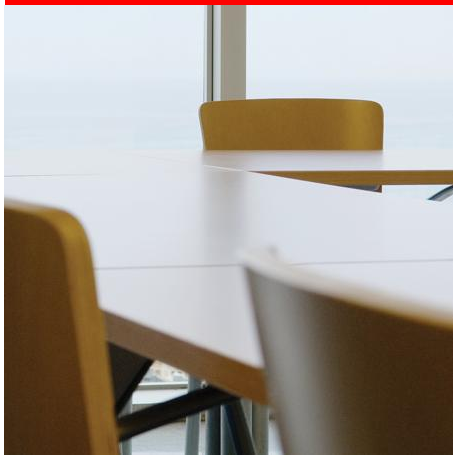
ORACLE®

MySQL入門 実践編

日本オラクル株式会社
MySQL Global Business Unit

以下の事項は、弊社の一般的な製品の方向性に関する概要を説明するものです。また、情報提供を唯一の目的とするものであり、いかなる契約にも組み込むことはできません。以下の事項は、マテリアルやコード、機能を提供することをコミットメント（確約）するものではないため、購買決定を行う際の判断材料になさらないで下さい。オラクル製品に関して記載されている機能の開発、リリースおよび時期については、弊社の裁量により決定されます。

MySQLインストール



インストール・パッケージの選択

- インストール・パッケージ
  - 32 bit / 64 bit
- 各種Linux ディストリビューション
  - .rpm / tar.gz
- Solaris
  - .pkg / .tar.gz
- Windows
  - GUIインストーラ付き / .zip
- その他
  - Mac OS X .dmg, ソースコード 等

MySQLインストールの推奨方法
– 開発用途のLinuxの場合

tar.gzを利用

メリット

- 全てのファイルが一つのディレクトリ内に配置される
- 複数のMySQLのインストールが簡単
- シンボリックリンクの切り替えでアップグレードが簡単
- 起動方法を選択可能（rpm版の場合はサービス登録される）
- インストール作業をスクリプト化しやすい

インストール作業例

```
> groupadd mysql
> useradd -r -g mysql mysql
> cd /usr/local
> tar zxvf /home/mysql/MySQL-5.5.55.linux3.0.x86_64.tar
> ln -s /home/mysql/MySQL-5.5.55.linux3.0.x86_64 mysql
> cd mysql
> chown -R mysql .
> chgrp -R mysql .
> scripts/mysql_install_db --user=mysql
> chown -R root .
> chown -R mysql data
```

- tar.gzを展開したディレクトリのINSTALL-BINARYを参照

http://dev.mysql.com/doc/refman/5.5/en/binary-installation.html
http://dev.mysql.com/doc/refman/5.1/ja/binary-installation.html

MySQLサーバーの設定

- デフォルトのMySQLの設定ファイル -- my.cnf
- 配置先（上記から順に検索)
  - /etc/my.cnf
  - /etc/mysql/my.cnf
  - SYSCONFDIR/my.cnf　*SYSCONFDIRコンパイル時に決定
  - $MYSQL_HOME/my.cnf
  - defaults-extra-file　*サーバー起動オプションでの指定
  - ~/.my.cnf　*サーバー起動ユーザーのホームディレクトリに配置

- 設定ファイルをサーバー起動時に明示的に指定する場合
  - --defaults-file=/path/to/file オプションを利用

http://dev.mysql.com/doc/refman/5.5/en/option-files.html
http://dev.mysql.com/doc/refman/5.1/ja/option-files.html

インスタンスの設定

- .tar.gzを利用するとデフォルトでは my.cnfが無い
- サンプルは$MYSQL_HOME/support-files
  - my-small.cnf
  - my-medium.cnf
  - my-large.cnf
  - my-huge.cnf
  - my-innodb-heavy-4G.cnf

my.cnfのベストプラクティス

特に複数のインスタンスを共存させる場合

- インスタンス毎にMYSQL_HOMEを定義
- $MYSQL_HOME/my.cnfを利用
- /etc/my.cnfなどが無いことを確認
  - 他の設定ファイルもサーバーが読み込んでしまうため

