PacSec/Core05

2005年11月15日および16日

セキュリティ体制をベースにした現代的軽量ディレクトリ アクセス プロトコルの構築

アンドレア バリザーニ
ヒンドゥー インフラストラクチャー チーム
<lcars@gentoo.org>

注意：
本書に記載のスクリプト、コマンド、あるいは構成は、すべて用例として処理しなければなりません。つまり、自己責任で利用しなければならないのです。 利用環境に関係なく、利用するときは事前にコードをすべてチェックしてください。

LDAPとは？

- 軽量ディレクトリ アクセス プロトコルのことです。
- ディレクトリ サービスのアップデートや検索に利用されるシンプルなプロトコルです。
- 高速性、信頼性、最小限のアップデート（ロック不要）、およびTCP上での起動を目的として設計されました。
- ディレクトリは記述的で属性をベースにした情報が搭載されたデータベースです。
- もっとも広範に利用されているオープン ソースのOpenLDAPをカバーします。OpenLDAP以外のオプションとしてはレッド ハットのフェドーラ ディレクトリ サーバー、アクティブ ディレクトリ、オラクルの インターネット ディレクトリ、およびiPlanetのディレクトリ サーバーがあります。..

LDAP ディレクトリへのエントリー

- エントリーは唯一識別できる名称DNで参照される属性のコレクションです。
- ディレクトリのエントリーは階層的なツリー構造で構成されています。

```
dn: cn= マネージャー、 dc=pacsec 、 dc=jp
オブジェクト クラス：組織の役割
オブジェクト クラス：単純セキュリティ オブジェクト
cn：マネージャー
ユーザー パスワード: e320499feefewFEWFDSFDSFdfje4
```

- ここにcnは共通名称であり、一方dcはドメイン コンポーネントです。
- 属性はオブジェクト クラスの一環として定義され、オブジェクトや関連属性はスキーマの中でグループ化されます。

LDAP ディレクトリ：その利用法

- ユーザー アカウントの保存：
- ユニックスのアカウント属性（uidNumber、gidNumber、ユーザー パスワードなど）
- マイクロソフト ウインドウズのアカウント属性（サンバ スキーマの使用）
- アパッチの認証属性（mod_ldapの使用）およびメール ルーティング属性
- カスタム属性（gpgKey、 gpgFingerprint、ロケーションなど）
- sshの認可キー（sshPublicKey）
- ユニックスのグループ保存
- sudo構成の保存
- 最終目標は世界中に点在するLDAPサーバーのユーザーを管理できるクロス プラットフォームの認証です。その際、サーバー プールでアクションを起こす必要はありません。（Nサーバーシナリオへのユーザー登録あるいはユーザー削除に対する拡張性）

LDAPの複雑性：
管理責任者の多くが適正に作業することが困難な理由

- マニュアルが乱雑の極みに達している。
- 正確なマニュアルが不足している。ユーザー、開発者、およびセキュリティの専門家に頼っています。
- 現存するマニュアルは時に正確ではないことがあります。
- 通常、重要機能を実行する際、文書化されていない機能を使わなければなりません。

