MySQL

データベースによるセキュリティ対策

RDBMSからNoSQLまでSIer向けデータシステムトレンドセミナー

～ NoSQL事例/データ解析/セキュリティと注目のトピックスをご紹介 ～

konekto

コネクト株式会社とMySQL

- 企業向けPHPソリューション「Zendプロダクト」の日本総代理店として、2001年9月に事業を開始。当時、LAMPとしてPHPと共にニーズが高いMySQLサポートを2003年に開始

  - 2001年9月 株式会社テンアートニ（現：サイオステクノロジー株式会社）の1部門としてスタート
  - 2002年12月 ゼンド・オープンソースシステムズ株式会社として独立
  - 2003年9月 MySQLプロダクトの取扱い開始/サポートサービス開始
  - 2004年9月 ゼンド・ジャパン株式会社に社名変更
  - 2005年3月 Apache / Tomcatサポートサービス開始
  - 2012年7月 コネクト株式会社に社名変更
  - 2012年11月 Cassandraサポートサービス提供開始
  - 2015年6月 MySQL Cluster 構築支援サービス提供開始
  - 2016年4月 MySQLの技術力とビジネス実績を認定する「Specialization」を取得

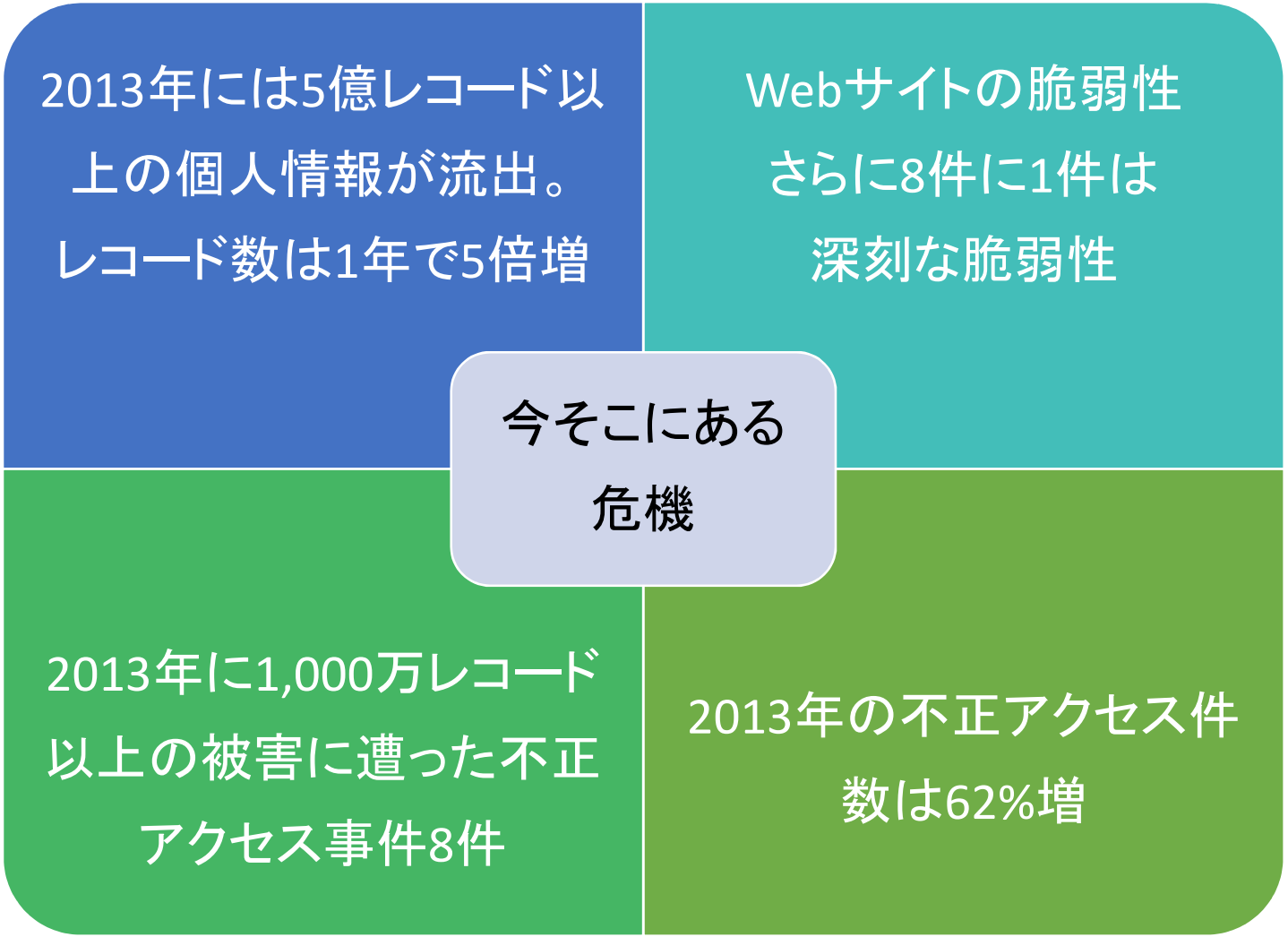
konekto

MySQLの現状

- 世界で最もダウンロードされているオープンソースデータベース
- デュアルライセンス
  - GPLライセンス(Community Edition)
  - コマーシャルライセンス(Standard Edition/Enterprise Edition/CGE)
  - 組込ライセンス(Classic Edition)
- MySQLはリリースから22年
  - Oracleプロダクトになって7年
- サービス中(メンテナンスされているバージョン)
  - MySQL 5.5/5.6/5.7 → MySQL 8 開発中
  - MySQL Cluster 7.2/7.3/7.4/7.5 → MySQL Cluster 7.6 開発中
- MySQL Cloud提供開始

konekto

大規模な不正アクセス



出展: Internet Security Threat Report 2014, Symantec

不正アクセスによる情報流出

	流出元	流出内容
4月25日	チケットぴあ	最大約15万5000件の個人情報と3万2000件のカード情報
3月17日	ニッポン放送	氏名や住所、電話番号、メールアドレスなど顧客情報1万1330件および会員に関するメールアドレス、ニックネーム、生年月など4万5984件
