株式会社 XXXX 御中

OpenLDAP + Samba

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:　2012年 10月3日
リビジョン:　2.0

目次

1. 要旨

本文書はOpenLDAP + Samba環境のパスワードポリシー運用手順書です。

1.1 目的

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 + Samba環境におけるパスワードポリシーの設定方法

LDAPに接続しているLinuxクライントとSambaに接続しているWindowsクライアントでは、パスワードポリシーの設定方法と保存先が異なります。

- Linuxクライアント：LDAPに保存
- Windowsクライアント：Sambaのポリシーとして保存(一部、LDAPに保存する設定あり)

本書ではOpenLDAPとSamba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。

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 バージョン

- OpenLDAP 2.4 (OSSTech版)

1.2.2 ホスト

- LDAPサーバー
  - LDAPマスターサーバー兼Samba PDCサーバー(master.osstech.co.jp)
  - LDAPスレーブサーバー兼Samba BDCサーバー(slave.osstech.co.jp)
  - suffix：以下のsuffixを想定

- dc=osstech,dc=co,dc=jp

- LDPA 管理アカウント：以下のアカウントを想定
  - cn=ldapadmin,dc=osstech,dc=co,dc=jp

1.2.3 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)
- Windows ログオン(Sambap パスワードポリシー)
- Windows クライアントからのパスワード変更

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

  以下の行を include ディレクティブ記述部分の末尾に追記します

```
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)をモジュールとして利用する場合はモジュールをロードする必要があります。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)。モジュールとして利用しない場合は、この内容は記述する必要はありません。

  - 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(ppolicy オーバーレイ)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ーとなります。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ーはコメントアウト(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
```

2.1.2 Samba パスワード同期機能の有効化

Linux ホスト上での passwd コマンドによるパスワード変更時に、Samba パスワードも変更されるように以下の設定を行います。LDAP マスターサーバーの 設定ファイルのみ変更します。

- モジュールのロード

  Samba パスワード同期機能(smbk5pwd オーバーレイ)をモジュールとして利用するため、モジュールをロードします。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 smbk5pwd
```

- 64bit 環境の場合

```
modulepath /opt/osstech/lib64/openldap2.4
moduleload smbk5pwd
```

- Samba パスワード同期機能(smbk5pwd オーバーレイ)の有効化

  slapd.conf の末尾に以下の内容を追記します。

