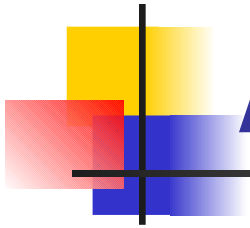
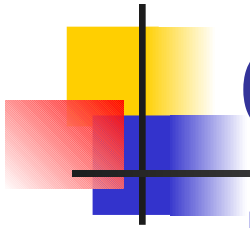
OpenLDAPの最新動向

日本LDAPユーザ会
関口　薫



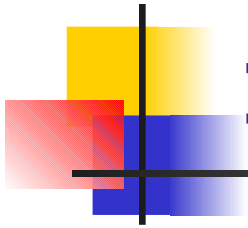
Agenda

- OpenLDAPの紹介
- OpenLDAPの最新機能
  - Configuration Backend
  - Password Policy
  - Access Log
  - Referential Integrity
- OpenLDAPのロードマップ



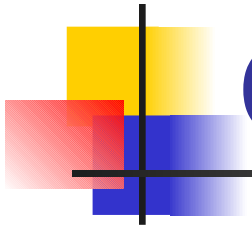
OpenLDAPとは

- 1998年からミシガン大学のUmich LDAPをもとに開発を開始
- LDAPソフトウェアスイート
  - LDAPサーバ：LDAPサーバ、データ管理用コマンド
  - LDAPライブラリ：LDAPアクセス用ライブラリ
  - LDAPクライアント：LDAPデータ操作コマンド類
- 主な機能
  - LDAP v3対応
  - 複数バックエンドデータベースを使用可能
  - SASL認証
  - SSL/TLS暗号化通信
  - レプリケーション



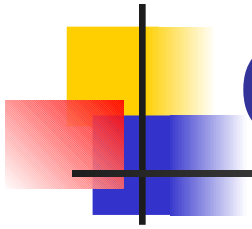
コミュニティ概況

- OpenLDAP Foundationを中心に開発
  - Core Team：3名
    アーキテクチャの方針決定、開発プロセスの管理
  - Engineering Team：13名
    主要な開発メンバ
- LDAPの新機能に対する標準化活動
  - IETFに対する提案
  - 機能の一部はRFCとして標準化
- 活動状況
  - メーリングリストによる活発な議論
    - ユーザ用：十数通／日
    - 開発者用（バグ報告含む）：十数通／日



OpenLDAPの最新機能

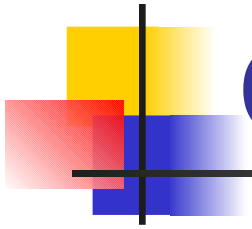
- OpenLDAP 2.3の新機能
  - Configuration Backend
  - Password Policy
  - Access log
  - Referential Integrity



OpenLDAPの準備

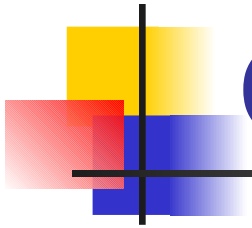
- OpenLDAP 2.3の最新機能を使用するため次の手順でインストールを行う

```
# tar zxvf openldap-2.3.35.tgz
# cd openldap-2.3.35
# ./configure --enable-overlays
# make
# make depend
# make install
```



Configuration Backend

- サーバ設定をデータベースに格納、管理する機能
  - OpenLDAP 2.2まではslapd.confというテキストファイルを直接編集することで設定
- 設定変更時にサーバの再起動が不要
- リモートからLDAPプロトコルによる設定変更が可能



Configuration Backend 設定

- slapd.confに以下の設定を追加

```
database    config
rootdn      cn=config
rootpw      secret
```