3月14日	日本郵便	顧客情報（メールアドレス）29,116件と、サイト上で作成した送り状1,104件
3月10日	都税納付サイト	クレジットカード情報流出の可能性：676,290件 カード番号・カード有効期限の流出：61,661件 2に加えメールアドレス：614,629件
3月10日	住宅金融支援機	クレジットカード情報流出の可能性：43,540件 カード番号、有効期限、セキュリティコード、その他個人情報：622件

原因は「Apache Struts 2 」の脆弱性によるもの

konekto

データベース攻撃による問題

- 情報流出: クレジットカードやその他の個人情報の不正な取得
  - 対策: データやネットワークの暗号化、強固なアクセス制御
- DoS(サービス拒否)攻撃: 負荷の極めて高いクエリの実行
  - 対策:各種のリソース利用制限 (最大接続数、セッション数、タイムアウトなど)
- 権限の昇格: 管理者の認証情報の不正な取得
  - 対策: 認証の強化、アクセス制御、監査
- なりすまし: 他社の認証情報を不正に利用
  - 対策: 強力なアカウントおよびパスワードポリシー
- 不正な改変: データの変更、トランザクション記録の削除
  - 対策: 認証の強化、監査、監視、バックアップ

konekto

データベースへの攻撃パターンと対策

- SQLインジェクション
  - 対策: データベースファイアウォール、ホワイトリスト、入力バリデーション
- バッファオーバーフロー
  - 対策: データベースソフトウェアの定期的な更新、データベースファイアウォール、ホワイトリスト、入力バリデーション
- ブルートフォースアタック (総当たり攻撃)
  - 対策: 設定回数を超えた回数ログインを試みたアカウントをロック
- ネットワーク傍受
  - 対策: 全ての接続とデータ転送に SSL/TLS を必須化
- マルウェア(クライアント乗っ取り)
  - 対策: 強固なアクセスコントロール、接続元IPアドレスの制限、デフォルト設定の変更
- サーバ乗っ取り
  - 対策: データベースファイアウォール、データベース暗号化

konekto

DBAによる基本的なセキュリティ対策

- アクセスする必要のあるユーザーのみが、権限を取得出来るよう確実な運用。
- ユーザーおよびアプリケーションの権限を適切にコントロールする。
- ユーザーおよびアプリケーションが、データにアクセスできる場所を制限する。
- 何が、いつ発生したかを適切にモニタリングしておく。
- バックアップが安全でセキュアに取得されている事を確実にしておく。
- 不正アクセスを受けないよう、アクセス出来るポイントを最小化しておく。