```
overlay smbk5pwd
```

編集完了後、LDAP サーバーを再起動します。

```
[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。各属性の属性値は設定例です。属性の意味については「3OpenLDAP パスワードポリシー解説」で説明します。

```
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ーターを登録します。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。

「9.1LDAP 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、貴社の LDAP + Samba 環境の仕様上、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ので、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ーなどについて説明します。

3.1 パラメーター一覧

パスワードポリシーのパラメーター一覧です。

属性名	説明	設定値
pwdCheckQuality	・パスワード構文(パスワードの最小文字数)の検査の有効化/無効化を指定 ・パスワードの最小文字数(pwdMinLength)を指定する場合はこの属性値を「1」もしくは「2」にする	・0 ： 検査しない ・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」：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。
pwdMaxAge	・パスワードの有効期間（秒）を指定 ・パスワードの有効期間が切れた場合は、ログイン時にパスワードの変更を促すメッセージが表示される ・パスワード有効期間が切れたユーザーは、ldap bind に失敗する ・「3.3 pwdMaxAge」参照	・0 ： 無期限(デフォルト)
pwdMinAge	・パスワードの変更禁止期間(秒)を指定 ・passwd コマンドでのパスワード変更時に「Password is too young to change」と表示される	・0 ： 禁止期間なし(デフォルト)
pwdMinLength	・パスワード最小文字数を指定 ・「pwdCheckQuality」パラメーターの値を「2」もしくは「1」に設定する必要がある ・passwd コマンドでのパスワード変更時に「Password fails quality checking policy」と表示される	0 ： パスワードの最小文字数の制限なし(デフォルト)
pwdExpireWarning	・パスワードの期限切れの事前警告期間(秒)を指定 ・期限切れ一日前までであれば、ログイン時に「Your LDAP password will expire in xx day.」と表示される	・0 ： 警告メッセージは表示されない(デフォルト)
pwdLockout	・連続した認証の失敗でアカウントをロックする ・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ない（※1） ・パスワード期限が切れた状態でも、不正	・TRUE ： アカウントをロックする ・FALSE ： アカウントをロックしない(デフォルト)

	なパスワード入力によって認証に連続して失敗するとアカウントがロックされる	
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 ： 何度失敗してもアカウントをロックしない(デフォルト) ・1以上 ： 認証失敗回数
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 ： 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る(デフォルト) ・1以上 ： 指定時間経過後にアカウントロックは解除される
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 (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る)	・0 ： 認証に成功しない限りリセットされない(デフォルト) ・1以上 ： 指定時間経過後にリセットされる
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ない ・passwd コマンドでのパスワード変更時に、履歴に残っているパスワードを入力した場合は「Password is in history of old passwords」と表示される	0 ： 履歴を記録しない(デフォルト)
pwdMustChange	・管理者によるパスワードリセット後の最初の bind の直後にパスワードを変更しなければならない ・管理者によるパスワードのリセット方法については、「8 管理者によるパスワードリセット」を参照 ・ログイン時に以下のメッセージが表示される 「You are required to change your LDAP password immediately. WARNING: Your password has expired. You must change your password now and login again!」	・TRUE：パスワードリセット後の初回 bind 時にパスワード変更を要求する ・FALSE：パスワード変更を要求されない(デフォルト)
pwdGraceAuthnLimit	・期限切れパスワードによる認証(ldap bind)の最大回数を指定	・0：パスワードの有効期限が切れた場合はログイン不

	・パスワード期限が切れた後に、この回数の bind に失敗すると、bind 不可能となる(Password expired となる)	可能 ・1 以上：パスワードの有効期限が切れた後に許可するログインの回数
pwdAllowUserChange	・ユーザーによるパスワード変更の許可/禁止を指定	・TRUE：ユーザーが自分のパスワードを変更できる(デフォルト) ・FALSE：ユーザーは自分のパスワードを変更できない。管理者のみ、ユーザー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	・TRUE：変更前のパスワードの入力が必要 ・FALSE：変更前のパスワードの入力は不要(デフォルト)

(※1)：slapd.conf に「ppolicy_use_lockout」を記述した場合でも、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。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「ppolicy_use_lockout」を記述した状態で、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。

3.2 pwdCheckQuality

pwdCheckQuality 属性を 1 または 2 に設定した場合の、各種 LDAP 操作の挙動を説明します。

- 属性値が 2 の場合
  - ldapadd コマンド
    - パスワードポリシーを満たすパスワードである必要がある(パスワード文字数)
  - ldapmodify コマンド
    - userPassword 属性変更時には、パスワードポリシーを満たすパスワードである必要がある。
  - ldapadd、ldapmodify コマンド実行時の LDIF ファイルの userPassword 属性の記述方法
    - LDIF ファイルにはパスワードを平文で記述する必要がある。LDIF ファイルに記載するパスワードをハッシュ化しているとエラーが発生する。当然、LDAP サーバーにも平文で保存される。

- ldappasswd コマンド
  - パスワード変更時にはパスワードポリシーを満たすパスワードである必要がある。
  - 変更後のパスワードは、slapd.conf の password-hash パラメータで指定したハッシュ形式で LDAP サーバーに保存される
- エラーメッセージ
  - いずれのコマンドの場合も、エラー発生時には、「Constraint violation (19) additional info: Password fails quality checking policy」というエラーメッセージが表示される。

3.3 pwdMaxAge

パスワードの有効期限は、以下のようなルールで各ユーザー毎に決定されます。

- パスワードポリシーを有効にすると、ユーザーエントリーにはパスワード変更時の時刻が記録されます(pwdChangedTime 属性)。この属性はパスワードポリシー機能(ppolicy オーバーレイ)を有効化した後に、パスワード変更を行なうことで記録されるようになります。そのため、各ユーザーはパスワードポリシー機能の有効化後に一度パスワードを変更する必要があります。
- パスワード有効期間のパラメーターである「pwdMaxAge」は、各ユーザーの前回パスワード変更日時からのパスワード有効期間を意味します。各ユーザーのパスワード有効期限は、前回パスワード変更時点からの経過時間で決定されます。そのため、有効期限はユーザにより異なり、pwdMaxAge の設定値によっては、パスワード有効期間(pwdMaxAge)を設定した時点でパスワードの有効期限が切れるユーザーが存在する可能性もあります。

3.4 pwdLockout

3.4.1 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「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。

3.4.2 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。

3.4.3 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。

3.5 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。

3.5.1 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。パラメーターの詳細については、「3OpenLDAP 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。

3.5.2 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。

3.5.3 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。

3.5.4 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（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（ASN.1 BER デコードされた 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	[★FIXME★]	[★FIXME★]
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 かつ	error: accountLocked (1)	30 03 81 01 01

アカウントロック		
パスワード有効期限切れ かつ 次回ログイン時のパスワード変更必要		30 08 A0 03 80 01 00 81 01 02
アカウントロック かつ 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 かつ アカウントロック かつ 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 かつ アカウントロック	error: accountLocked (1)	30 03 81 01 01

※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. Samba のパスワードポリシー設定

本章では、Samba ドメインのパスワードポリシーを有効にする手順を説明します。Samba のパスワードポリシーは /opt/osstech/bin/pdbedit コマンドで設定可能です。pdbedit コマンドは Samba PDC サーバー上で実行します。

5.1 Samba 設定ファイルの編集

パスワード履歴を LDAP で一元管理するために以下の設定を行います。

Samba の設定ファイルである /opt/osstech/etc/samba/smb.conf に以下のパラメータを記述します。設定ファイルはマスターサーバーと全てのスレーブサーバーで編集する必要があります。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。

