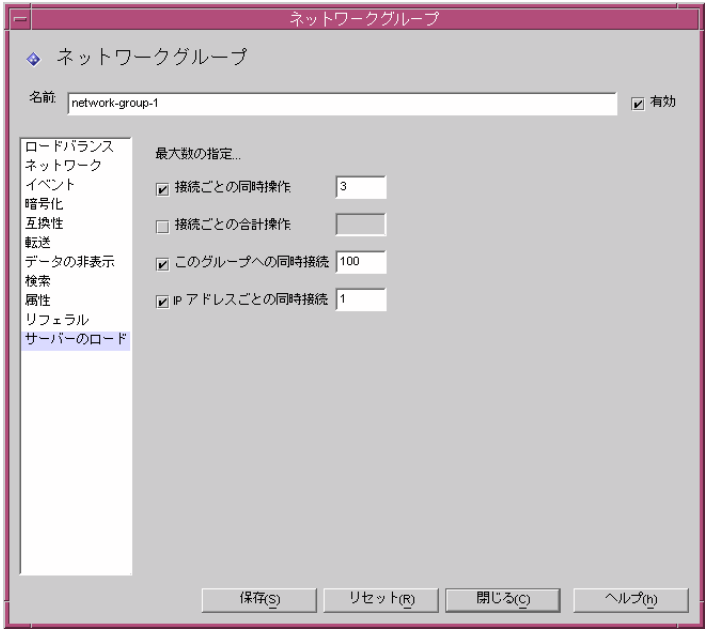
操作ごとの最大リフェラルを指定：0 (ゼロ) 以上の整数値を入力します。この値により、1 つの操作に対して実行される参照の最大数が制限されます。デフォルトは 15 です。0 (ゼロ) を指定すると、無制限になります。

リフェラル SSL ポリシー：このパネルを有効にするためには、「暗号化」ビューで SSL オプションが有効になっている必要があります。

クライアントが実行していない場合は SSL を確立：クライアントが Directory Proxy Server との SSL セッションをすでに確立していてネットワークグループが SSL を開始するだけの場合に、このオプションを有効にします。このオプションはデフォルトで選択されています。

すべてのリフェラルに SSL セッションを確立：リフェラルに対して、操作が転送される前にグループが SSL セッションを開始する場合は、このオプションを有効にします。

23. グループのサーバーロード条件を指定するときは、左のフレームで「サーバーのロード」を選択し、右のフレームに適切な値を指定します。



画面要素の説明は、次のとおりです。

接続ごとの同時操作：そのグループの 1 つの接続で Directory Proxy Server が同時に処理できる操作の数を制限する場合は、このオプションを選択します。この値には、0 (ゼロ) よりも大きい整数を指定します。この属性を指定しない場合、操作の数は無制限になります。たとえば、この値を 1 に設定すると、そのグループに含まれるすべてのクライアントは、同時に発生した LDAP 操作を強制的に実行します。同時に発生したその他の要求は、操作を中断させる要求を除き、サーバー使用中のエラーにより失敗します。

接続ごとの合計操作：そのグループの 1 つの接続で Directory Proxy Server が処理できる操作の合計数を制限する場合は、このオプションを選択します。この値には、0 (ゼロ) よりも大きい整数を指定します。クライアントが 1 つの接続に対してグループに許可されている最大操作数を超えた場合は、Directory Proxy Server によってその接続は閉じられます。この属性を指定しない場合、操作の数は無制限になります。

このグループへの同時接続：このネットワークグループへの同時接続の数を制限し、その値を指定するときは、このオプションを選択します。

IP アドレスごとの同時接続：クライアントが 1 つの IP アドレスから確立できる同時接続の数を制限する場合は、このオプションを選択します。デフォルトでは、任意の数の接続を確立できます。

24. 「保存」をクリックして、グループを作成します。

    Directory Proxy Server の設定が変更され、この設定が適用されるサーバーを再起動するように促すメッセージが表示されます。この時点では、まだサーバーを再起動しません。再起動は、すべての設定変更が完了してから実行します。

25. 必要なすべての追加グループについて、手順 3 から手順 24 を繰り返します。

26. 「ネットワークグループ」ウィンドウにアクセスし (手順 2 を参照)、グループに適切な優先度を設定します。

27. サーバーを再起動します。57 ページの「Directory Proxy Server の再起動」を参照してください。

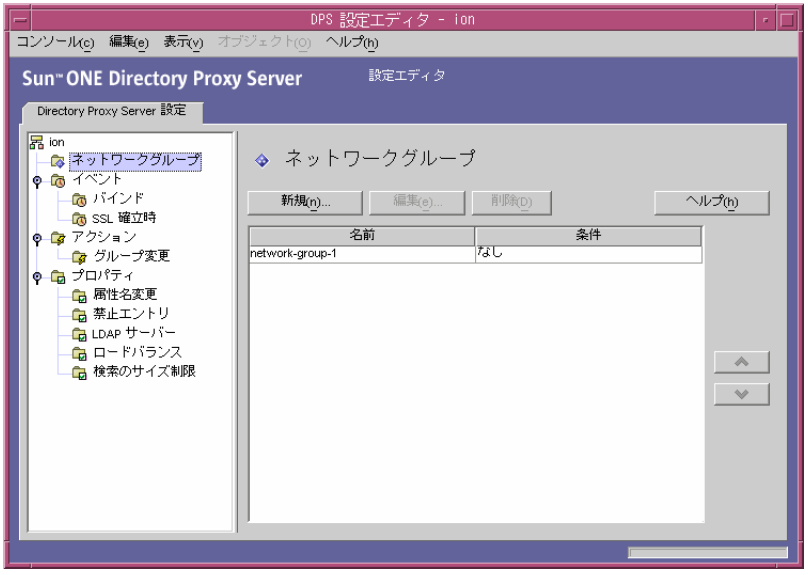
グループの変更

グループを変更するには、次の手順を実行します。

1. Directory Proxy Server 設定エディタコンソールにアクセスします。45 ページの「Directory Proxy Server コンソールへのアクセス」を参照してください。

2. ナビゲーションツリーで、Network Groups を選択します。

   右側のペインには既存のグループがリスト表示されます。



3. 変更するグループをリストから選択し、「編集」をクリックします。

4. 必要な修正を加えます。

5. 「保存」をクリックして、変更内容を保存します。

   Directory Proxy Server の設定が変更され、この設定が適用されるサーバーを再起動するように促すメッセージが表示されます。この時点では、まだサーバーを再起動しません。再起動は、すべての設定変更が完了してから実行します。

6. 変更が必要なすべてのグループについて、手順 3 から手順 5 を繰り返します。

7. サーバーを再起動します。57 ページの「Directory Proxy Server の再起動」を参照してください。

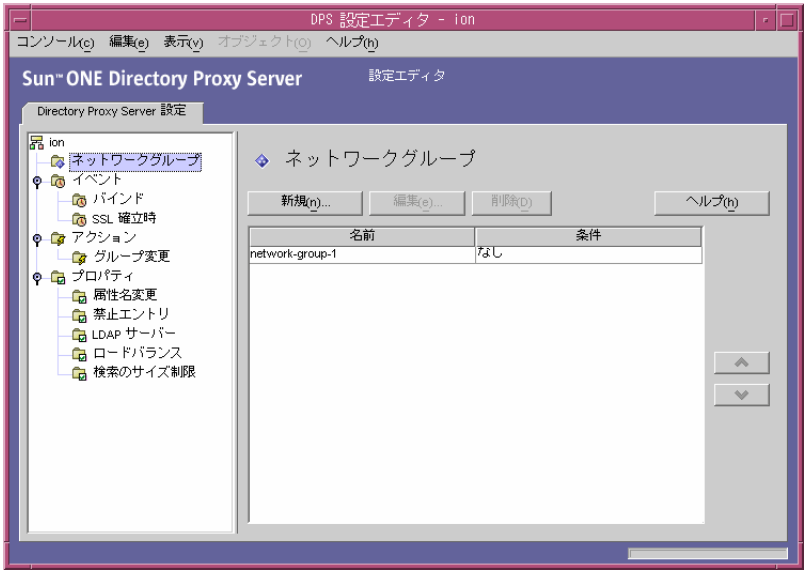
グループの削除

不要なネットワークグループは、Directory Proxy Server の設定から削除できます。グループを削除するには、次の手順を実行します。

1. Directory Proxy Server 設定エディタコンソールにアクセスします。45 ページの「Directory Proxy Server コンソールへのアクセス」を参照してください。

2. ナビゲーションツリーで、Network Groups を選択します。

   右側のペインには既存のグループがリスト表示されます。



3. 削除するグループをリストから選択し、「削除」をクリックします。

4. 処理を承認します。

   削除したグループの名前は、リストに表示されなくなります。Directory Proxy Server の設定が変更され、この設定が適用されるサーバーを再起動するように促すメッセージが表示されます。この時点では、まだサーバーを再起動しません。再起動は、すべての設定変更が完了してから実行します。

5. 削除が必要なすべてのグループについて、手順 3 と手順 4 を繰り返します。

6. サーバーを再起動します。57 ページの「Directory Proxy Server の再起動」を参照してください。

第 7 章

プロパティオブジェクトの定義と管理

このマニュアルの配備に関する章でも説明しましたが、Sun ONE Directory Proxy Server は LDAP アクセスルータとして機能し、非公開ディレクトリ情報を未認証のアクセスから保護しながら、公開情報を安全に公表するのに役立ちます。サーバーは、数千の LDAP クライアント要求を処理し、要求をディレクトリサーバーにルーティングする前に詳細なアクセス制御規則とプロトコルフィルタリング規則を適用できます。

Directory Proxy Server のプロパティオブジェクトを使用することで、特別な制限を LDAP クライアントに適用することができます。これらのプロパティは、制限の適用が必要なその他のエントリに含めることもできます。この章では、各プロパティの概要を示し、Directory Proxy Server 設定エディタコンソールを使用してプロパティオブジェクトを作成する方法について説明します。

この章で説明する項目は、次のとおりです。

属性名変更プロパティ

通常、LDAP ディレクトリには組織の従業員やネットワークリソースなどのエントリに関する情報が含まれます。それぞれのエントリは、ディレクトリ内に 1 つのエントリを持ちます。ディレクトリ内の各エントリは、識別名 (DN) によって識別され、属性セットとその値によって表されます。各エントリは、そのエントリが記述するオブジェクトの種類を指定するオブジェクトクラス属性を持ち、そこに含まれる追加属性のセットを定義します。各属性は、エントリの特性を示します。たとえば、オブジェクトクラスが `organizationalPerson` で、特定の組織のメンバーを表すエントリがあるとします。このオブジェクトクラスには、`givenname` 属性と `telephoneNumber` 属性があります。これらの属性に割り当てられた値は、エントリが示すメンバーの名前と電話番号を表します。

多くのディレクトリ配備では、LDAP クライアント側に定義されている属性は、サーバー側に定義されている属性にマップしません。このような状態でクライアントとサーバーの間の通信を利用できるように、Directory Proxy Server は属性名の変更をサポートします。つまり、Directory Proxy Server は、クライアントクエリをディレクトリサーバーに渡す前に、クエリ内の属性名をディレクトリサーバーが認識できる形式に変更し、サーバーからの応答をクライアントに渡す前にも同様の処理を行うことができます。

図 7-1 は、スキーママッピングで Directory Proxy Server の属性名変更機能がどのように使用されるかを示しています。

図 7-1　属性名変更プロパティによるスキーマのマッピング

電子メールクライアントは、人名の姓を「surname」という属性の値として想定し、LDAP サーバーは姓を「sn」という属性の値として想定しています。Directory Proxy Server がこの 2 つの属性をマップするときに、変更されるのは属性名だけで、属性の値は変更されません。

クライアントとサーバーの属性名に影響する規則を定義するときは、属性名変更プロパティを使用します。対応するサーバー属性にマップしたり逆にマップされたりする必要があるクライアント属性の名前を指定します。これにより、クライアント要求にサーバーが認識できない属性名が含まれている場合でも、Directory Proxy Server はそれをサーバーが認識できる名前にマップできるので、クライアントからサーバーへの通信が可能になります。同様に、サーバーが応答を返す場合にも、Directory Proxy Server はクライアントが認識できない属性を認識できる形式に変換します。

次に、Directory Proxy Server 設定エディタコンソールを使用して、属性名変更プロパティのオブジェクトを作成する方法について説明します。

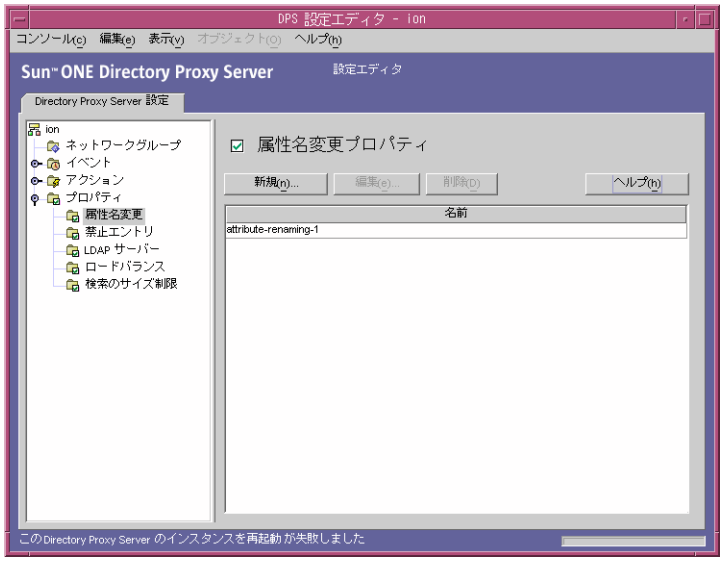
注 属性名変更プロパティのオブジェクトを作成するときは、サーバー属性とクライアント属性の両方を指定する必要があります。指定していない場合、Directory Proxy Server は起動に失敗します。

属性名変更プロパティオブジェクトの作成

Directory Proxy Server が名前を変更するクライアントとサーバーの属性を指定するには、次の手順を実行します。

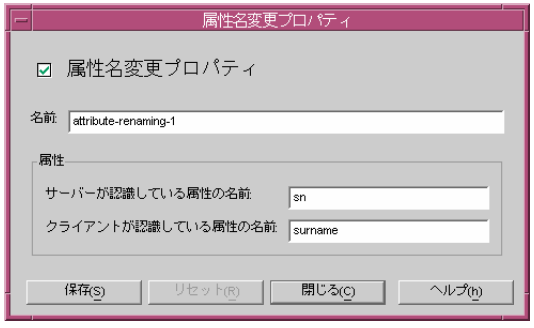
1. Directory Proxy Server 設定エディタコンソールにアクセスします。45 ページの「Directory Proxy Server コンソールへのアクセス」を参照してください。
2. ナビゲーションツリーで、「プロパティ」ノードを展開し、「属性名変更」を選択します。

   属性名変更プロパティの既存のオブジェクトが右のペインにリスト表示されます。



3. 「新規」をクリックします。

   「属性名変更プロパティ」ウィンドウが表示されます。



4. 「名前」フィールドにプロパティオブジェクトの名前を入力します。この名前には、一意の英数文字列を指定する必要があります。

注	属性名は、7 ビット文字だけで指定する必要があります。

5. マッピングする属性を残りのフィールドに指定します。

   属性名変更の値は、それぞれがピリオドで区切られた 10 進数として指定することができます (`2.5.4.10` など)。また、属性タイプとしてテキスト形式の名前を 1 つ以上割り当てることができます。これらの名前は文字で始める必要がありますが、2 番目以降には ASCII 文字、数字、およびハイフンを使用することもできます。大文字と小文字は区別されません。

   サーバーが認識している属性の名前 : サーバーが認識している属性の名前を入力します。

   クライアントが認識している属性の名前 : クライアントが認識している属性の名前を入力します。

   クライアントの要求に、「クライアントが認識している属性の名前」で指定した属性名が含まれている場合、その属性名は「サーバーが認識している属性の名前」の値に変換されます。同様に、サーバーから送信された結果に、「サーバーが認識している属性の名前」で指定した属性名が含まれている場合、その属性名は「クライアントが認識している属性の名前」の値に変換されます。

6. 「保存」をクリックして、オブジェクトを作成します。

   Directory Proxy Server の設定が変更され、この設定が適用されるサーバーを再起動するように促すメッセージが表示されます。この時点では、まだサーバーを再起動しません。再起動は、すべての設定変更が完了してから実行します。

7. 必要なすべての追加オブジェクトについて、手順 3 から手順 6 を繰り返します。

8. サーバーを再起動します。57 ページの「Directory Proxy Server の再起動」を参照してください。

禁止エントリプロパティ

さまざまな理由から、LDAP ディレクトリ内の特定のエントリ (または、そのエントリを表わす属性) を LDAP クライアントで表示できないように設定しなければならないことがあります。たとえば、全従業員のエントリがディレクトリに含まれ、名前、電子メールアドレス、部署、勤務地、事務所の電話番号、自宅の電話番号などの従業員データに対応する属性が各エントリに含まれている場合、従業員の自宅の電話番号をクライアント側で表示できないようにすることができます。

禁止エントリは、LDAP クライアントで非表示にする必要のある、LDAP ディレクトリ内のエントリです。このような状況でクライアントとディレクトリサーバーとの通信を利用できるように、Directory Proxy Server は禁止エントリをサポートしています。Directory Proxy Server は、これらのエントリの LDAP エントリと属性を LDAP クライアント側で非表示にすることができます。

ディレクトリエントリとその属性の非表示に影響する規則を定義するときは、禁止エントリプロパティを使用します。このプロパティを使用することで、非表示にする必要のあるエントリまたはその属性のリストを、いくつかの方法で指定できます。たとえば、次のような方法で指定できます。

- 非表示にするエントリのエントリまたは属性の DN を指定します。
- 非表示にするエントリのエントリまたは属性の DN を正規表現で指定します (たとえば、`.*OU=INTERNAL.*`)。
- エントリの属性名と値のペアを指定します (たとえば、`secret:yes`)。指定した属性名 / 値のペアと一致する属性名 / 値のペアがエントリに含まれている場合、そのエントリまたはそのコンテンツの一部は非表示になります。

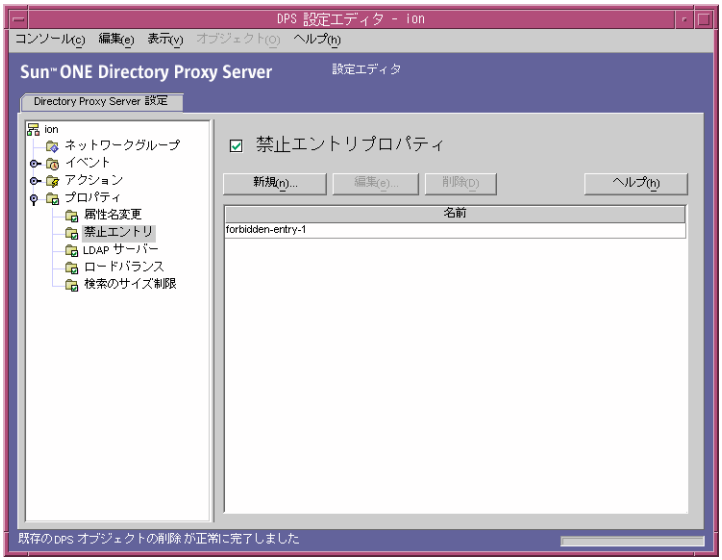
次に、Directory Proxy Server 設定エディタコンソールを使用して、禁止エントリプロパティのオブジェクトを作成する方法について説明します。

禁止エントリプロパティオブジェクトの作成

Directory Proxy Server がクライアント側で非表示にするエントリまたはエントリの属性を指定するには、次の手順を実行します。

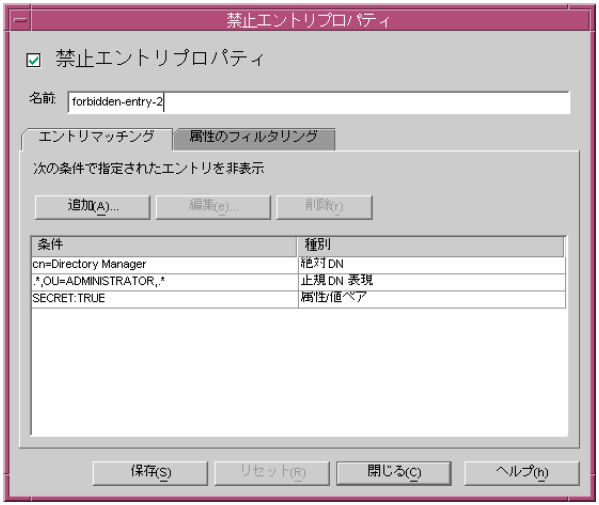
1. Directory Proxy Server 設定エディタコンソールにアクセスします。45 ページの「Directory Proxy Server コンソールへのアクセス」を参照してください。
2. ナビゲーションツリーで、「プロパティ」ノードを展開し、「禁止エントリ」を選択します。