（ただし、ソースコードを文書の一種と見るなら別ですが。）

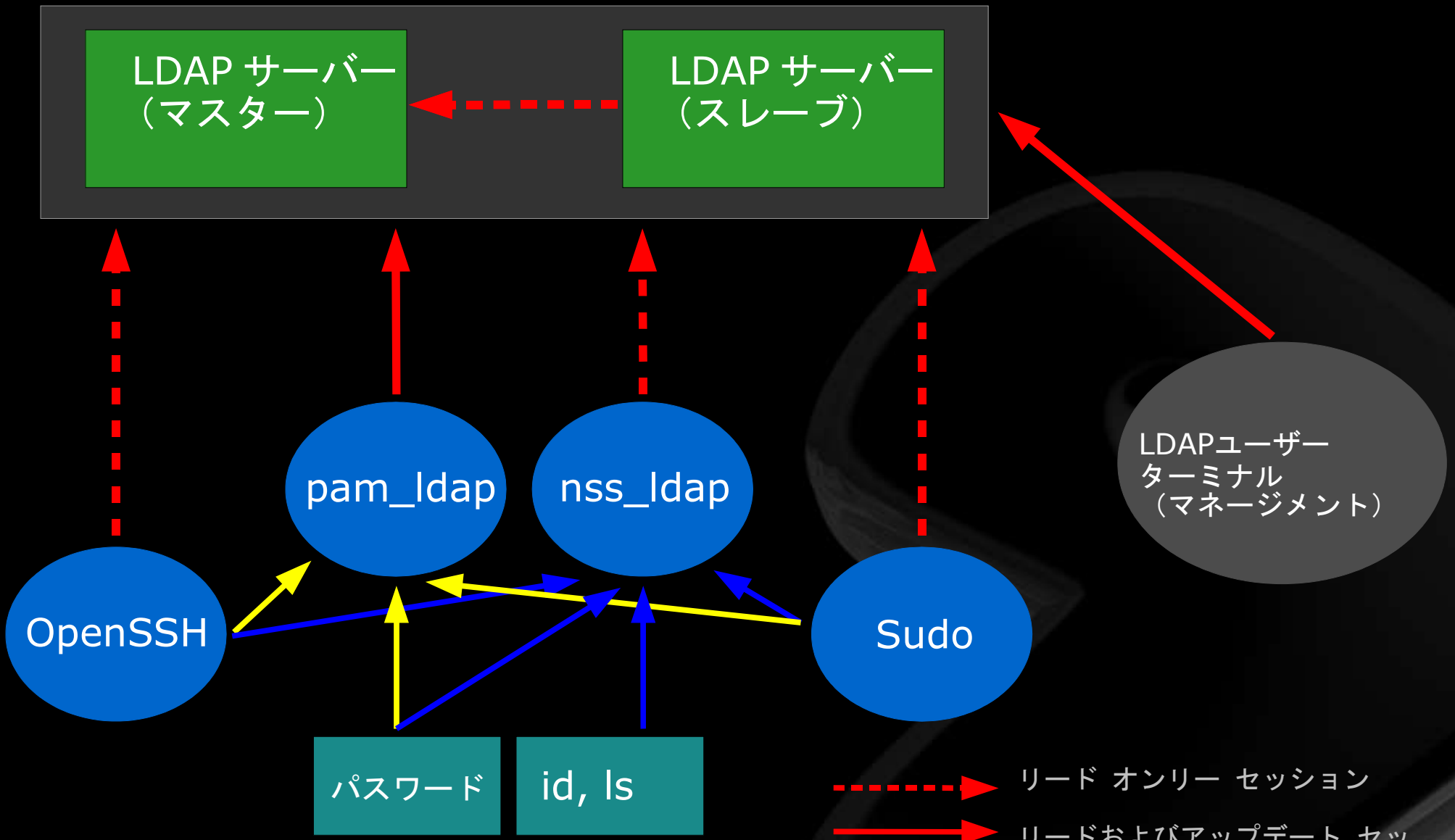
- 様々なコンポーネント レイヤーやソフトウエア レイヤーの多くが完全な基礎構造の中に包含されています。そのため、ディバッグは予想よりも難しいのです。
- LDAPソフトウエアに関するメーリング リストやフォーラムに共通する疑問やエラーの喧騒はかなり大きいものがあります。
- LDAPの機能や問題点の一般的な把握が不正確なオペレーションにつながっている場合があるのです。

LDAPの複雑性：

それでは、LDAPを利用しようとする理由は何か？

- それほど悪くはないからです。（脅威を感じさせる必要があると感じていました。その程度が、必要以上だったとお考えください。） 1 度でも問題なく機能すれば、 LDAP は強固な事業グレードのフレームワークとなります。
- マニュアルには問題がありますが、セントラル アカウント マネージメント システムとしては信頼性があり、安全性も高いのです。あるいは、それ以上かもしれません。
- LDAPのフレームワークを正確に実行すれば、ユーザー管理のセキュリティを効率的に高めることができます。（特に、NIS/YPから移動したときは安全性が強固になります。）
- 高い拡張性
- acl、 ipベース、および ソケット ベースのアクセス制限、TLS、utf-8サポート、カスタム データベース バックエンド、および複製
- openssh-lpkやsudoなどのように認識が高まれば、将来、LDAPによるアプリケーションや良質のマニュアルが期待されます。

フレームワーク


LDAP サーバー
（マスター）
LDAP サーバー
（スレーブ）
pam_ldap
nss_ldap
LDAPユーザー
ターミナル
（マネージメント）
OpenSSH
Sudo
パスワード
id, ls
リード オンリー セッション
リードおよびアップデート セッション

