

OSSTech Windows 版 OpenLDAP インストール ガイド



OSSTech 株式会社

更新日

2025 年 7 月 4 日

目次

1	はじめに	1
1.1	ソフトウェア要件	1
1.2	Windows 版 OpenLDAP パッケージのインストール	1
2	OpenLDAP の設定	2
2.1	設定ファイルのチェック	3
2.2	OpenLDAP の起動・停止	3
2.3	起動確認	4
2.4	Windows ファイアウォールの設定	5
2.5	LDAP ログファイル	5
2.6	ログレベルの変更	6
2.7	ログディレクトリの変更	6
2.8	サービスポートの変更	6
2.9	スキーマ拡張	7
2.10	インデックス再生成	7
2.11	LDAP データの初期化	7
2.12	Windows 版 OpenLDAP のアンインストール	7
2.13	Windows 版 OpenLDAP の制限等	8

1 はじめに

本ドキュメントは、弊社提供の Windows 版 OpenLDAP パッケージを導入するための手順書です。

1.1 ソフトウェア要件

Windows 版 OpenLDAP では以下の OS 環境が必要です。

- Windows Server 2022 (x86-64)
- Windows Server 2025 (x86-64)

Active Directory が導入された Windows Server は LDAP(389/tcp)/LDAPS(636/tcp) のポートが Active Directory によって利用されていることと、ディスクに対する I/O 同期設定の影響でパフォーマンスが大幅に低下します。そのため、Active Directory として運用している Windows Server に OpenLDAP をインストールして利用することは避けてください。

1.2 Windows 版 OpenLDAP パッケージのインストール

Windows の管理者アカウントでログオン後、弊社提供の Windows 版 OpenLDAP パッケージをダブルクリックしてインストールを行います。

- OSSTech-OpenLDAP-2.6.X.Y.msi

インストール処理は数秒で完了し、画面上には入力欄等は表示されません。

`C:\Program Files\OSSTech\OpenLDAP` 配下に `ldapadd` などのコマンドがインストールされていれば、Windows 版 OpenLDAP のインストールは完了です。

2 OpenLDAP の設定

OpenLDAP の設定は、`C:\ProgramData\OSSTech\OpenLDAP\etc\slapd.conf` ファイルで行います。

* `C:\ProgramData` フォルダは隠しフォルダとなっています。

インストール直後には以下の主要なパラメーターが設定されています。

```
include "C:/ProgramData/OSSTech/OpenLDAP/etc/schema/core.schema"
include "C:/ProgramData/OSSTech/OpenLDAP/etc/schema/cosine.schema"

database mdb
maxsize 1073741824
suffix "dc=example,dc=com"
rootdn "cn=Manager,dc=example,dc=com"
rootpw secret
directory "C:/ProgramData/OSSTech/OpenLDAP/data"
index objectClass eq

database monitor
```

運用環境に合わせて、slapd.conf ファイルの設定を変更後、LDAP サービスを起動してください。

- slapd.conf ファイル内でフォルダの区切りは”/“で表すことができます。
- フォルダ名の一部に空白を含む場合、フォルダのパスを” “で括ってください。
- slapd.conf ファイルは BOM 無しの UTF-8 で作成してください。

設定パラメーターの詳細については、OSSTech 版 OpenLDAP のインストールガイドをご参照ください。

2.0.1 slapd.conf の設定例

下記に標準的な slapd.conf の設定例を示します。

```
include "C:/ProgramData/OSSTech/OpenLDAP/etc/schema/core.schema"
include "C:/ProgramData/OSSTech/OpenLDAP/etc/schema/cosine.schema"
include "C:/ProgramData/OSSTech/OpenLDAP/etc/schema/inetorgperson.schema"
include "C:/ProgramData/OSSTech/OpenLDAP/etc/schema/nis.schema"

moduleload ppolicy.la
moduleload argon2.la
moduleload pw-pbkdf2.la
moduleload pw-sha2.la

sizelimit unlimited
```

```
database mdb
maxsize 1073741824
suffix "dc=example,dc=com"
rootdn "cn=admin,dc=example,dc=com"
rootpw password
directory C:/ProgramData/OSSTech/OpenLDAP/data
index objectClass eq
index entryCSN,entryUUID eq
index cn,sn,givenName,uid,ou,mail eq,pres,sub

access to attrs=userPassword
      by anonymous auth
      by * none

access to *
      by * none

database monitor
access to *
      by dn="cn=admin,dc=example,dc=com" read
      by * none
```

2.1 設定ファイルのチェック

LDAP サービス起動前に、設定ファイルの不備を確認する際には、次のコマンドを実行してください。

```
PS C:\> slaptest.exe
```

設定に問題がある場合には、設定ファイルの不備について **bad configuration file!** のメッセージと合わせてエラーメッセージが表示されます。

```
C:\ProgramData\OSSTech\OpenLDAP\etc\slapd.conf: line 85: duplicate index definition for attr "cn"
slaptest: bad configuration file!
```