```
ldap passwd sync = only
```

編集完了後、Samba サーバーを再起動します。

- マスターサーバー

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

- スレーブサーバー(以下は owl12 のみの例ですが、全てのスレーブサーバーの LDAP サーバーを再起動します)

```
[owl12]# /sbin/service osstech-smb restart
```

このオプションは Samba 側でのパスワード変更時(Windows クライアントからのパスワード変更、smbpasswd コマンドによるパスワード変更)に、Samba サーバー側で LDAP ユーザー用のパスワードのみを変更するオプションです。「2.1.2 Samba パスワード同期機能の有効化」で LDAP サーバー側の Samba パスワード同期機能を有効にしていることから、Samba 側でパスワード変更が実行されると、以下のような流れで LDAP と Samba のパスワードが変更されます。

1. Samba 側でパスワード変更が実行される
2. Samba は LDAP サーバーに存在するユーザーエントリーの LDAP パスワードのみ変更する
3. LDAP サーバーは、LDAP パスワードが変更されると、同ユーザーエントリーの Samba パスワードを変更する
4. パスワード変更が完了する

このような動作により、常に LDAP パスワードと Samba パスワードが同じパスワードになります。また、パスワード履歴も LDAP 側で一元管理されます。

smb.conf で「ldap passwd sync = yes」と設定されている場合、Samba に対するパスワード変更(smbpasswd コマンド/Windows クライアントからの変更)でパスワード履歴は Samba と LDAP のパスワード履歴両方が更新されます。しかし、pam_ldap を設定した Linux 上の passwd コマンドでパスワードを変更した場合は LDAP のパスワード履歴しか更新されません。パスワードの有効期限が切れた際に、Linux コンソールログイン/SSH ログインプロンプトでパスワード変更が要求されパスワード変更した場合も、同様に LDAP のパスワード履歴しか更新されません。この場合、Samba と LDAP でパスワード履歴に差異が発生し、問題が発生する可能性があります。

「ldap passws sync = only」とすることで、結果的にパスワード履歴が LDAP のパスワード履歴で一元管理されることになり、Linux ホスト/Windows クライアントのどちらからパスワードを変更しても、パスワード履歴に差異が発生しないようになります。

また、「ldap passws sync = only」とすることで、Samba 側でのパスワード変更時には、Samba ではなく LDAP 側のポリシー(パスワード変更不可能期間、パスワードの文字数制限、パスワード履歴の保存数)が適用されます。そのため、これらのポリシーは Samba 側には設定しません。

5.2 パスワード有効期限

パスワードの有効期限を秒数で指定します。例は 7 日間です(60x60x24x7=604800)です。

```
[master]# /opt/osstech/bin/pdbedit -P "maximum password age" -C 604800
```

5.3 パスワードの有効期限切れの警告日数

パスワードの有効期限切れの警告日数は Samba では変更できません。Windows 既定となっており、Windows 側のレジストリ変更が必要となります。詳細は以下の Web サイトをご参照ください。

- http://support.microsoft.com/kb/135403/ja

5.4 ユーザーロックアウトまでのパスワード試行回数

指定回数パスワードを間違えるとロックアウトされます。例は 5 回です。

```
[master]# /opt/osstech/bin/pdbedit -P "bad lockout attempt" -C 5
```

5.5 ユーザーロックアウトの時間

ロックアウトは辞書攻撃などパスワード総当たりを防ぐためにあるため、管理者が介在せず時間で解除されるほうが手間が少ないと思われます。時間は分で指定します。例は 30 分です。