ソフトウエア バージョン

- openldap-2.2.28
- nss_ldap-239 / pam_ldap-180
- openssh-4.1p1 | openssh-4.0p1 | openssh-3.9p1 + openssh-lpkパッチ

参照：http://www.opendarwin.org/en/projects/openssh-lpk

- sudo-1.6.8p9
- 我々のシステム改善によって、ヒンドゥー バージョンでは重大エラーの多くが補正されました。これらの問題は深刻な製造環境に影響を与えるところでした。
- 参照追跡の安全性が改善されました。（GLSA 200507-13 | CAN-2005-2069）
- sudoの作業フェイルオーバーを作業

参照：http://dev.gentoo.org/~lcars/misc/sudo-ldap_timelimit.diff

セキュリティ パッチ：
CAN-2005-2069

- この問題はTLSに影響を与えています。（SSL上のLDAPには問題があると見られていることから、TLSはデフォルト選択となっています。）
- マスターおよびスレーブのセットアップ用書き込みはマスターが処理します。しかし、ユーザー ターミナルは時として最初にスレーブに接続され、エントリーをアップデートするとき、新しいマスター用ウエブ サイトに参照されます。
- 参照接続でTLSを起動すべきなのでしょうか?（ウエブ サイトに情報はありません。）
- pam_ldap/nss_ldapは起動には影響しません。しかし、OpenLDAPのマニュアルにはそうすべきとの記述がありません。（バグ1）
- いずれにしろ、OpenLDAPでは起動できません。初期接続を除き、このバグによってTLSを起動することができません。（バグ2）
- アプリケーションの相関バグ
- 参照を追跡しているとき、結果は自由に転送されたパスワードとなります。

セキュリティ パッチ：
CAN-2005-2069

- 誰も気づかない理由
- 2005年10月1日時点の現状
- 多くのソフトウエア メーカーはpam_ldapおよびOpenLDAPのパッチを極めてすばやく提供しています。（ただし、nss_ldapの問題を多くのメーカーが解決していません。）
- pam_ldap/nss_ldapの管理用ツールは問題を解決するのに1ヶ月近くかかりました。（ただし、最初の警告と共にパッチは既に入手可能です。）
- OpenLDAPのパッチはまだリリースされていません。(ただし、共同開発中です。)
- バグは1ヵ月半以上無視されてきました。
- 上流段階に遡って解決しない理由は？

http://dev.gentoo.org/~lcars/ldap/nss_ldap-239-tls-security-bug.patch

http://dev.gentoo.org/~lcars/ldap/pam_ldap-176-fix-referral-tls.patch

http://dev.gentoo.org/~lcars/ldap/openldap-2.2.26-tls-fix-connection-test.patch

OpenLDAPの構成：
スキーマの拡張

- 独自のオブジェクト識別子の取得 (OID):1.3.6.1.4.1.2242.1.1.1
- 属性： 1.3.6.1.4.1.2242.1.1.*
- オブジェクト クラス：1.3.6.1.4.1.2242.1.2.*

属性タイプ(1.3.6.1.4.1.22242.1.1.4
名称：アクセス レベル
DESC ：ユーザー アクセス レベル（カスタム スキーマ）
等価性：caseIgnoreMatch
SUBSTR： caseIgnoreSubstringsMatch
シンタックス1.3.6.1.4.1.1466.115.121.1.15)

- 可能なら、既存スキーマの属性を使用してください。

オブジェクト クラス：(1.3.6.1.4.1.22242.1.2.1
名称：pacsecユーザー
DESC：pacsecユーザー
補助が必要な要素（アクセス レベル$など）
MAY： （gpgkey $ gpgfingerprint $など）

http://www.alvestrand.no/objectid/1.3.6.1.4.1.1466.115.121.1.html
http://www.iana.org/assignments/enterprise-numbers

OpenLDAPのslapd構成

- /etc/openldap/slapd.confはOpenLDAPのデーモン プロセス用コンフィグレーション ファイルです。なお、このデーモン プロセスはLDAPのリクエスト(slapd)に対応します。

