# OpenLDAP パスワードポリシー運用ガイド


オープンソース・ソリューション・テクノロジ(株)

文書番号:　XXXXXX
作成者:　野村　健太郎
更新日:　2013年 3月1日
リビジョン:　2.1

# 目次

# 1. 要旨

本文書はOpenLDAPのパスワードポリシー運用手順書です。

## 1.1 はじめに

本書では以下の環境におけるパスワードポリシーの設定方法について説明します。

- OpenLDAPにおけるパスワードポリシーの設定
- OpenLDAP環境におけるパスワードポリシーの設定方法

なお、本ドキュメントでは必要に応じて以下のような略語を使います。

- Red Hat Enterprise Linux5 を RHEL5と表記します。
- Red Hat Enterprise Linux6 を RHEL6と表記します。

## 1.2 対象環境

### 1.2.1 OS

- RHEL 5（x86/x86_64） もしくは RHEL 6（x86_64）
  - SELinux: 無効
  - ファイアウォール: 無効

### 1.2.2 バージョン

- OpenLDAP 2.4（OSSTech版）

### 1.2.3 ホスト

- LDAPマスターサーバー
  - ホスト名: master.osstech.co.jp
- LDAPスレーブサーバー
  - ホスト名: slave.osstech.co.jp

### 1.2.4 LDAP 基本設定

- suffix: dc=osstech,dc=co,dc=jp
- LDPA 管理アカウント:  cn=ldapadmin,dc=osstech,dc=co,dc=jp

### 1.2.5 パスワードポリシー適用範囲

以下の操作時に、パスワードポリシーが適用されます。

- 各種 LDAP 操作実行時の認証時
- pam_ldap(5)を利用して OS のログインに LDAP 認証を設定している UNIX サーバーでの認証時
- その他、LDAP 認証を行うアプリケーションなどの認証時(Web アプリケーションなど)

# 2.　OpenLDAP のパスワードポリシー設定

本章では、LDAP サーバーのパスワードポリシーを有効にする手順を説明します。

## 2.1 OpenLDAP 設定ファイルの編集

まず、OpenLDAP の設定ファイルである/opt/osstech/etc/openldap/slapd.conf を編集します。

### 2.1.1 パスワードポリシーの有効化

パスワードポリシーを有効にするための設定を記述します。設定ファイルの編集は以下の順序で行います。

1. スレーブサーバーの設定ファイル編集
2. スレーブサーバーの LDAP サーバー再起動
3. マスターサーバーの設定ファイル編集
4. マスターサーバーの LDAP サーバー再起動

設定ファイルの編集内容は以下のようになります。マスターサーバー/スレーブサーバーとも編集内容は同じです。

- パスワードポリシー用スキーマファイルのインクルード

  設定ファイルに以下の行が記述されていることを確認します。記述がない場合は末尾に追記します。

```
include /opt/osstech/etc/openldap/schema/ppolicy.schema
```

- モジュールのロード

  パスワードポリシー機能(ppolicy オーバーレイ)を有効化するためにモジュールをロードする設定を記述します。以下の内容を追記します(コメントアウトされている場合は、コメントアウトを無効化し、設定を有効にします)。

  - 32bit 環境の場合

```
modulepath /opt/osstech/lib/openldap2.4
moduleload ppolicy
```

  - 64bit 環境の場合

```
modulepath /opt/osstech/lib64/openldap2.4
```

```
moduleload ppolicy
```

- パスワードポリシー機能の有効化

  slapd.conf の末尾に以下の内容を追記します。

```
overlay ppolicy
ppolicy_default "cn=DefaultPolicy,ou=Policies,dc=osstech,dc=co,dc=jp"
ppolicy_use_lockout # このオプションの使用は要検討
```

  「ppolicy_use_lockout」は LDAP クライアントにアカウントロックのエラーを返すことを意味するパラメータとなります。場合によっては、サーバーへの攻撃者に有用な情報を返す結果となることもあります。デバッグ時には有用なオプションですが、本番運用へ移行後は、セキュリティを重視する場合はこのパラメータはコメントアウト(もしくは削除)して下さい。詳細は slapo-ppolicy(5) のマニュアルをご参照ください。

編集完了後、LDAP サーバーを再起動します。 スレーブサーバー、マスターサーバーの順で再起動します。

- スレーブサーバー

```
[slave]# /sbin/service osstech-ldap restart
```

- マスターサーバー

```
[master]# /sbin/service osstech-ldap restart
```

## 2.2 パスワードポリシーエントリーの登録

パスワードポリシーの設定はLDAPデータベース内のLDAPデータとして保存されます。

適用されるパスワードポリシーは以下の2つに分かれます。

1. 全ユーザーに適用されるデフォルトのパスワードポリシー(デフォルトパスワードポリシーと呼びます)

2. ユーザー毎に個別に適用されるパスワードポリシー

優先順位は「ユーザー毎に個別に適用されるパスワードポリシー」の方が高くなります。デフォルトパスワードポリシーが設定されている場合でも、ユーザーに個別のパスワードポリシーが設定されている場合は、ユーザーのパスワードポリシーが優先されます。ここでは、それぞれのパスワードポリシーの設定方法を説明します。