   禁止エントリプロパティの既存のオブジェクトが右のペインにリスト表示されます。



3. 「新規」をクリックします。

   「禁止エントリプロパティ」ウィンドウが表示されます。



4. 「名前」フィールドにプロパティオブジェクトの名前を入力します。この名前には、一意の英数文字列を指定する必要があります。
5. 「エントリマッチング」タブで、適切な値を指定します。このタブには、このプロパティの名前と非表示にする LDAP エントリの設定が表示されます。

追加 : LDAP エントリを非表示にする条件を追加するためのメニューを表示します。指定できる条件のタイプは、「絶対 DN」、「正規 DN 表現」、または「属性 / 値ペア」です。エントリ名は、直接入力するだけでなく、ディレクトリ情報ツリーで既存のエントリを参照することができます。

絶対 DN : 非表示にするエントリの DN を入力するためのダイアログを表示します。

正規 DN 表現 : 非表示にするエントリの DN の正規表現を入力するためのダイアログを表示します。DN の正規表現は、通常の形式で指定する必要があります。つまり、RDN コンポーネントと等号 (=) の間には空白文字を挿入せず、属性名と値をすべて大文字で指定する必要があります。

たとえば、すべての DN を「ou=internal」という RDN コンポーネントと一致させるには、次のように指定する必要があります。

.*OU=INTERNAL.*

「属性のフィルタリング」タブに、含まれる属性名がリストされていて、任意の属性がそのリストのどの属性とも一致しない場合、その属性は返されません。「属性のフィルタリング」タブで除外される属性と一致する属性が LDAP エントリに含まれていない場合、その LDAP エントリは返されます。

正規表現については、次の文献を参考にしてください。『Mastering Regular Expressions』、Friedl および Oram 著、O'Reilly 発行、ISBN: 1565922573

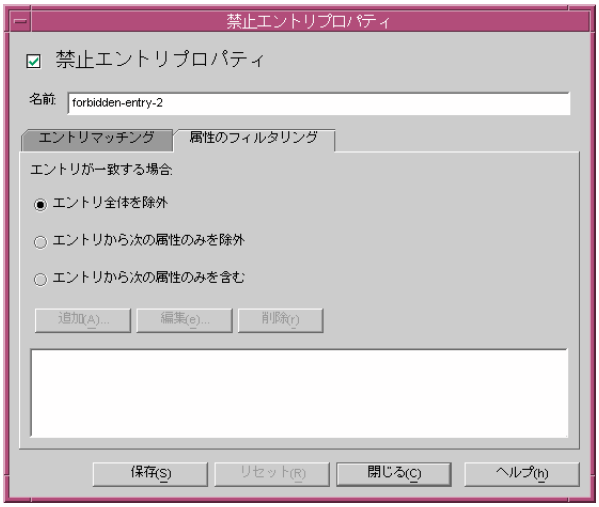
属性 / 値ペア : 属性の名前と値の組み合わせを指定するためのダイアログを表示します。指定した属性名 / 値のペアと一致する属性名 / 値のペアがエントリに含まれている場合、そのエントリまたはそのコンテンツの一部は非表示になります。

たとえば、「ou=internal」または「secret=yes」のどちらかを属性の 1 つとして含むエントリをすべて非表示にする場合は、「ou」という属性と「internal」という値を指定します。

編集 : 現在選択されているテーブル内のエントリを編集するためのダイアログを表示します。

削除 : 現在選択されているテーブル内のエントリを削除します。

6. 「属性のフィルタリング」タブを選択し、適切な値を指定します。



このタブには、ある特定の属性を除外したり、含めたりすることができる設定が表示されます。

エントリ全体を除外：属性のフィルタリングを実行せず、エントリ全体を非表示にする場合は、このオプションを選択します。

エントリから次の属性のみを除外：上記のどの指定にも適合するエントリから除外する属性名のリストがテーブルに含まれるようにする場合は、このオプションを選択します。

エントリから次の属性のみを含む：上記のどの指定にも適合するエントリの一部として返すことができる属性名のリストがテーブルに含まれるようにする場合は、このオプションを選択します。

7. 「保存」をクリックして、オブジェクトを作成します。

   Directory Proxy Server の設定が変更され、この設定が適用されるサーバーを再起動するように促すメッセージが表示されます。この時点では、まだサーバーを再起動しません。再起動は、すべての設定変更が完了してから実行します。

8. 必要なすべての追加オブジェクトについて、手順 3 から手順 7 を繰り返します。

9. サーバーを再起動します。57 ページの「Directory Proxy Server の再起動」を参照してください。

LDAP サーバープロパティ

ディレクトリの配備では、Directory Proxy Server は LDAP クライアントと LDAP ディレクトリサーバーの間に配置されます。Directory Proxy Server は、LDAP クライアントからの要求を LDAP ディレクトリサーバーにルーティングする前、およびディレクトリサーバーからの応答をクライアントに渡す前に、これらの要求と応答をフィルタリングします。また、Directory Proxy Server は、レプリケートされた複数のディレクトリサーバー間で自動ロードバランスと、自動フェイルオーバーおよびフェイルバックをサポートしています。

Directory Proxy Server でバックエンドサーバーとして使用するディレクトリサーバーを指定するには、LDAP サーバープロパティを使用します。このプロパティを定義するときは、Directory Proxy Server が必要とするすべての詳細を指定する必要があります。たとえば、ディレクトリサーバーとの通信については、ディレクトリサーバーの IP アドレスまたは完全修飾ホスト名、ディレクトリサーバーがクライアント接続を待機するポートの番号、サーバーが対応している LDAP のバージョン、Directory Proxy Server とこのサーバーの間の通信に適用されるバージョンなどを指定する必要があります。

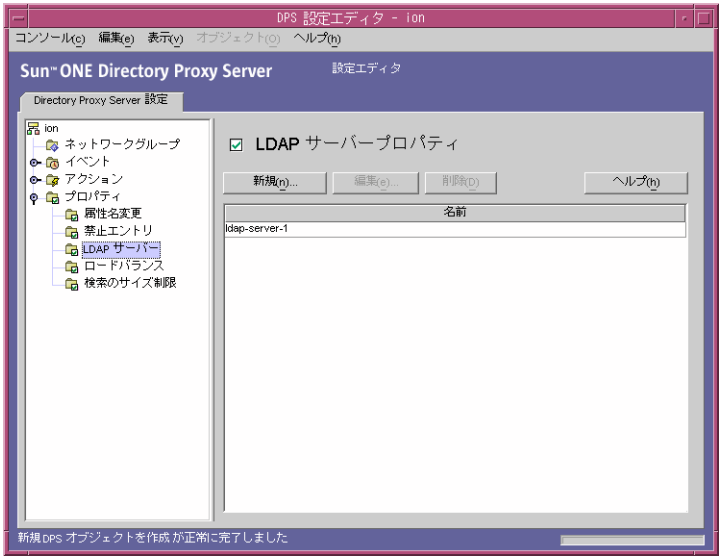
次に、Directory Proxy Server 設定エディタコンソールを使用して、LDAP サーバープロパティのオブジェクトを作成する方法について説明します。

LDAP サーバープロパティオブジェクトの作成

Directory Proxy Server の通信対象となるディレクトリサーバーを指定するには、次の手順を実行します。

1. Directory Proxy Server 設定エディタコンソールにアクセスします。45 ページの「Directory Proxy Server コンソールへのアクセス」を参照してください。
2. ナビゲーションツリーで、「プロパティ」ノードを展開し、「LDAP サーバー」を選択します。

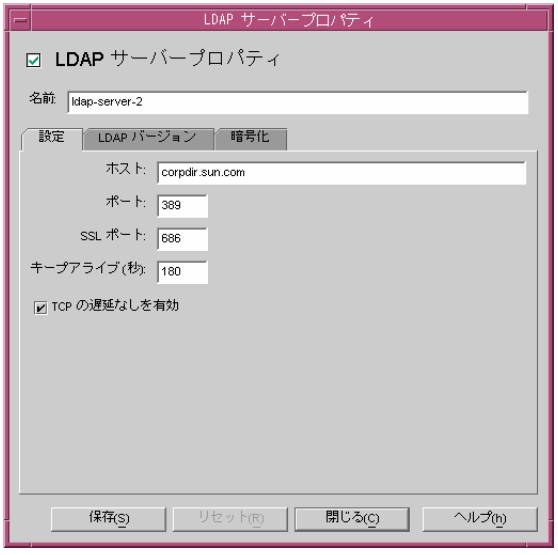
   LDAP サーバープロパティの既存のオブジェクトが右のペインにリスト表示されます。



3. 「新規」をクリックします。

   「LDAP サーバープロパティ」ウィンドウが表示されます。

4. 「名前」フィールドにプロパティオブジェクトの名前を入力します。この名前には、一意の英数文字列を指定する必要があります。



5. 「設定」タブには、このプロパティが参照する LDAP サーバーの基本設定が表示されます。

   ホスト：バックエンドの LDAP サーバーが稼動しているホストの完全なドメイン名または IP アドレスを入力します。この属性の指定は必須です。

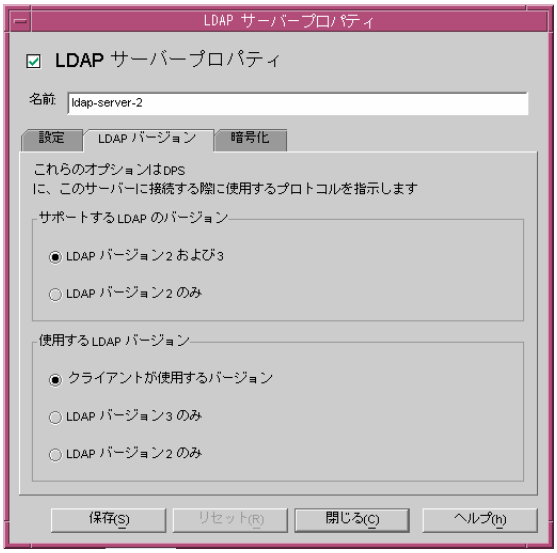
   ポート：バックエンドの LDAP サーバーが稼動しているポートの番号を入力します。この属性を指定しない場合に使用されるデフォルトのポート番号は、389 です。

   SSL ポート：バックエンドサーバーが LDAPS (SSL 経由の LDAP) 接続を待機するポートの番号を入力します。バックエンドの LDAP サーバーが LDAPS をサポートしていない場合は、この属性には値を設定しないでください。

   キープアライブ：Directory Proxy Server が反応しないサーバーをポークして、LDAP ディレクトリサーバーへのネットワークリンクがダウンしたのか、LDAP ディレクトリサーバーが反応しなくなったのかを判断するまでの秒数を入力します。ここに指定した秒数の間、Directory Proxy Server に接続しているクライアントが操作を保留し、Directory Proxy Server が接続先の LDAP サーバーからデータを受信しない場合、Directory Proxy Server はその LDAP サーバーに対して別の通信チャネルを開いて LDAP サーバーの可用性をテストします。Directory Proxy Server がこの処理を正常に行えない場合は、使用可能な別の LDAP サーバーで処理を継続します。この属性のデフォルト値は 180 秒です。LDAP サーバーが Directory Proxy Server と同じローカルネットワーク上にない場合は、この値を大きくすることをお勧めします。

   TCP の遅延なしを有効：この設定を無効にすると、Directory Proxy Server はこのサーバーへの接続に Nagle アルゴリズムを使用します。このオプションは、Directory Proxy Server と、このオブジェクトエントリで定義したサーバーとのネットワーク帯域幅が極端に制限されている場合にのみ無効にする必要があります。デフォルトでは、この設定は有効になっています。

6. 「LDAP バージョン」タブを選択し、適切な値を指定します。



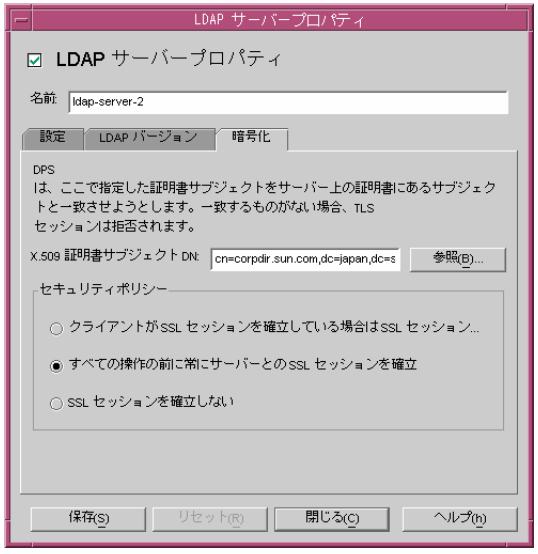
このタブには、このサーバーがサポートしている LDAP のバージョン、および Directory Proxy Server とこのサーバーとの通信に使用する LDAP バージョンを示す設定が表示されます。

サポートする LDAP のバージョン：「LDAP バージョン 2 および 3」または「LDAP バージョン 2 のみ」という 2 つのオプションのどちらかを選択します。デフォルトは、「LDAP バージョン 2 および 3」です。

使用する LDAP バージョン：「クライアントが使用するバージョン」、「LDAP バージョン 3 のみ」、「LDAP バージョン 2 のみ」という 3 つのオプションのいずれかを選択します。この属性は、このエントリで定義されるバックエンドサーバーとの通信時での使用が選択されている LDAP プロトコルのバージョンを Directory Proxy Server に通知します。デフォルトでは、「クライアントが使用するバージョン」が選択されます。

このオプションは、Directory Proxy Server がリフェラルを実行する必要のある LDAPv2 クライアントを使用する場合に便利です。この場合、バックエンドサーバーがリフェラルを送り返せるように、Directory Proxy Server 自体が LDAPv3 クライアントとしてバックエンドサーバーに接続する必要があります。このプロパティを参照するネットワークグループが複数の LDAP バージョン 2 のバインドを行えるようにする場合は、「LDAP バージョン 3 のみ」を選択する必要があります。

7. 「暗号化」タブを選択し、適切な値を指定します。



このタブには、このプロパティが参照する LDAP サーバーのセキュリティ保護された通信に関連する設定が表示されます。

X.509 証明書サブジェクト DN : LDAP サーバーの証明書のサブジェクト名を指定します。これを指定すると、Directory Proxy Server は指定した証明書のサブジェクトを LDAP サーバーの証明書に含まれるサブジェクトと照合し、一致しない場合は TLS セッションを拒否します。(この属性により、Directory Proxy Server は接続先の LDAP サーバーを認証します。この属性が設定されていない場合、Directory Proxy Server は、どのようなサブジェクト名でも受け付けます。)

セキュリティポリシー : Directory Proxy Server とバックエンドサーバーとの接続のためのセキュリティポリシーを定義するオプションとして、「クライアントが SSL セッションを確立している場合は SSL セッションを確立」、「すべての操作の前に常にサーバーとの SSL セッションを確立」、または「SSL セッションを確立しない」のいずれかを選択します。

8. 「保存」をクリックして、オブジェクトを作成します。

   Directory Proxy Server の設定が変更され、この設定が適用されるサーバーを再起動するように促すメッセージが表示されます。この時点では、まだサーバーを再起動しません。再起動は、すべての設定変更が完了してから実行します。

9. 必要なすべての追加オブジェクトについて、手順 3 から手順 8 を繰り返します。

10. サーバーを再起動します。57 ページの「Directory Proxy Server の再起動」を参照してください。

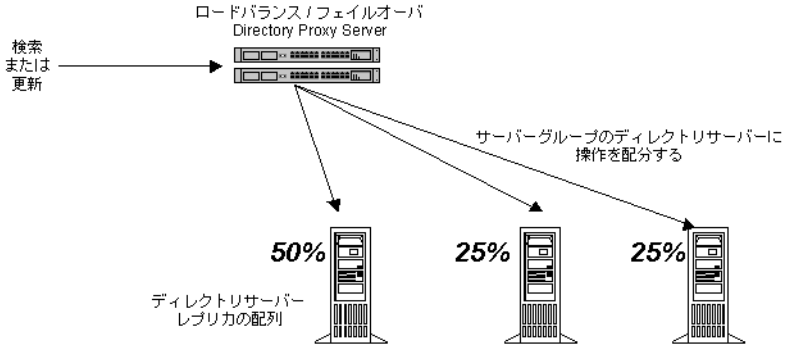
ロードバランスプロパティ

Directory Proxy Server は、レプリケートされた複数の LDAP ディレクトリサーバーの間でロードバランス、フェイルオーバー、フェイルバックを自動的に実行することで、ディレクトリ配備の高可用性を実現します。Directory Proxy Server でこの処理を行うには、Directory Proxy Server が管理するディレクトリサーバーを指定し、クライアントからの負荷をサーバー間でどのように分散するかを指定する必要があります。

Directory Proxy Server によるロードバランスを設定するには、ロードバランスプロパティを使用します。このプロパティにより、Directory Proxy Server が通信するバックエンドディレクトリサーバーを指定し、クライアントからの合計負荷の何パーセントを各ディレクトリサーバーに負担させるかを指定することができます。この設定を行うと、Directory Proxy Server は、この設定に定義されている負荷条件に合わせて、各ディレクトリサーバーにクライアントクエリを自動的に配分します。ディレクトリサーバーが使用不能になると、Directory Proxy Server はこのサーバーの受け持ち負荷を、残りのサーバーのそれぞれの受け持ち負荷の割合に基づいて再配分します。すべてのバックエンド LDAP サーバーが使用不能になると、Directory Proxy Server はクライアントからのクエリを拒否するようになります。

図 7-2 は、3 つのディレクトリサーバーレプリカ間でのクライアントロードの分散を示しています。

図 7-2　複数の LDAP ディレクトリレプリカ間でのロードバランス



Directory Proxy Server のロードバランスはセッションベースで行われます。つまり、クライアントからのクエリを担当させるディレクトリサーバーを選択する決定機能は、クライアントセッションごとに、特にクライアントセッションの開始時に適用されます。そのセッションの以後のすべてのクライアントクエリは、セッションの開始時に選択されたディレクトリサーバーに向けられます。

Directory Proxy Server が負荷を分散できるバックエンドディレクトリサーバーの数は、次のような要因によって異なります。

- Directory Proxy Server を稼動するホストのサイズ
- 利用できるネットワーク帯域幅
- Directory Proxy Server が受信するクエリミックス
- クライアントセッションの時間的な長さ
- Directory Proxy Server の設定

一般に、ほとんどのセッションの存続時間が短く、クエリがコンピュータ集約型である場合は、Directory Proxy Server がサポートできるディレクトリサーバーの数は少なくなります。コンピュータ集約型のクエリとは、属性名変更機能 (106 ページの「属性名変更プロパティ」を参照) が使用される場合のように、メッセージ全体の検査を必要とするクエリです。

ディレクトリサーバーが使用不能になったことを Directory Proxy Server が検出するのは、接続試行時に接続拒否が返された場合と、タイムアウトが生じた場合です。どちらもセッションの初期段階で発生し、そのセッションのための処理はまだ行われていないため、Directory Proxy Server は透過的に使用可能な別のサーバーがあれば、そのサーバーにフェイルオーバーします。接続試行時にタイムアウトが生じた場合は、クライアントは応答の取得まで長く待たされる可能性があります。Directory Proxy Server とバックエンドサーバーとの間の接続が急に失われた場合、Directory Proxy Server は進行中のすべての処理について、影響を受けるクライアントに `LDAP_BUSY` エラーを返します。続いて、Directory Proxy Server はそのクライアントセッションを別のディレクトリサーバーにフェイルオーバーします。

Directory Proxy Server がディレクトリ配備のシングルポイント障害となることがないように、少なくとも 2 つの Directory Proxy Server を使用し、その前段に IP 関連装置を構成することをお勧めします。詳細は、第 2 章「Sun ONE Directory Proxy Server の配備例」を参照してください。Directory Proxy Server をこのように配備できない場合は、M スイッチを使用することをお勧めします。このスイッチを使用することで、Directory Proxy Server はそれ自体を監視することができます。

Directory Proxy Server は、監視プロセスを使用してバックエンドサーバーを診断します。ロードバランスを使用する場合は、この機能は自動的に有効になります。Directory Proxy Server は、それぞれのバックエンドディレクトリサーバーに対して 10 秒おきに Root DSE の匿名検索を実行します。いずれかが使用不能になったり応答を返さない場合、Directory Proxy Server はロードバランスを適用中のサーバーセットからそのサーバーを外します。使用可能な状態に戻ると、このサーバーはセットに戻されます。監視機能を効率的に機能させるには『Directory Proxy Server Installation Guide』の第 2 章「Computer System Requirements」で説明している `idsktune</code>` ユーティリティの推奨事項に従って、Directory Proxy Server が稼動するホストを設定する必要があります。サーバーが、セキュリティ保護されたポートだけを使用できる場合、Directory Proxy Server はセキュリティ保護された状態で診断を試みます。