- 利用するスキーマを追加しなければなりません。

追加するスキーマは以下の通りです。
/etc/openldap/schema/core.schema
/etc/openldap/schema/cosine.schema
/etc/openldap/schema/inetorgperson.schema
/etc/openldap/schema/nis.schema
/etc/openldap/schema/custom.schema
/etc/openldap/schema/sudo.schema
/etc/openldap/schema/opensshlpk. schema

- イニシャル テストでは冗長ログは有用であると見られています。ただし製造中は、冗長ログの機能をはずすか、適正値に設定しなければなりません。

ログ レベル：256
#ログ レベル：0

OpenLDAPのslapd構成：
トランスポート レイヤーのセキュリティ(TLS)

- 暗号化のないトラヒックは禁止です。すべての接続はTLS で保護されています。

セキュリティ： tls を 1 に設定してください

- 認証機構（CA)が承認した認証ファイル（ルート ユーザーやslapdユーザーでは読み込みに限定されたファイルです）が必要です。

TLS認証ファイル：/etc/openldap/ssl/cert.pem
TLS認証キー ファイル：/etc/openldap/ssl/req.pem
TLS CA認証ファイル：/etc/openldap/ssl/ca.pem

- トランスポートの保護のほかに、ユーザー ターミナルも認証したいと思います。認証を目的としてネットワーク レイヤーに依存したいとは思わないからです。

TLSが確認したクライアントの要求

- サーバー サイドでハッシングするパスワードの使用は可能です。この機能はいわゆるパスワード修正用拡張オペレーションのために利用されるのです。ただし、この機能はユーザー ターミナル サイドで有効化する必要があります。

パスワード：ハッシュ「MD5」

OpenLDAPのslapd構成：
アクセス リスト (ACL)

- ACLのシンタックスは完全なものとはいえず、最初は混乱するかもしれません。しかし、大変強力で、ほどよく柔軟性があります。したがって、その事例を見てください。

- 選択書き込みのアクセスを認め、どこでも読める保護属性：

```
dn.subtree=”ou=users,dc=pacsec,dc=jp” attrs=”accessLevel”へのアクセス

その方法は以下の通りです。
dn.subtree=”ou=admin,ou=users,dc=pacsec,dc=jp” \ peername.regex=”10\.1\.7\.1” write
dn.subtree=”ou=admin,ou=users,dc=pacsec,dc=jp” \ sockurl.exact=”ldapi://%2var%2run%2openldap%2slapd.sock” write
読み込み
```

- 認証ユーザーだけが読める保護属性

```
dn.subtree”dc=pacsec,dc=jp” attrs=”userPassword”へのアクセス

その方法は以下の通りです。
dn.subtree=”ou=admin,ou=users,dc=pacsec,dc=jp” \ peername.regex=”10\.1\.7\.1” write
dn.base=”cn=syncrepl,dc=pacsec,dc=jp” \ peername.regex=”10\.1\.7\.2” read
自己書き込み
```

OpenLDAPのslapd構成：
アクセス リスト (ACL)

- ユーザー アクセスの書き込みを認め、どこでも読める保護属性：
dn.subtree=”dc=pacsec,dc=jp” attrs=”sshPublicKey,gpgkey”へのアクセス
その方法は以下の通りです。
dn.subtree=”ou=admin,ou=users,dc=pacsec,dc=jp” \ peername.regex=”10\.1\.7\.1”
write
自己書き込み
読み込み

- その他aclエントリー以降の全領域にかかわるポリシー（発注要件です。）

読み込みへのアクセス
その方法は以下の通りです。
dn.subtree=”ou=admin,ou=users,dc=pacsec,dc=jp” \ peername.regex=”10\.1\.7\.1”
write
読み込み

- 特定のユーザーやユーザー グループにエントリーや属性への選択的アクセスを許可することができます。（特定ボックスへのアクセスおよびファイル システム認証のマッチングが必要です。）ただし、これまで、IPアドレスやソケット名によって規制（TLS認証に一致する基幹ホスト名によって規制が強化されています。）を受けています。

OpenLDAPのslapd構成：
バックエンド データベース

- データベースにさまざまなバックエンドを選択することができます。各バックエンドのデータ構造やオプションは異なっています。デフォルトではbdbが選択されています。（現在、シンク複製エンジンによる複製ではbdbは必要な選択肢となっています。）

データベース：bdb
サフィックス：dc=pacsec,dc=jp
ディレクトリ：/var/lib/openldapdata
セッション ログ：100 500
インデックス：オブジェクト クラス、uid、uidNumber、gidNumber、アクセス レベル pres、eq
インデックス：エントリーUUID pres、eq
キャッシュ サイズ：10000
サイズ上限：1000