### 2.2.1 全ユーザーに適用されるデフォルトパスワードポリシーの登録

まず、以下の内容のLDIFファイルを作成します(ファイル名は任意)。各属性の属性値は設定例です。属性の意味については「3 OpenLDAPパスワードポリシー解説」で説明します。

全ユーザーに適用されるデフォルトパスワードポリシーファイル

```
dn: ou=Policies,dc=osstech,dc=co,dc=jp
objectClass: organizationalUnit
ou: Policies

dn: cn=DefaultPolicy,ou=Policies,dc=osstech,dc=co,dc=jp
objectClass: pwdPolicy
objectClass: organizationalRole
cn: DefaultPolicy
pwdAttribute: userPassword
pwdCheckQuality: 2
pwdMinLength: 8
pwdMaxAge: 7776000
pwdMinAge: 180
pwdExpireWarning: 1209600
pwdLockout: TRUE
pwdMaxFailure: 5
pwdLockoutDuration: 90
pwdFailureCountInterval: 180
pwdInHistory: 3
pwdMustChange: TRUE
```

パスワードポリシーエントリーのDNはslapd.confの「ppolicy_default」ディレクティブで指定したDNと同じDNにします。

ldapaddコマンドにより、LDAPサーバーにLDIFデータを登録します。

```
#/opt/osstech/bin/ldapadd -x -W -D "cn=ldapadmin,dc=osstech,dc=co,dc=jp" -f 作成したLDIFファイル
```

以上でパスワードポリシーの初期設定は完了です。

この時点でパスワードポリシーは有効になります。ただし、パスワード有効期間(pwdMaxAge)に関しては、パスワードポリシー有効後にパスワード変更を行なうことで、有効期間が適用されます。

### 2.2.2 ユーザー毎の個別のパスワードポリシーの登録

ユーザー毎の個別のパスワードポリシーは以下の2通りの方法で管理します。

1. デフォルトパスワードポリシーとは別に、複数ユーザーで共有するパスワードポリシーを作成し、各ユーザーがそのパスワードポリシーを参照するように設定する（以降、「共有パスワードポリシー」と呼ぶ）

2. 各ユーザーエントリーにパスワードポリシーを設定する。そのユーザーに対してのみ有効なパスワードポリシーとなる（以降、「ユーザーパスワードポリシー」と呼ぶ）。

## 共有パスワードポリシーの設定

まず、共有パスワードポリシーエントリーを登録します。以下のようなLDIFファイルを作成します。

```
dn: cn=SubPolicy,ou=Policies,dc=osstech,dc=co,dc=jp
objectClass: pwdPolicy
objectClass: organizationalRole
cn: DefaultPolicy
pwdAttribute: userPassword
pwdCheckQuality: 2
pwdMinLength: 8
pwdMaxAge: 7776000
pwdMinAge: 180
pwdExpireWarning: 1209600
pwdLockout: TRUE
pwdMaxFailure: 5
pwdLockoutDuration: 90
pwdFailureCountInterval: 180
pwdInHistory: 3
pwdMustChange: TRUE
```

ldapaddコマンドにより、LDAPサーバーにLDIFデータを登録します。

```
#/opt/osstech/bin/ldapadd-x -W -D "cn=ldapadmin,dc=osstech,dc=co,dc=jp" -f 作成したLDIFファイル
```

次に、ユーザーがこのパスワードポリシーを参照するように設定します。以下の内容のLDIFファイルを作成します。「username」部分には、共有パスワードポリシーを適用するユーザー名を記述します。

```
dn: uid=username,ou=Users,dc=osstech,dc=co,dc=jp
changetype: modify
add: pwdPolicySubentry
pwdPolicySubentry: cn=SubPolicy,ou=Policies,dc=osstech,dc=co,dc=jp
```

「pwdPolicySubentry」属性に共有パスワードポリシーエントリーのDNを指定します。

ldapmodifyコマンドによりLDAPサーバーにLDIFデータを登録します。

```
[master]# /opt/osstech/bin/ldapmodify -x -W -D "cn=ldapadmin,dc=osstech,dc=co,dc=jp" -f 作成したLDIFファイル
```

以上で完了です。これで該当ユーザーには「cn=SubPolicy,ou=Policies,dc=osstech,dc=co,dc=jp」のパスワードポリシーが適用されます。該当ユーザーにデフォルトパスワードポリシーを適用する場合は、「pwdPolicySubentry」属性を削除します。