目的

- 1サーバー上に複数のインスタンスを起動するため
- より簡単なアップグレードのため

主なディレクトリ配置

設定オプション (コマンドラインまたはmy.cnf)

- basedir　　(i.e. $MYSQL_HOME)
  - e.g. /opt/mysql-5.5.22-linux-i686-glib23
- datadir　　(デフォルトは $MYSQL_HOME/data)
- tmpdir　　(デフォルトは /tmp)
- innodb_data_file_path
- innodb_data_home_dir
- innodb_log_group_home_dir

ログファイル

変更の際は
再起動が必要

- エラーログ
  - log-error （デフォルトは$MYSQL_HOME/data/hostname.err）
- バイナリログ
  - log-bin （デフォルトは $MYSQL_HOME/data/hostname-bin.NNNNN）
- スロークエリログ
  - log-slow-queries （デフォルトは$MYSQL_HOME/data/hostname-slow.log）
  - log-queries-not-using-indexes
  - long_query_time
- 一般ログ
  - log （デフォルトは$MYSQL_HOME/data/hostname.log）

ログファイル（SQL文関連）

- general_log, slow_log
  5.1からはテーブルにログ出力可能に
- SQLでログの取得開始/停止を制御可能に

```
#my.cnf
log-output=FILE,TABLE

mysql> SET GLOBAL GENERAL_LOG=1;
mysql> SELECT user FROM mysql.user;
mysql> SELECT * FROM mysql.general_log;
```

ディレクトリ配置のベストプラクティス

- datadirをbasedirとは別の場所に
- エラーログ、スローログ、一般ログは、
  一般ユーザーがアクセスできないディレクトリに
- バイナリログはdatadirとは別ディスクに
  - メリット: パフォーマンスの改善
    ディスク障害発生からの復旧可能性の向上
  - デメリット: バックアップの際に注意が必要
- InnoDBのREDOログはバイナリログと同じディレクトリでも可
- tmpdirは必要な容量のあるディレクトリへ
- エラーログを定義(syslogへも出力可能)

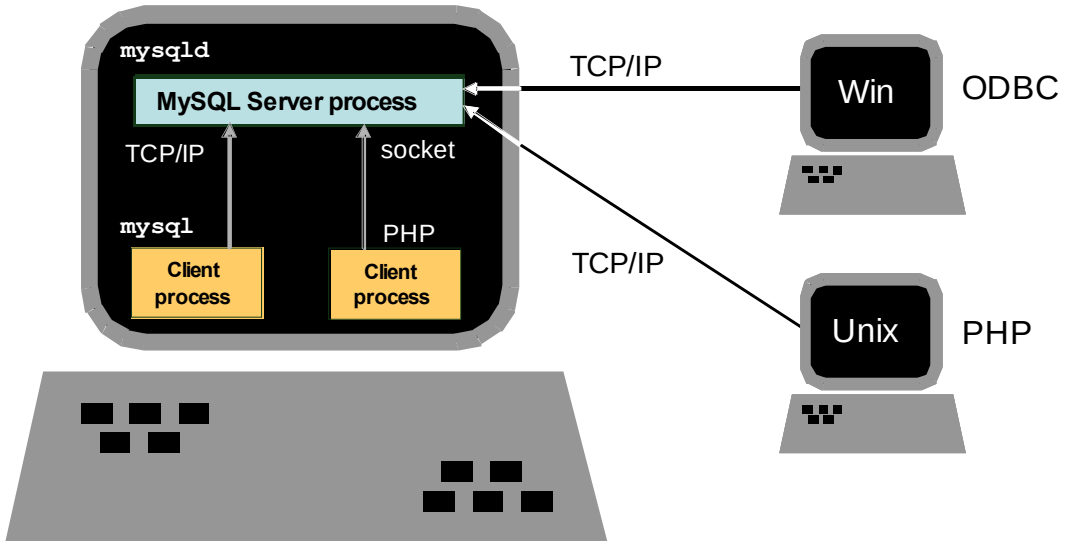
MySQLのプロセス

- MySQLサーバー関連プログラム
  - mysqld　　MySQLデーモン
  - mysqld_safe　　起動スクリプト
- MySQLクライアント関連プログラム
  - mysql　　MySQLクライアント
  - mysqldump　　エクスポートツール
  - mysqladmin　　管理用コマンド