- 初期データベースの作成にはrootdn/rootpwを一時的に使用することができます。ただし、配置するときはrootdn/rootpwは消去しなければなりません。aclをすべてバイパスするからです。

rootdn：cn=Manager,dc=pacsec,dc=jp

OpenLDAPのslapd構成：
スレーブ サーバー

- slurpdは標準選択と考えられていますが、プッシュ ベースのシステムであり（マスターによるスレーブのアップデート）拡張性はなく、ネットワーク問題を適正に処理することができません。

- シンク複製エンジンは最適の選択肢を提供します。シンク複製エンジンはプル ベース（スレーブがマスターからアップデートを取り出す方式）であり、アクセスコントロールが最適です。

- ダミーのrootdnを使用します。その際、シンク複製エンジンによってスレーブ用データベースを書き込むとき、パスワードは使用しません。スレーブ上に書き込みオペレーションを実行する際のアクセスはマスターに参照されます。

アップデートリファレンス：ldap://ldap1 pacsec.jp:389
データベース：bdb
rootdn：cn=Replication,dc=pacsec,dc=jp..

- slurpdは標準選択と考えられていますが、プッシュ ベースのシステムであり（マスターによるスレーブのアップデート）拡張性はなく、ネットワーク問題を適正に処理することができません。

- シンク複製エンジンは最適の選択肢を提供します。シンク複製エンジンはプル ベース（スレーブがマスターからアップデートを取り出す方式）であり、アクセスコントロールが最適です。

- ダミーのrootdnを使用します。その際、シンク複製エンジンによってスレーブ用データベースを書き込むとき、パスワードは使用しません。スレーブ上に書き込みオペレーションを実行する際のアクセスはマスターに参照されます。

アップデートリファレンス：ldap://ldap1 pacsec.jp:389
データベース：bdb

OpenLDAPのslapd構成：
スレーブ サーバー

- ridはマスターslapd.conf sessionlog idと一致します。

- 重要な（ただし、OpenLDAP 2.2ではマニュアルなし）再トライ機能は再接続時間を規定します。（最初の10回までは60秒で、11回以降の接続では300秒ですが、+の定義はありません。）

シンク複製エンジンのrid：100
プロバイダー：ldap://ldap1.pacsec.jp:389
タイプ：リフレッシュのみ
インターバル：00:00:00:60
再トライ：60 10 300 +
上限時間：10
サーチベース：dc=pacsec,dc=jp
アップデートdn：cn=Replication,dc=pacsec,dc=jp
バインドdn：cn=syncrepl,dc=pacsec,dc=jp
バインド方法：シンプル
認証：パスワード
startssl：重要

- マスターaclsに対するアクセスの認可

その方法は以下の通りです。
dn.base=”cn=syncrepl,dc=pacsec,dc=jp” \ peername.regex=”10\.1\.7\.2” read

OpenLDAP クライアント ライブラリー用 コンフィグレーションおよびディレクトリ アクセス

- /etc/openldap/ldap.confはクライアント用ライブラリーのコンフィグレーションです。

ベース：dc=pacsec, dc=jp
ウエブ サイト：ldap://ldap1.pacsec.jp ldap://ldap2.pacsec.jp
TLS_REQCERTの要求
TLS_CACERT： /etc/openldap/ssl/ca.pem
上限時間：5

- サーバー認証が必要です。再度申し上げますが、ネットワーク レイヤーを信頼することはできないからです。

- /root/.ldaprcのルートにはクライアントの認証仕様が必要です。（その他のユーザーには後続の「認証」で説明します。）また、この認証は閲読可能にしてはなりません。