### ユーザーパスワードポリシーの設定

ユーザーエントリーにパスワードポリシーパラメターを登録します。以下の内容のLDIFファイルを作成します。「username」部分には、ユーザーパスワードポリシーを適用するユーザー名を記述します。「pwdPolicySubentry」属性が自分自身のDNを指し示している点に注意してください。

```
dn: uid=username,ou=Users,dc=osstech,dc=co,dc=jp
changetype: modify
add: objectClass
objectClass: pwdPolicy
-
add: pwdPolicySubentry
pwdPolicySubentry: uid=username,ou=Users,dc=osstech,dc=co,dc=jp
-
add: pwdAttribute
pwdAttribute: userPassword
-
add: pwdCheckQuality
pwdCheckQuality: 2
-
add: pwdMinLength
pwdMinLength: 8
-
add: pwdMaxAge
pwdMaxAge: 7776000
-
add: pwdMinAge
pwdMinAge: 180
-
add: pwdExpireWarning
pwdExpireWarning: 1209600
-
add:pwdLockout
pwdLockout: TRUE
-
add:pwdMaxFailure
pwdMaxFailure: 5
-
add: pwdLockoutDuration
pwdLockoutDuration: 90
-
add: pwdFailureCountInterval
```

```
pwdFailureCountInterval: 180
-
add: pwdInHistory
pwdInHistory: 3
```

ldapmodify コマンドにより LDAP サーバーに LDIF データを登録します。

```
[master]# /opt/osstech/bin/ldapmodify -x -W -D "cn=ldapadmin,dc=osstech,dc=co,dc=jp" -f 作成した LDIF ファイル
```

以上で完了です。これで該当ユーザーには、自分自身のエントリーに設定されているパスワードポリシーが適用されます。

該当ユーザーにデフォルトパスワードポリシーを適用する場合は、「pwdPolicySubentry」属性を削除します。

ユーザー個別のパスワードポリシーの設定操作は LDAP 管理者で実行する必要があります。一般ユーザーが自分自身のパスワードポリシー(関連の属性)を変更することはできません。

## 2.3 パスワードポリシーの変更

パスワードポリシーは LDAP データベース内で管理されるため、パスワードポリシーを変更する場合は LDAP データベース内のデータを変更する必要があります。ここでは、ldapmodify コマンドを使用してパスワードポリシーを変更する手順を説明します。

例として、連続認証失敗時のアカウントロックに関連するパラメータを変更する手順を説明します。連続して 5 回認証に失敗した場合に 30 分間アカウントロックを行うことを想定します。以下のような LDIF ファイルを作成します。

```
dn: cn=DefaultPolicy,ou=Policies,dc=osstech,dc=co,dc=jp
changetype: modify
replace:pwdLockout
pwdLockout: TRUE
-
replace:pwdMaxFailure
pwdMaxFailure: 5
-
replace: pwdLockoutDuration
pwdLockoutDuration: 1800
```

LDAP 変更操作用の LDIF ファイルの書式については ldapmodify(1)のマニュアルをご参照ください。

続いて、ldamopdify コマンドを実行し、パスワードポリシーの変更を適用します。

```
# /opt/osstech/bin/ldapmodify -x -W -D "cn=ldapadmin,dc=osstech,dc=co,dc=jp" -f 作成したLDIFファイル
```

パスワードの入力が求められるため、LDAPサーバー管理者のパスワードを入力します。

以上で完了です。

ユーザー毎の個別のパスワードポリシーの変更も手順は同様となります。この場合、「cn=DefaultPolicy,ou=Policies,dc=osstech,dc=co,dc=jp」部分をユーザーエントリーのDNに書き換えます。

## 2.4 パスワードポリシーを適用しないユーザー

特定のユーザーだけパスワードポリシーを適用しない設定方法を説明します。

デフォルトパスワードポリシーを登録することで、rootdn(slapd.conf で指定)以外の全てのユーザーにパスワードポリシーが適用されますが、LDAP管理者ユーザーなどにパスワードポリシーを適用させたくない場合には、そのユーザーに対して個別のパスワードポリシー(空のパスワードポリシー)を設定します。

「7.1 LDAP管理用アカウントはパスワードポリシーを適用しない」に、仕様上パスワードポリシーを未適用とするのが望ましいLDAPアカウントに関する説明を記載しております。必ずご検討ください。

まず、以下の内容のLDIFファイルを作成します。
「uid=username,ou=Users,dc=osstech,dc=co,dc=jp」部分には、個別のパスワードポリシーを適用するユーザーのDN(識別名)を記述します。

```
dn: uid=username,ou=Users,dc=osstech,dc=co,dc=jp
changetype: modify
add: pwdPolicySubentry
pwdPolicySubentry: cn=none,ou=Policies,dc=osstech,dc=co,dc=jp
```

「cn=none,ou=Policies,dc=osstech,dc=co,dc=jp」というエントリーは存在しなくてかまいません。

続いて、ldamopdifyコマンドを実行し、パスワードポリシーを適用します。

```
[master]# /opt/osstech/bin/ldapmodify -x -W -D "cn=ldapadmin,dc=osstech,dc=co,dc=jp" -f 作成したLDIFファイル
```