次に、Directory Proxy Server 設定エディタコンソールを使用して、ロードバランスプロパティのオブジェクトを作成する方法について説明します。

注	ロードバランスプロパティのオブジェクトには、少なくとも 1 つの LDAP サーバープロパティを指定し、負担割合の合計が 100% になるように設定する必要があります。指定していない場合、Directory Proxy Server は起動に失敗します。

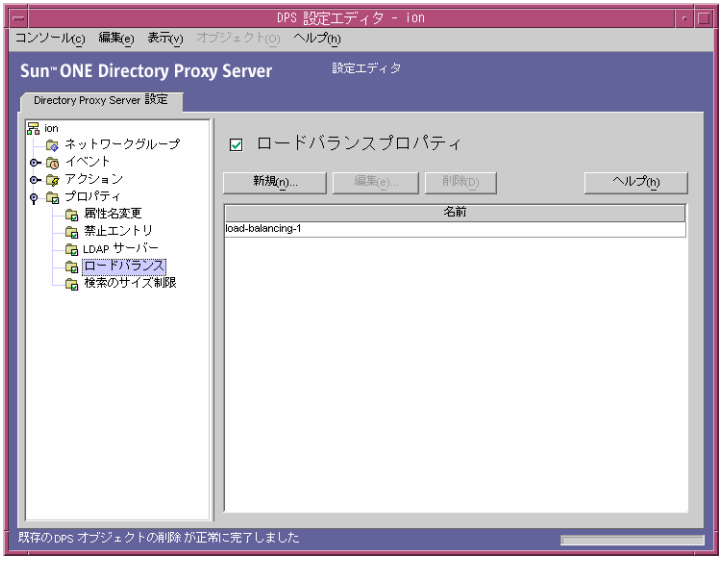
ロードバランスプロパティオブジェクトの作成

ここでは、Directory Proxy Server のロードバランスを設定する方法について説明します。ロードバランスプロパティのオブジェクトを作成する前に、Directory Proxy Server がクライアントロードの分散に使用する LDAP ディレクトリサーバーを指定してください。詳細は、114 ページの「LDAP サーバープロパティ」を参照してください。

複数のディレクトリサーバー間で Directory Proxy Server が負荷を分散する方法を定義するには、次の手順を実行します。

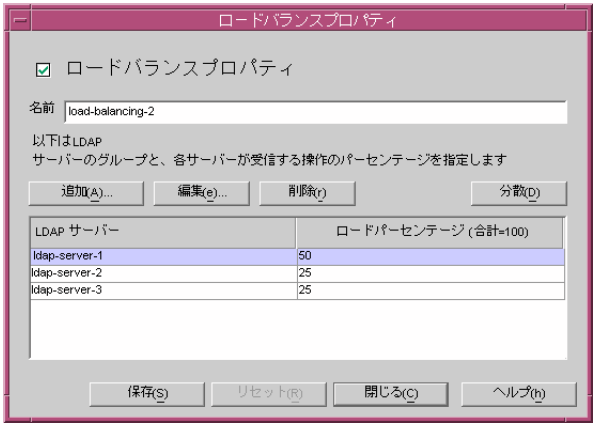
1. Directory Proxy Server 設定エディタコンソールにアクセスします。45 ページの「Directory Proxy Server コンソールへのアクセス」を参照してください。
2. ナビゲーションツリーで、「プロパティ」ノードを展開し、「ロードバランス」を選択します。

   ロードバランスプロパティの既存のオブジェクトが右のペインにリスト表示されます。



3. 「新規」をクリックします。

   「ロードバランスプロパティ」ウィンドウが表示されます。



4. 「名前」フィールドにプロパティオブジェクトの名前を入力します。この名前には、一意の英数文字列を指定する必要があります。
5. 適切な結果が得られるように、残りのフォーム要素を設定します。

割合を編集するときは、「LDAP サーバー」行の隣の「ロードのパーセンテージ」列に 0 ～ 100 の値を入力し、「適合」ボタンをクリックします。この操作によって、選択している行に指定のパーセントが割り当てられ、すべての割合の合計が 100% になるように計算されます。現在の合計パーセントは、「ロードのパーセンテージ」列の見出しに表示されます。

追加 : LDAP サーバープロパティへの参照を追加するためのダイアログを表示します。デフォルトでは、最初に追加されたサーバーに 100% の負荷が割り当てられ、その後に追加されたサーバーの負荷は 0% となります。

編集 : 現在選択されているテーブル内の項目を編集するためのダイアログを表示します。

削除 : 現在選択されている LDAP サーバーを、ロードバランスが実行されるサーバーのリストから削除します。

分散 : テーブル内で現在参照されているすべての LDAP サーバー間で負荷の割合を均等に分散します。

6. 「保存」をクリックして、オブジェクトを作成します。

   Directory Proxy Server の設定が変更され、この設定が適用されるサーバーを再起動するように促すメッセージが表示されます。この時点では、まだサーバーを再起動しません。再起動は、すべての設定変更が完了してから実行します。

7. 必要なすべての追加オブジェクトについて、手順 3 から手順 6 を繰り返します。
8. サーバーを再起動します。57 ページの「Directory Proxy Server の再起動」を参照してください。

検索のサイズ制限プロパティ

通常、LDAP ディレクトリは企業の中央リポジトリとして機能し、企業内の各所に配備された LDAP クライアントは情報を検索することができます。一般に、LDAP クライアントは検索フィルタを使用して特定の情報を検索することで、情報を検索しています。エントリを検索するときに、多くのクライアントはそのエントリのタイプに関連付けられている属性を指定しています。たとえば、人物のエントリを検索するときは、CN 属性を使用して特定の共通名を持つ人物を検索します。

Directory Proxy Server は数千の LDAP クライアント要求を処理することができ、LDAP ディレクトリに対する詳細なアクセス制御ポリシーを設定することができます。たとえば、ディレクトリ情報ツリー (DIT) の特定部分に対して特定の操作を実行できるユーザーを制御することができます。また、Web トローラやロボットがディレクトリ内の情報を収集するために実行する操作など、特定の種類の操作を許可しないように Directory Proxy Server を設定することもできます。

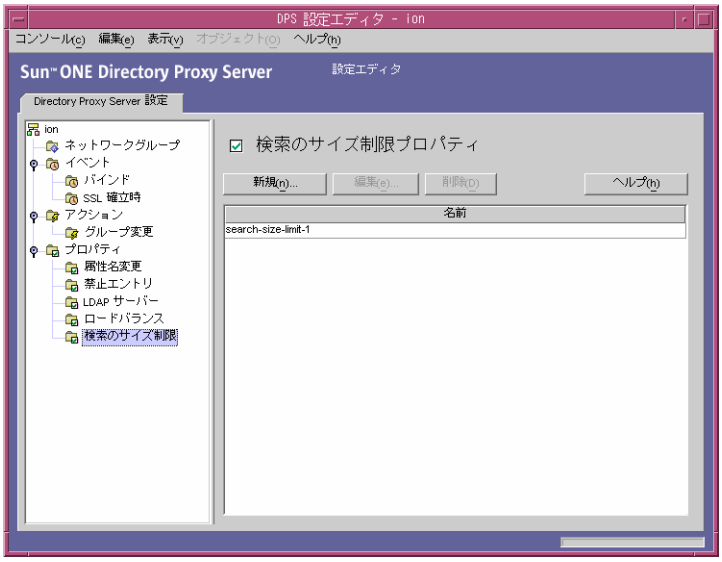
検索ベースと検索範囲に基づいて検索のサイズ制限を行うときは、検索のサイズ制限プロパティを使用します。実行する検索が、このプロパティオブジェクトのエントリに指定した検索ベースおよび検索範囲のどちらにも一致しない場合は、デフォルトのサイズ制限が適用されます。デフォルトのサイズ制限は、ネットワークグループオブジェクトエントリに指定されます。第 6 章「グループの作成と管理」を参照してください。

次に、Directory Proxy Server 設定エディタコンソールを使用して、検索のサイズ制限プロパティのオブジェクトを作成する方法について説明します。

検索のサイズ制限プロパティオブジェクトの作成

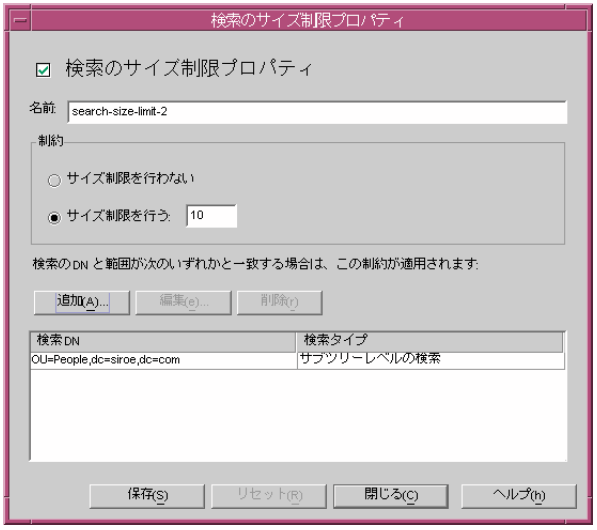
Directory Proxy Server が検索サイズを制限する方法を定義するには、次の手順を実行します。

1. Directory Proxy Server 設定エディタコンソールにアクセスします。45 ページの「Directory Proxy Server コンソールへのアクセス」を参照してください。
2. ナビゲーションツリーで、「プロパティ」ノードを展開し、「検索のサイズ制限」を選択します。



3. 「新規」をクリックします。

   「検索のサイズ制限プロパティ」ウィンドウが表示されます。



4. 「名前」フィールドにプロパティオブジェクトの名前を入力します。この名前には、一意の英数文字列を指定する必要があります。
5. 適切な結果が得られるように、残りのフォーム要素を設定します。

制約：サイズ制限の制約事項を適用するかどうかを指定します。

サイズ制限を行わない：サイズ制限を行わないことを指定する場合は、このオプションを選択します。

サイズ制限を行う：適用するサイズ制限を指定する場合は、このオプションを選択して、整数値を入力します。

追加：サイズ制限の条件を追加するためのメニューを表示します。「1 レベル検索」と「サブツリーレベルの検索」のいずれかのタイプを条件として指定します。

1 レベル検索：DN を入力して条件テーブルに追加するためのダイアログを表示します。1 レベル検索の検索ベースの DN が条件テーブルの 1 レベル検索に指定したいずれかの識別名と一致する場合は、指定したサイズ制限がその検索のサイズ制限として適用されます。

サブツリーレベルの検索：DN を入力するためのダイアログを表示します。サブツリー検索の検索ベースの DN が条件テーブルのサブツリーレベル検索に指定したいずれかの識別名と一致する場合は、指定したサイズ制限がその検索のサイズ制限として適用されます。

編集：現在選択されているテーブル内のエントリを編集するためのダイアログを表示します。

削除：現在選択されているテーブル内のエントリを削除します。

6. 「保存」をクリックして、オブジェクトを作成します。

   Directory Proxy Server の設定が変更され、この設定が適用されるサーバーを再起動するように促すメッセージが表示されます。この時点では、まだサーバーを再起動しません。再起動は、すべての設定変更が完了してから実行します。

7. 必要なすべての追加オブジェクトについて、手順 3 から手順 6 を繰り返します。

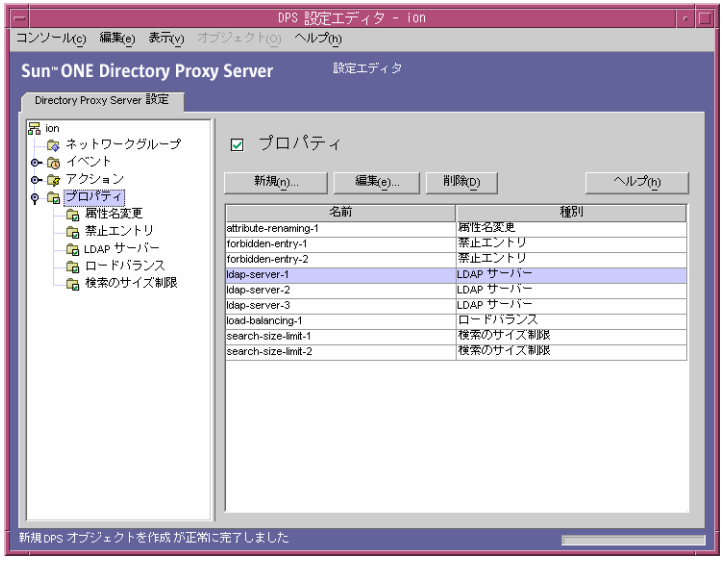
8. サーバーを再起動します。57 ページの「Directory Proxy Server の再起動」を参照してください。

プロパティオブジェクトの変更

プロパティオブジェクトを変更するには、次の手順を実行します。

1. Directory Proxy Server 設定エディタコンソールにアクセスします。45 ページの「Directory Proxy Server コンソールへのアクセス」を参照してください。
2. ナビゲーションツリーで、「プロパティ」ノードを選択します。

   既存のプロパティオブジェクトが右のペインにリスト表示されます。特定のプロパティに含まれるオブジェクトを表示するには、「プロパティ」ノードを展開し、適切なプロパティを選択します。



3. 変更するオブジェクトをリストから選択し、「編集」をクリックします。
4. 必要な修正を加えます。
5. 「保存」をクリックして、変更内容を保存します。

   Directory Proxy Server の設定が変更され、この設定が適用されるサーバーを再起動するように促すメッセージが表示されます。この時点では、まだサーバーを再起動しません。再起動は、すべての設定変更が完了してから実行します。
6. 変更が必要なすべてのオブジェクトについて、手順 3 から手順 5 を繰り返します。
7. サーバーを再起動します。57 ページの「Directory Proxy Server の再起動」を参照してください。

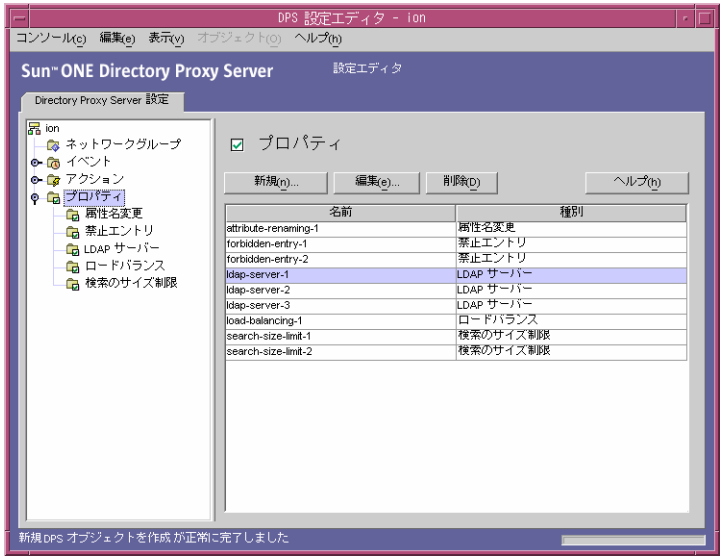
プロパティオブジェクトの削除

不要なプロパティオブジェクトは、Directory Proxy Server の設定から削除できます。オブジェクトを削除する前に、そのオブジェクトが別の設定エントリで使用されていないことを確認してください。

プロパティオブジェクトを削除するには、次の手順を実行します。

1. Directory Proxy Server 設定エディタコンソールにアクセスします。45 ページの「Directory Proxy Server コンソールへのアクセス」を参照してください。
2. ナビゲーションツリーで、「プロパティ」ノードを選択します。

   既存のプロパティオブジェクトが右のペインにリスト表示されます。特定のプロパティに含まれるオブジェクトを表示するには、「プロパティ」ノードを展開し、適切なプロパティを選択します。



3. 削除するオブジェクトをリストから選択し、「削除」をクリックします。
4. 処理を承認します。

   Directory Proxy Server の設定が変更され、この設定が適用されるサーバーを再起動するように促すメッセージが表示されます。この時点では、まだサーバーを再起動しません。再起動は、すべての設定変更が完了してから実行します。
5. 削除が必要なすべてのオブジェクトについて、手順 3 と手順 4 を繰り返します。
6. サーバーを再起動します。57 ページの「Directory Proxy Server の再起動」を参照してください。

第 8 章

イベントオブジェクトの作成と管理

Sun ONE Directory Proxy Server は、イベント駆動型のアクションをサポートしています。指定したイベントが発生したときに指定した処理を実行するように Directory Proxy Server を設定することができます。ここでは、Directory Proxy Server 設定エディタコンソールを使用してイベントオブジェクトを作成、管理する方法について説明します。

この章で説明する項目は、次のとおりです。

イベントの概要

イベントとは、稼動している Directory Proxy Server のある時点での特定の状態を意味します。イベントオブジェクトを使用して、事前に定義した状態が発生したときに Directory Proxy Server が評価する条件を指定します。イベントオブジェクトの定義の一部として、条件が満たされた場合に Directory Proxy Server が実行するアクションを指定することもできます。アクションについては、第 9 章「アクションオブジェクトの作成と管理」を参照してください。

現時点では、Directory Proxy Server は次の 2 種類のイベントを認識または追跡できます。

- OnBindSuccess イベント : このイベントは、クライアントがバインド操作を正常に完了したときに評価されます。

- SSL 確立時イベント : このイベントは、クライアントが SSL セッションを確立したときに評価されます。このイベントは条件に関連付けられることはなく、常にその一連の処理を実行します。

定義できるイベントオブジェクトは、この 2 つのイベントに基づくものだけです。たとえば、クライアントがバインドを正常に完了したことを検出するイベントオブジェクトを定義できます。この定義の一部として、イベントの発生時にそのクライアントのアクセスグループを変更するなどの特定アクションを指定できます。グループについては、第 6 章「グループの作成と管理」を参照してください。

イベントオブジェクトの作成

ここでは、OnBindSuccess イベントと SSL 確立時イベントに基づくイベントオブジェクトを作成する方法について説明します。これらのイベントについては、129 ページの「イベントの概要」を参照してください。

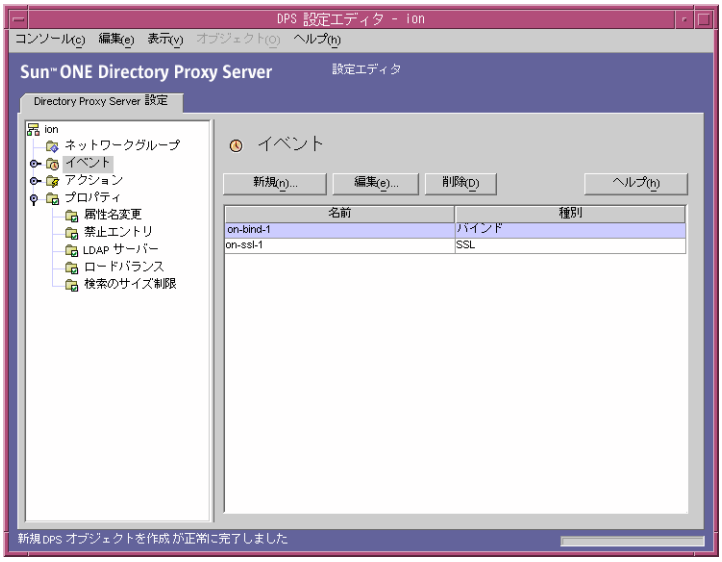
- OnBindSucess イベントオブジェクトの作成
- SSL 確立時イベントオブジェクトの作成

OnBindSucess イベントオブジェクトの作成

OnBindSuccess イベントに基づくイベントオブジェクトを作成するには、次の手順を実行します。

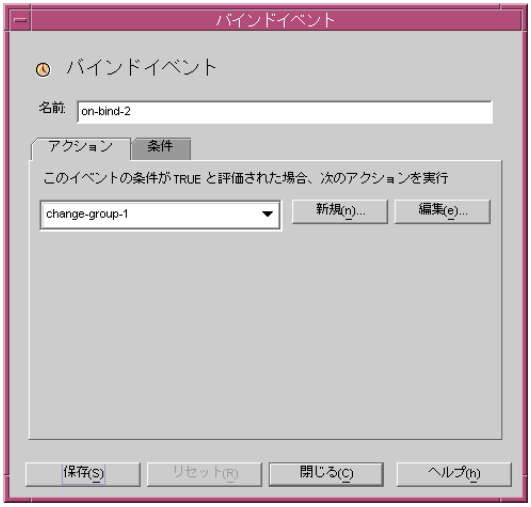
1. Directory Proxy Server 設定エディタコンソールにアクセスします。45 ページの「Directory Proxy Server コンソールへのアクセス」を参照してください。
2. ナビゲーションツリーで、「イベント」ノードを展開し、「バインド」を選択します。