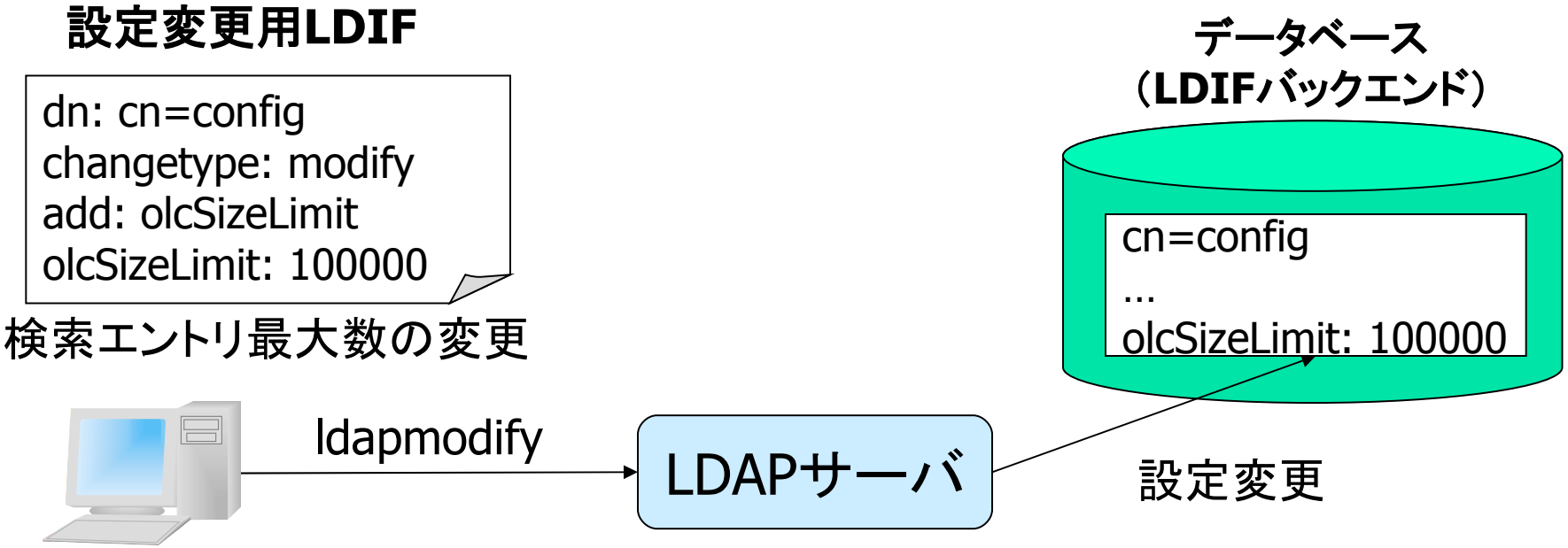
- 設定データベースの作成
  - LDIFバックエンドDBとして作成

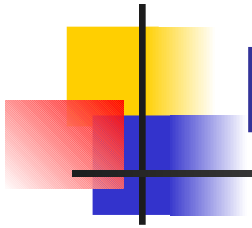
```
# mkdir /usr/local/etc/openldap/slapd.d

# slaptest –f /usr/local/etc/openldap/slapd.conf
–F /usr/local/etc/openldap/slapd.d
```

Configuration Backend 使用法

- LDAPのmodifyにより設定を変更可能
- LDAPサーバデーモンの再起動不要





Password Policy

- パスワードで認証を行う際のポリシーを定義可能
- 定義可能なポリシー
  - パスワード最小文字数
  - パスワード履歴
  - パスワード有効期間
  - パスワード変更禁止期間
  - 認証失敗時のアカウントロックアウト

Password Policy 設定 (1)

- ポリシー情報をLDAPに登録

```
dn: cn=Policy,dc=test,dc=com
objectClass: device
objectClass: pwdPolicy
cn: Policy
pwdAttribute: userPassword
pwdMinLength: 6          # パスワード最小文字数
pwdInHistory: 3          # パスワード履歴数
pwdMaxAge: 2592000       # パスワード有効期間
pwdMinAge: 604800        # パスワード変更禁止期間
pwdLockout: TRUE         # アカウントロック機能有効
pwdMaxFailure: 3         # アカウントロックまでの認証失敗回数
```

※　ポリシー情報を登録するにはppolicy.schemaが必要

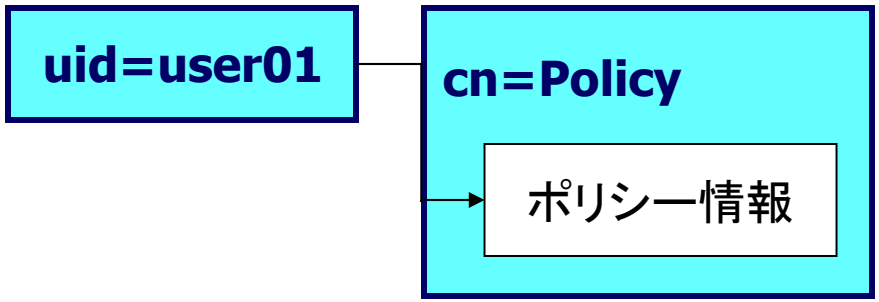
Password Policy 設定(2)