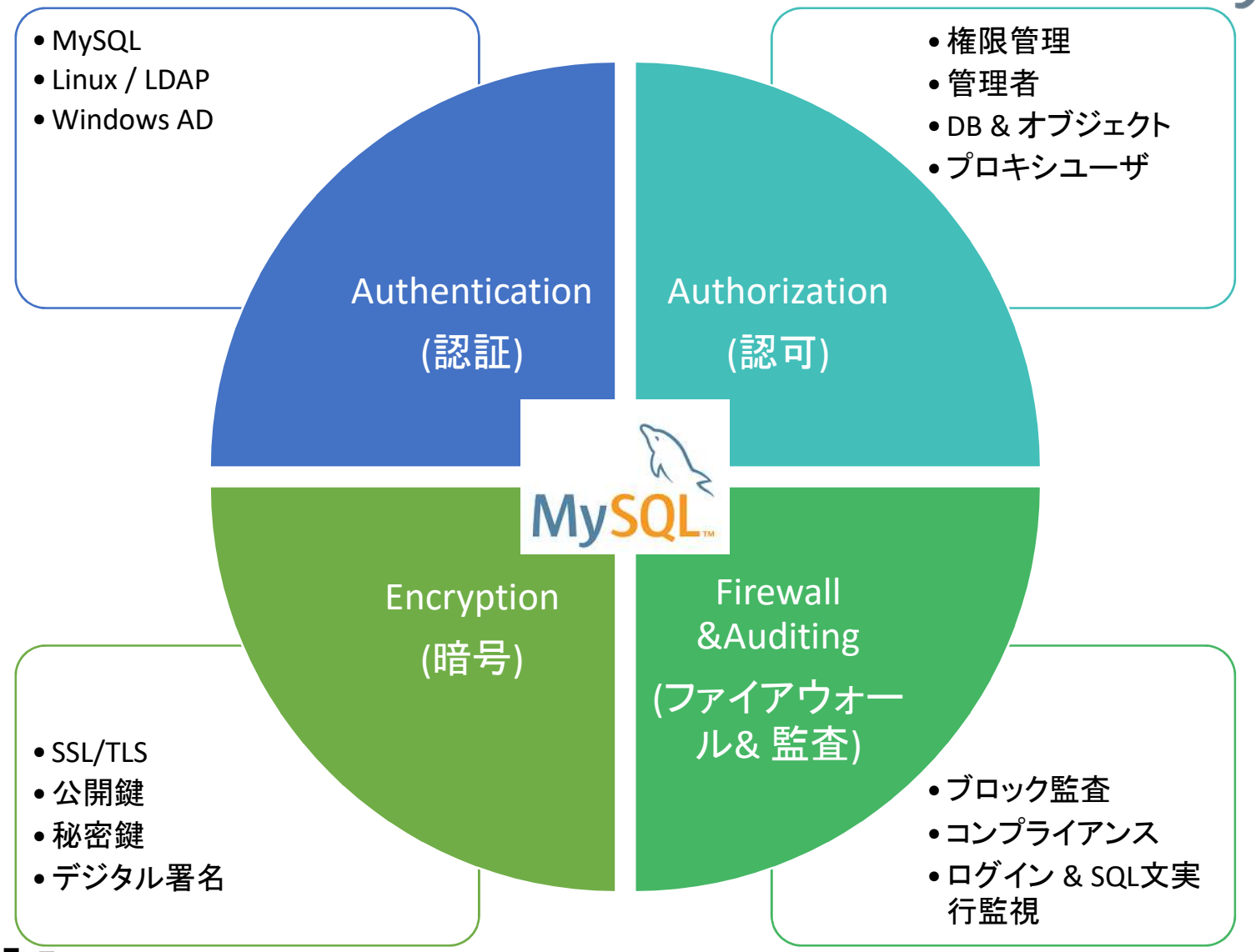
konekto

データベースの脆弱性と対策

- 設定の不備
  - デフォルト設定からの変更
- 過剰な権限の付与
  - 権限設定ポリシー
- 貧弱なアクセス制御
  - 管理者権限付与の限定
- 貧弱な認証
  - 複雑なパスワードの強制
- 貧弱な監査
  - コンプライアンス & 監査ポリシー
- 暗号化の不足
  - データ、バックアップ & ネットワークの暗号化
- 認証情報の不十分な管理
  - mysql_config_editor利用, Key Vaults
- 無防備なバックアップデータ
  - バックアップデータの暗号化
- 監視の不備
  - ユーザ & オブジェクト監視
- アプリケーションの脆弱性
  - データベースファイアウォール