   OnBindSuccess イベントに基づく既存のオブジェクトが右のペインにリスト表示されます。



3. 「新規」をクリックします。

   「バインドイベント」ウィンドウが表示されます。

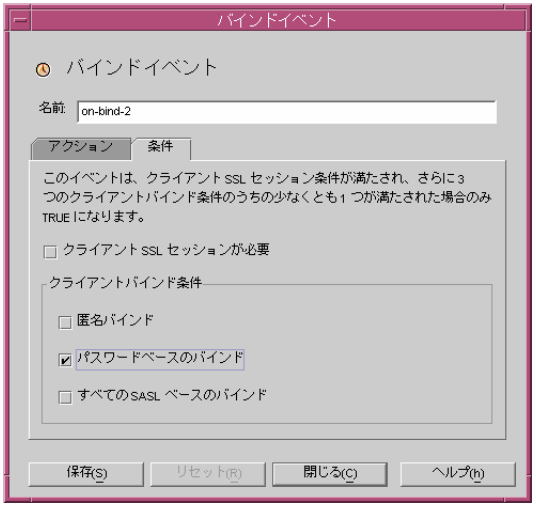


4. 「名前」フィールドにイベントオブジェクトの名前を入力します。この名前には、一意の英数文字列を指定する必要があります。
5. 「アクション」タブでは、イベント発生時 (イベントが TRUE と評価されたとき) に実行するアクションを選択します。

新規：「新規」ボタンをクリックして、新しいアクションオブジェクトを定義することもできます。

編集：「編集」ボタンをクリックして、現在選択しているアクションオブジェクトのパラメータを変更することができます。

6. 「条件」タブをクリックして、条件を指定します。



イベントは、指定した条件を満たした場合にだけ TRUE と評価されます。つまり、「アクション」タブで指定したアクションを実行するには、このタブに指定した条件が TRUE と評価される必要があります。これらの条件が TRUE になるのは、クライアントの SSL セッション条件が満たされ、かつ 3 つのクライアントバインド条件のうちの 1 つ以上が満たされた場合に限られます。

クライアント SSL セッションが必要：このオプションを選択すると、クライアントが Directory Proxy Server との SSL セッションを確立した場合にのみ条件が TRUE と評価されます。デフォルトは FALSE です。

クライアントバインド条件：条件は、「匿名バインド」、「パスワードベースのバインド」、「すべての SASL ベースのバインド」のいずれかです。

匿名バインド：このオプションを選択すると、クライアントの SSL セッション要件が満たされ、クライアントが匿名バインドを正常に完了した場合にのみ条件が TRUE と評価されます。

パスワードベースのバインド：このオプションを選択すると、クライアントの SSL セッション要件が満たされ、クライアントがパスワードベースのバインドを正常に完了した場合にのみ条件が TRUE と評価されます。

すべての SASL ベースのバインド: このオプションを選択すると、クライアントの SSL セッション要件が満たされ、クライアントが SASL メカニズムを使用したバインドを正常に完了した場合にのみ条件が TRUE と評価されます。

7. 「保存」をクリックして、イベントオブジェクトを作成します。

   Directory Proxy Server の設定が変更され、この設定が適用されるサーバーを再起動するように促すメッセージが表示されます。この時点では、まだサーバーを再起動しません。再起動は、すべての設定変更が完了してから実行します。

8. 必要なすべての追加オブジェクトについて、手順 3 から手順 7 を繰り返します。

9. サーバーを再起動します。57 ページの「Directory Proxy Server の再起動」を参照してください。

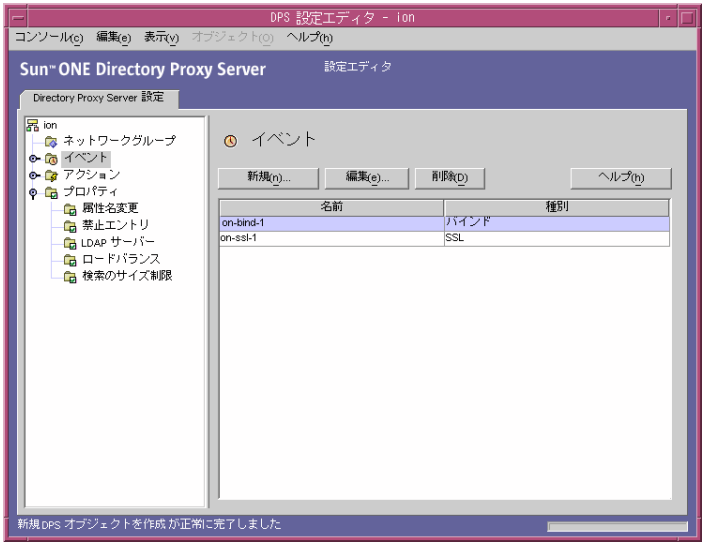
SSL 確立時イベントオブジェクトの作成

SSL 確立時イベントに基づくイベントオブジェクトを作成するには、次の手順を実行します。

1. Directory Proxy Server 設定エディタコンソールにアクセスします。45 ページの「Directory Proxy Server コンソールへのアクセス」を参照してください。

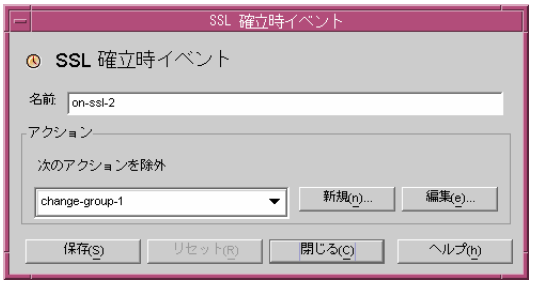
2. ナビゲーションツリーで、「イベント」ノードを展開し、「SSL 確立時」を選択します。

   SSL 確立時イベントに基づく既存のオブジェクトが右のペインにリスト表示されます。



3. 「新規」をクリックします。

   「SSL 確立時イベント」ウィンドウが表示されます。



4. 「名前」フィールドにイベントオブジェクトの名前を入力します。この名前には、一意の英数文字列を指定する必要があります。

5. 「アクション」セクションでは、イベント発生時 (イベントが TRUE と評価されたとき) に実行するアクションを選択します。

   「編集」ボタンをクリックして、現在選択しているアクションのパラメータを変更することができます。「新規」ボタンをクリックして、新しいアクションを定義することもできます。

6. 「保存」をクリックして、イベントオブジェクトを作成します。

   Directory Proxy Server の設定が変更され、この設定が適用されるサーバーを再起動するように促すメッセージが表示されます。この時点では、まだサーバーを再起動しません。再起動は、すべての設定変更が完了してから実行します。

7. 必要なすべての追加オブジェクトについて、手順 3 から手順 6 を繰り返します。

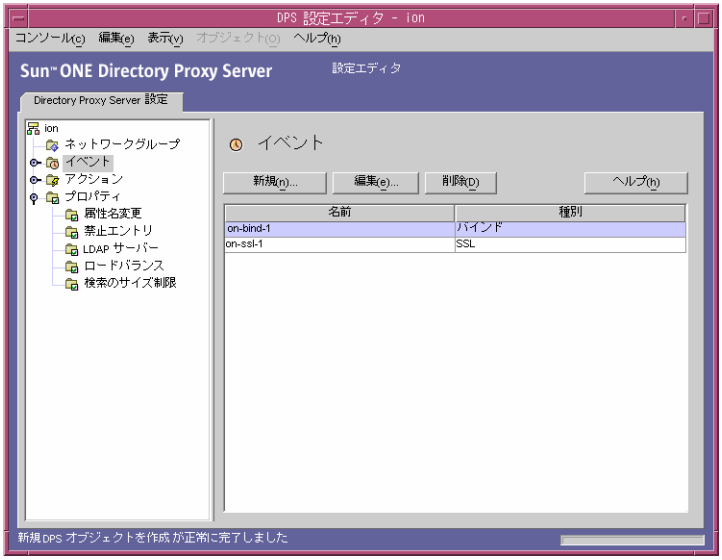
8. サーバーを再起動します。57 ページの「Directory Proxy Server の再起動」を参照してください。

イベントオブジェクトの変更

イベントオブジェクトを変更するには、次の手順を実行します。

1. Directory Proxy Server 設定エディタコンソールにアクセスします。45 ページの「Directory Proxy Server コンソールへのアクセス」を参照してください。
2. ナビゲーションツリーで、「イベント」を選択します。

   既存のイベントオブジェクトが右のペインにリスト表示されます。特定のイベントタイプに含まれるオブジェクトを表示するには、「イベント」ノードを展開し、適切なイベントタイプを選択します。



3. 変更するイベントオブジェクトをリストから選択し、「編集」をクリックします。
4. 必要な修正を加えます。
5. 「保存」をクリックして、変更内容を保存します。

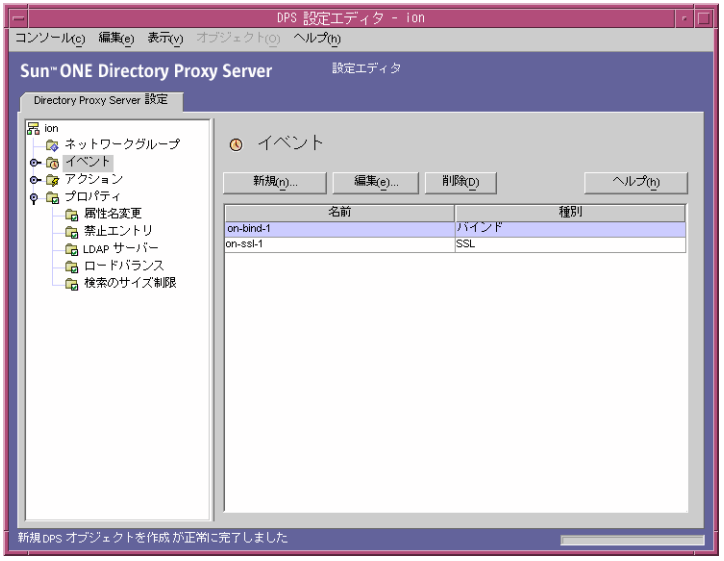
   Directory Proxy Server の設定が変更され、この設定が適用されるサーバーを再起動するように促すメッセージが表示されます。この時点では、まだサーバーを再起動しません。再起動は、すべての設定変更が完了してから実行します。
6. 変更が必要なすべてのオブジェクトについて、手順 3 から手順 5 を繰り返します。
7. サーバーを再起動します。57 ページの「Directory Proxy Server の再起動」を参照してください。

イベントオブジェクトの削除

不要なイベントオブジェクトは、Directory Proxy Server の設定から削除できます。イベントオブジェクトを削除するには、次の手順を実行します。

1. Directory Proxy Server 設定エディタコンソールにアクセスします。45 ページの「Directory Proxy Server コンソールへのアクセス」を参照してください。
2. ナビゲーションツリーで、「イベント」ノードを選択します。

   既存のイベントオブジェクトが右のペインにリスト表示されます。特定のイベントタイプに含まれるオブジェクトを表示するには、「イベント」ノードを展開し、適切なイベントタイプを選択します。



3. 削除するイベントオブジェクトをリストから選択し、「削除」をクリックします。
4. 確認メッセージが表示されたら、処理を承認します。

   削除したイベントオブジェクトの名前は、リストに表示されなくなります。Directory Proxy Server の設定が変更され、この設定が適用されるサーバーを再起動するように促すメッセージが表示されます。この時点では、まだサーバーを再起動しません。再起動は、すべての設定変更が完了してから実行します。
5. 削除が必要なすべてのオブジェクトについて、手順 3 と手順 4 を繰り返します。
6. サーバーを再起動します。57 ページの「Directory Proxy Server の再起動」を参照してください。

第 9 章

アクションオブジェクトの作成と管理

Sun ONE Directory Proxy Server は、イベント駆動型のアクションをサポートしています。指定したイベントが発生したときに指定した処理を実行するように Directory Proxy Server を設定することができます。ここでは、Directory Proxy Server 設定エディタコンソールを使用してアクションオブジェクトを作成、管理する方法について説明します。

この章で説明する項目は、次のとおりです。

アクションの概要

アクションは、Directory Proxy Server が実行するタスクです。イベントオブジェクトに定義されている規則または条件が `TRUE` と評価された場合に Directory Proxy Server が実行するアクションを指定するには、アクションオブジェクトを使用します。指定した状態が発生した場合に Directory Proxy Server が評価する条件を指定するには、イベントオブジェクトを使用します。イベントについては、第 8 章「イベントオブジェクトの作成と管理」を参照してください。

現時点では、Directory Proxy Server が実行できるアクションは `ChangeGroup` だけです。このアクションを使用することで、規則の評価に基づいて、クライアントのアクセスグループを別のグループに変更するように Directory Proxy Server を設定できます。グループについては、第 6 章「グループの作成と管理」を参照してください。

グループ変更機能は、LDAP ディレクトリに遠隔ユーザー (別の IP アドレスから、または物理的に離れた場所からディレクトリに接続するユーザーなど) に関する情報が含まれている場合に特に便利です。遠隔ユーザーがダイナミックな IP アドレスを使って Directory Proxy Server に接続し、デフォルトのアクセスグループに入るように Directory Proxy Server を設定できます。デフォルトのアクセスグループには、遠隔ユーザーが指定する信用情報が認証された場合にだけ TRUE と評価される、`OnBindSuccess` イベントに基づく規則を適用します。この規則には、遠隔ユーザーのアクセスグループを「デフォルト」から通常のグループ (スタティックな IP アドレスで Directory Proxy Server にアクセスした場合にその遠隔ユーザーが割り当てられるグループ) に変更する `ChangeGroup` アクションも設定します。

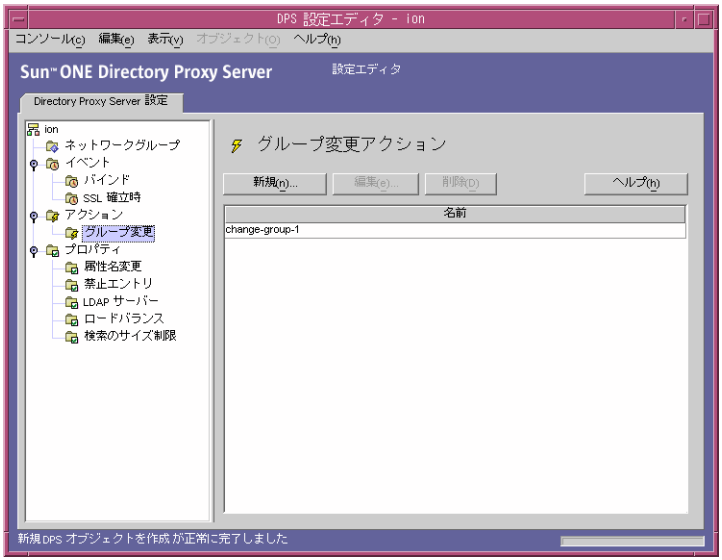
アクションオブジェクトの作成

特定のイベントが発生したときに実行するアクションのオブジェクトを作成できます。次に、グループ変更のアクションオブジェクトを作成する方法について説明します。

クライアントのグループを別のグループに変更するアクションオブジェクトを作成するには、次の手順を実行します。

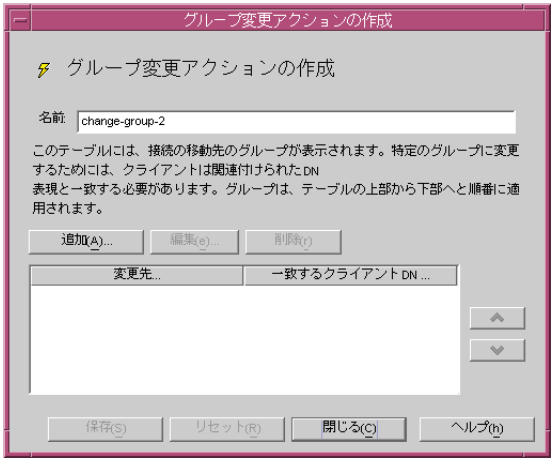
1. Directory Proxy Server 設定エディタコンソールにアクセスします。45 ページの「Directory Proxy Server コンソールへのアクセス」を参照してください。
2. ナビゲーションツリーで、「アクション」ノードを展開し、「グループ変更」を選択します。

   既存のアクションオブジェクトが右のペインにリスト表示されます。



3. 「新規」をクリックします。

   「グループ変更アクションの作成」ウィンドウが表示されます。



4. 「名前」フィールドには、オブジェクト名を入力します。この名前には、一意の英数文字列を指定する必要があります。

5. 「アクション」タブでは、イベント発生時 (イベントが TRUE と評価されたとき) に実行するアクションを選択します。

変更先 ...：クライアントが変更できるグループのリストを表示します。変更を行うには、クライアントは各グループに関連付けられた DN 式に一致する必要があります。特定のグループまたは変更なしエントリに関連付けられた DN 式を編集するには、テーブル内の「クライアント DN が一致する場合 ...」列をクリックします。DN 式が一致するまで、リストの上から下へ評価が行われます。したがって、すべての式が評価されるように、最も一般的な DN 式がリストの一番下にあることが重要です。

正規表現は標準化する必要があります。RDN コンポーネントと等号 (=) の間には空白文字を挿入せず、すべての属性名と値は大文字で表記します。

正規表現については、次の書籍が参考になります。『Mastering Regular Expressions』、Friedl および Oram 著、O'Reilly 発行、ISBN: 1565922573

追加：クライアント接続が変更する可能性のあるグループを追加するためのメニューを表示します。グループ変更エントリには、「グループ変更のエントリ」または「変更なしのエントリ」の各タイプを指定できます。

グループ変更のエントリ：関連付けられた DN 式が TRUE と評価されるかどうかによってクライアントが変更するネットワークグループを選択するためのダイアログを表示します。

変更なしのエントリ：関連付けられた DN 式が TRUE と評価された場合に何も変更しないことを示す行をテーブルに追加します。これは、グループ変更リストの評価を省略する場合に便利です。

編集：現在選択されているテーブル内のエントリを編集するためのダイアログを表示します。

削除：現在選択されているテーブル内のエントリを削除します。

6. 「保存」をクリックして、アクションオブジェクトを作成します。

   Directory Proxy Server の設定が変更され、この設定が適用されるサーバーを再起動するように促すメッセージが表示されます。この時点では、まだサーバーを再起動しません。再起動は、すべての設定変更が完了してから実行します。

7. 必要なすべての追加オブジェクトについて、手順 3 から手順 6 を繰り返します。

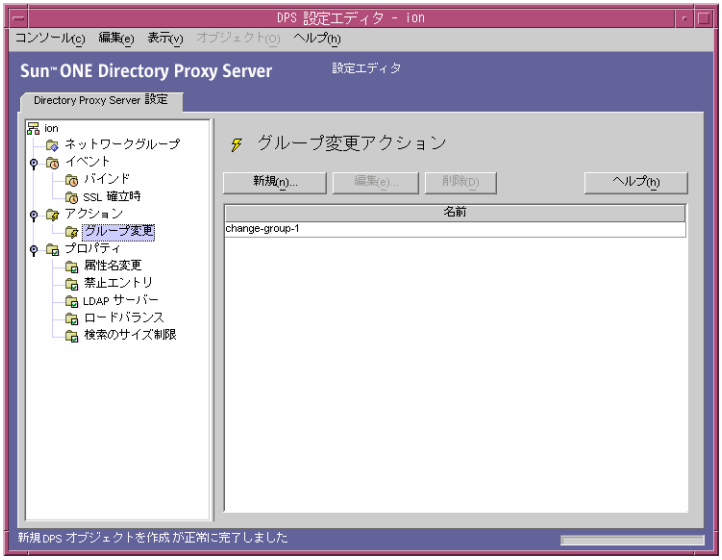
8. サーバーを再起動します。57 ページの「Directory Proxy Server の再起動」を参照してください。

アクションオブジェクトの変更

アクションオブジェクトを変更するには、次の手順を実行します。

1. Directory Proxy Server 設定エディタコンソールにアクセスします。45 ページの「Directory Proxy Server コンソールへのアクセス」を参照してください。
2. ナビゲーションツリーで、「アクション」を選択します。

   既存のアクションオブジェクトが右のペインにリスト表示されます。



3. 変更するアクションオブジェクトをリストから選択し、「編集」をクリックします。
4. 必要な修正を加えます。
5. 「保存」をクリックして、変更内容を保存します。

   Directory Proxy Server の設定が変更され、この設定が適用されるサーバーを再起動するように促すメッセージが表示されます。この時点では、まだサーバーを再起動しません。再起動は、すべての設定変更が完了してから実行します。
6. 変更が必要なすべてのオブジェクトについて、手順 3 から手順 5 を繰り返します。
7. サーバーを再起動します。57 ページの「Directory Proxy Server の再起動」を参照してください。

