OSSTech

OpenLDAP

オープンソースで安全・安心のLDAPサーバー製品

Linux・Windows・macOS・Unix の
ユーザー情報と認証の統合管理を実現

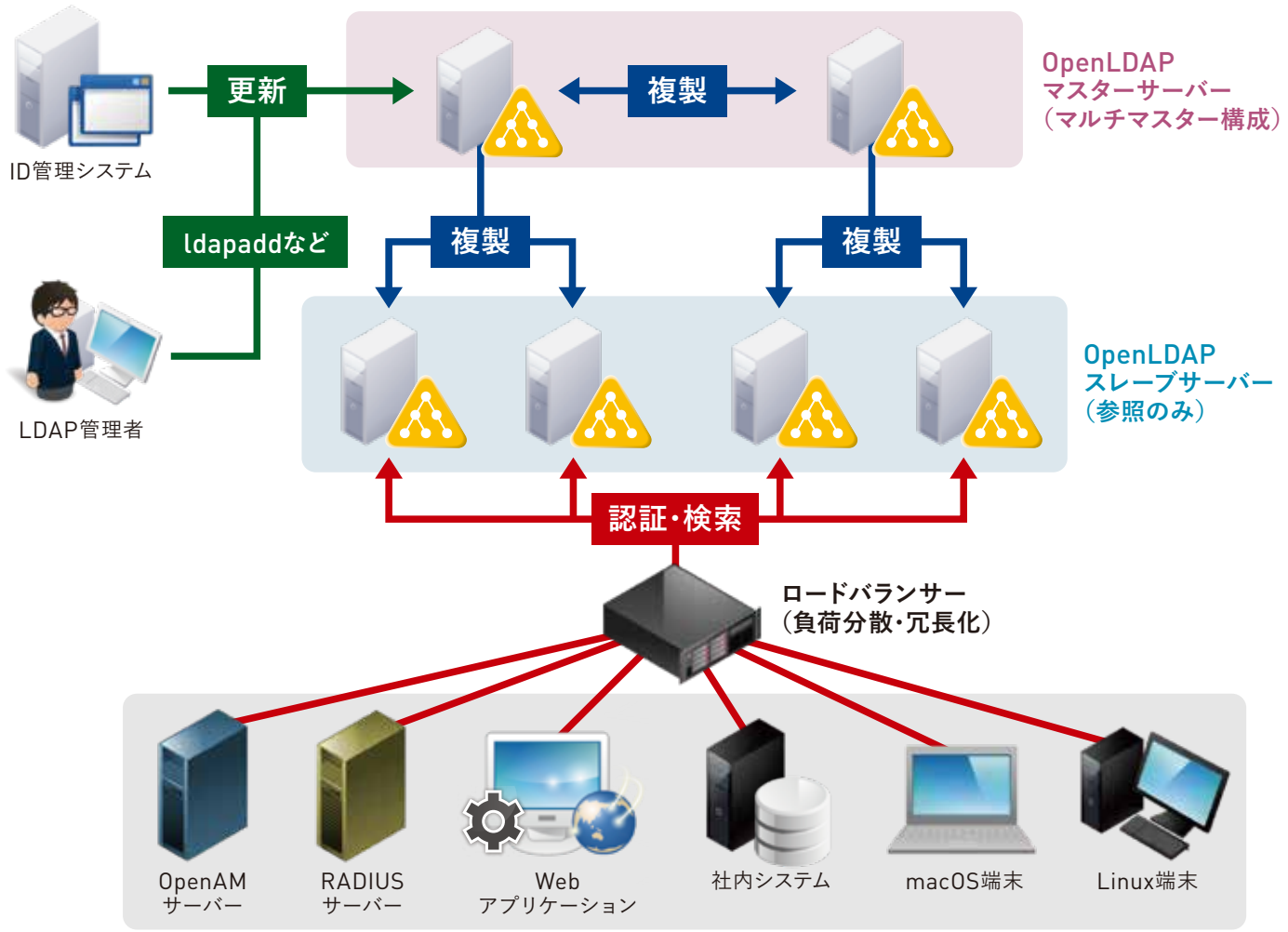
OpenLDAP とは?