```
[master]# /opt/osstech/bin/pdbedit -P "lockout duration" -C 30
```

管理者が手動で解除する場合は以下のコマンドを実行します。

```
[master]# /opt/osstech/bin/pdbedit -z ユーザー名
```

5.6 ログオンに失敗したカウンタのリセット間隔

最後のログオン失敗から指定時間(分)経過したら、ログオン失敗カウンタをリセットします。例は30分です。

```
[master]# /opt/osstech/bin/pdbedit -P "reset count minutes" -C 30
```

5.7 パスワード変更不可能期間

LDAP サーバーのパスワードポリシーが適用されます。

5.8 パスワードの文字数制限

LDAP サーバーのパスワードポリシーが適用されます。

5.9 パスワード履歴の保存数

LDAP サーバーのパスワードポリシーが適用されます。

6. 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。

- 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。

7.　smbldap-tools の設定

OpenLDAP にパスワードポリシーを設定した場合、smbldap-tools ではユーザーの登録、パスワードの更新操作でエラーが発生するようになります。

smbldap-tools はユーザー登録・更新・パスワード変更時に、ハッシュ化したパスワードを LDAP サーバーに対して送信しますが、OpenLDAP サーバー側で「pwdCheckQuality」パラメーターの値を「2」に設定した場合は、送られてきたパスワードが検査不可能なパスワードであると判断され、エラーが返るためです。

これを回避するためには、smbldap-tools の設定ファイルに記述する LDAP 操作実行アカウントを rootdn(slapd.conf の”rootdn”パラメータで指定)にします。rootdn による操作であれば、OpenLDAP サーバー側のパスワードポリシーを回避できるためです。

設定を変更する手順は以下のようになります。

/opt/osstech/etc/smbldap-tools/smbldap_bind.conf を以下のように編集します。

```
slaveDN="cn=Manager,dc=osstech,dc=co,dc=jp"
slavePw="XXXXX"
masterDN="cn=Manager,dc=osstech,dc=co,dc=jp"
masterPw="XXXXX"
```

XXXXX の部分には、/opt/osstech/etc/openldap/ldap.secret に記載されているパスワードを記入します。

注意点として、この設定を行った場合、パスワードポリシーに違反したパスワードも登録可能となります(正確には、パスワード文字数がポリシーを満たしていなくても登録可能です)。前述の通り、rootdn による操作であれば、OpenLDAP サーバー側のパスワードポリシーを回避できるためです。

ポリシーに違反したパスワードによる運用を回避するために、「3OpenLDAP パスワードポリシー解説」の「pwdMustChange」を利用することを推奨します。このパラメーターを「TRUE」に設定することで、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、ユーザーに対して強制的にパスワードの変更を要求します。パスワードを変更しなければ、ユーザーはログインできません。管理者によるパスワードリセットの手順については、「8 管理者によるパスワードリセット」をご参照ください。

8.　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。パスワードのリセットはLDAPパスワードとSambaパスワードそれぞれに対して行う必要があります。

8.1 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パスワードとSambaパスワードを変更する(smbldap-passwd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。

8.2 新しいパスワードの登録

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

```
[master]# /opt/osstech/sbin/smbldap-passwd ユーザー名
```

このとき、「7smbldap-toolsの設定」の設定を行っているため、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。

8.3 LDAPパスワードのリセット設定

「pwdMustChange」パラメーターを利用し、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。

8.4 Samba パスワードのリセット設定

以下のコマンドを実行します。

```
[master]# /opt/osstech/sbin/smbldap-usermod -B 1 ユーザー名
```

ユーザーはパスワードリセット後の初回 Windows ログイン時にパスワードの変更を要求されます。

8.5 注意点

「pwdMustChange」パラメーター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。

9.　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。

9.1 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。

10.　社内動作検証情報

以降の章の内容は、弊社内において、動作検証を行った際の調査情報です。お客様向け資料では以降の内容は削除してください。

11.　一般ユーザーによるパスワード変更

一般ユーザーによるパスワードの変更方法として、以下の方法が存在します。

パスワード変更方法	使用可能な認証環境
passwd コマンド	・LDAP ・LDAP + Samba ドメイン
smbpasswd コマンド	・LDAP + Samba ドメイン
Windows クライアント上でのパスワード変更	・LDAP + Samba ドメイン

ここでは、それぞれの方法の利用手順と注意点を説明します。

11.1 passwd コマンドによるパスワード変更

「6LDAP 対応 PAM モジュールの設定」の設定を行えば、Linux ホスト上から passwd コマンドを実行することで LDAP のパスワードが変更されますが、Samba のパスワードは変更されません。そのため、Linux と Windows のパスワードが異なる状態が発生します。

passwd コマンドの実行により Samba のパスワードも変更する場合は、「2.1.2Samba パスワード同期機能の有効化」の設定を行います。

passwd コマンドの使用について、次の注意点があります。

smb.conf で「ldap passwd sync = ldap」と設定し、かつ Samba 側でパスワード履歴の保存を有効にしている場合、passwd コマンドでパスワードを変更しても、Samba 側のパスワード履歴は更新されません。

11.2 sbmpasswd によるパスワード変更

smbpasswd コマンドを使用することで、LDAP パスワードと Samba パスワードの両方を変更することが可能です。