パスワードの入力が求められるため、LDAPサーバー管理者のパスワードを入力します。

以上で完了です。

# 3. OpenLDAP パスワードポリシー解説

本章では、OpenLDAP パスワードポリシーのパラメータなどについて説明します。

## 3.1 パラメータ一覧

パスワードポリシーのパラメータ一覧です。

- **pwdCheckQuality**

  パスワードの構文検査の有効化/無効化を指定。設定値には以下を指定できます。
  ・0 : 検査しない(デフォルト値)
  ・1 : 検査する(ただし、検査が不可能な場合は検査せずに受け入れる)
  ・2 : 検査する(検査が不可能な場合はエラーを返す)
  「検査が不可能な場合」とはクライアント側でパスワードがハッシュ化されている場合などです。
  ldapadd、ldapmodify で ldif ファイルによりパスワードを変更する場合はパスワードを平文で記載する必要があります。その場合、データベースには平文で保存されます。ハッシュ化して保存するためには ldappasswd を使用してください(password-hash パラメータでハッシュ形式を指定しておく必要があります)。

- **pwdMaxAge**

  パスワードの有効期間（秒）を指定。「0」を指定した場合はパスワードの有効期間は無期限となります。デフォルト値は「0」。
  このパラメータを有効にすると最後にパスワードを変更した時刻が記録されます(pwdChangedTime 属性)。パスワードの有効期間は最後にパスワードを変更してからの期間となります。
  なお、最後のパスワード変更時刻は、パスワードポリシー機能を有効化した後にパスワード変更を行うことで記録されるようになります。

- **pwdMinAge**

  パスワードの変更禁止期間(秒)を指定。「0」を指定した場合は禁止期間は設けられません。デフォルト値は「0」。

- **pwdMinLength**

  パスワード最小文字数を指定。「0」を指定した場合、最小文字数の制限はなくなります。このパラメータを有効にするためには、「pwdCheckQuality」パラメータの値を「2」もしくは「1」に設定する必要があります。デフォルト値は「0」。

- **pwdExpireWarning**

  パスワードの期限切れの事前警告期間(秒)を指定。「0」を指定した場合は警告が表示されません。警告期間中、警告メッセージは期限切れ一日前まで表示されます。デフォルト値は「0」。

- pwdLockout
  連続した認証の失敗でアカウントをロックするかどうかを指定。設定値にはTRUEかFALSEを指定します。アカウントロック後のログイン時には、デフォルトではアカウントロックのメッセージは表示されません。デフォルト値はFALSE(アカウントをロックしない)。詳細は「3.2 pwdLockoutに関する補足説明」をご参照ください。
- pwdMaxFailure
  アカウントロックが発動するまでの、連続した認証の失敗回数を指定。「0」を指定した場合、何度失敗してもアカウントをロックされません。デフォルト値は「0」。
- pwdLockoutDuration
  アカウントロックが解除されるまでの期間(秒)を指定。「0」を指定した場合、 管理者が解除しない限りアカウントはロックされたままとなります。デフォルト値は「0」。なお、アカウントロックの解除方法については「3.3 アカウントロックの解除」をご参照ください。
- pwdFailureCountInterval
  認証失敗回数カウンターがリセットされるまでの期間（秒）を指定。「0」を指定した場合、認証に成功しない限りリセットされません。なお、pwdLockoutDurationで指定した時間より短い時間を設定しても、アカウントロックは継続されます。デフォルト値は「0」。
- pwdInHistory
  パスワード履歴保持数を指定。履歴に記録されているパスワードは再利用できません。「0」を指定した場合は履歴を記録されません。デフォルト値は「0」。
- pwdMustChange
  管理者によるパスワードリセット後、最初のbind直後にパスワードの変更を必須とするかどうかを指定。設定値にはTRUEかFALSEを指定します。デフォルト値はFALSE(パスワード変更は要求されない)。なお、管理者によるパスワードのリセット方法については、「6 管理者によるパスワードリセット」をご参照ください。
- pwdGraceAuthnLimit
  期限切れパスワードによる認証(ldap bind)の最大猶予回数を指定。「0」を指定した場合、猶予回数は設けられません。パスワードの期限が切れた後にここで指定した回数bindに失敗すると、bind不可能となります(Password expiredとなる)。デフォルト値は「0」。
- pwdAllowUserChange
  ユーザーによるパスワード変更の許可/禁止を指定。設定値にはTRUEかFALSEを指定します。デフォルト値はTRUE(ユーザーが自分のパスワードを変更できる)。
- pwdSafeModify
  パスワード変更時に変更前のパスワードの入力が必要か不要か指定。設定値にはTRUEかFALSEを指定します。デフォルト値はFALSE(変更前のパスワードの入力は不要)。

## 3.2 pwdLockoutに関する補足説明

### 3.2.1 アカウントロック状態の確認方法

slapd.confに「ppolicy_use_lockout」を記述した場合でも、Linuxホストへのログイン時にはアカウ

ントロックに関するメッセージは表示されません。これは、サーバーのセキュリティを向上させるための仕様となっております。アカウントロックは、パスワードの総当たり攻撃を防止するための仕組みです。OpenLDAP のマニュアルには「アカウントがロックされているという情報を返すことは、攻撃者にとって有利な情報を与えるとになる場合がある」という記述があります。「2.1.1 パスワードポリシーの有効化」の「ppolicy_use_lockout」パラメータに関する説明にも同様の注意書きを記載しております。

アカウントロック時のメッセージを確認する方法として、slapd.conf に「2.1.1 パスワードポリシーの有効化」の「ppolicy_use_lockout」パラメータ記述したうえで、ldapsearch コマンドに"-e ppolicy" オプションを付加して実行するという方法があります。