- LDAPサーバーの中で、最も普及し、安定性に優れた20年の動作実績
- LDAPv3 に準拠し、各種LDAP対応製品との接続において、豊富な接続情報・接続実績を提供
- 費用はユーザー数に依存せず、大規模環境においても低コストで導入・運用が可能
- マスターサーバーを冗長構成(マルチマスター)とすることができ、高い可用性を提供
- スレーブサーバーを追加することで、認証・検索処理の負荷分散、スケールアウトが可能

基本機能

- LDAPv3に準拠したディレクトリサービスを提供
- TLSによる通信経路の暗号化
- IPアドレスやグループ属性によるアクセス権の管理
- パスワードポリシーによるユーザーパスワードの保護強化
- カスタムスキーマによる任意の属性の登録
- マルチマスター/マスタースレーブ複製機能による冗長構成、スケールアウト、負荷分散

システム構成例



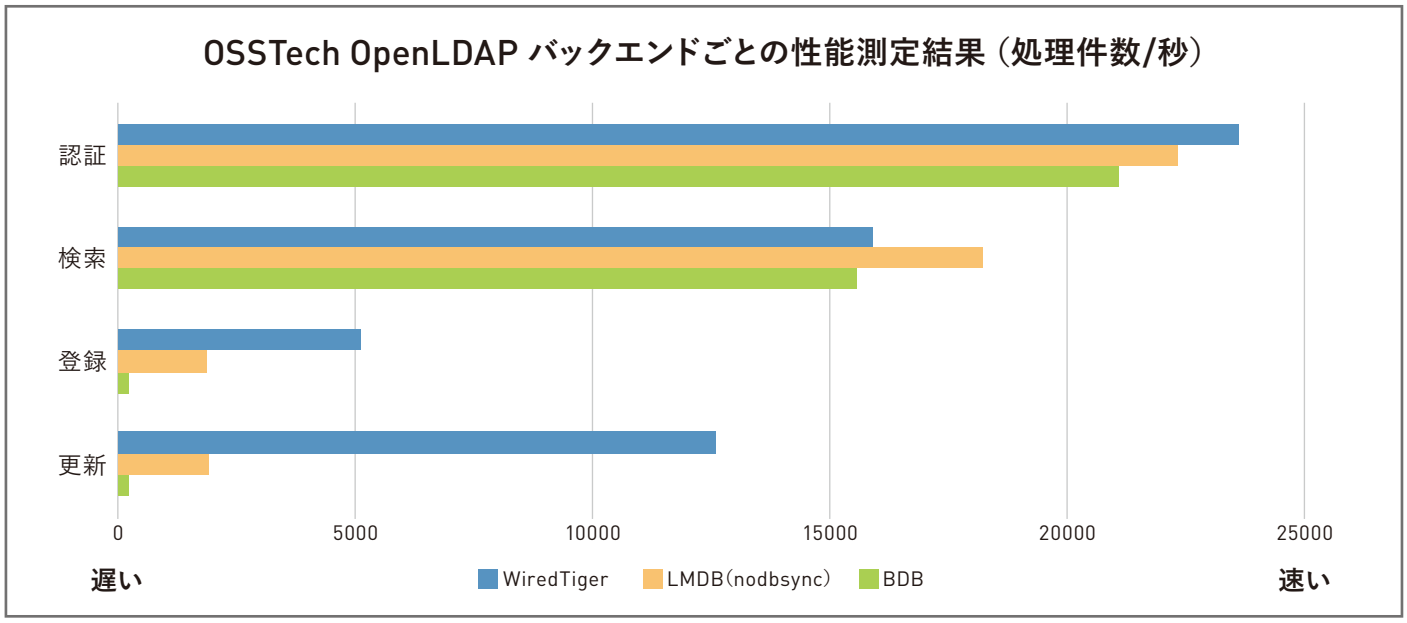
さまざまなLDAPクライアント

OSSTech OpenLDAP の機能・特長

パスワードハッシュの強化	パスワードのハッシュアルゴリズムとして、SHA-2、PBKDF2を実装し、 パスワード漏洩に対する保護を強化します。
パスワードポリシーの強化	OpenLDAPの ppolicyオーバーレイと連携して パスワードの複雑性の制約を設定可能です。
各種オーバーレイの同梱	OpenLDAPで利用可能な各種オーバーレイを 設定のみで利用できる状態でパッケージング済みです。
同時接続数拡大	OSSTech OpenLDAPは同時接続を 16384まで対応。 大規模システムでの運用に適しています。
Active Directoryとの パスワード双方向同期	OSSTech OpenLDPの機能のみでWindows Active DirectoryとOpenLDAPの パスワード双方向同期が可能です。Windowsに 追加モジュールの導入が不要です。
運用管理の強化	日次バックアップ機能とログローテート機能をパッケージに組込済みで、 障害時のリカバリや操作ログの監査が実施できます。