設定に問題がない場合には、‘config file testing succeeded’ のメッセージが記録されます。

```
config file testing succeeded
```

2.2 OpenLDAP の起動・停止

slapd.conf ファイルの設定が完了したら、LDAP サービスを起動します。LDAP サービスの起動は以下の手順で行います。

1. 管理者権限で PowerShell を起動します。
2. sc コマンドでサービスを起動します。

```
PS C:\> sc.exe start slapd
```

LDAP サービスの停止は以下の手順で行います。

1. 管理者権限で PowerShell を起動します。
2. sc コマンドでサービスを停止します。

```
PS C:\> sc.exe stop slapd
```

2.3 起動確認

LDAP サービスの状態は次のコマンドで行います。

```
PS C:\> sc.exe query slapd

SERVICE_NAME: slapd
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 1   STOPPED
        ...
```

- LDAP サービスが停止している場合、STATE に “1 STOPPED” が表示されます。
- LDAP サービスが起動している場合、STATE に “4 RUNNING” が表示されます。

LDAP サービスの正常起動を確認するために ldapsearch コマンドで接続を確認し、以下の結果が得られることを確認してください。

```
PS C:\> ldapsearch -x -H ldap://localhost
# extended LDIF
#
# LDAPv3
# base <> (default) with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# search result
search: 2
result: 32 No such object
```

```
# numResponses: 1
```

2.4 Windows ファイアウォールの設定

Windows Server の標準設定では、LDAPS(636/TCP) や LDAP(389/TCP) のポートに外部からアクセスできません。

Windows ファイアウォールの「受信の規則」の設定を変更し、外部からの LDAPS/LDAP 通信を許可してください。

2.5 LDAP ログファイル

LDAP サービスから出力されるログは、以下の 2 つのファイルに出力されます。

1. “C:/ProgramData/OSSTech/OpenLDAP/log/slapd.wrapper.log”
2. “C:/ProgramData/OSSTech/OpenLDAP/log/slapd_yyyymmdd.log”

1 の「slapd.wrapper.log」ファイルは、スーパーバイザーが記録した slapd サービスの起動・停止ログとなります。メッセージは以下の形式で記録されます。

```
2025-05-19 10:30:21,284 DEBUG - Starting WinSW in console mode
2025-05-19 10:30:21,552 INFO - Starting C:\Program Files\OSSTech\OpenLDAP\sv\..
\slapd.exe
```

2 の「slapd_yyyymmdd.log」ファイルは、slapd サービスのログメッセージが記録されるログファイルとなり、slapd.conf に設定したログレベルに従いログが記録されます。

```
2025-05-19T12:13:47.265931600 6b8 conn=1000 fd=3 ACCEPT from IP=10.0.3.31:52310
(IP=0.0.0.0:389)
2025-05-19T12:13:47.266333500 6b8 conn=1000 op=0 BIND dn="cn=admin,dc=example,dc=com" method=128
2025-05-19T12:13:47.266439400 6b8 conn=1000 op=0 BIND dn="cn=admin,dc=example,dc=com" mech=SIMPLE bind_ssf=0 ssf=0
2025-05-19T12:13:47.266683200 6b8 conn=1000 op=0 RESULT tag=97 err=0 qtime=0.000100 etime=0.000478 text=
2025-05-19T12:13:47.268850100 6b8 conn=1000 op=1 SRCH base="dc=example,dc=com" scope=2 deref=0 filter="(objectClass=*)"
2025-05-19T12:13:47.269616600 6b8 conn=1000 op=1 SEARCH RESULT tag=101 err=0 qtime=0.000090 etime=0.000866 nentries=5 text=
2025-05-19T12:13:47.272362600 1938 conn=1000 op=2 UNBIND
```

2.6 ログレベルの変更

slapd のログレベルは `slapd.conf` に設定します。設定例:

```
loglevel stats
```

ログレベル	数値	意味
trace	1	関数呼び出しのトレース
args	4	詳細なトレース
conns	8	コネクション管理のログ
filter	32	検索フィルター処理のログ
config	64	設定ファイルの解析ログ
ACL	128	アクセスコントロールのログ
stats	256	接続状況、リクエストのログ
stats2	512	クライアントに対して送信したエントリのログ
parse	2048	エントリ解析のログ
sync	16384	複製処理のログ
none	32768	ログレベルに関係なく記録される重要なログ以外は記録しない
any	FFFFFFFF	全てのログを記録する