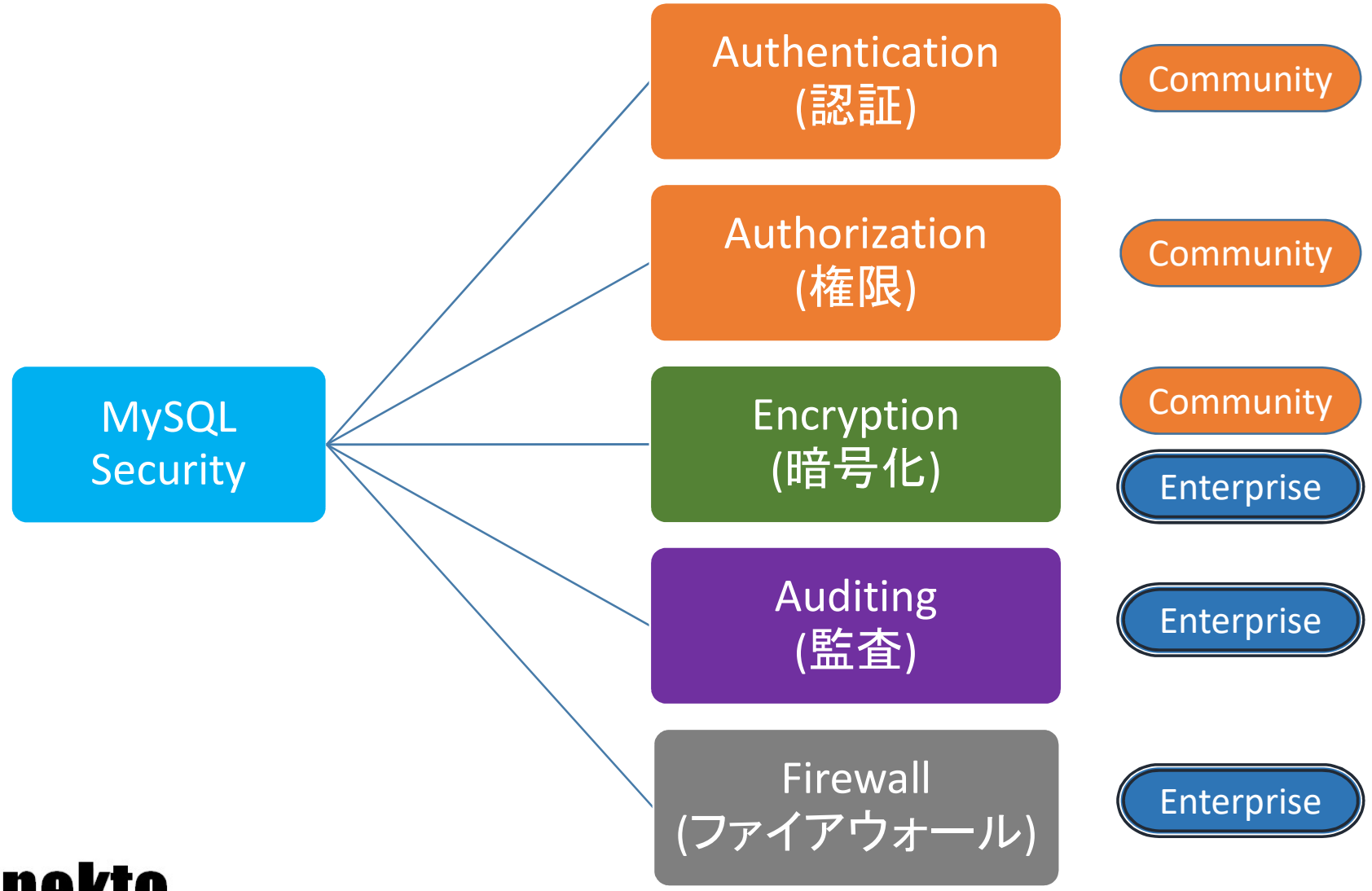
konekto

MySQLに備わっているセキュリティ



konekto

MySQLセキュリティ機能



konekto

Authentication(認証)

Community

ロユーザアカウント

- ユーザ名＠ホスト
  - ユーザ名は、最大16文字のASCII 文字(ASCII以外は設定が必要)
  - ホストには、ホスト名やIPアドレス(ワイルドカードが使用可能)
    - root@localhost　'konekto'@'192.168.10.%'

ロパスワード

- 強制化(5.7より)
  - SQLモードNO_AUTO_CREATE_USERによるパスワード無しユーザが作成できない
- パスワードポリシー(5.6.6より)
  - プラグインvalidate_passwordにより有効化()
- パスワードの失効ポリシー(5.7.11より)
  - パスワードローテーションポリシー (パスワード有効期間を日数で設定)
  - インスタンス全体、ユーザー単位で設定可能

ロMySQL Enterprise Authentication

- 外部認証との連携
  - PAM/Windows

konekto

Authentication(認証)

Community

MySQL

Connection-Control Plugin

– 連続してログインに失敗した場合に応答を遅延する機能

有効化(プラグイン設定)

- INSTALL PLUGIN connection_control SONAME 'connection_control.dll';
- INSTALL PLUGIN connection_control_failed_login_attempts SONAME 'connection_control.dll';
- INSTALL PLUGIN connection_control SONAME 'connection_control.so';
- INSTALL PLUGIN connection_control_failed_login_attempts SONAME 'connection_control.so';

デフォルト設置内容

```
mysql> SHOW GLOBAL VARIABLES LIKE 'connection_control%';
+-----------------------------------------------+------------+