MySQL通信モデル

複数の通信手段

- TCP/IP
- Socket
- 共有メモリ
- 名前付きパイプ



	TCP/IP	Unix socket	Shared memory	NT pipes
Windows local	X		X	X
Unix/Linux local	X	X		
Remote	X			

主な設定項目

パラメタ設定

- Top 20
  - 接続/スレッド/テーブル/ファイル
  - メモリ
  - セッション単位
  - その他各種

主なパラメタ

接続/スレッド/テーブル/ファイル関連 (推奨値)

- max_connections
  - データベースへの最大接続数 (50-150)
- thread_cache_size
  - 新規接続用にプールするスレッド数 (16)
- table_cache
  - オープンするテーブル用のファイル・ディスクリプタのプール (256)
- innodb_thread_concurrency
  - 同時実行可能なコネクション数 [InnoDBストレージエンジン用](4-8)
- open_files_limit
  - オープン可能な最大ファイル数 (2048)

主なパラメタ

メモリ関連

- key_buffer_size
  - MyISAMのインデックスのバッファ（up to 4GB）
- innodb_buffer_pool_size
  - InnoDBのデータとインデックスのバッファ（70%-80% of RAM）
- query_cache_size, query_cache_limit
  - SQL文と実行結果のキャッシュ。同じSQL文を繰り替えしパース/実行せずに迅速なレスポンスを返すため（32M, 1M）
- tmp_table_size, max_heap_table_size
  - 中間テーブルおよびオンメモリ・テーブルのサイズの上限（max_heap_table_size ≧ tmp_table_sizeとすること）（32M - 64M）

主なパラメタ

セッション（コネクション）単位のバッファ関連

- sort_buffer_size
  - ORDER BY や GROUP BY によるソート処理で利用 (2-8M)
- join_buffer_size
  - インデックスを使用しないJOIN処理で利用 （2-8M）
- read_buffer_size
  - テーブルフルスキャンの処理で利用 （2-8M）
- read_rnd_buffer_size
  - テーブル・フルスキャン時にソート処理後のデータ読みだしで利用 (2-8M)

主なパラメタ

その他各種パラメタ

- log-slow-queries, slow_query_time
  - スロークエリログに記録する秒数 slow_query_time (秒単位) (2)
- innodb_log_file_size
  - InnoDBのREDOログサイズ - サイズが大きいとチェックポイントを減らせるが、リカバリにかかる時間が長くなる (innodb_buffer_pool_size / 2 / innodb_log_files_in_group)
- wait_timeout / interactive_timeout
  - コネクションを強制的に切断するまでのwait時間
- tx_isolation
  - トランザクション分離レベル (READ UNCOMMITTED, READ COMMITTED, REPEATABLE READ (default), SERIALIZABLE)

Web上の参考情報

- MySQLの全てのパラメター一覧
  - http://dev.mysql.com/doc/refman/5.5/en/server-system-variables.html
  - http://dev.mysql.com/doc/refman/5.1/ja/server-system-variables.html
- 動的に変更可能なパラメター一覧

  (SET [GLOBAL|SESSION] ... = ...;コマンドにて)
  - http://dev.mysql.com/doc/refman/5.5/en/dynamic-system-variables.html
  - http://dev.mysql.com/doc/refman/5.1/ja/dynamic-system-variables.html
- InnoDB固有のパラメター一覧
  - http://dev.mysql.com/doc/refman/5.5/en/innodb-parameters.html
  - http://dev.mysql.com/doc/refman/5.1/ja/innodb-parameters.html
- オプションや変数の一覧
  - http://dev.mysql.com/doc/refman/5.5/en/mysqld-option-tables.html
  - http://dev.mysql.com/doc/refman/5.1/ja/mysqld-option-tables.html

複数のサーバーを起動する場合

- 以下のパラメタをサーバー毎に異なる値にする
  - `--datadir`
  - `--port`
  - `--socket`
  - `--pid-file`
  - `--log-bin`
  - `--log-error`

