



**Samba LDAP  
認証統合,SSOなら  
OSSTechへ**

**オープンソース・  
ソリューション・  
テクノロジー株式会社**

<http://www.osstech.co.jp>

〒141-0031  
品川区西五反田1-29-1  
コイズミビル8F

電話 : 03-6417-0753  
FAX : 03-6417-0754  
Email: [info@osstech.co.jp](mailto:info@osstech.co.jp)



# OpenLDAP 2.4 for Linux/Solaris/AIX

## 製品情報



OpenLDAP 2.4 for Linux/Solaris/AIX 製品機能概要

- **LDAPv3準拠**
  - SASL による厳密認証とデータセキュリティサービスを提供
  - TLS (SSL)による証明書認証とデータセキュリティサービスを提供
  - Unicode による国際化対応
  - 紹介(referral)と継続(continuation)をサポート
  - IPv4, IPv6, Unix IPCをサポート
  - アクセス制御:LDAP の認可情報、IP アドレス、ドメイン名などといった基準を基にしてエントリへのアクセスを制御でき、静的 と 動的 の両方のアクセス制御情報をサポート
- **選択可能なデータベースバックエンド**
  - 高速でトランザクション制御可能なデータベースバックエンド BDB、階層構造を持った高速でトランザクション制御可能なデータベースバックエンド HDB、任意のシェルスクリプトに対するデータベースインタフェース SHELL、簡単なパスワードファイルデータベース PASSWD
  - 同時に複数のデータベース実態を扱うように設定可能  
LDAP ツリーの論理的に異なる部分についての要求に単一応答可能。LDAP ツリーの各部には、同じバックエンドデータベースを使う事も異なるデータベースバックエンドを使う事も可能
- **OSSTech独自の改良**
  - 大規模システム向けの品質向上とチューニング
  - 独自にパスワードポリシーを強化
  - 機能、性能、品質強化により商用製品からの移行に対応

## OpenLDAP 2.4 for Linux/Solaris/AIX

### ●動作環境

- ・対応 OS :  
Red Hat Enterprise Linux, Solaris, AIX, CentOS

### ・提供パッケージ形式

RPM(RedHat Package Manager)

### ●製品詳細

- ・最新のOpenLDAP2.4系を採用し、商用Linux同梱のOpenLDAPよりも数々の不具合を修正
- ・バックエンドデータベース：Berkeley DB (BDB) 4.8.24を採用し、高性能・高品質
- ・高負荷でデータが破壊する、ハングアップする、リカバリできないなどの多くの不具合を修正
- ・商用Linux同梱のOpenLDAPには同時接続数として1024や4096という制限がありますが、弊社製品は16384接続まで拡大しており、大規模システムでの運用に適しています。
- ・マルチ・マスター・レプリケーション対応（品質検証済み）
- ・高速で安定したシングル・マスター(sync repl)レプリケーション対応（品質検証済み）
- ・LDAPベンチマーク（SLAMD）により、1秒間にLDAPデータ検索3万4千、LDAPデータ追加性能570件以上を達成

LDAP検索性能

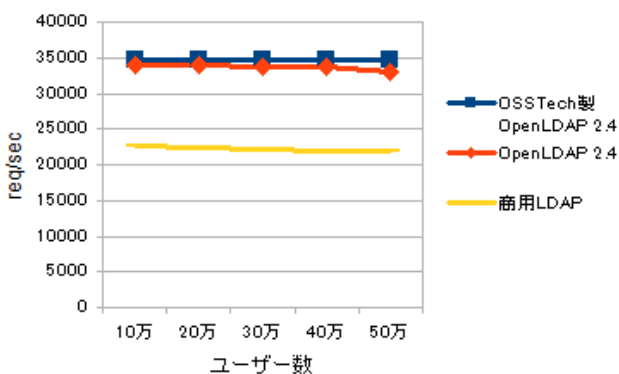


図1. OSSTech 製 OpenLDAP とオリジナル OpenLDAP / 商用 LDAP 製品との LDAP 検索性能比較

### ●オープンソース・ソリューション・テクノロジー株式会社独自の修正内容、改良項目

- ・同時接続数拡大

OpenLDAP2.2には同時接続数として1024という制限がありますが、弊社製品は16384接続まで拡大しており、大規模システムでの運用に適しています。

- ・BDB破壊の防止

BerkeleyDB (BDB)のバージョンを最新の4.8.24にし、高負荷でデータが破壊する、ハングアップする、リカバリできないなどの多くの不具合を修正しています。

数多くのOpenLDAPの不具合を修正

- ・パスワードポリシー機能の強化

OSSTech社のOpenLDAPは独自にパスワードポリシーの強化を行っています。

- ・パスワードの有効期限の指定
- ・パスワードの変更禁止期間の指定
- ・パスワード最小文字数の指定
- ・パスワードの期限切れの事前警告期間の指定（クライアント側がLDAPパスワードポリシーコントロールに対応している必要があります）
- ・認証失敗時のアカウントロック
- ・アカウントロックされる認証失敗回数の指定
- ・アカウントロックが解除される期間指定
- ・認証失敗回数のカウンターがリセットされる期間の指定
- ・初回認証時のパスワード変更要求
- ・パスワード履歴の記録（履歴に残っているパスワードは使用不可能）
- ・期限切れパスワードによる認証(bind)の最大回数指定（パスワード有効期限が切れた後に許可するログインの回数）
- ・パスワードの複雑性のチェック
- ・パスワードに含まれる文字種の最小数指定
- ・パスワードに含まれる英文字の最小数指定
- ・パスワードに含まれる英大文字の最小数指定
- ・パスワードに含まれる英小文字の最小数指定
- ・パスワードに含まれる数字の最小数指定
- ・パスワードに含まれる記号の最小数指定