- slapd.confに以下の設定を追加

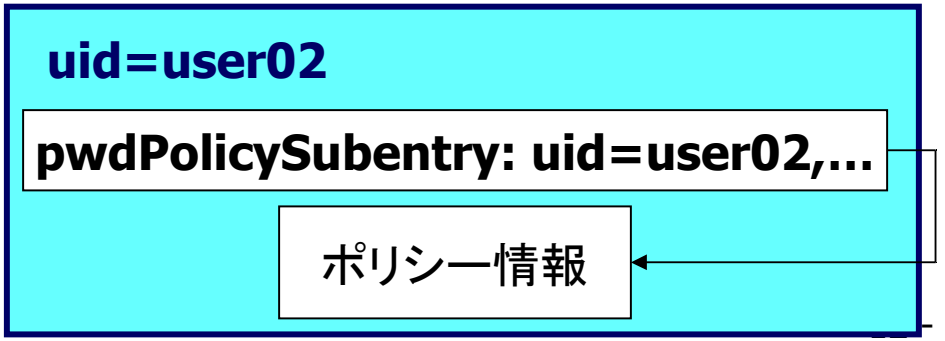
```
overlay     ppolicy

# 共通に使用するパスワードポリシー
ppolicy_default     cn=Policy,dc=test,dc=com
```

共通のパスワードポリシー



ユーザ毎のパスワードポリシー



Password Policy 使用法

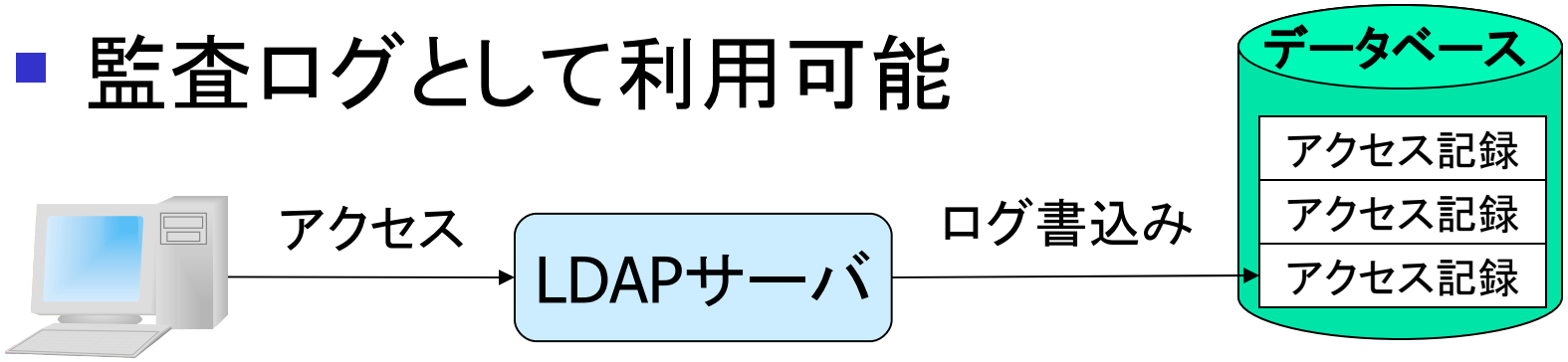
- パスワードポリシーの使用
  - LDAPクライアントコマンドの実行時に“-e ppolicy”を付加

```
$ ldapsearch –x –D
‘uid=user01,ou=People,dc=example,dc=com’ –
w xxx –b ‘’ –e ppolicy
```

- LDAPクライアントアプリケーションからの使用
  - bind実行時にパスワードポリシー用のコントロール情報を付加する必要がある
  - 現在パスワードポリシー用APIが提供されているのはC言語のみ

Access Log

- アクセスのログをデータベースに記録
- 記録対象の情報
  - writes: add、delete、modify、modrdn
  - reads: compare、search
  - session: abandon、bind、unbind
- 監査ログとして利用可能