  - `--server-id`　　# 設定することを推奨

サーバーの監視

- エラーログ
  - $MSQL_HOME/hostname.err
  - またはサーバー起動オプションで設定 --log-error
  - /var/log/messages （5.1以降では設定可能）
- エラーコード内容の確認
  - `$ perror [options] errorcode ...`

ドキュメント

- 複数バージョンを用意
  - 3.23/4.0/4.1
  - 5.0
  - 5.1
  - 5.5
  - 5.6
- 日本語版は5.1用をご参照ください

http://dev.mysql.com/doc

インストール手順まとめ

- .tar.gzを利用
- $MYSQL_HOME/my.cnfを使用
- 可能ならデータとログをサーバーとは別ディスクに
- mysql_secure_installationを実行

セキュリティ設定の基本

ファイルシステム

- 実行バイナリの所有者はroot
- データディレクトリの所有者は一般ユーザー
  （例 mysql）
  - 他のユーザーがOS上でこのディレクトリにアクセスできないように設定すること
- ログディレクトリの所有者は一般ユーザー（例 mysql）
- 一般ユーザー(例 mysql)はログイン不可にしておく
- ソケットファイルにアクセス可能であること
  (全てのユーザーから参照可能に)

ファイルシステム

```
$ groupadd mysql
$ useradd -g mysql mysql
$ chown -R root:mysql $MYSQL_HOME
$ chmod 750 $MYSQL_HOME
$ chown -R mysql:mysql $MYSQL_HOME/data
$ chmod 700 $MYSQL_HOME/data
```

NOTE: デフォルトのログ出力先は$MYSQL_HOME/data

データベース

- MySQLサーバーは‘root’ユーザー以外で起動
  - デフォルトでは‘root’ユーザーでの起動不可
  - ‘mysql’ユーザーとして起動する場合：--user=mysql
  - MySQLサーバーの起動ユーザーはOS上で必要以上の権限やファイル・システムのアクセス許可を与えないこと
  - ファイル・システム上のファイル操作にはFILE権限が必要
- デフォルトでは全ネットワーク・インターフェースを使用
  - 特定のインターフェースを使用する場合：--bind-address
  - TCP/IP経由でのアクセスを無効にする場合：--skip-networking

mysql_secure_installation

- MySQLインストール後のデフォルト状態から
  セキュリティを向上させるスクリプト
  - rootアカウントのパスワードを設定
  - localhost以外からrootアカウントでのアクセスを無効化
  - アノニマス・ユーザー・アカウントを削除
  - デフォルトでアノニマス・ユーザーがアクセス可能な
    testデータベースを削除

```
$ mysql_secure_installation
```

権限関連のシステムテーブル（メタデータ）

- ’mysql’データベース
  - db
  - host
  - user
  - tables_priv
  - columns_priv
  - procs_priv

http://dev.mysql.com/doc/refman/5.5/en/grant-table-structure.html
http://dev.mysql.com/doc/refman/5.1/ja/grant-table-structure.html

ユーザー

- CREATE USER コマンド
- 接続許可はユーザーとパスワードだけでなく、クライアントのホストを含む
- ホストの指定はホスト名またはIPアドレス、およびワイルドカードを使用する方法がある

```
mysql> CREATE USER 'oper@localhost' IDENTIFIED BY 'sakila';
mysql> CREATE USER 'oper@10.1.1.32' IDENTIFIED BY 'sakila';
```

ホスト

- ホストの指定はホスト名またはIPアドレス、およびワイルドカードを使用する方法がある
- ワイルドカード使用例
  - '10.0.%'
  - '%.domain.com'

推奨 (DNSのルックアップを回避)

- --skip-name-resolve
- IPアドレスを使用

ユーザー

- 以前のバージョンでのユーザー追加方法（5.0未満）
  [現在は推奨されていない方法]

```
mysql> INSERT INTO mysql.user(...) VALUES (...);
mysql> FLUSH PRIVILEGES;
```

- ’mysql.users’テーブルの直接操作は推奨されていない

Grant/Revoke

- 権限はON database.table で付与
- 権限は TO ‘user’@’host’ で付与
- 権限の剥奪は REVOKE 文を利用

```
mysql> GRANT SELECT ON db.* TO 'oper'@'10.1.%';
mysql> GRANT INSERT,UPDATE ON db.table TO 'oper'@'localhost';
mysql> REVOKE SELECT ON db.* FROM 'oper@'10.1.%';
```