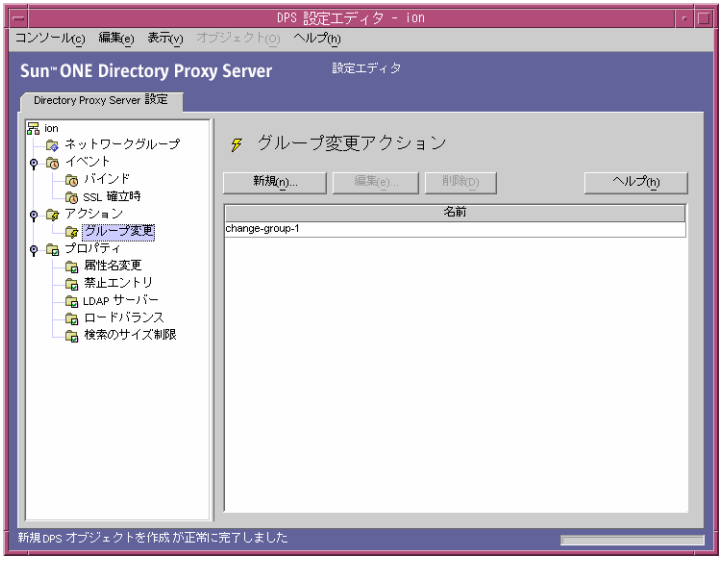
アクションオブジェクトの削除

不要なアクションオブジェクトは、Directory Proxy Server の設定から削除できます。アクションオブジェクトを削除する前に、そのオブジェクトがどのイベントオブジェクトでも使用されていないことを確認してください。

アクションオブジェクトを削除するには、次の手順を実行します。

1. Directory Proxy Server 設定エディタコンソールにアクセスします。45 ページの「Directory Proxy Server コンソールへのアクセス」を参照してください。
2. ナビゲーションツリーで、「アクション」を選択します。

   既存のアクションオブジェクトが右のペインにリスト表示されます。



3. 削除するアクションをリストから選択し、「削除」をクリックします。
4. 処理を承認します。

   削除したオブジェクトの名前は、リストに表示されなくなります。Directory Proxy Server の設定が変更され、この設定が適用されるサーバーを再起動するように促すメッセージが表示されます。この時点では、まだサーバーを再起動しません。再起動は、すべての設定変更が完了してから実行します。
5. 削除が必要なすべてのオブジェクトについて、手順 3 と手順 4 を繰り返します。
6. サーバーを再起動します。57 ページの「Directory Proxy Server の再起動」を参照してください。

第 10 章

ログの設定と監視

この章では、エントリまたはメッセージをログに記録するように Sun ONE Directory Proxy Server を設定し、記録したエントリを Directory Proxy Server コンソールに表示してアクティビティを監視する方法について説明します。

この章で説明する項目は、次のとおりです。

ログの概要

Directory Proxy Server では、次の 2 種類のログを維持できます。

- システムログ
- 監査ログ

次に、それぞれの詳細について説明します。

システムログ

Directory Proxy Server は、システムの監視やデバッグを行えるように、各種のイベントやシステムエラーの膨大なログの記録を管理することができます。ログの記録はすべてテキストファイルで管理し、簡単に検索できるようにローカルファイルシステムに格納することができます。デフォルトでは、Directory Proxy Server はログエントリを次のファイルに書き込みます。

```
<server-root>/dps-<hostname>/logs/fwd.log
```

ログファイルの各メッセージには、タイムスタンプが記されます。また、Directory Proxy Server に返されるプロセス番号とメッセージ番号も記録されます。

識別とフィルタリングのために、Directory Proxy Server が記録するイベントはさまざまなカテゴリに分類されます。表 10-1 を参照してください。各カテゴリは、性質が同じまたは似ているメッセージ、または特定の機能領域に属するメッセージを示します。設定によっては、1 つまたは複数のカテゴリに該当するエントリを記録することができます。

Directory Proxy Server の設定では、各メッセージカテゴリは、特定のログレベルに対応します。ログレベルとは、サーバーがログを記録するレベルのことで、どれだけ詳細に記録するかを決定します。

- 重要度が高いレベルでは、高い重要度のイベントだけが記録されるため、詳細度は低くなります。
- 重要度が低いレベルでは、より多くの種類のイベントがログファイルに記録されるため、詳細度は高くなります。

表 10-1 は、メッセージのカテゴリを重要度の高い順に示しています。`Critical` は重要度が最大で、`Detailed trace` は重要度が最低となります。

表 10-1 ログレベル

ログレベルまたは重要度	説明
Mandatory	Mandatory メッセージは、ログに常に書き込まれるメッセージです。これらのメッセージは、Directory Proxy Server が読み取る設定を示し、起動時の Directory Proxy Server のバージョン番号などが含まれます。 このレベルのメッセージは設定を変更できません。
Critical	Directory Proxy Server がすぐに対処する必要がある問題を検出したことを示すメッセージを記録します。たとえば、*Directory Proxy Server process 1234 has exited, attempting restart in 10 seconds* などです。
Exception	Directory Proxy Server が間違った形式の LDAP メッセージをクライアントまたはサーバーから受信した場合など、予期しないエラー状態を示すメッセージを記録します。たとえば、*Could not decode search request* などです。
Warning	Directory Proxy Server では無視できるが、管理者による調査が必要なエラー状態を示すメッセージを記録します。たとえば、*Local host name lookup failed. System default group may not function correctly* などです。
Notice	情報を提供するメッセージを記録します。たとえば、*Received NULL continuation reference from server. Discarding..* などです。

表 10-1　ログレベル (続き)

ログレベルまたは重要度	説明
Trace	デバッグメッセージを記録します。たとえば、*Result received from server lderr =32, matched=o=sun.com, errtxt=no such object* などです。Trace メッセージにはプロトコルダンプが含まれます。Trace レベルを指定すると、ログファイルのサイズが急速に拡大します。
Detailed trace	接続を再利用するために要求された匿名バインドなどの詳細なデバッグ情報を提供するメッセージを記録します。通常、これらのメッセージは Directory Proxy Server の技術チームやサポートチームに役立ちます。

Directory Proxy Server では、ログに記録する情報の量を指定できます。ログレベルを指定することで、イベントの重要度に基づいてログエントリをフィルタリングできます。デフォルトのログレベルは `Warning` です。

注　より詳細なログレベルにはそれより下のレベルがすべて含まれます。つまり、`Warning` をログレベルとして選択すると、`Warning`、`Exception`、`Critical` レベルのメッセージが記録されます。ログデータは膨大な量になることがあります。ログレベルが低い (詳細な) 場合は特にそうです。ホストコンピュータにすべてのログファイルを格納できるだけの十分なディスク容量があることを確認してください。

オプションとして、Windows 以外のプラットフォームでは、ログファイルではなく、`syslog` デーモンにログメッセージを出力するように Directory Proxy Server を設定することができます。ログファイルと `syslog` デーモンの両方に同時にログメッセージを出力することはできません。このように設定する場合は、`syslogd` が適切に設定されていることを確認してください。たとえば、`/var/adm/messages` というファイルにすべてのメッセージを記録するには、`/etc/syslog.conf` ファイルに次の行を追加します。

```
daemon.crit;daemon.warning;daemon.info;daemon.debug
/var/adm/messages
```

Directory Proxy Server は、`crit`、`warning`、`info`、`debug` という重要度 (ログレベル) を示す `daemon` のファシリティを使用します。syslog イベントと Directory Proxy Server イベントの対応については、表 10-1 を参照してください。

表 10-2　ログレベルのマッピング

Directory Proxy Server イベント	syslog イベント
Mandatory	info
Critical	crit
Exception	err
Warning	warning
Notice	info
Trace	info
Detailed trace	info

Directory Proxy Server ログのローテーション、およびその他のログ機能の制御には、次のオブジェクトクラスを使用します。

`ids-proxy-sch-LogProperty`

このオブジェクトクラスの説明と使用方法については、191 ページの「dpsconfig2ldif」を参照してください。

監査ログ

Directory Proxy Server は、システムメッセージやエラーメッセージを記録するほかに、すべてのイベントや接続の統計の監査トレールも管理することができます。たとえば、LDAP ディレクトリとのバインドまたはバインド解除が終了したばかりのクライアントの DN を記録することができます。

デフォルトでは、Directory Proxy Server は監査メッセージを記録するように設定されていません。この機能はいつでも有効にすることができます。また、システムログのエントリと同じファイルに監査メッセージを記録するか、別のファイルに記録するかを指定できます。別のファイルへの書き込みを設定しない限り、監査メッセージはその他のログメッセージとともにシステムログのエントリと同じファイルに書き込まれます。詳細は、143 ページの「システムログ」を参照してください。

注　監査記録を参照することで、未認証のアクセスやアクティビティを検出することができます。この機能を有効化することをお勧めします。また、セキュリティ対策として、異常なアクティビティについて Directory Proxy Server 監査ログを定期的に調べる必要があります。

ログの設定

Directory Proxy Server がエントリをログに記録するように設定するには、次の手順を実行します。

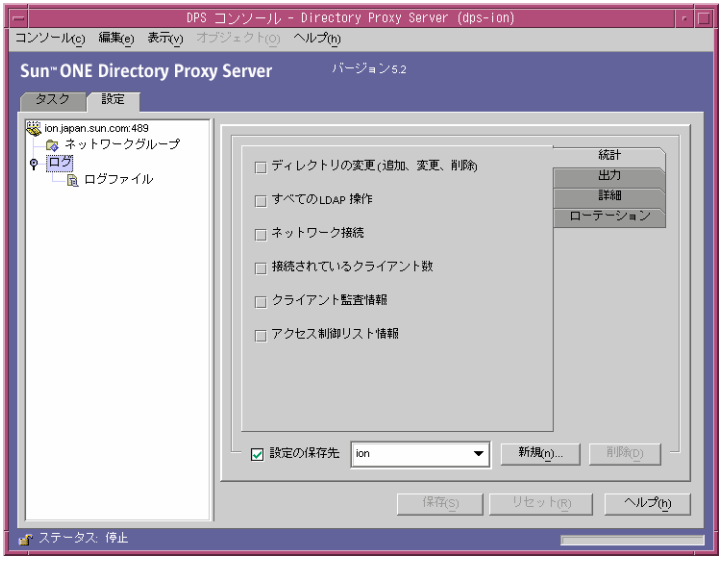
- 手順 1: ログ設定の定義
- 手順 2: 使用するロギングプロパティの指定

手順 1: ログ設定の定義

この設定が必要なのは、ロギングプロパティのオブジェクトを作成または定義する場合だけです。ロギングプロパティのオブジェクトがすでに作成されており、それを使用する場合は次の手順に進んでください。

1. Directory Proxy Server コンソールにアクセスします。45 ページの「Directory Proxy Server コンソールへのアクセス」を参照してください。
2. 「設定」タブを選び、ナビゲーションツリーで「ログ」を展開します。

   ロギングプロパティの既存のオブジェクトが右のペインにリスト表示されます。



3. 「新規」をクリックして新しいオブジェクトを定義します。

   「ログプロパティ」ウィンドウの「統計」タブが有効になります。

4. 「名前」フィールドには、オブジェクト名を入力します。この名前には、一意の英数文字列を指定する必要があります。

5. 「統計」タブでは、ログに記録する情報の種類を指定します。

   必要なログメッセージの種類を示すボックスにチェックマークを付けます。デフォルトでは、どのオプションも選択されていません。ログメッセージは、「ディレクトリの変更」、「すべての LDAP 操作」、「ネットワーク接続」、「接続されているクライアント数」、および「クライアント監査情報」の各グループに分類されます。

   ディレクトリの変更 : ディレクトリへの書き込みを行う操作 (追加、変更、削除など) に関する統計情報が記録されます。

   すべての LDAP 操作 : すべての LDAP 操作に関する統計情報が記録されます。

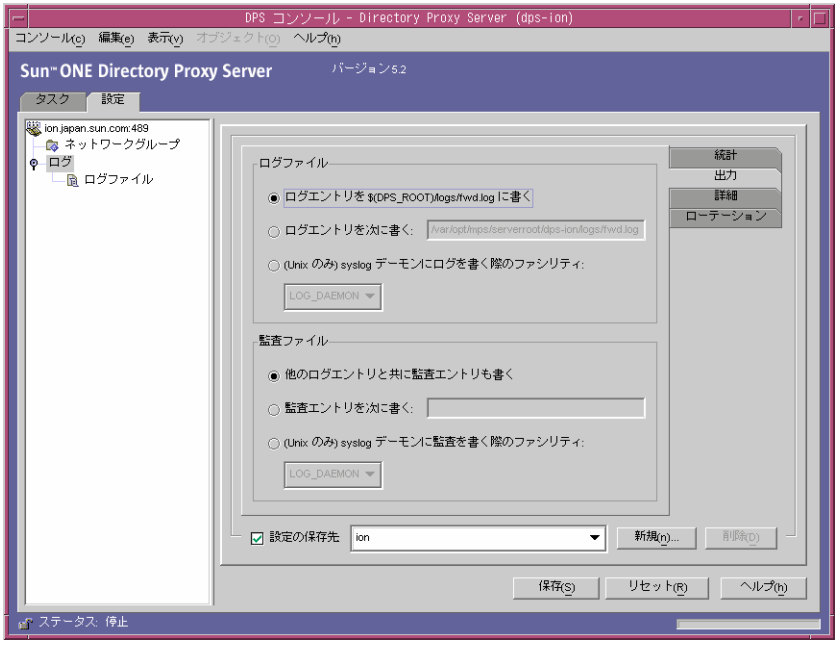
   ネットワーク接続 : ネットワークの接続に関する統計情報が記録されます。

   接続されているクライアント数 : 接続されているクライアントの数などの一般的な統計情報が記録されます。

   クライアント監査情報 : バインドまたはバインド解除が完了したばかりのクライアントの DN などの監査情報が記録されます。

   アクセス制御リスト情報 : ここには、情報を記録する権限を持つユーザーのリストが表示されます。

6. 「出力」タブを選択し、ログエントリの出力先と、ログ監査追跡をログに記録するかどうかを指定します。



ログファイル: Directory Proxy Server がそのログエントリを書き込む場所を管理するオプションを示します。

ログエントリを $(DPS_ROOT)/logs/fwd.log に書く：これはデフォルトの設定であり、Directory Proxy Server はそのログエントリを `$(dps_ROOT)/logs/fwd.log` ファイルに書き込みます。この `$(dps_ROOT)` は、Directory Proxy Server がインストールされているサーバールートの下にあるディレクトリで、通常は `/usr/sunone/servers/dps-<hostname>` または `¥Program Files¥sunone¥Servers¥dps-<hostname>` です。

ログエントリを次に書く: Directory Proxy Server がそのログエントリを書き込むファイルを指定します。ファイル区切り文字は、プラットフォームに関係なく、UNIX 規則に準拠している必要があります。

(Unix のみ) syslog デーモンにログを書く際のファシリティ：Directory Proxy Server がエントリを記録する時に使用するファシリティコードを選択します。この設定は、UNIX コンピュータにインストールした Directory Proxy Server がこのログプロパティを使用する場合にだけ選択する必要があります。Windows システムにインストールした Directory Proxy Server にこのオプションを指定すると、Directory Proxy Server は動作しなくなります。この属性の値を指定する場合は、Windows と UNIX のログプロパティを別々に作成する必要があります。

監査ファイル: Directory Proxy Server がその監査ログエントリを書き込む場所を管理するオプションを示します。この機能を使用するには、「統計」タブの「クライアント監査情報」オプションを選択して、監査ログを有効にする必要があります。

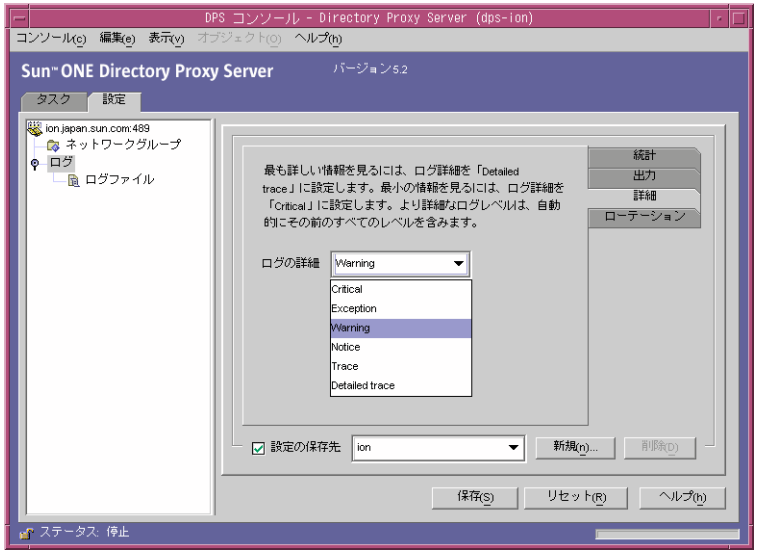
他のログエントリと共に監査エントリも書く：これはデフォルトの設定です。Directory Proxy Server はその監査ログエントリを上記のログファイル設定と同じ出力先に書き込みます。

ログエントリを次に書く: Directory Proxy Server がその監査ログエントリを書き込むファイルを指定します。ファイル区切り文字は、プラットフォームに関係なく、UNIX 規則に準拠している必要があります。

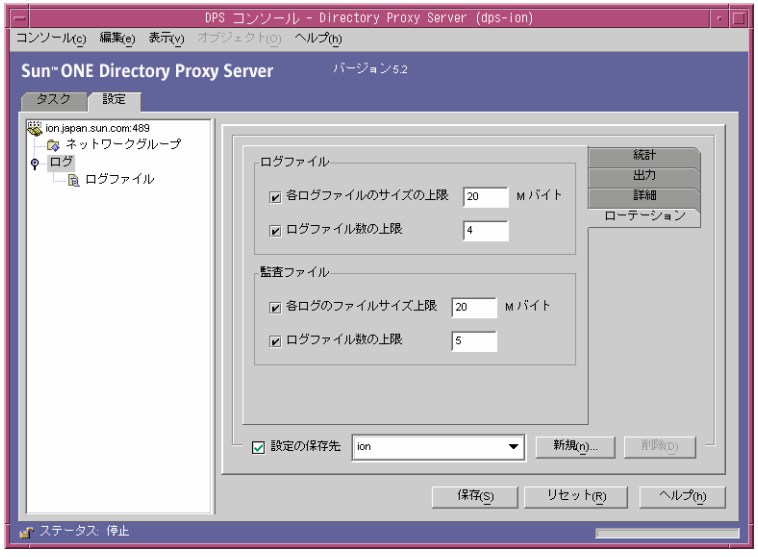
(Unix のみ) syslog デーモンに監査を書く際のファシリティ Directory Proxy Server が監査ログエントリを記録する時に使用するファシリティコードを選択します。この設定は、UNIX コンピュータにインストールした Directory Proxy Server がこのログプロパティを使用する場合にだけ選択する必要があります。このオプションを指定すると、Windows ベースの Directory Proxy Server は動作しなくなります。この属性の値を指定する場合は、Windows と UNIX のログプロパティオブジェクトを別々に作成する必要があります。

7. 「詳細」タブを選択し、ログレベル (ログの適切な詳細度) を指定します。

   ドロップダウンメニューからログレベルを選択します。



8. 「ローテーション」タブを選択し、ログのサイズとローテーションを設定します。



ログファイル : Directory Proxy Server のログファイルのサイズや最大数を制限するオプションを示します。

各ログファイルのサイズの上限 : 各ログファイルの最大サイズ (M バイト) を入力します。

ログファイル数の上限：作成およびローテーションするログファイルの最大数を入力します。

監査ファイル：Directory Proxy Server の監査ファイルのサイズや最大数を制限するオプションを示します。

各ログのファイルサイズ上限：各監査ファイルの最大サイズ (M バイト) を入力します。

ログファイル数の上限：作成およびローテーションする監査ログファイルの最大数を入力します。

9. 「保存」をクリックして、変更内容を保存します。

   オブジェクト名がリストに表示されるようになります。Directory Proxy Server の設定は変更され、サーバーの再起動を促すメッセージが表示されます。

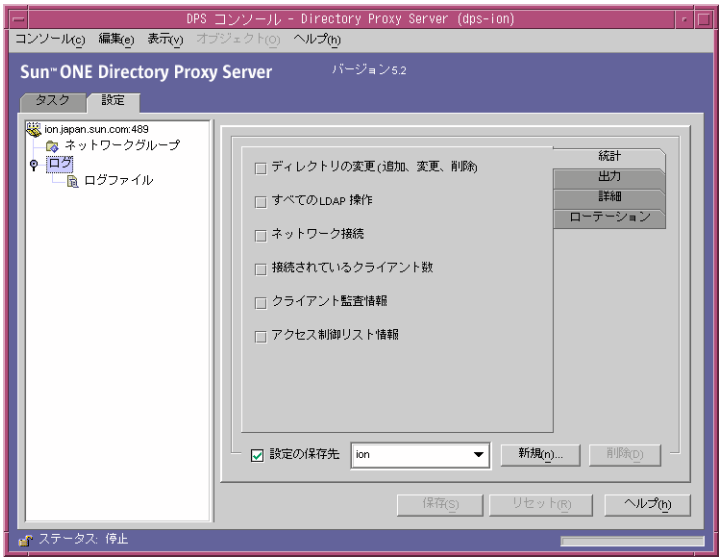
10. サーバーを再起動します。57 ページの「Directory Proxy Server の再起動」を参照してください。