Access Log 設定

- slapd.confに以下の記述を追加

```
database    bdb
suffix       cn=log
rootdn       cn=Manager,cn=log
rootpw       secret
directory    /usr/local/var/openldap-log
index        reqStart  eq

overlay      accesslog
logdb        cn=log       # ログ用DBのsuffix
logops       wirtes       # 記録対象の情報
# 更新前の情報を記録するエントリ(フィルタで指定)
logold       (objectClass=Person)
```

Access Log データ項目

- ログの参照

```
$ ldapsearch –x –b ‘cn=log’
```

データ項目	説明
reqStart	アクセス開始時間
reqFind	アクセス終了時間
reqType	アクセスの種類（add、modify、delete等）
reqAutzID	アクセスを実行したユーザのDN
reqDN	アクセス先エントリのDN
reqresult	アクセスに対するLDAPのリターンコード
reqMod	add、modifyによって書き込んだ内容
reqOld	更新前の内容

Access Log 性能への影響

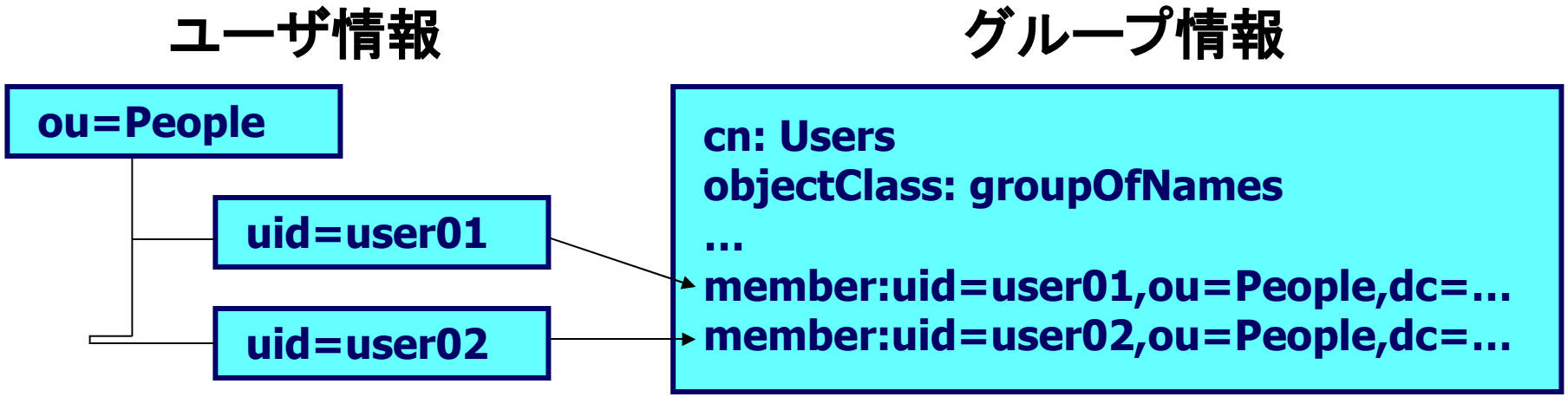
- Access Log無効、有効での性能比較
  - ldapadd、ldapmodify、ldapdeleteの処理時間を測定
  - エントリ数：10000件
  - エントリサイズ：約600B

	ldapadd	ldapmodify	ldapdelete
Access Log無効（秒）	84	39	88
Access Log有効（秒）	149	100	158
処理時間増加率（%）	77	156	80