```
[master]$ /opt/osstech/bin/smbpasswd
Old SMB password: 古いパスワードを入力
New SMB password: 新しいパスワードを入力
Retype new SMB password: 新しいパスワードを入力
Password changed for user testuser
```

smbpasswd コマンドの使用について、次の注意点があります。

smb.conf で「ldap passwd sync = ldap」と設定している場合、smbpasswd コマンドはまず Samba パス

ワードを変更し、次にLDAPパスワードを変更します。ことのき、何らかの原因でLDAPパスワードの変更に失敗すると、Sambaパスワードの変更のみ成功し、LDAPパスワードは古いままとなってしまいます。LDAPパスワードの変更に失敗する原因として、LDAPサーバーのパスワードポリシーの違反が考えられます。

また、OpenLDAPとSambaのパスワード履歴保存を有効にしている場合、smbpasswdコマンドであればOpenLDAPとSamba両方のパスワード履歴が更新されます。

12.　パスワード履歴について

OpenLDAP と Samba でパスワード履歴の保存を有効にした場合、パスワード変更の手段により履歴保存の挙動が異なります。ここでは、各パスワード変更手段における、パスワード履歴保存について説明します。

なお、以下を前提条件とします。

- OpenLDAP と Samba 両方でパスワード履歴の保存を有効にしている
- OpenLDAP で smbk5pwd オーバーレイを有効にしている(passwd コマンドでのパスワード変更により、OpenLDAP と Samba のパスワードが変更される)
- smb.conf に以下のパラメーターを設定している(以下の２パターン)

  1. ldap passwd sync = yes
  2. ldap passwd sync = only

12.1 smb.conf の「ldap passwd sync = yes」の場合

パスワード履歴の更新は以下のようになります。

パスワード変更手段	OpenLDAP の履歴	Samba の履歴
passwd コマンド	更新される	更新されない
smbpasswd コマンド	更新される	更新される
Windows クライント上での変更	更新される	更新される
smbldap-tools（管理者のみ）	更新される	更新されない

パスワード変更時のパスワード履歴のチェックは以下のようになります。

パスワード変更手段	OpenLDAP の履歴	Samba の履歴
passwd コマンド	チェックする	チェックしない
smbpasswd コマンド	チェックする	チェックする
Windows クライント上での変更	チェックする	チェックする

smbldap-tools（管理者のみ）	チェックしない	チェックしない

smbldap-tools によるパスワード変更は rootdn 権限で実行されるため、パスワードポリシーが適用されません。

12.2 smb.conf の「ldap passwd sync = only」の場合

パスワード履歴の更新は以下のようになります。

パスワード変更手段	OpenLDAP の履歴	Samba の履歴
passwd コマンド	更新される	更新されない
smbpasswd コマンド	更新される	更新されない
Windows クライント上での変更	更新される	更新されない
smbldap-tools（管理者のみ）	更新される	更新されない

パスワード変更時のパスワード履歴のチェックは以下のようになります。

パスワード変更手段	OpenLDAP の履歴	Samba の履歴
passwd コマンド	チェックする	チェックしない
smbpasswd コマンド	チェックする	チェックしない
Windows クライント上での変更	チェックする	チェックしない
smbldap-tools（管理者のみ）	チェックしない	チェックしない

smbldap-tools によるパスワード変更は rootdn 権限で実行されるため、パスワードポリシーが適用されません。

13. 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
  - 「3.4.3 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
  - 「6 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2.0とする
  - 本文書名を「OSTD-OpenLDAP-PasswordPolicy」から「OSTD-OpenLDAP-PasswordPolicy-with-Samba」に変更
  - 「6 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