以下は、アカウントがロックされた状態で、ldapsearch コマンドに "-e ppolicy"オプションを付加して実行した結果です。

```
$ ldapsearch -x -W -D "uid=test01,ou=Users,dc=osstech,dc=co,dc=jp" -LLL -e ppolicy
Enter LDAP Password: ユーザー test01 の正しいパスワードを入力
ldap_bind: Invalid credentials (49); Account locked
```

アカウントロックされているため、ユーザ名/パスワードが正しいにも関わらず「Invalid credentials (49)」となり、アカウントロックに関するメッセージ「Account locked」が表示されます。

### 3.2.2 他のパスワードポリシーに抵触している状態でのアカウントロック

パスワードの有効期限が切れている状態で pwdMaxFailure で指定した回数だけ不正なパスワードを入力するとアカウントロック状態となります。認証失敗回数については以下のような挙動となります。

- パスワードの有効期限が切れた状態であり、かつ、アカウントロックされていない状態の場合、正しいパスワードを入力すると認証失敗回数はリセットされます。
- パスワードの有効期限が切れた状態であり、かつ、アカウントロック状態の場合、正しいパスワードを入力しても認証失敗回数はリセットされません。

### 3.2.3 認証失敗回数のカウントについて

OpenLDAP のパスワードポリシーの実装では、認証に失敗した際、ユーザーのエントリに pwdFailureTime という属性を追加します。この属性の数が、pwdMaxFailure に設定した数に達した場合にアカウントがロックされます。

pwdFailureTime には認証に失敗した時刻を記録します。

- 例 : pwdFailureTime: 20120608040000Z

pwdFailureTime に記録される時刻は秒単位である為、一秒間に記録できる認証失敗回数は 1 度に制限されます。従って、例えば pwdMaxFailure を 5 に設定した場合、最低でも 5 秒間はロックされないとい

う挙動になるため、ご注意ください。

## 3.3 アカウントロックの解除

LDAP 認証に連続して失敗しアカウントがロックされた場合に、ロックを解除する方法を説明します。

アカウントロックの解除方法として、以下の 2 つの方法があります。

1. 一定時間経過後に自動的にアカウントロックを解除する
2. パスワードを変更する
3. LDAP のユーザーエントリーに含まれるアカウントロックを意味する属性を削除する

以降で具体的な手順を説明します。

### 3.3.1 一定時間経過後に自動的にアカウントロックを解除する

「pwdLockoutDuration」属性にアカウントロック解除までの時間を設定します。パラメータの詳細については、「3 OpenLDAP パスワードポリシー解説」をご参照ください。また、解除時間の設定方法については「2.3 パスワードポリシーの変更」をご参照ください。

### 3.3.2 パスワードを変更する

管理者がユーザーのパスワードを変更することで、アカウントロックが解除されます。パスワード変更には ldappasswd コマンドなどを利用します。

### 3.3.3 LDAP のユーザーエントリーに含まれるアカウントロック属性を削除する

アカウントがロックされると、ユーザーエントリーに「pwdAccountLockedTime」という属性が保存されます。この属性を削除することで、強制的にアカウントロックを解除することができます。削除の手順は以下のようになります。

まず、以下の内容の LDIF ファイルを作成します。

```
dn: uid=username,ou=Users,dc=osstechd,dc=co,dc=jp
changetype: modify
delete: pwdAccountLockedTime
```

「uid=username,ou=Users,dc=osstechd,dc=co,dc=jp」部分には、対象ユーザーの DN を記述します。

次に、ldapmodify コマンドを実行して属性を削除します。

```
[master]# /opt/osstech/bin/ldapmodify -x -W -D "cn=ldapadmin,dc=osstechd,dc=co,dc=jp" -f 作成した LDIF ファイル
```

パスワードの入力が求められるため、LDAP サーバー管理者のパスワードを入力します。

以上で完了です。

ユーザーエントリーに pwdAccountLockedTime 属性を登録することで、該当のユーザーを意図的にアカウントロック状態にすることも可能です。pwdAccountLockedTime にはアカウントロックされた日時を GeneralizedTime 型(例：20110621072759Z)で保存します。

### 3.3.4 認証失敗回数のリセットについて

LDAP 管理者が「pwdAccountLockedTime」属性を削除し、強制的にアカウントロックを解除した場合でも、認証失敗回数(LDAP に保存されている)はリセットされません。そのため、
「pwdAccountLockedTime」属性の削除後に、ユーザーが一度でもパスワードを間違えると再びアカウントがロックされてしまいます。

ここでは 認証失敗回数のリセット方法について説明します。リセットするための方法として、以下の3つの方法があります。

1. 一定時間経過後に認証失敗回数をリセットする
2. アカウントロック解除後に正しいパスワードでログインする

#### 一定時間経過後に認証失敗回数をリセットする

強制的アカウントロック解除後にも「pwdMaxFailure」で指定した認証失敗回数分のパスワード入力ミスを許す場合は、「pwdFailureCountInterval」属性を設定します。この属性には認証失敗回数がリセットされるまでの期間(秒)を指定します。そのため、以下のような基準から設定値を決定します。