TLS認証： /etc/openldap/ssl/cert.pem
TLSキー： /etc/openldap/ssl/req.pem

- 初期ディレクトリはslapadd|slapmodify（バックエンドへの直接アクセス）あるいはldapadd|ldapmodifyで構成することができます。

LDAPの初期化：組織ユニット（OU）

- init.ldif

```
dn: dc=pacsec,dc=jp
オブジェクトクラス : organization
オブジェクトクラス : dc オブジェクト
o: pacsec.jp
dc: pacsec

dn: ou= ユーザー ,dc=pacsec,dc=jp
オブジェクトクラス : 組織ユニット
ou: devs

dn: ou=groups,dc=pacsec,dc=jp
オブジェクトクラス : 組織ユニット
ou: グループ

dn: ou=SUDO 利用者 ,dc=pacsec,dc=jp
オブジェクトクラス : 組織ユニット
ou: SUDO 利用者

dn: ou=admin,ou=users,dc=pacsec,dc=jp
オブジェクトクラス : 組織ユニット
ou: infra
```

```
dn: cn=syncrepl,dc=pacsec,dc=jp
オブジェクトクラス : 組織の役割
オブジェクトクラス : シンプル セキュリティ オブジェクト
cn: syncrepl
ユーザーパスワード : {SSHA}s83JkijBCAEE3409...
構造的オブジェクトクラス : 組織の役割
```

オブジェクトクラス

- 必要な組織部門やシンク複製エンジンdnエントリーを作成して、ディレクトリ階層を初期化します。

```
slapadd -p -w -l init.ldif
```

```
ldapadd -Z -W \
 -D “cn=Manager,dc=pacsec,dc=jp” \
 -f init.ldif
```

LDAPの初期化：
ユーザー エントリー

dn: uid=lcars,ou=admin,ou=users,dc=pacsec,dc=jp
cn: アンドレア バリザーニ
ファーストネーム：アンドレア
sn：バリザーニ
オブジェクト クラス：トップ
オブジェクト クラス：パーソン
オブジェクト クラス：組織人
オブジェクト クラス：inet組織人
オブジェクト クラス：posixAccount
オブジェクト クラス：pacsecUser
オブジェクト クラス：ldapPublicKey
ユーザー パスワード: {crypt}$1$2f93D3A30fBCAEE34r3rf
ログイン シェル：/bin/bash
gidNumber: 100
uidNumber: 660
uid: lcars
gecos: アンドレア バリザーニ
gpgkey: 0x864C9B9E
gpgfingerprint: 0A76 074A 02CD E989 CE7F AC3F DA47 578E 864C 9B9E
記述：開発者トリエステ、イタリア
電話番号：(555) 593 342 430
アクセス レベル：サーバー1.pacsec.jp
アクセス レベル：サーバー2.pacsec.jp
sshパブリック キー：sshdss
AAAAB3NZdjoie293t4tjfdklofj997438o9t5ru43ioyf8439Dr333...

nss_ldap / pam_ldapのコンフィグレーション

- /etc/ldap.confはnss_ldapおよびpam_ldapのコンフィグレーションに利用する共通ファイルで、閲読可能にしなければなりません。また、/etc/nsswitch.confはnssデータベース検索の順序を規定します。
- /etc/ldap.confファイルは/etc/openldap/ldap.confとは一切関係がありません。
- 誤字やエラーはエラー表示されません。シンタックス チェックは高すぎると考えられているからです。
- nss_ldapは名称サービス スイッチ コードで利用されるCライブラリーの拡張で、LDAPディレクトリへの透明アクセスを提供します。また、その目的はユーザーやグループ（getpwent、 getgrentなど）に関係する標準Cライブラリーの機能です。
- アプリケーションがLDAPディレクトリに対する認証が必要なとき、pam_ldapはそのアプリケーションにリンクされたPAM モジュールです。
- クライアントに欠陥が生じた場合、アクセス レベル属性にフィルターをかけます。その目的は選択的にユーザーのクライアント サイド利用のオン/オフを切り替え、ユーザー アカウンティングを防ぐことにあります。また、slapd上で一定の細粒度aclが必要となります。

nss_ldap / pam_ldapのコンフィグレーション

- /etc/ldap.conf

```
ldap_バージョン：  3
スコープ：サブ
上限時間：3
バインド上限時間：3
バインド ポリシー：ハード
非稼働時間の上限：3600
PAMログイン属性：uid
PAMメンバー属性：gid
PAMパスワード：md5
#PAMパスワード：exop
PAMフィルター：アクセス  レベル=サーバー1.pacsec.jp
ウエブ サイト：ldap://ldap1.pacsec.jp ldap://ldap2.pacsec.jp
サフィックス：dc=pacsec,dc=jp
ベース：ou=users,dc=pacsec,dc=jp?sub
nssベースのパスワード：ou=users,dc=pacsec,dc=jp?sub?accessLevel=server1.pacsec.jp
nssベースのシャドウ：ou=users,dc=pacsec,dc=jp?sub?accessLevel=server1.pacsec.jp
nssベースのグループ：ou=users,dc=pacsec,dc=jp?sub?accessLevel=server1.pacsec.jp
ssl：スタートtls
tlsチェック  ピア：イエス
tls_cacertfile：  /etc/openldap/ssl/ca.pem
tls_cert：  /etc/openldap/ssl/cert.pem
TLSキー：  /etc/openldap/ssl/req.pem
```