ログレベルの変更後、slapd サービスの再起動により反映されます。

2.7 ログディレクトリの変更

`C:/ProgramData/OSSTech/OpenLDAP/etc/slapd.env` に `SLAPD_LOG_DIR` を設定します。

設定例:

```
SLAPD_LOG_DIR = "C:\ProgramData\OSSTech\OpenLDAP\log"
```

2.8 サービスポートの変更

LDAP サーバーは既定で 389 と 636 ポートを利用します。

これを変更したい場合、`C:/ProgramData/OSSTech/OpenLDAP/etc/slapd.env` に `SLAPD_LDAP_SERVICES` を設定します。

設定例:

```
SLAPD_LDAP_SERVICES = "ldap://:10389/ ldaps://:10686/"
```

2.9 スキーマ拡張

スキーマを拡張するには、`C:\ProgramData\OSSTech\OpenLDAP\etc\schema` フォルダ内にスキーマファイルを追加し、`slapd.conf` ファイルに拡張スキーマファイルを `include` 文で取り込む設定を追加してください。

```
include "C:/ProgramData/OSSTech/OpenLDAP/etc/schema/custom.schema"
```

2.10 インデックス再生成

インデックス再作成のため、`slapindex` 相当のコマンドを実行する必要があるときは、次のコマンドを実行してください。

```
PS C:\> slapindex.exe
```

2.11 LDAP データの初期化

LDAP データを初期化したい場合、LDAP サービスを停止後、次のフォルダ内のファイルを全て削除してから LDAP サービスを起動してください。

- `C:\ProgramData\OSSTech\OpenLDAP\data`

2.12 Windows 版 OpenLDAP のアンインストール

アンインストールの際は以下の手順で実施してください。

1. LDAP サービスの停止

```
PS C:> sc.exe stop slapd
```

2. ソフトウェアのアンインストール

Windows の「設定」-「アプリ」-「アプリと機能」から「OSSTech OpenLDAP」を選択してアンインストールを行います。

2.13 Windows 版 OpenLDAP の制限等

2.13.1 複製機能

Windows 版 OpenLDAP では 1 台構成のみをサポートします。複製機能についてはサポートしていません。

2.13.2 利用可能な LDAP クライアントコマンド

Windows 版 OpenLDAP では、以下のコマンドを利用可能です。

コマンド名	用途
ldapadd	LDAP エントリの登録
ldapcompare	LDAP エントリの比較
ldapdelete	LDAP エントリの削除
ldapexop	LDAP 拡張コントロールの送信
ldappasswd	LDAP エントリのパスワード変更
ldapsearch	LDAP 検索
ldapwhoami	LDAP の自分のエントリの認証確認

これらのコマンドは `C:\Program Files\OSSTech\OpenLDAP` フォルダ配下にインストールされます。Windows 版 OpenLDAP インストール時に本フォルダへのパスが設定されますので、コマンド名のみで実行が可能です。

```
PS C:> ldapsearch -x -W -D cn=admin,dc=example,dc=com -b dc=example,dc=com
```

エントリの登録や削除するための LDIF ファイルは、BOM 無しの UTF-8 のファイルとして作成してください。(ノートパッドなどで作成する際に BOM が付かないように注意してください)

2.13.3 パスワードハッシュ化方式

Windows 版 OpenLDAP では以下のハッシュ化方式に対応しています。

- ARGON2
- PBKDF2
- SSHA2(非推奨)
- SSHA(非推奨)

SSHA 及び SSHA2 は互換性の為に利用できますが、利用は推奨されません。

CRYPT 形式には非対応です。

ハッシュ化済みパスワード文字列の生成は次のコマンドで行います。

- ARGON2 形式のハッシュ化済みパスワード文字列の生成

```
PS C:> slapd.exe -T passwd -h '{ARGON2}' -o module-load=pw-pbkdf2.1a -s "パスワード"
```

- PBKDF2 形式のハッシュ化済みパスワード文字列の生成

```
PS C:> slapd.exe -T passwd -h '{PBKDF2-SHA512}' -o module-load=pw-pbkdf2.1a -s "パスワード"
```

- SSHA512 形式のハッシュ化済みパスワード文字列の生成 (非推奨)

```
PS C:> slapd.exe -T passwd -h '{SSHA512}' -o module-load=pw-sha2.1a -s "パスワード"
```

2.13.4 LDAP のバックアップ

Windows 版 OpenLDAP にはバックアップスクリプトによる自動バックアップは含まれていません。適切なタイミングで下記のコマンドで LDAP エントリの全件取得を実施してください。

```
PS C:> slapcat.exe -l backup.ldif
```

上記コマンドを実行する際、PowerShell でリダイレクトを行わないでください。UTF-16 エンコーディングの LDIF が生成され、LDIF ファイルからのリストアができなくなる可能性があります。

2.13.5 LDAP データのリストア

LDIF ファイルを LDAP データとして登録したい場合、次のコマンドで行います「Closing DB ...」のメッセージが表示されるとデータ登録は完了です。

```
PS C:\> slapadd.exe -l backup.ldif
...
Closing DB ...
```