- 「pwdLockoutDuration」で指定した時間と同じか、それよりも短い時間
    - 一定時間経過後に自動的にアカウントロックが解除された後に、「pwdMaxFailure」で指定した認証失敗回数分のパスワード入力ミスを許可するため
- 「アカウントロック発生 → 管理者により強制的アカウントロック解除」に要する時間よりも短い時間
    - 管理者による強制的アカウントロック解除後に、「pwdMaxFailure」で指定した認証失敗回数分のパスワード入力ミスを許可するため

設定値の変更方法は「2.3 パスワードポリシーの変更」をご参照ください。

#### アカウントロック解除後に正しいパスワードでログインする

アカウントロック解除後に正しいパスワードでログイン(LDAP BIND)することでも、認証失敗回数はリセットされます。

### 注意点

認証失敗回数はユーザーエントリの「pwdFailureTime」という属性で管理されます。この属性は認証に失敗した時刻を複数属性値で保持します。前述の方法で認証失敗回数をリセットすると、この属性もユーザーエントリから削除されます。ただし、この属性をLDAP操作にて直接削除することはできません。

# 4.　OpenLDAP パスワードポリシーレスポンス解説

本章では、パスワードポリシーを有効化した場合に OpenLDAP サーバーが返すレスポンスについて解説します。

## 4.1 LDAP Control/ResponseValue 一覧

応答コントロールの LDAP Control Type は「1.3.6.1.4.1.42.2.27.8.5.1」となる。

[★FIXME★] bindResponse も追記すること(横幅が足りないので、別途エクセル形式の表にまとめ直す予定)。パスワードポリシーに抵触して bind に失敗した場合のレスポンスはいずれも「Invalid credentials(49)」である。

以下の表に、各パスワードポリシーに違反した場合の LDAP Control Value を観す。

| エラー原因 | 応答コントロール<br>(Wireshark によりキャプチャしたパケットから取得) | 応答コントロール<br>(ASN.1 BER デコードされた<br>16 進数文字列) |
|---|---|---|
| 正常時(bind 成功時) | 無し | 30 00 |
| パスワード間違いによる bind 失敗 | 無し | 30 00 |
| パスワードポリシーに抵触した状態で、正しいパスワードを入力した場合 | | |
| パスワード有効期限切れ | error: passwordExpired (0) | 30 03 81 01 00 |
| アカウントロックアウト(※1) | error: accountLocked (1) | 30 03 81 01 01 |
| 次回ログイン時のパスワード変更必要 | error: changeAfterReset (2) | 30 03 81 01 02 |
| パスワードポリシーに抵触した状態で、不正なパスワードを入力した場合 | | |
| パスワード有効期限切れ | 無し | 30 00 |
| アカウントロックアウト(※1) | error: accountLocked (1) | 30 03 81 01 01 |
| 次回ログイン時のパスワード変更必要 | error: changeAfterReset (2) | 30 03 81 01 02 |
| 複数のパスワードポリシーに抵触した状態で、正しいパスワードを入力した場合 | | |
| パスワード有効期限切れ<br>かつ<br>アカウントロック | error: accountLocked (1) | 30 03 81 01 01 |
| パスワード有効期限切れ<br>かつ<br>次回ログイン時のパスワード変更必要 | error: passwordExpired (0) | 30 03 81 01 00 |
| アカウントロック<br>かつ<br>次回ログイン時のパスワード変更必要 | error: accountLocked (1) | 30 03 81 01 01 |

| | | |
|---|---|---|
| パスワード有効期限切れ<br>かつ<br>アカウントロック<br>かつ<br>次回ログイン時のパスワード変更必要 | error: accountLocked (1) | 30 03 81 01 01 |
| 複数のパスワードポリシーに抵触した状態で、不正なパスワードを入力した場合 | | |
| パスワード有効期限切れ<br>かつ<br>アカウントロック | 無し | 30 00 |

※1：アカウントロックの場合の「PasswordPolicyResponseValue」はslapd.confに「ppolicy_use_lockout on」を記述した場合のみに得られる。

# 5. LDAP 対応PAMモジュールの設定

Linux 環境のユーザ認証時に LDAP サーバーのユーザ情報を参照するように設定している(pam_ldap(5) を利用している)場合、パスワードポリシーを適用するためには設定を変更する必要があります。変更対象の設定ファイルはOSのバージョンによって異なります。

- RHEL5: /etc/ldap.conf
- RHEL6: /etc/pam_ldap.conf

上記いずれかの設定ファイルに以下の設定を記述します(該当箇所のみ抜粋)。あるいは、行頭が「#」になっている該当箇所の「#」を削除します。すでにパラメータが別の値で設定されている場合は、以下の値で置換します。

```
pam_password exop
pam_lookup_policy yes
```