- 再度申し上げますが、tlsや認証確認を強力に推し進めます。
- クライアント サイドのアクセス レベルにフィルターをかけます。
- ルートのためにクライアント認証を規定します。
- PAMパスワードexopを利用すればslapdパスワード用ハッシュが可能になります。

プラグ化可能な認証モジュール用コンフィグレーション

- /etc/pam.d/system-auth

認証にはpam_env.soが必要です。
認証にはpam_ldap.soで充分です。
認証にはpam_unix.so likeauth nullok nodelay use_first_passで充分です。
認証にはpam_deny.soが必要です。

アカウントにはpam_ldap.soで充分です。
アカウントにはpam_unix.soが必要です。

パスワードにはpam_cracklib.so retry=3が必要です。
パスワードにはpam_unix.so nullok md5 shadow use_authtokで充分です。
パスワードにはpam_ldap.so use_authtokで充分です。
パスワードにはpam_deny.soが必要です。

セッションにはpam_limits.soが必要です。
セッションにはpam_unix.soが必要です。
セッション用オプションにはpam_ldap.soがあります。

● /etc/pam.d/sshd（ホーム ディレクトリがなくなった場合、自動的に作成します。）
セッションにはpam_mkhomedir.so skel=/etc/skel/ umask=0077が必要です。

OpenSSHのコンフィグレーション

- LPK 用パッチ（Ldap 公開キー）を搭載した OpenSSH は ssh 公開キー属性（複数キーには値が複数になります）を調べ、その属性を認証キー ファイルとして使用します。（ファイルをマニュアルで作成する、あるいはコピーするは必要ありません。）

- 一致するエントリーがなくとも、ハードウエア上の認証キー用ファイルは依然として利用されます。

- 最新のopenssh用lpkパッチを使用すれば、そのコンフィグレーションを目的として/etc/ldap.confを構文解析することができます。（サポートする設定：uri、ベース、上限時間、バインド用上限時間、ssl、およびスタートtls）

- 情報は公開されていますので、属性は閲読可能で、ユーザーは利用に合わせて修正することができます。..

- /etc/ssh/sshd_config

```
...
```

PAMの利用：イエス
LPKの利用：イエス
LpkLdapConf /etc/ldap.conf

sudo用コンフィグレーション

- SudoはLDAPディレクトリの中でsudo利用者の設定を調べることができます。
- ハードディスク上のファイルを管理することはできませんが、主に、sudoプロファイルの管理や問い合わせをすることができます。

- 一致するエントリーがなくとも、ハードウエア上のsudo利用者ファイルは依然として利用されます。（ローカルsudo利用者無視属性を無効にすることはできますが、お勧めできません。物理的なフェイルセーフのエントリーを確保すれば安全です。）

- コンパイル時間（withldapconffile=/ etc/ldap.conf.sudo）に分離コンフィグレーション ファイルを有効にすることをお勧めします。その目的は、スーパー ユーザーだけに（標準的な/etc/sudoers認可と同様に）にsudo属性の閲読禁止にすることにあります。

- sudoエントリーにアクセスするために、認証を使用して分離したLDAP用プロファイルを作成します。

sudo用コンフィグレーション

- ou を保護するために、 sudo エントリーおよび新規ユーザー用新規 ou を作成します。

aclを使用して :

dn.subtree=”ou=sudoers,dc=pacsec,dc=jpへのアクセス
その方法は以下の通りです。
dn.base=”cn=sudoers,dc=pacsec,dc=jp” read
dn.subtree=”ou=admin,ou=users,dc=pacsec,dc=jp” \
peername.regex=”10\.1\.7\.1” write
dn.base=”cn=syncrepl,dc=pacsec,dc=jp” \ peername.regex=”10\.1\.7\.2”
read