OSSTech OpenLDAP WiredTiger バックエンド

最新のデータベース採用で更新性能の大幅向上を実現！！



【測定環境】OS: CentOS 7 (x86-64) / OSSTech OpenLDAP 2.4.45 ・KVM上の仮想OSとして実行 ・CPU数 : 24、メモリ 10GB

複数CPU、大容量メモリを前提とした
WiredTiger DBの特長を発揮することで
登録・更新処理の性能向上を実現

データの初期登録時やリカバリなどの
一括登録処理の時間も大幅な削減
100万件以上の大規模環境でもチューニング不要で、
運用上の制約を低減し運用管理を簡素化

OSSテクノロジが開発を行い
OpenLDAP 2.5の新機能として取り込み済み
いち早くお客様環境で利用可能に

既存環境もパッケージのアップデート、
LDAPデータのエクスポート・インポートで
WiredTigerバックエンドに移行可能

OSSTech OpenLDAP 機能一覧

- LDAPv3 に準拠し、LDAPサービスを提供
- カスタムスキーマの定義により任意の属性の登録が可能
- エントリに対して、ユーザー、グループ、IPアドレスなどによるアクセス制限が可能
- LDAP接続時にシンプル認証・SASL認証による認証が可能
- LDAP通信をTLS（1.0以降のバージョン）により暗号化可能
- LDAPサービスの接続ユーザー、接続元IPアドレス、操作内容をsyslogに記録
- パスワード格納時の暗号化アルゴリズムとして、CRYPT、MD5、SHA-1、SHA-2、PBKDF2などに対応
- パスワードポリシーとして有効期限、パスワードの最小文字数、複雑性、アカウントロックなどの制約を設定可能
- データ格納先のバックエンドとして、WiredTiger、BDB、LMDBに対応
- WiredTigerバックエンドに1000万件のLDAPエントリの格納が可能
- 設定方式として、slapd.confによる設定ファイル方式と、configバックエンドによるLDAPデータベースの両方式に対応
- LDAPの登録データをUTF-8で保存し、言語タグ（RFC 3866にて規定）に対応
- 複数のLDAPツリー（DIT）を1つのLDAPサービス内で管理可能
- Active Directoryとのパスワード双方向同期が可能

OpenLDAPパッケージ同梱オーバーレイ

モジュール名	用途
syncprov	LDAP複製機能
ppolicy	パスワードポリシー
pw-sha2	SHA-2 形式パスワード
pw-pbkdf2	PBKDF2 形式パスワード
auditlog	変更履歴の記録
memberof	グループメンバーの自動更新
unique	属性値の一意制約
valsort	検索結果のソート機能
smbk5pwd	Sambaパスワードの自動同期
rwm	属性値などのリライト機能
lastbind	ログイン時刻の記録
psync	ADとのパスワード双方向同期

OSSTech OpenLDAP 製品

- 稼働ノードに対するノードライセンス体系
- 登録・利用ユーザー数無制限
- RPM形式で提供
- 導入・運用に役立つバックアップ設定などを初期設定済み

OpenLDAP 年間サポート

- OpenLDAP運用・障害に関する問い合わせ対応
- アップデートパッケージ提供
- 対応時間：平日 9時 – 17時
- システム単位の年間サポート契約
- 長期間サポートを提供

OpenLDAP 導入・移行 技術支援サービス

- LDAPサービス導入案件の営業支援
- OpenLDAP 設計支援・導入支援サービスの提供
- OpenLDAP サーバー構築作業
- OpenLDAP スキーマのカスタマイズ対応
- 旧システムのOpenLDAPからのデータ移行
- 各種商用LDAP製品からOpenLDAPへの移行支援

OpenLDAPの開発・導入に長年携わってきた
LDAPのスペシャリストによる支援をご活用ください！

ハードウェア要件	■ Intel Xeon CPU 2core以上 ■ メモリ 4GB以上 ■ ディスク 20GB以上（OS領域含む）
対応OS	■ Red Hat Enterprise Linux 7（x86-64） ■ CentOS 7（x86-64） ※ その他のOSについてはお問合せください。

OSSTech オープンソース・ソリューション・テクノロジ株式会社 Open Source Solution Technology Corporation
〒141-0031 東京都品川区西五反田1-29-1 コイズミビル 8F Tel:03-6417-0753 Fax:03-6417-0754 Mail:info@osstech.co.jp