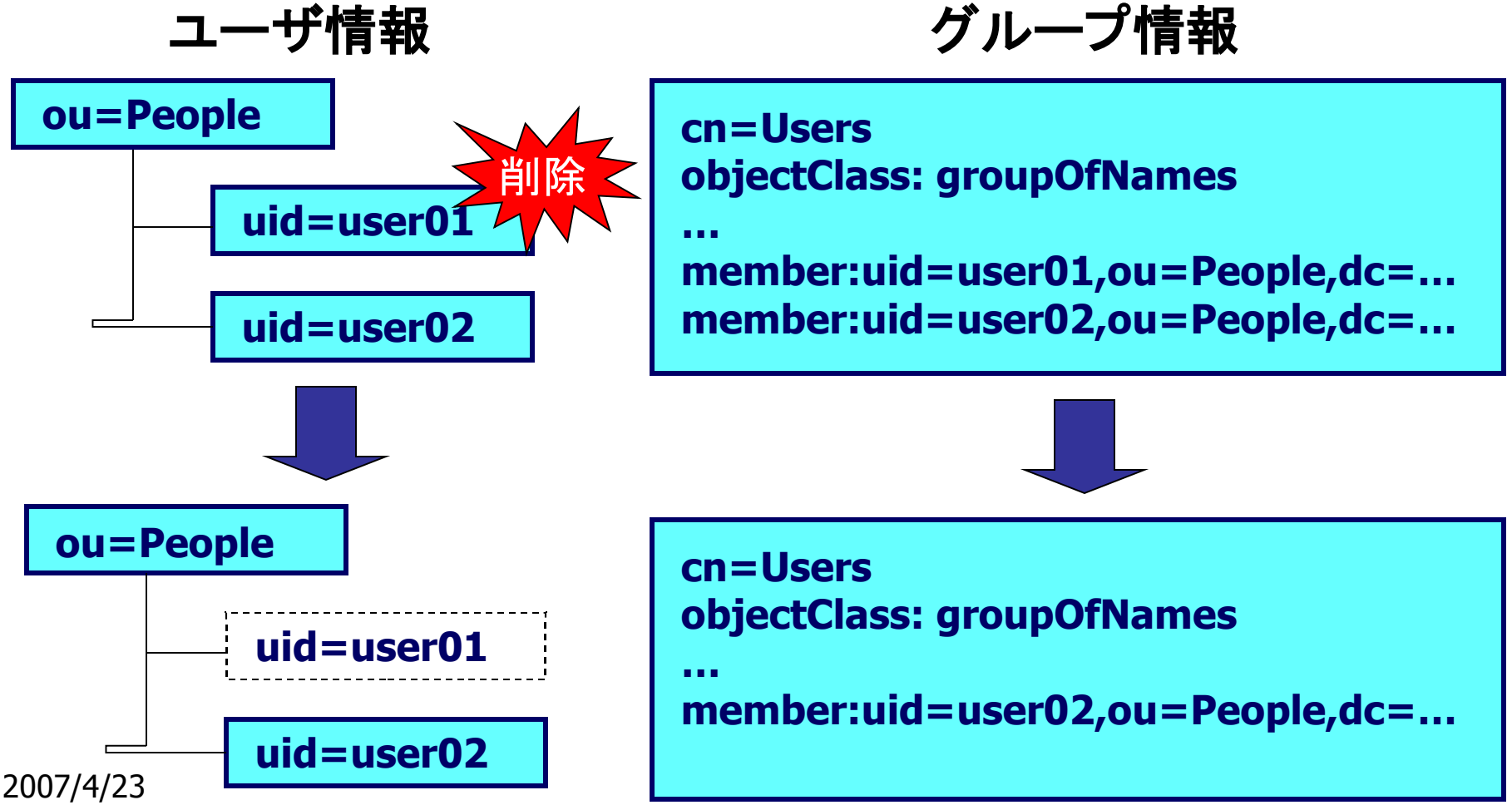
Access Logを有効にすると処理時間が大幅に増加

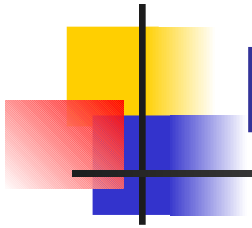
Referential Integrity (1)

- エントリ削除、移動時にそのDNを値に持つ属性を自動的に削除、変更する機能
  - ユーザ、グループ、ロール情報の管理が容易になる



Referential Integrity (2)

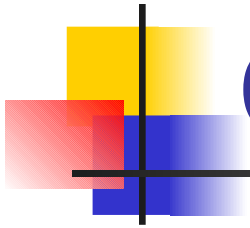




Referntial Integrity 設定

- slapd.confに以下の記述を追加

```
overlay     refint
# refintの対象属性名（複数指定可能）
refint_attributes     member owner seeAlso
```



OpenLDAPのロードマップ

- OpenLDAP 2.4で実装予定の機能
  - マルチマスタ
    - マスタサーバを複数設置し、更新処理の冗長化が可能
  - LDAPトランザクション
    - LDAPの更新処理にトランザクションを追加
  - LDAP Dynamic Directory Services(RFC2589)
    - データが動的に出現、消滅する機能
  - LDAP Don't use Copy Control
    - 複製、レプリケーションされたデータを送信しないように要求する機能