以上で完了です。この設定により、Linuxホスト上でpasswdコマンドを実行した時に、LDAPサーバーで設定したパスワードポリシーが適用されます。

なお、それぞれのパラメータの意味は以下のとおりです。

- pam_password exop
  - Linux(LDAPクライアント側)のpasswdコマンドでパスワード変更を実行した際に、LDAPサーバーに対してPassword Modify Operationと呼ばれる拡張操作によるパスワード変更を行うことを意味します。
- pam_lookup_policy
  - PAM経由のLDAP認証時にパスワードポリシーも考慮した認証処理を行います。例えばパスワードの有効期限が切れている場合にはpasswdコマンド経由によるパスワードの変更を強制したうえで、ログインを許可する動作となります。

# 6.　管理者によるパスワードリセット

本章では、管理者が一般ユーザーのパスワードをリセットする方法を説明します。

## 6.1 パスワードリセットの流れ

ここでは、以下のようなパスワードリセットの運用を想定しています。

1. ユーザーが管理者にパスワードリセットを依頼
2. 管理者はLDAPパスワードを変更する(ldappasswdコマンド)
3. 管理者は、ユーザーの次回ログイン時に必ずパスワードを変更させるように設定する
    i. 管理者はLDAPパスワードをリセットしたことを意味する属性をユーザーエントリーに登録する
    ii. 管理者はSambaパスワードをリセットしたことを意味する属性をユーザーエントリーに登録する
4. ユーザーはパスワードリセット後のログイン時に、必ずパスワード変更をしなければならない

以降で詳細な手順を説明します。

## 6.2 新しいパスワードの登録

まず、管理者はldappasswdコマンドでユーザーのパスワードを変更します。

```
[master]# /opt/osstech/bin/ldappasswd -x -W -D “cn=ldapadmin,dc=osstech,dc=co,dc=jp” -S ユーザーのDN
New password:                    <--対象ユーザの新しいパスワード
Re-enter new password:           <--対象ユーザの新しいパスワード
Enter LDAP Password:              <--管理者のパスワード
```

なお、rootdnによりbindした場合、パスワードポリシーを満たさないパスワードも登録可能となっています。

## 6.3 LDAPパスワードのリセット設定

「pwdMustChange」パラメータを利用し、管理者によるパスワードリセット後の初回ログイン時に強制的にパスワードの変更を要求させるするためには、通常のパスワード変更操作に加えて、パスワードリセットを意味する属性をユーザーエントリーに登録する必要があります。具体的には、ユーザーエントリーに「pwdReset」属性を登録し、属性値を「TRUE」に設定します。

以下のようなLDIFファイルを作成します。「uid=username,ou=Users,dc=osstech,dc=co,dc=jp」部分には、パスワードリセットするユーザーのDNを記述します。

```
dn: uid=username,ou=Users,dc=osstech,dc=co,dc=jp
changetype: modify
add: pwdReset
pwdReset: TRUE
```

ldamopdifyコマンドを実行し、パスワードリセット属性をユーザーエントリーに登録します。

```
[master]# /opt/osstech/bin/ldapmodify -x -W -D "cn=ldapadmin,dc=osstech,dc=co,dc=jp" -f 作成したLDIFファイル
```

パスワードの入力が求められるため、LDAPサーバー管理者のパスワードを入力します。

以上で完了です。

Linuxへのログイン時に以下のようなメッセージが表示され、パスワード変更が要求されます。ユーザーはパスワードを変更しなければログインすることはできません。また、この時入力する新しいパスワードはパスワードポリシーを満たしている必要があります。

```
You are required to change your LDAP password immediately.
Last login: Thu Apr  1 21:25:06 2010 from 192.168.170.1
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user testuser.
Enter login(LDAP) password:
```

パスワード変更により、ユーザーエントリーから pwdReset 属性は削除されます。ユーザーがldappasswdコマンドでパスワードを変更することも可能です。

## 6.4 注意点

「pwdMustChange」パラメータを利用する際には以下の点にご注意ください。

- ユーザーエントリーに「pwdReset」属性を登録しても、ldap bindは可能です。認証にLDAPを利用しているアプリケーションなどは、ほとんどの場合においてユーザー認証時にldap bindを実行していることが予想されますが、ldap bindは成功するため、アプリケーションによっては認証が成功し、パスワード変更要求もされない可能性があります。パスワード変更が必要な状態を取得するためには、LDAPクライントがLDAP Controlに対応している必要があります。
- 前述のpam_ldap(5)の例では、pam_ldapがLDAP Controlに対応しているため、OSログイン時にパスワード変更が要求されます。

# 7.　パスワードポリシー設定例

本章では、具体的な運用を想定したパスワードポリシーの設定例を説明します。

## 7.1 LDAP 管理用アカウントはパスワードポリシーを適用しない

弊社の標準 LDAP サーバー環境設定では、以下のエントリーが LDAP 管理用のアカウントとして登録されています。

- LDAP サーバー管理(Inter Process Communication、プロセス間通信) 用エントリー(人間がこのアカウントで直接操作することはない)
  - cn=replica,dc=osstech,dc=co,dc=jp
    - 用途: LDAP データ複製処理用
  - cn=samba,dc=osstech,dc=co,dc=jp
    - 用途: smbldap-tools 処理用
- LDAP サーバー管理者用エントリー
  - cn=ldapadmin,dc=osstech,dc=co,dc=jp
    - 用途: LDAP 管理者
  - uid=Administrator,ou=Users,dc=osstech,dc=co,dc=jp
    - 用途: ドメイン管理者