手順 2: 使用するロギングプロパティの指定

この手順では、メッセージをログに記録するときに適用する、既存のログプロパティを選択します。

1. Directory Proxy Server コンソールにアクセスします。45 ページの「Directory Proxy Server コンソールへのアクセス」を参照してください。
2. 「設定」タブを選び、ナビゲーションツリーで「ログ」を選択します。

   現在のシステムプロパティによって指定されているログプロパティに関する情報が右のペインに表示されます。



3. 「設定の保存先」ドロップダウンリストから、適用するプロパティを選択します。
4. 「保存」をクリックして、変更内容を保存します。

   Directory Proxy Server は、設定に定義されている条件でメッセージをログに記録するように設定されます。Directory Proxy Server の設定は変更され、サーバーの再起動を促すメッセージが表示されます。
5. 「タスク」タブを選択し、サーバーを再起動します。57 ページの「Directory Proxy Server の再起動」を参照してください。

Directory Proxy Server コンソールによるログの監視

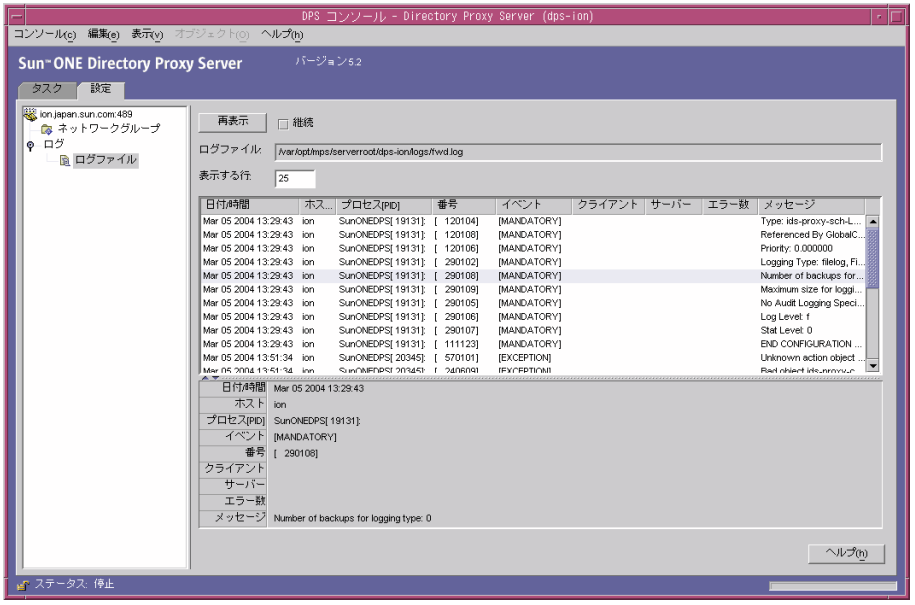
メッセージをログに記録するように Directory Proxy Server を設定すると (147 ページの「ログの設定」を参照)、ログメッセージを参照してアクティビティを監視できるようになります。たとえば、トラブルシューティングが必要な問題が Directory Proxy Server で発生した場合に、サーバーがログに記録したエラーメッセージや情報メッセージが役立つことがあります。また、ログファイルを調べることで、Directory Proxy Server の動作についてさまざまな事項を確認することができます。

Directory Proxy Server コンソールには、ログファイルの内容を確認するためのシンプルな機能が用意されています。確認用に選択したログファイルの内容は、テーブル形式で表示されます。ログテーブルは上下に分割され、上のペインにはログレコードが表形式で表示され、下のペインには選択しているレコードの詳細が表示されます。各ログレコードには、メッセージを記録した日時、メッセージの重要度、そのログの一般的な説明などの情報が含まれます。

ログファイルを開いて表示した後に、表示するレコードまたはエントリの数を指定して、ファイルの内容を部分的に参照することができます。次に、ファイルに記録されたログレコードを表示する方法について説明します。

1. Directory Proxy Server コンソールにアクセスします。45 ページの「Directory Proxy Server コンソールへのアクセス」を参照してください。
2. 「設定」タブを選び、ナビゲーションツリーで「ログ」を展開します。
3. 「ログファイル」を選択します。

   ファイルに記録されるエントリのオプションが右のペインに表示されます。現在のログプロパティに指定されているログファイルであれば、どれでも選択できます。Directory Proxy Server では、設定に応じてログ情報と監査情報を別のファイルに記録できます。



各要素の説明は、次のとおりです。

再表示：ログを読み込み、下のテーブルにレコードを表示します。

継続：この設定を選択すると、この表示を継続的に更新して、最新のログレコードを表示することができます。

ログファイル：現在表示されているファイルの名前を表示します。

表示する行：ログファイルから読み込む最大行数を指定します。

第 11 章

セキュリティの設定

Sun ONE Directory Proxy Server は、クライアントとバックエンドディレクトリサーバーの間での通信をセキュリティ保護するために、SSL/TLS をサポートしています。この章では、次の内容について説明します。

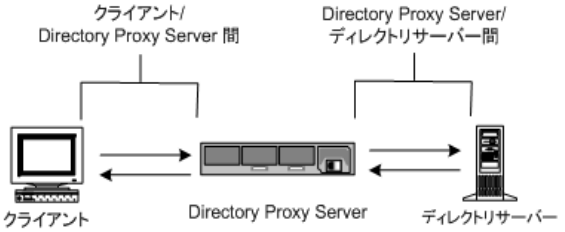
- SSL と TLS の設定準備
- SSL 通信の設定

ここで提供する一部の情報は、公開鍵暗号化方式と SSL (Secure Sockets Layer) プロトコルの概念に習熟し、イントラネット、エクストラネット、インターネットのセキュリティと企業内のデジタル証明書の役割を理解していることを前提に記述されています。これらの概念に初めて接する方は、『Managing Servers with Sun ONE Console』でセキュリティに関連する付録を参照することをお勧めします。

iDAR 5.0x からアップグレードする場合は、『Directory Proxy Server Installation Guide』で SSL 設定の移行手順を参照してください。

Directory Proxy Server には、設定可能な 2 つの異なる通信リンクがあります。各通信リンクは、プレーンテキストを利用するだけでなく、TLS (Transport Layer Security) プロトコルまたは SSL (Secure Sockets Layer) プロトコルによって暗号化することもできます。2 つの独立した通信リンクを利用できるので、LDAP クライアントと Directory Proxy Server の間、および Directory Proxy Server と LDAP ディレクトリの間で TLS または SSL が有効な通信を設定することができます。図 11-1 は、Directory Proxy Server の対応能力を示しています。

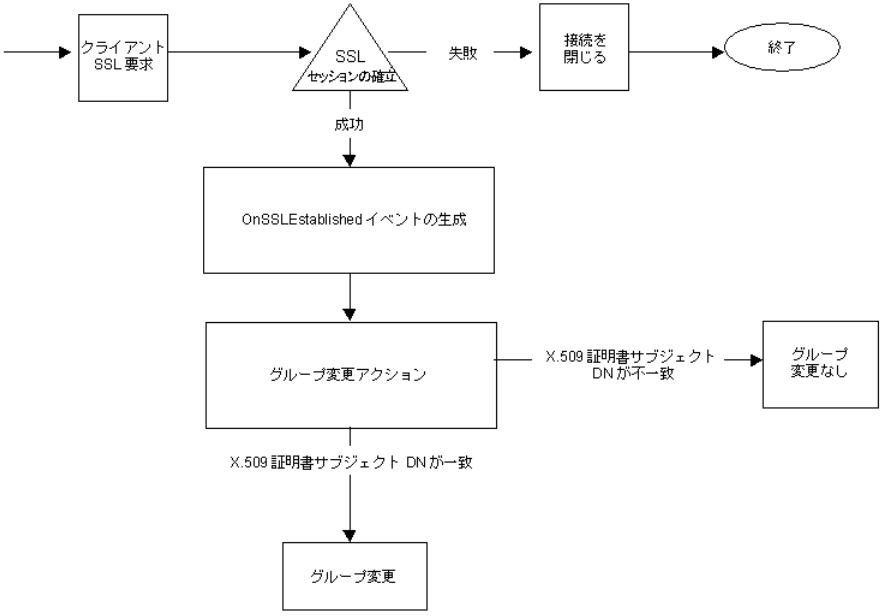
図 11-1　Directory Proxy Server の 2 つの独立した通信リンク



検証される証明書のルート CA 証明書がインストールされ、Directory Proxy Server がそれを利用できる場合、Directory Proxy Server はクライアントとサーバーの両方の証明書を検証できます。

図 11-2 は、クライアントとの SSL セッションの確立後にクライアントから提示された証明書を Directory Proxy Server がどのように検証するかを示しています。

図 11-2　証明書に基づくクライアントの認証



SSL と TLS の設定準備

SSL と TLS の設定は、内部セキュリティデバイスを使用するか、外部ハードウェアデバイスを使用するか、または両方を使用するかによって異なります。ここでは、その方法について説明します。

内部セキュリティデバイスを使用する場合の SSL または TLS の設定

内部セキュリティデバイスを使用する場合に SSL または TLS を設定するには、証明書を要求し、それをインストールする必要があります。証明書を要求するときは、証明書リクエストウィザードを使用します。証明書をインストールするときは、証明書インストールウィザードを使用します。プロンプトが表示されるので、内部セキュリティデバイスに証明書をインストールすることを指定します。

外部セキュリティデバイスを使用する場合の SSL または TLS の設定

FORTEZZA などの外部セキュリティデバイスを使用する場合に SSL を設定するときは、まず、外部デバイスに付属する PKCS #11 モジュールをインストールします。次に、証明書リクエストウィザードを実行し、プロンプトが表示されたら外部セキュリティデバイスを指定します。

内部と外部のセキュリティデバイスを使用する場合の SSL の設定

企業によっては、サーバーとクライアントで内部セキュリティデバイスだけを使用しますが、内部と外部、両方のセキュリティデバイスを使用する企業もあります。サーバーが内部と外部のセキュリティデバイスを両方とも実行する製品と通信する場合は、証明書リクエストウィザードを 2 回実行します。最初の実行では、プロンプトが表示されたときに内部セキュリティデバイスを指定します。2 回目の実行では、プロンプトが表示されたときに外部セキュリティデバイスを指定します。

SSL 通信の設定

一般に、Directory Proxy Server での SSL 対応通信の設定では、次の手順で行われます。

- 手順 1: Directory Proxy Server のサーバー証明書のインストール
- 手順 2: Directory Proxy Server とクライアントの間の SSL 接続の設定
- 手順 3: Directory Proxy Server と LDAP サーバーの間の SSL 接続の設定

手順 1: Directory Proxy Server のサーバー証明書のインストール

証明書を要求し、それをインストールするときは、2 つのウィザードを使用します。新しいサーバー証明書を要求する、またはすでに使用している証明書を更新するときは、証明書リクエストウィザードを使用します。認証局 (CA) から受け取った証明書をインストールするときは、証明書インストールウィザードを使用します。証明書リクエストウィザードを初めて使用するときは、鍵と証明書のデータベースも作成およびインストールされます。

Directory Proxy Server のサーバー証明書をインストールするには、次の手順を実行します。

- 手順 A: サーバー証明書要求の作成
- 手順 B: サーバー証明書要求の送信
- 手順 C: 証明書のインストール
- 手順 D: CA 証明書またはサーバー証明書チェーンのインストール
- 手順 E: 証明書データベースのバックアップと復元

SSL 証明書

Sun ONE Directory Proxy Server では、サーバー証明書、サーバー証明書チェーン、信頼された CA 証明書という 3 種類の証明書をインストールできます。

サーバー証明書は、そのサーバーだけに関連付けられる 1 つの証明書です。これは、クライアントがこのサーバーを識別するための証明書です。この証明書を CA に要求する必要があります。サーバー証明書を取得してインストールするには、要求を作成して CA に送信します。次に、その証明書をインストールします。

サーバー証明書チェーンは、企業の社内証明書サーバーまたは既知の CA によって自動的に生成される証明書の集合です。チェーンに含まれる証明書は、元の CA にまで遡ることができ、識別情報が裏付けられます。この裏付けは、新しいサーバー証明書を取得またはインストールするたびに必要となります。

信頼された CA 証明書は、企業の社内証明書サーバーまたは既知の CA によって自動的に生成される 1 つの証明書です。信頼された CA 証明書は、クライアントの認証に使用されます。

信頼された CA 証明書を取得するには、まず、社内証明書サーバーまたは CA の Web サイトにアクセスします。必要な証明書情報をコピーしてファイルとして保存します。次に、証明書インストールウィザードを使用してその証明書をインストールします。

サーバーにインストールできる SSL 証明書の数には制限はありません。Directory Server のインスタンスで SSL を設定するには、少なくともサーバー証明書と信頼された CA 証明書をインストールする必要があります。

手順 A: サーバー証明書要求の作成

Sun ONE Directory Proxy Server を使用して、認証局 (CA) に送信する証明書要求を作成できます。

1. Sun ONE Directory Proxy Server のナビゲーションツリーで、SSL 暗号化を適用するサーバーインスタンスを選択します。
2. サーバーインスタンスをダブルクリックするか、「開く」をクリックして、そのサーバーインスタンスの管理ウィンドウを表示します。
3. 「コンソール」メニューから、「セキュリティ」>「証明書の管理」を選択します。

   「証明書の管理」タスクをクリックすることもできます。

   セキュリティデバイスがパスワードを持たない場合、パスワードの入力を促すメッセージが表示されます。
4. 「要求」をクリックして「証明書リクエストウィザード」を開きます。
5. 「手動で証明書を要求」を選択し、「次へ」をクリックします。

6. 次の情報を入力します。

   サーバー名 : (省略可) 証明書を要求するマシンの完全修飾ホスト名を入力します。

   組織 : (省略可) 組織の名前を入力します。

   組織単位 : (省略可) 部門、部署などの組織単位を入力します。

   都市 / 地域 : (省略可) 組織単位が存在する都市または地域を入力します。

   都道府県 : (省略可) 組織単位が存在する都道府県を入力します。

   国 / 地域 : (省略可) 組織単位が存在する国または地域をドロップダウンメニューから選択します。

   次のボタンを使用して、要求の表示形式を切り替えることができます。

   DN を表示 : クリックすると、識別名 (DN) の形式で要求者情報が表示されます。このボタンは、フィールドに情報を入力する場合にだけ表示されます。

   フィールドの表示 : クリックすると、要求者情報がフィールドに表示されます。このボタンは、情報を DN 形式で入力する場合にだけ表示されます。

7. 「次へ」をクリックします。

8. この証明書を格納するセキュリティデバイスのパスワードを入力します。

   内部 (ソフトウェア) セキュリティデバイスを使用している場合は、鍵と証明書のデータベースのパスワードを入力します。外部 (ハードウェア) モジュールを使用している場合は、SmartCard などのセキュリティデバイスのパスワードを入力します。

9. 「次へ」をクリックします。

10. 次のどちらかを選択します。

    クリップボードにコピー : クリックすると、証明書要求がクリップボードにコピーされます。

    ファイルに保存 : クリックすると、要求がテキストファイルとして保存されます。ファイルの名前と場所を選択するためのダイアログボックスが表示されます。

11. 「終了」をクリックして、証明書リクエストウィザードを終了します。

手順 B: サーバー証明書要求の送信

サーバー証明書要求を作成したら、それを CA に送信します。多くの CA では、Web サイトで証明書要求を受け付けています。要求を含む電子メールメッセージの送信を必要とする CA もあります。

1. 電子メールプログラムを使用して、新しい電子メールメッセージを作成します。

2. 証明書要求をメッセージとして貼り付けます。

   証明書要求をファイルとして保存した場合は、そのファイルをテキストエディタで開きます。要求をコピーし、メッセージの本文として貼り付けます。

   証明書要求をクリップボードにコピーした場合は、それをメッセージの本文として貼り付けます。

3. 件名と要求の受信者を入力します。件名と受信者のタイプは、利用する CA によって異なります。詳細は、CA の Web サイトを参照してください。

4. このメッセージを電子メールで CA に送ります。

要求を送信したら、CA から証明書が送られてくるまで待ちます。応答時間は CA によって大きく異なります。社内 CA がある場合は、1 ～ 2 日で証明書を受け取れます。外部の CA を利用する場合は、CA が要求に応じるまでに数週間かかることもあります。

手順 C: 証明書のインストール

証明書を電子メールメッセージとして受け取るか、CA の Web サイトで受け取るかは、CA によって異なります。証明書を入手したら、バックアップをとってインストールします。

1. CA から受け取った証明書データをテキストファイルとして保存します。

   これにより、証明書データを失っても、このバックアップファイルから証明書を再インストールできます。

2. Sun ONE Directory Proxy Server のナビゲーションツリーで、証明書をインストールするサーバーインスタンスを選択します。

3. 「開く」をクリックして、そのサーバーインスタンスの管理ウィンドウを開きます。

4. 「タスク」タブで、「証明書の管理」タスクボタンをクリックします。

   「コンソール」メニューから「セキュリティ」>「証明書の管理」を選択することもできます。

5. 「サーバー証明書」タブを選択します。

6. この証明書の格納先を指定します。

   - この証明書を内部セキュリティデバイスに格納する場合は、「セキュリティデバイス」ドロップダウンリストから内部 (ソフトウェア) を選択し、「インストール」をクリックします。
   - この証明書を外部ハードウェアデバイスに格納する場合は、「セキュリティデバイス」ドロップダウンリストからデバイスを選択し、「インストール」をクリックします。

7. 証明書の場所を指定するか、その内容を入力します。

   このローカルファイル内：証明書がシステム上のテキストファイルとして保存されているときは、そのファイルへの完全パスを入力します。

   次の符号化されたテキストブロック中：証明書をクリップボードにコピーしたときは、「クリップボードから貼り付け」ボタンをクリックして、証明書の内容をテキストフィールドに貼り付けます。

8. 「次へ」をクリックします。

   入力した証明書情報が有効であれば、証明書の詳細を示すページが表示されます。

9. 証明書情報が正しいことを確認し、「次へ」をクリックします。

10. 証明書名を入力し、「次へ」をクリックします。

11. この証明書を格納するセキュリティデバイスのパスワードを入力します。

    証明書を内部 (ソフトウェア) セキュリティデバイスにインストールする場合は、鍵と証明書のデータベースのパスワードを入力します。証明書を外部 (ハードウェア) セキュリティデバイスにインストールする場合は、そのデバイスのパスワードを入力します。

12. 「終了」をクリックします。

手順 D: CA 証明書またはサーバー証明書チェーンのインストール

1. CA から CA 証明書またはサーバー証明書チェーンを取得します。
2. Sun ONE Directory Proxy Server のナビゲーションツリーで、CA 証明書をインストールするサーバーインスタンスを選択します。
3. 「開く」をクリックして、そのサーバーインスタンスの管理ウィンドウを開きます。
4. 「タスク」タブで、「証明書の管理」タスクボタンをクリックします。

   「コンソール」メニューから「セキュリティ」> 「証明書の管理」を選択することもできます。

5. 「CA 証明書」タブを選択し、「インストール」をクリックします。
6. 証明書の場所を指定するか、その内容を入力します。

   このローカルファイル内：証明書がシステム上のテキストファイルとして保存されているときは、そのファイルへの完全パスを入力します。

   次の符号化されたテキストブロック中：証明書をクリップボードにコピーしたときは、「クリップボードから貼り付け」ボタンをクリックして、証明書の内容をテキストフィールドに貼り付けます。

7. 「次へ」をクリックします。

   入力した証明書情報が有効であれば、証明書の詳細を示すページが表示されます。

8. 証明書情報が正しいことを確認し、「次へ」をクリックします。

9. 証明書名を入力し、「次へ」をクリックします。

10. この証明書の信頼オプションを選択します。

    クライアントからの接続を受け入れる：この CA が発行するクライアント証明書を信頼するときは、このボックスにチェックマークを付けます。

    ほかのサーバーに接続する：この CA が発行するサーバー証明書を信頼するときは、このボックスにチェックマークを付けます。

11. 「終了」をクリックします。

手順 E: 証明書データベースのバックアップと復元

証明書をインストールするときは、証明書データベースのバックアップをその都度行う必要があります。データベースが破損した場合でも、このバックアップから証明書情報を復元することができます。