dn: ou=sudo 利用者 ,dc=pacsec,dc=jp
オブジェクトクラス： 組織ユニット
ou: SUDO 利用者

dn: cn=sudo 利用者 ,dc=pacsec,dc=jp
オブジェクトクラス： 組織の役割
オブジェクトクラス： シンプル セキュリティ オブジェクト
cn: sudo 利用者
ユーザー パスワード: {SSHA}i38fdaf8923prfWE...
構造的オブジェクトクラス： 組織の役割

dn:cn=admin,ou=SUDO 利用者 ,dc=pacsec,dc=jp
cn: 管理者
オブジェクトクラス： トップ
オブジェクトクラス : sudo の役割
sudo ユーザー : lcars
sudo ホスト : cvs.pacsec.jp
sudo オプション： 全て
sudo オプション： 認証

dn:cn= メール l,ou=SUDO 利用者 ,dc=pacsec,dc=jp
cn: メール
オブジェクトクラス： トップ
オブジェクトクラス : sudo の役割
sudo ユーザー : foo
sudo の起動対象： メール
sudo ホスト メール .pacsec.jp
sudo コマンド : /usr/bin/newaliases
sudo オプション : ! 認証

sudo用コンフィグレーション

- /etc/ldap.conf.sudo

ldap_バージョン： 3
上限時間：3
バインド上限時間：3
ウエブ サイト：ldap://ldap1.pacsec.jp ldap://ldap2.pacsec.jp
ssl：スタートtls
tlsチェック ピア：イエス
tls_cacertfile： /etc/openldap/ssl/ca.pem
tls認証： /etc/openldap/ssl/cert.pem
TLSキー： /etc/openldap/ssl/req.pem
binddn： cn=sudoers,dc=pacsec,dc=jp
bindpw：<パスワード>
sudo利用者のベース：ou=SUDO利用者,dc=pacsec,dc=jp
sudo利用者のディバッグ：2

- binddnおよびbindpwが結合しているとき、sudo属性だけが視認できます。

- /etc/ldap.conf.sudoは /etc/sudoersの認可と一致しなければなりませんが、閲読可能にしてはなりません。
- （/etc/ldap.confの場合とは異なります。）

ネーム サービス キャッシュ用デーモン（**nscd**）および クライアント認証

- 稼動中のサーバーでシステムがgetpwnam(3)、getpwuid(3)、および類似したlibc機能を実行すると、パフォーマンスに大きな影響を与える可能性があります。なお、libc機能とはnss_ldapがLDAPサーバーに照会する動作のことを指します。

- nscdはこうした照会をキャッシュに保存するのです。

- あらゆる種類の照会がキャッシュされます。（TTLを/etc/nscd.confにセットすることができます。）

- 新規アカウントの照会に時間がかかった場合を除き、以下の条件下でnscdは問題を起こす場合があります。
  nscdの使用
  ユーザー特権のオン/オフ切り替え
  nscdの存在を無視

- /etc/init.d/nscd再起動やnscdの無効化は有用です。

- 認証データはキャッシュされません。

- nscd を利用すると、各ユーザーに認証を発行しないで、ルート用認証と pam 認識アプリケーションだけを保存することができます。しかし、nscd はトランスペアレントなプロキシキャッシュとして機能するので、nss_ldap を直接起動することはできないのです。

フェイルオーバーのシナリオ

- uri仕様では、最初は常に直近のslapdサーバーを使用してください。
- ネットワークの接続がダウンすると、すべてのサーバーは順次接続を図ろうとします。したがって、2台をこえるスレーブ サーバーの保有はお勧めできません。
- LDAPサーバーが接続不全に陥ったとき、ログイン時のタイムアウトを防ぐために、sshd LoginGraceTimeを規定値に設定しなければなりません。（3台のLDAPサーバーを使用しているとき、少なくとも120秒は設定しなければなりません。）
- 起動時、sudoおよびopensshは少なくとも2台のLDAPと結合するので、timelimit/bind_timelimitの設定には3秒が妥当だと思われます。
- TCP/IPやICMPがネットワークから接続をはずされていないのに、LDAPサーバーが完全に機能しないときが最悪となります。（問題のシステム管理者によってローカル ファイアウォールが混乱したときと類似しています。こうしたことは起こりがちなのです。）
- LDAPに問題がある場合、ホイール アカウントはLDAPやローカルで保存しておかなければなりません。

何かご質問は?