プロセス間通信用アカウントに関しては、デフォルトパスワードポリシーが適用されないようにした方がよいかもしれません。パスワードの有効期限切れによるレプリケーションのエラー発生など可能性があるためです。

LDAP サーバー管理者用エントリーに関しては、デフォルトパスワードポリシーの適用/未適用はセキュリティ要件などの影響も受けるかと思いますので、ご検討の上、判断して頂くようにお願い致します。

デフォルトパスワードポリシーを未適用とする場合は、「2.2.2 ユーザー毎の個別のパスワードポリシーの登録」、もしくは「2.4 パスワードポリシーを適用しないユーザー」の手順で個別のパスワードポリシーを適用します。LDIF ファイルの DN(識別名)部分に対象のアカウントの DN(例えば、”cn=ldapadmin,dc=osstech,dc=co,dc=jp”)を記述し、ldapmodify コマンドを実行してください。

# 8. SHA-2 パスワードハッシュの利用

弊社 OpenLDAP は独自の改良により、SHA-2 パスワードハッシュに対応しています。本章では、SHA-2 パスワードハッシュ利用のための設定及びコマンドの利用方法について記載いたします。

## 8.1 SHA-2 パスワードハッシュのための設定

以下の通り、slapd.conf のグローバル領域に SHA-2 パスワードハッシュ利用のための設定を記載します。なお、グローバル領域は、最初の「database ～」行より前の位置を指します。編集後、LDAP サーバーを再起動してください。

slapd.conf

```
moduleload pw-sha2
password-hash {SSHA512}
```

password-hash に指定できる SHA-2 形式のスキームは次のものになります。

- {SHA256}
- {SHA384}
- {SHA512}
- {SSHA256}
- {SSHA384}
- {SSHA512}

## 8.2 SHA-2 パスワードハッシュによる文字列の生成

SHA-2 パスワードハッシュによって生成した文字列を取得するためには次のコマンドを使用します。

```
# /opt/osstech/sbin/slappasswd -h '{SSHA512}' -o module-load=pw-sha2
New password:
Re-enter new password:
{SSHA512}pxPSV6J1MEu9Mphe+oMM5ruzjmi2ERRuDF/WrRDLIAL64Gs9CIMe8RfZeqHqR3alpPw+UIwY7Z2hxBCfwDfkXww2wXWD9H8h
```

「-h」オプションの引数には前節のスキームを指定できます。

# 9. 改版履歴

- 2010年3月17日　　野村 健太郎
  - 新規作成
- 2010年3月29日　　野村 健太郎
  - 特定のユーザーにパスワードポリシーを適用しない手順を追記
- 2010年4月1日　　野村 健太郎
  - パスワードリセット方法(pwdReset属性を利用)を追記
- 2010年4月12日　　野村 健太郎
  - 客先提出物の内容をマージ
  - 章構成を変更。ひとまず、完成版とする(リビジョン1.1)
- 2010年10月6日　　野村 健太郎
  - pwdMaxAge(パスワード有効期間)に関する説明を修正
- 2011年1月18日　　野村 健太郎
  - 文書中に記載のOpenLDAPのバージョンを2.4に修正
- 2011年6月6日　　野村 健太郎
  - pwdSaveModifyに関する説明を追記
- 2011年6月16日　　野村 健太郎
  - pwdLockout、pwdGraceAuthnLimitに関する説明を追記
- 2011年6月22日　　野村 健太郎
  - 「2.2.2 ユーザー毎の個別のパスワードポリシーの登録」にpwdPolicySubentryに関する説明を追記。
  - パスワードリセットに関する説明を追記
- 2011年8月23日　　野村 健太郎

- 認証失敗回数のリセットに関する説明を追記

- 2011年8月30日　　野村 健太郎
  - 複数のパスワードポリシーに抵触した状態におけるLDAPレスポンス、LDAP応答コントロールについて追記
- 2012年6月8日　　野村 健太郎
  - 「3.2.3 認証失敗回数のカウントについて」を追記。
- 2012年8月30日　　野村 健太郎
  - リビジョン 1.8
  - 「5 LDAP 対応PAMモジュールの設定」に説明を追記。
- 2012年10月3日　　亀井 裕
  - 大改定によりリビジョンを2.0とする
  - 本手順書よりSamba関連の設定を削除(従来のOpenLDAP + Sambaについての手順書は「OSTD-OpenLDAP-PasswordPolicy-with-Samba」として分離)
  - 「3.1 パラメータ一覧」の体裁を変更
  - 「4 OpenLDAPパスワードポリシーレスポンス解説」の表のうち抜けのある箇所を追記、及び一部修正
  - 「5 LDAP 対応PAMモジュールの設定」にRHEL5/RHEL6それぞれの対応を追記
  - その他細かい修正
- 2013年3月1日　　亀井 裕
  - SHA-2 パスワードハッシュの利用方法について追記