証明書データベースのバックアップ

1. サーバールートフォルダを開きます。

2. `alias` フォルダに含まれるすべてのファイルを別の場所 (可能であれば別のディスク) にコピーします。

   このフォルダには、証明書だけでなく、信頼データベースの公開鍵も保存されています。

バックアップからの証明書データベースの復元

- バックアップしたファイルを、サーバールートフォルダ内の `alias` サブフォルダにコピーします。

警告 証明書データベースをバックアップから復元した場合、バックアップ後にインストールしたすべての証明書は失われます。再インストールが必要な場合は、証明書データベースを復元する前に、すべての証明書のコピーが存在することを確認してください。

手順 2: Directory Proxy Server とクライアントの間の SSL 接続の設定

Directory Proxy Server と LDAP クライアントの間の SSL 接続を設定するときは、次の手順を実行します。

- 手順 A: クライアントの信頼データベースへの Directory Proxy Server CA 証明書の追加
- 手順 B: Directory Proxy Server のシステム設定の変更
- 手順 C: Directory Proxy Server ネットワークグループの変更

手順 A: クライアントの信頼データベースへの Directory Proxy Server CA 証明書の追加

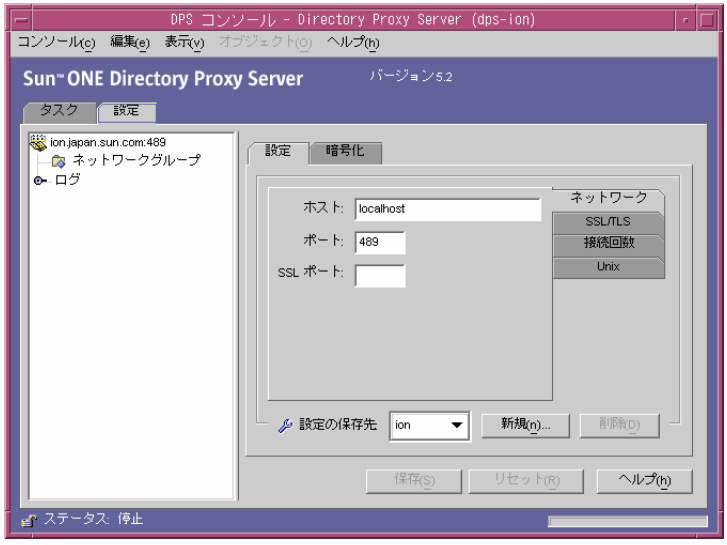
注 この手順が必要となるのは、クライアントがサーバー証明書を検証する場合だけです。Netscape と Sun のすべてのクライアントは検証を行います。しかし、検証を行わないクライアントもあります。その場合は、信頼データベースの設定は不要です。

Directory Proxy Server が証明書を LDAP クライアントに提示すると、クライアントはその証明書の有効性を検証しようとします。クライアントは、この検証プロセスの一部として、証明書を発行した CA がクライアントによって信頼されているかどうかを確認します。このため、Directory Proxy Server のサーバー証明書を発行した CA のルート証明書がクライアントの信頼データベースにインストールされている必要があります。

Directory Proxy Server のサーバー証明書をインストールする最後の手順で、Directory Proxy Server の証明書をテキストファイルとして保存しました。クライアントアプリケーションのマニュアルを参照し、信頼データベースに CA 証明書をインストールします。

手順 B: Directory Proxy Server のシステム設定の変更

Directory Proxy Server コンソールの「設定」タブと「暗号化」タブでは、SSL 対応通信の条件を Directory Proxy Server に定義することができます。詳細は、65 ページの「システム設定インスタンスの作成」を参照してください。



適切なシステム設定インスタンスに次の変更を加え、変更内容を保存します。

- 「設定」タブの「SSL ポート」フィールドに値を指定します。Directory Proxy Server は、指定した番号のポートで LDAPS (LDAP over SSL) 接続を待機します。デフォルトでは、Directory Proxy Server は LDAPS クライアントからの接続を待機しません。TLS/SSL 接続の確立に代替ポート 636 を使用するクライアントからの LDAPS 接続を有効にするには、この値を指定する必要があります。この値は、「ポート」フィールドの値とは異なる必要があります。(このオプションでは、「暗号化」タブの TLS/SSL 設定も必要です。)

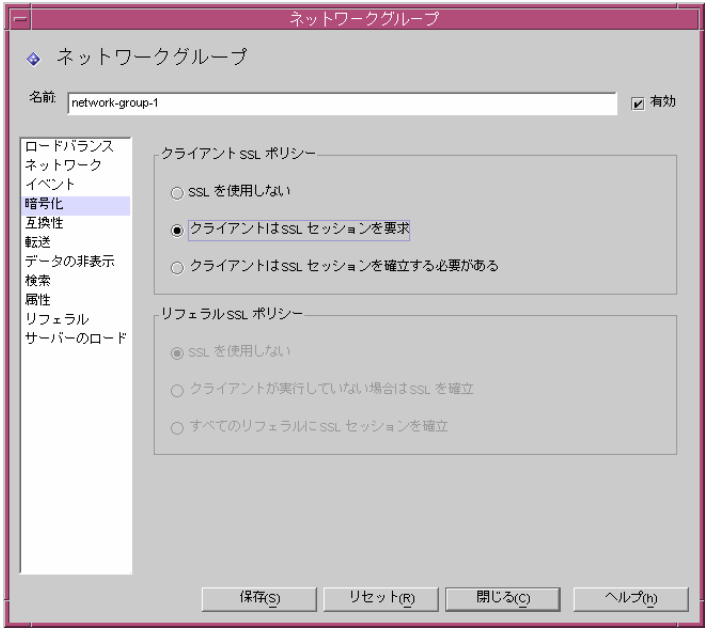
  パラメータの説明を参照するときは、「ヘルプ」ボタンをクリックします。

- SSL/TLS の「暗号化」タブで、必要なすべての情報を指定します。

  パラメータの説明を参照するときは、「ヘルプ」ボタンをクリックします。

手順 C: Directory Proxy Server ネットワークグループの変更

Directory Proxy Server は、ネットワークグループを使用してクライアントを識別し、LDAP ディレクトリ内の情報に対するアクセス権を決定しています。詳細は、第 6 章「グループの作成と管理」を参照してください。



すでに設定されている各グループについて、「暗号化」タブで適切なオプションを指定します。LDAP 操作を送信する前にクライアントが TLS セッションを開始するように強制する、TLS セッションを利用するかどうかの判断をクライアントに任せる、またはクライアントによる TLS セッションの開始を許可しないように指定できます。たとえば、「SSL は利用可能です」と「クライアントは SSL セッションを確立する必要がある」の 2 つのオプションの有効化が必要になるかもしれません。「暗号化」タブのオプションについては、第 6 章「グループの作成と管理」の 84 ページに記載されている手順 9 を参照してください。

リフェラルの実行が有効な場合は、「リフェラル SSL ポリシー」も指定します。リフェラルの実行を有効にするには、ウィンドウの左側のリストで「リフェラル」を選択します。

Directory Proxy Server は、バックエンドサーバーから返されるリフェラルを実行できます。返される LDAP URL は、RFC 2255 形式である必要があります。ホストポートが指定されていない場合、クライアントは、接続する適切な LDAP サーバーについて何らかの情報を持っている必要があります。

Directory Proxy Server は、ホストまたはポート番号が指定されていない LDAP URL を、そのリフェラルの送信元と同じホストへのリフェラルであると解釈します。次の例を参照してください。

`ldap:///dc=central,dc=sun,dc=com`	同一ホスト、ベースが異なるポートへのリフェラル
`ldap://:10389/`	同一ホスト、別ポートへのリフェラル
`ldap://host/`	「host」というホスト、デフォルトポート (389) へのリフェラル

手順 3: Directory Proxy Server と LDAP サーバーの間の SSL 接続の設定

Directory Proxy Server と LDAP サーバーの間の SSL 接続を設定するときは、次の手順を実行します。

- 手順 A: CA 証明書またはサーバー証明書チェーンのインストール
- 手順 B: LDAP サーバーの信頼データベースへの Directory Proxy Server CA 証明書の追加
- 手順 C: LDAP サーバープロパティの変更

手順 A: CA 証明書またはサーバー証明書チェーンのインストール

この手順が必要になるのは、LDAP サーバーが提示する証明書を Directory Proxy Server に検証させる場合だけです。詳細は、162 ページの「手順 D: CA 証明書またはサーバー証明書チェーンのインストール」を参照してください。

手順 B: LDAP サーバーの信頼データベースへの Directory Proxy Server CA 証明書の追加

Directory Proxy Server が証明書を LDAP サーバーに提示すると、サーバーはその証明書の有効性を検証しようとします。サーバーは、この検証プロセスの一部として、Directory Proxy Server の証明書を発行した CA がサーバーによって信頼されているかどうかを確認します。このため、Directory Proxy Server のサーバー証明書を発行した CA のルート証明書が LDAP サーバーの信頼データベースにインストールされている必要があります。

Directory Proxy Server のサーバー証明書をインストールする最後の手順で、Directory Proxy Server の証明書をテキストファイルとして保存しました。LDAP サーバーのマニュアルを参照し、信頼データベースに CA 証明書をインストールします。Sun ONE Directory Server を使用している場合は、Directory Server コンソールの「タスク」タブから「証明書の管理」ウィザードを呼び出して、CA 証明書を Directory Server の信頼データベースに追加できます。

手順 C: LDAP サーバープロパティの変更

「LDAP サーバープロパティ」ウィンドウの「暗号化」タブでは、各 LDAP サーバーの SSL 対応通信の条件を設定できます。詳細は、114 ページの「LDAP サーバープロパティオブジェクトの作成」を参照してください。

適切な LDAP サーバープロパティオブジェクトに次の変更を加え、変更内容を保存します。

- 「セキュリティポリシー」を設定します。バックエンドサーバーとの接続で Directory Proxy Server が常に SSL/TSL を確立する、TLS/SSL 接続を確立しない、またはクライアントが Directory Proxy Server との接続に SSL/TLS を利用している場合にだけバックエンドサーバーとの間で SSL/TLS 接続を確立するように指定できます。

- 「X.509 証明書サブジェクト DN」フィールドを、LDAP サーバー証明書のサブジェクト名 (X.509 証明書のサブジェクト属性) に設定します。これを指定すると、Directory Proxy Server は指定した証明書のサブジェクトを LDAP サーバーの証明書に含まれるサブジェクトと照合し、一致しない場合は TLS セッションを拒否します。(この属性により、Directory Proxy Server は接続先の LDAP サーバーを認証します。この属性が設定されていない場合、Directory Proxy Server は、どのようなサブジェクト名でも受け付けます。)

第 3 部

付録

付録 A 「Directory Proxy Server の判断機能」

付録 B 「Directory Proxy Server の FAQ、機能の説明、トラブルシューティング」

付録 C 「Directory Proxy Server の起動用設定ファイル」

付録 D 「コマンドリファレンス」

付録 A

Directory Proxy Server の判断機能

この付録では、一部の特定機能での Directory Proxy Server の制御の流れについて説明します。次の内容が含まれます。

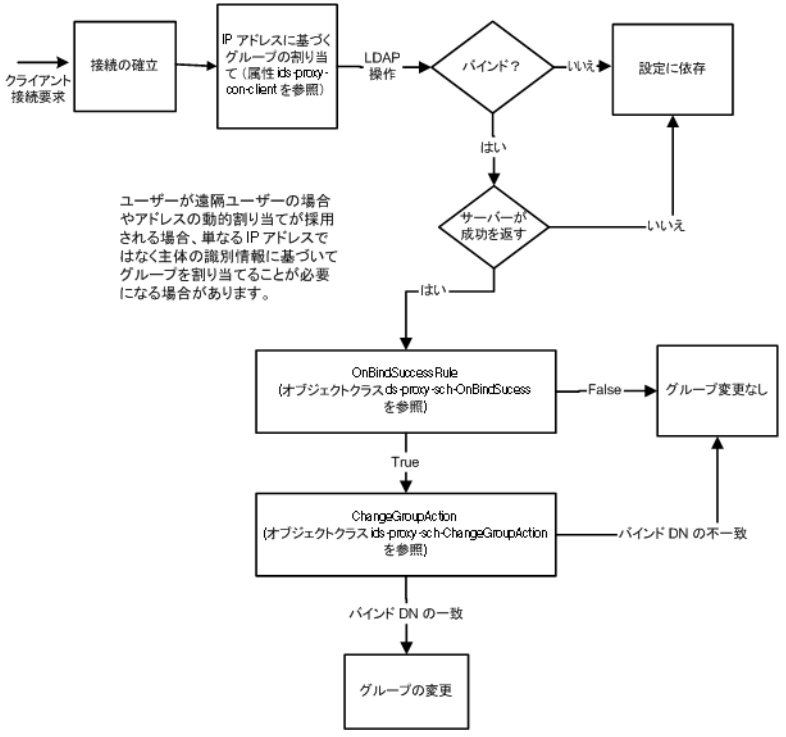
接続時のグループの特定

クライアントが Directory Proxy Server に接続すると、Directory Proxy Server は一致が見つかるまで `ids-proxy-sch-NetworkGroup` オブジェクトの `ids-proxy-con-Client` 属性を調べます。`ids-proxy-sch-NetworkGroup` オブジェクトは、`ids-proxy-con-priority` 属性によって定義される重要度の高いものから低いものへと順に調べられます。Directory Proxy Server は、クライアントの IP アドレスと `ids-proxy-con-client` 属性が一致する最初のグループをクライアントに割り当てます。一致するグループが見つからない場合、接続は閉じられます。

バインド時のグループ変更

接続後、クライアントにはまず、IP アドレスに基づくグループが割り当てられます。ディレクトリへのバインド時に、クライアントは別のアクセス制御を持つ別のグループに切り替えることができます。これを行うには、バインド操作の成功時に評価される規則オブジェクトが、最初のグループのオブジェクトに含まれている必要があります。この規則が TRUE と評価されると、グループ変更アクションが実行され、クライアントに別のグループが割り当てられます。図 A-1 は、この機能を示しています。

図 A-1　　バインド時のグループ変更



バインド時のグループ変更の設定

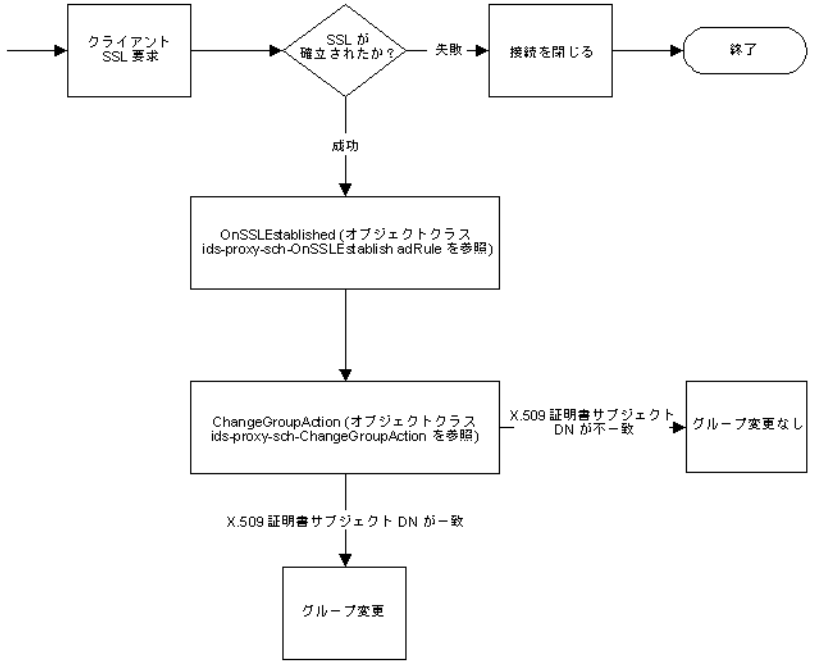
次の手順は、簡単なバインド認証メカニズムを利用して、バインドが正常に行われたときに「cn=Directory Manager」によってグループを変更するように Directory Proxy Server を設定する方法を示しています。

1. バインドが正常に行われたときに、ユーザー「cn="Directory Manager"」の切り替え先となる新しいネットワークグループを作成します。詳細は、79 ページの「グループの作成」を参照してください。切り替えによってユーザーのグループをそのグループだけに限定するときは、「ネットワークグループ」パネルの「ネットワーク」タブで「IP バインドなし」を設定します。この場合、このグループが、一部の IP バインドを許可するすべてのネットワークグループの後に位置することを確認してください。
2. 新しい「グループ変更」アクションを作成します。詳細は、138 ページの「アクションオブジェクトの作成」を参照してください。「変更先」には、手順 1 で作成したグループの名前を指定します。「一致するクライアント DN」には「cn=Directory Manager」を指定します。その他すべてのグループに (「.*」)、「なし」(グループ変更なし) を設定することもできます。
3. バインドイベントを作成します。詳細は、130 ページの「OnBindSucess イベントオブジェクトの作成」を参照してください。「アクション」タブで、手順 2 で作成したグループ変更アクションを指定します。「条件」タブでは、「パスワードベースのバインド」を選択します。
4. 手順 1 で作成したネットワークグループの「イベント」タブで、手順 3 で作成したバインドイベントを選択します。詳細は、102 ページの「グループの変更」を参照してください。

TLS 接続確立時のグループの変更

バインド時のグループ変更メカニズムと似ている TLS 接続確立時のグループ変更では、クライアントが TLS セッションを正常に確立した時点でグループが変更されます。クライアントが TLS 接続を確立すると、SSL 確立時規則が評価され、その結果によってグループ変更アクションが実行されます。図 A-2 は、この機能を示しています。

図 A-2　　TLS 接続確立時のグループの変更



高可用性の設定

複数のバックエンドディレクトリサーバーが設定されている環境では、サーバー間でのロードバランスと、いずれかのバックエンドサーバーが停止した場合の別サーバーへのフェイルオーバーを Directory Proxy Server に設定できます。これを行うには、ロードバランスプロパティオブジェクト (119 ページの「ロードバランスプロパティ」または 222 ページの「ids-proxy-sch-LoadBalanceProperty オブジェクトクラス」を参照) を作成し、負荷を分散するグループのオブジェクトに含める必要があります。また、バックエンドサーバーごとに LDAP サーバープロパティオブジェクト (114 ページの「LDAP サーバープロパティ」または 227 ページの「ids-proxy-sch-LDAPServer オブジェクトクラス」を参照) を作成し、ロードバランスプロパティオブジェクトに含める必要もあります。ロードバランスプロパティオブジェクトには、それぞれのバックエンドサーバーが、合計負荷の何パーセントを負担するかを指定します。いずれかのバックエンドディレクトリサーバーが停止した場合、Directory Proxy Server はこの設定に基づいてサーバー間で負荷を再配分します。サーバーが停止すると、クライアントは別のサーバーにフェイルオーバーされます。Directory Proxy Server と LDAP サーバーの間のネットワークリンクが使用不能になった場合、または LDAP サーバーが応答しなくなった場合もフェイルオーバーが行われます (229 ページの「ids-proxy-con-keepalive-interval」を参照)。

注 クライアントが SASL メカニズムを利用してバインドしている場合、Directory Proxy Server はフェイルオーバーを実行できません。

リフェラルの実行

Directory Proxy Server は、リフェラルを実行できない LDAPv2 クライアントに代わってリフェラルを実行するように設定できます。バックエンド LDAP ディレクトリサーバーには、リフェラルを送信する機能が必要です。つまり、LDAPv3 標準をサポートしている必要があります。ディレクトリサーバーからのリフェラルを Directory Proxy Server が受信できるように、Directory Proxy Server とバックエンド LDAP サーバーの間では LDAPv3 を使用するように設定します (228 ページの「ds-proxy-con-use-version」を参照)。次に、グループのリフェラル (217 ページの「リフェラルの戻しを制御する」を参照) と、継続リフェラルポリシー (217 ページの「ids-proxy-con-search-reference」を参照) を設定します。

付録 B

Directory Proxy Server の FAQ、機能の説明、トラブルシューティング

この付録には、Sun ONE Directory Proxy Server に関する有用な情報が記載されています。Directory Proxy Server についてのよくある質問 (FAQ) に対する回答、機能の説明、トラブルシューティングに関する情報が含まれています。

この付録で説明する内容は次のとおりです。

Directory Proxy Server の FAQ

Directory Proxy Server とは何ですか？

Directory Proxy Server は、LDAP クライアントと LDAP サーバーのための LDAP プロキシです。LDAP クライアントからの要求は、Directory Proxy Server の設定情報として定義されている規則に基づいて LDAP サーバーに転送されます。サーバーからの応答も、設定情報に定義されている規則に基づいてクライアントに戻されます。このプロセスは、クライアントには完全に透過的です。クライアントは、通常の LDAP サーバーに接続するように Directory Proxy Server に接続します。