メモ: 同一のユーザー名でもホスト毎に権限を変えることが可能

Grant/Revoke

権限が影響するタイミングは

- テーブルとカラム：データ参照/変更時
- データベース：USE <dbname>実行時
- グローバル権限とパスワード：接続時

http://dev.mysql.com/doc/refman/5.5/en/privilege-changes.html

http://dev.mysql.com/doc/refman/5.1/ja/privilege-changes.html

グローバル権限

- SUPER （CHANGE MASTER, KILL, PURGE MASTER LOGS, SET GLOBAL）
  - SHOW ENGINE INNODB STATUSの実行にも必要
  - 5.0ではトリガ関連コマンドにも必要
  - TRIGGER 権限が 5.1 で追加
- SHUTDOWN
- RELOAD
- PROCESS
- FILE
- ALL
- WITH GRANT OPTION

付与されている権限の確認

ユーザーに付与されている権限の確認コマンド

```
mysql> SHOW GRANTS [FOR user]
```

http://dev.mysql.com/doc/refman/5.5/en/show-grants.html

http://dev.mysql.com/doc/refman/5.1/ja/show-grants.html

利用するリソースの制限

- MAX_QUERIES_PER_HOUR
- MAX_UPDATES_PER_HOUR
- MAX_CONNECTIONS_PER_HOUR
- MAX_USER_CONNECTIONS

http://dev.mysql.com/doc/refman/5.5/en/user-resources.html
http://dev.mysql.com/doc/refman/5.1/ja/user-resources.html
http://dev.mysql.com/doc/refman/5.5/en/grant.html
http://dev.mysql.com/doc/refman/5.1/ja/grant.html

パスワードの強制 – SQL_MODE

デフォルトではパスワードの無いユーザーも作成可能

- セキュリティ向上のために強制可能

```
mysql> SET GLOBAL sql_mode=NO_AUTO_CREATE_USER;
```

ネットワークアクセスの制限

TCP/IPアクセスの無効化（localhostのアクセスのみ）

- --skip-networking

他のネットワークアクセスの変更方法

- ポートをデフォルトの3306から変更
- ポートをあけておく場合、root@localhostユーザーのみにSUPER権限を付与

SSLに関する権限

権限付与時にREQUIRE SSLを利用可能

- REQUIRE NONE
- REQUIRE SSL
- REQUIRE X509
- REQUIRE ISSUER 'issuer'
- REQUIRE SUBJECT 'subject'
- REQUIRE CIPHER 'cipher '

http://dev.mysql.com/doc/refman/5.5/en/secure-connections.html
http://dev.mysql.com/doc/refman/5.1/ja/secure-connections.html

SSLに関する権限

```
GRANT ALL PRIVILEGES ON test.* TO 'root'@'localhost'
  IDENTIFIED BY 'goodsecret'
  REQUIRE SUBJECT '/C=EE/ST=Some-State/L=Tallinn/
    O=MySQL demo client certificate/
    CN=Tonu Samuel/Email=tonu@example.com'
  AND ISSUER '/C=FI/ST=Some-State/L=Helsinki/
    O=MySQL Finland AB/CN=Tonu
Samuel/Email=tonu@example.com'
  AND CIPHER 'EDH-RSA-DES-CBC3-SHA';
```

パスワード

- SET PASSWORD [FOR user] = PASSWORD('some password')

- NOTE: 4.1にてパスワードのハッシュ化方式変更
- --old-passwords

ベストプラクティス

- 'root'ユーザーに必ずパスワードを設定すること
- SUPER権限の付与は必要最小限にすること
- MySQLはクエリ毎に権限をチェック。
  GRANTコマンドを多用しないこと
- ホスト名に'%'を使用しないこと
- 全データベースに対する権限の付与(ON *.*使用)は
  必要最小限にすること
- 'mysql'データベースへのアクセス可能なユーザーは
  最小限にすること

Hardware and Software

ORACLE

Engineered to Work Together


ORACLE®