なぜ LDAP プロキシサーバーが必要なのですか？

多くの企業は、一部の情報を広く公開し、別の一部の情報を非公開情報として社内で保持したいと考えています。Directory Proxy Server を利用することで、社外クライアントにディレクトリパスワードを割り当てることなくこの目標を達成することができます。また、ロードバランス機能とフェイルオーバー機能により、企業ディレクトリサーバーの高可用性ソリューションとして Directory Proxy Server を利用することもできます。

サービス拒否攻撃や検索制限などから保護するための追加セキュリティ機能も提供されます。

Directory Proxy Server はどのバージョンの LDAP プロトコルをサポートしていますか？

Directory Proxy Server は、LDAP v 2 または LDAPv3 プロトコルを使用する LDAP クライアントまたは LDAP サーバー連鎖をサポートしています。

Directory Proxy Server はセキュリティ保護された認証と暗号化をサポートしていますか？

Directory Proxy Server は、証明書を使用する公開鍵ベースのデータ暗号化のために SSLv3 サービスをサポートしています。LDAP クライアントで利用できるセキュリティ保護された認証と暗号化は、セキュリティ保護された LDAP ポート、または Diffie-Hellman、デジタル署名標準 (DSA)、およびトリプル DES アルゴリズムを使用するインターネット TLS (Transport Layer Security) モデルのいずれかを使用できます。

Directory Proxy Server は、どのような LDAP 対応ディレクトリサーバーでも利用できますか？

Directory Proxy Server は、どのような LDAP 対応ディレクトリサーバーでも利用できます。ディレクトリ製品の一部のベンダーは、マーケティング資料に LDAP の実装を明記していますが、現実は異なることが多いようです。Directory Proxy Server のほとんどのテストは、Sun ONE Directory Server を使って行われています。

Directory Proxy Server 5.0 コンソールを利用している場合、サポートされる設定レポジトリは、Sun ONE Directory Server 5.0 です。

Directory Proxy Server を設定するための設定ユーティリティは用意されていますか？

Directory Proxy Server 5.0 には、Directory Proxy Server を設定するための Java ベースの GUI (コンソール) が含まれています。このコンソールは、生成される設定情報の格納に Sun ONE Directory Server を使用します。

Directory Proxy Server の機能

サービス拒否攻撃からの保護に Directory Proxy Server を利用できますか？

利用できます。1 つの接続で並行して処理できる操作の数、1 つの接続で処理できる操作の数、並行接続の総数、定義されているグループ (ネットワーク、サブネットワーク、またはバインド DN ベース) あたりの最大並行接続数、1 IP アドレスあたりの最大並行接続数を制限することができます。

Directory Proxy Server は「逆」プロキシをサポートしていますか？

厳密に言えば、Directory Proxy Server は逆プロキシです。ただし、LDAP プロトコルは逆プロキシの概念をサポートしていません。

LDAP ディレクトリの「トローリング」からの保護に Directory Proxy Server を利用できますか？

利用できます。トローリングは、ディレクトリの大部分をダウンロードするための検索範囲の広いクエリで、多くのサイトが対策を求めています。Directory Proxy Server は、さまざまな方法でトローリングを禁止または制限できます。

- 検索範囲をディレクトリツリーの単一レベルに限定する、サブツリー全体を非表示にする、およびクエリに対する応答として返されるエントリの数をハード制限することができます。
- 不等値検索を禁止することで、除外に基づいて多数の検索結果を得られないようにし、部分文字列検索の長さを制限することができます。たとえば、姓が A ～ Z で始まるすべてのエントリの検索を禁止できます。
- インデックスが付けられていない検索を拒否するように Directory Proxy Server を設定することもできます。インデックスが付けられていない検索は非効率的で、パフォーマンスに影響を生じる可能性もあります。

Directory Proxy Server はクエリの自動ロードバランスを行いますか？

Directory Proxy Server は、複数のバックエンド LDAP サーバーの間での自動サーバーロードバランスをサポートしています。また、Directory Proxy Server は、主 LDAP サーバーが停止した場合の 2 次 LDAP サーバーへの自動フェイルオーバーもサポートしています。

Directory Proxy Server は、いくつの LDAP サーバーに負荷を分散できますか？

Directory Proxy Server がロードバランスできるディレクトリサーバーの最適数は、ディレクトリサーバーのパフォーマンス要件、および Directory Proxy Server が実行する処理の複雑さによって異なります。たとえば、Directory Proxy Server が属性名の変更のように複雑な処理を行う場合、Directory Proxy Server に設定するディレクトリサーバーの数は少なくするべきです。Directory Proxy Server の複雑な設定がパフォーマンスに影響する可能性に備えて、Directory Proxy Server の追加を検討してください。

検索要求をフィルタリングすることはできますか？

できます。特定の属性に対する検索を拒否するように Directory Proxy Server を設定することができます。また、指定されている最小検索ベース、検索範囲、タイムリミットを満たせるように、受け取った検索要求を変更するように Directory Proxy Server を設定することもできます。

検索結果をフィルタリングすることはできますか？

できます。検索結果は、返される検索結果の数、および結果セットに含まれる属性に基づいてフィルタリングすることができます。また、エントリの DN や内容に基づいて検索結果エントリをフィルタリングすることもできます。

アクセスグループはどのように定義するのですか？

クライアントには、クライアントのネットワークアドレスに基づいて、ディレクトリに対するさまざまなレベルのアクセス権が割り当てられます。このため、企業ファイアウォールの外のクライアント、ファイアウォール内のクライアント、排他的サブネットワーク上のクライアント、個々のマシンにも異なるレベルのアクセス権を割り当てることができます。さらに、クライアントによる LDAP バインド操作の正常完了、または SSL セッションの確立時に、アクセスレベルを変更することもできます。

Directory Proxy Server は、保護されたパスワード認証をサポートしていますか？

サポートしています。SASL メカニズムを使用することで、さまざまな保護されたパスワード認証スキームを実装できます。これらのメカニズムは、バックエンドディレクトリサーバー側でサポートされている必要があります。Directory Proxy Server は、接続が保護された SASL メカニズムと SASL EXTERNAL メカニズムをサポートしていません。

Directory Proxy Server は自動的にリフェラルを実行しますか？

リフェラルの実行は、アクセスグループごとに設定できます。リフェラルの自動的な実行、転送、破棄をさまざまなアクセスグループに設定できます。

Directory Proxy Server は検索結果情報をキャッシュしますか？

Directory Proxy Server Version 5.0 SP1 は検索結果のキャッシングをサポートしていません。

Directory Proxy Server は属性名を変更できますか？

Directory Proxy Server は、クライアントとサーバーの間で属性名を透過的に変更できます。

トラブルシューティング

接続試行のログは、どうすれば分析できますか？

Directory Proxy Server は、`syslog` を使用するか、指定のログファイルにログを書き込むように設定することができます。スタンフォード大学の FTP (`ftp://ftp.stanford.edu/general/security-tools/swatch`) では、swatch という UNIX ユーティリティを無償で入手できます。swatch を使用して、Directory Proxy Server から出力されるログファイルを監視し、定義されているイベントが発生した場合に管理者に通知することができます。

リフェラルを実行するように Directory Proxy Server を設定しました。しかし、LDAPv2 クライアントで検索を実行すると、エラー 32 (オブジェクトが存在しない) またはその他のエラーが返されます。

Directory Proxy Server がバックエンドサーバーからリフェラルを受信するには、LDAPv3 を使用する必要があります。各 LDAP サーバープロパティで「LDAP バージョン 3 のみ」が選択されていることを確認してください。

すべてのバックエンドサーバーが稼動しているのに、ログファイルを調べると、一部のアイドルクライアント接続が定期的にフェイルオーバーされているようです。

バックエンドディレクトリサーバーでアイドル接続のタイムアウトが発生し、接続が閉じられています。Directory Proxy Server は、これらの閉じられた接続をフェイルオーバーします。Directory Proxy Server のアイドル接続タイムアウトも設定する必要があります。これにより、アイドルクライアント接続とリークしたクライアント接続を整理することができ、サービス拒否攻撃から接続を保護することもできます。

presence フィルタを含む検索要求を制限する方法はありますか？

Directory Proxy Server Version 5.0 SP1 には、presence フィルタの使用についてクライアントを制限する直接的なメカニズムは用意されていません。この問題には、次の 2 つの間接的な方法で対応しています。

比較させない属性の名前として、`ids-proxy-con-forbidden-compare` を設定できます。この方法では、(mail=*) フィルタと (mail=Andy*) フィルタの両方を含む検索が拒否されるため、制限が厳しくなります。

一方、presence フィルタ (attrName=*) は常に同じ結果を返すことから (データが変更されていない場合)、ids-proxy-con-size-limit 属性と `ids-proxy-sch-SizeLimitProperty` を併用することで、影響を限定的にすることができます。LDAP では、エントリを特定の順序で返す必要はありませんが、ほとんど (すべて) の実装では、結果セットはソートされた順序またはソートされない順序で返され、これは毎回変わりません。このため、Directory Proxy Server にサイズ制限を設定した場合 (size-limit 属性または SizeLimitProperty を使用)、これらの結果セットの最初の「n」エントリだけが毎回返されます。これらの「n」エントリは 2 セット (ソートされている場合とソートされていない場合) しかないため、ディレクトリがトローリングされるリスクは大幅に軽減されます。

Directory Proxy Server は、要求自体にもできるだけこのサイズ制限を適用しようとするため、ディレクトリサーバーはエントリをすべて返すわけではなくなります。

サイズ制限プロパティにより、必要に応じてサイズ制限に例外を適用できます。たとえば、「o=A」というエントリがあり、その下には 400 の組織単位が登録されていると仮定します。それぞれの組織単位の下には人物が登録されています。クライアントにすべての OU を公開し、一度に表示できる人物を 5 人に制限するときは、ベースが「o=A」の検索には制限を適用せずに、検索範囲が 1 レベルになるように `SizeLimitProperty` を設定できます。その他のすべての検索には、5 エントリの制限が適用されます。

処理を実行しようとしたり、一部のコンソール機能を実行しようとすると、管理サーバーが正常に稼動していること、およびこのホストが管理サーバーに接続する権限を持っていることを確認するように求めるエラーメッセージが表示されます。

エラーメッセージを出力したコンソールの Directory Proxy Server を管理する管理サーバーにログインしてください。管理サーバーのホストマシンで Sun ONE コンソールを起動しなければならない可能性があります。タスクを実行できなかった Directory Proxy Server を管理する管理サーバーのサーバーコンソールを開きます。「設定」タブをクリックし、次に「ネットワーク」タブをクリックします。「接続の制限」の下で、Directory Proxy Server の管理に失敗している Sun ONE コンソールのホストマシンが、管理サーバーへのアクセスを制限されていないことを確認します。詳細については、『Sun ONE Console Server Management Guide』を参照してください。

Directory Proxy Server の起動用設定ファイル

この付録には、Directory Proxy Server の設定ファイルに関する情報が記載されています。次の内容が含まれます。

設定ファイルの概要

`tailor.txt` ファイルには、Directory Proxy Server が主設定の場所を特定するために必要なブートストラップ情報が記録されています。このファイルに含まれる指令は、Directory Proxy Server が主設定用に追加ファイルを使用するか、または Directory Proxy Server が主設定を LDAP サーバーから取得するかを決定します。デフォルトでは、Directory Proxy Server は、起動用設定ファイル `tailor.txt` をインスタンスのインストールディレクトリ内の `etc` サブディレクトリから探します。注 : コマンド行パラメータ `-t` を使用することで、Directory Proxy Server が別のファイルを起動用設定ファイルとして使用するように指定できます。

高可用性設定をサポートするために、起動用設定ファイルには、主設定の検索先として複数のポイントを指定できます。検索先ポイントは、2 つのキーワード `Begin` および `End` を使用して起動用設定ファイルに指定されます。Directory Proxy Server は、検索先ポイントを指定されている順序で一つずつ処理します。各検索先ポイントでの Directory Proxy Server の動作は、指定の検索先ポイントの種類 (LDAP URL またはファイルへの絶対パス名による指定) によって異なります。

LDAP URL ベースの検索先ポイントでは、Directory Proxy Server は指定されたホストに接続を試みます。ホストが設定を返さない、または返せない場合は、Directory Proxy Server は次の検索先ポイントの処理を開始します (指定されている場合)。ホストが設定を返す場合は、Directory Proxy Server は返された設定を編集し、主設定に指定されている指令に従うか、設定が無効であると見なされる場合は処理を終了します。

ファイルベースの検索先ポイントでは、Directory Proxy Server は指定されたファイルを主設定としてロードしようとします。指定された設定が見つからない、または無効であると見なされる場合、Directory Proxy Server は処理を終了します。ファイルベースの検索ポイントが指定されている場合、Directory Proxy Server は次の検索先ポイントの処理を行いません。

Directory Proxy Server が主設定を LDAP ホストから取得した場合、Directory Proxy Server は匿名、単純、SASL 使用のいずれかの方法でホストにバインドできます。

匿名バインドは、`configuration_bind_pw` 指令と `configuration_bind_dn` 指令を省略することで行われます。つまり、起動用設定の検索先情報には、`configuration_url` 以外の指令を指定しません。

単純バインドは、`configuration_bind_pw` と `configuration_bind_dn` の両方の指令によって行われます。

SASL バインドでは、`sasl_bind_mechanism` 指令と `conguration_bind_pw` 指令のほかに、`configuration_bind_dn` 指令、または `configuration_username` 指令のどちらか (1 つのみ) を指定する必要があります。

起動用設定のキーワード

指定されている各検索先ポイントでは、検索先ポイントエントリの開始が `Begin` というキーワードによって指定されます。反対に、各検索先ポイントエントリの終了は、`End` というキーワードによって指定されます。起動用設定ファイルに指定されるすべての指令は、1 つの行で表現されます。起動用設定内での改行による行の継続は認識されず、サポートされません。設定のオプションは、オプション、コロン、値の 3 つで指定されます。

configuration_url

`configuration_url` オプションは、Directory Proxy Server の設定がが格納されている LDAP ディレクトリサーバーとエントリの識別名、または LDIF 形式のローカルファイルを指定します。たとえば、Directory Proxy Server の設定が `ldap.sun.com` ホスト上の LDAP ディレクトリに格納され、LDAP サービスがポート `389` で稼動している場合、Directory Proxy Server のエントリが「`ids-proxy-con-Server-Name=Directory Proxy Server`」であれば、設定ファイルに次の内容を追加します。

```
Begin
configuration_url:
ldap://ldap.sun.com:389/ids-proxy-con-Server-Name=Directory Proxy
Server
End
```

設定が LDAP サーバー内に維持されている場合は、ホストディレクトリのネーミングコンテキストに合わせて、ids-proxy-con-Server-Name=Directory Proxy Server の後にサフィックスの指定が必要な場合があります。次の例を参照してください。

```
Begin
configuration_url:
ldap://ldap.sun.com:389/ids-proxy-con-Server-Name=Directory Proxy
Server,
ou=services, dc=sun, dc=com
End
```

起動用設定の各指令は、設定ファイル内の 1 つの切れ目ない行として指定する必要があります。

注 configuration_url の例に見られる行の折り返しは、設定ファイル内の指令に改行を挿入することを意味していません。

たとえば、LDIF 形式の <server-root>/dps-<hostname>/etc/tailor.ldif というファイルに設定が格納されている場合は、設定ファイルに次の内容を追加する必要があります。

```
Begin
configuration_url:
file://<server-root>/dps-<hostname>/etc/tailor.ldif#ids-proxy-con-S
erver-Name=Directory Proxy Server
End
```

configuration_bind_dn

configuration_bind_dn オプションは、configuration_url オプションによって指定される LDAP サーバーに Directory Proxy Server がバインドするときに使用される識別名を指定します。Directory Proxy Server はこの識別名に対して単純バインドを行い、configuration_bind_pw の値をパスワードとして使用します。次の例を参照してください。

```
Begin
configuration_url:
ldap://ldap.sun.com:389/ids-proxy-con-Server-Name=Directory Proxy
Server
configuration_bind_dn: cn=Directory Manager
configuration_bind_pw: secret
End
```

configuration_url の設定が「ファイル」形式の場合は、configuration_bind_dn オプションを指定する必要はなく、このオプションは無視されます。注 : configuration_bind_dn 指令と configuration_username 指令は互いに排他的です。

configuration_bind_pw

configuration_bind_pw オプションは、LDAP ディレクトリへのバインド時に使用されるパスワードを指定します。この指令は、単純バインドまたは SASL ベースのバインドで使用されるパスワードを指定します。セキュリティを確保するために、設定ファイルを未認証の読み取りから保護する必要があります。configuration_url の設定が「ファイル」形式の場合は、configuration_bind_pw オプションを指定する必要はなく、このオプションは無視されます。(例については、configuration_bind_dn を参照してください。)

configuration_username

configuration_username オプションは、configuration_url オプションによって指定される LDAP サーバーに Directory Proxy Server がバインドするときに使用されるユーザー名を指定します。このオプションは、SASL バインドメカニズムを使用する場合にだけ使用します。注 : configuration_bind_dn 指令と configuration_username 指令は互いに排他的です。

```
Begin
configuration_url:
ldap://ldap.sun.com:389/ids-proxy-con-Server-Name=Directory Proxy
Server
configuration_username: administrator
configuration_bind_pw: secret
sasl_bind_mechanism: CRAM-MD5
End
```

sasl_bind_mechanism

sasl_bind_mechanism オプションは、Directory Proxy Server が使用する SASL バインドメカニズムの種類に応じて、CRAM-MD5 または DIGEST-MD5 のどちらかに設定できます。このオプションが指定されていない場合、Directory Proxy Server は単純バインドまたは匿名バインドを行います。DIGEST-MD5 は CRAM-MD5 より高度なセキュリティを提供しますが、CRAM-MD5 ほど広く普及していません。

付録 D

コマンドリファレンス

この付録では、Sun ONE Directory Proxy Server の便利なコマンド行プログラムについて説明します。

この付録では、次の内容について説明します。

dpsconfig2ldif

Directory Proxy Server の設定をダウンロードし、LDIF ファイルとして保存するには、`dpsconfig2ldif` というユーティリティを使用します。このユーティリティは、次の場所にあります。

```
<Install Root>/bin/dps_utilities/dpsconfig2ldif
```

このユーティリティでは、2 つの引数を指定する必要があります。

引数 :	説明
-t *filename*	*filename* は、起動用設定ファイルへのパスです。これは、通常は etc ディレクトリ内の tailor.txt ファイルです。
-o *filename*	設定の出力先ファイル名を指定します。

dpsldif2config

ImportConfigLdif は、dpsConfig2Ldif が生成した LDIF ファイルをインポートします。このユーティリティは、次の場所にあります。

```
<Install Root>/bin/dps_utilities/dpsldif2config
```

このユーティリティでは、次の引数を指定する必要があります。

引数 :	説明
ldif	Directory Proxy Server のオブジェクトオプションを含む ldif ファイルの名前
-C	作成する設定の名前 (未指定の場合は「imported-configuration」)
-h	ディレクトリのホスト名 (未指定の場合は「localhost」)
-p	ディレクトリのポート番号 (未指定の場合は「389」)
-D	ディレクトリのユーザー識別名 (未指定の場合は匿名バインド)
-w	ディレクトリのユーザーパスワード (未指定の場合は匿名バインド)
-v	冗長モード

ImportConfigLdif は、次の 3 種類のオブジェクトをインポートします。

- 共有設定 (「Directory Proxy Server 設定」ノードのメインコンソールトポロジツリーに含まれる設定)
- 共有システムプロパティ
- 共有ログプロパティ

「設定名」パラメータは、この共有設定だけに適用されます。システムとログのプロパティは、ldif ファイルに記録されているとおりに追加されます。指定パラメータ名を持つ共有設定オブジェクトが存在しない場合、このスクリプトはそのパラメータ名で新しい設定を作成します。指定した名前の設定がすでに存在する場合は、インポートは行われません。システムとログのプロパティも、ディレクトリ内にすでに存在する場合は追加されません。

設定のインポート後、設定をトポロジツリーに表示するには、メインコンソールを再起動する必要があります。設定を利用するには、Directory Proxy Server インスタンスは、それ自体を各設定に割り当てる必要があります。共有設定の割り当ては、Directory Proxy Server コンソールの「ネットワークグループ」ノードで行います。システムプロパティの割り当ては、Directory Proxy Server コンソールの「システム」ノードで行います (「設定の保存先」)。ログプロパティの割り当ては、Directory Proxy Server コンソールの「ログ」ノードで行います (「設定の保存先」)。

前提条件

- 5.0 (sp 1) からの移行がすでに完了していること

事後条件

- インポートされる ldif ファイル内の belongs-to 属性が無視される

索引

き

く

け

さ

し

せ

そ

た

つ

て

と

ふ

へ

ゆ

ろ