| Variable_name                                 | Value      |
+-----------------------------------------------+------------+
| connection_control_failed_connections_threshold | 3          | 適用回数
| connection_control_max_connection_delay       | 2147483647 |
| connection_control_min_connection_delay       | 1000       | 遅延時間(ms)
+-----------------------------------------------+------------+
3 rows in set, 1 warning (0.00 sec)
```

konekto

Authorization(権限)

Community

- ユーザ
- データベース
- テーブル
- カラム
- プロシージャ(proc)
- プロキシ

- MySQL 8 では、ロールが導入される

konekto

Encryption(暗号化)①

Community

MySQL

ロコネクションの暗号化

- サーバとクライアントの通信を暗号化

ロデータベース(データ)

- SQLステートメントによる暗号化
  - AES_ENCRYPT関数によるデータの暗号化
  - AES_DECRYPT関数によるデータの復号化

konekto

Encryption(暗号化)②

Enterprise

MySQL

Enterprise Encryption
- アプリケーションによる暗号化(アプリに組み込む必要あり)

Enterprise Backup
- バックアップデータの暗号化

Enterprise Transparent Data Encryption
- MySQL自身が透過的に暗号化を実施(アプリに組み込む必要なし)
  - Community キーファイルの保管場所をサーバ内
  - Enterprise キーファイルの保管場所を外部キーサーバー
    - early-plugin-load に keyring_file.so を指定 (MySQLサーバ内にキーファイルを保存)
    - early-plugin-load に keyring_okv.so を指定 (外部のキーサーバにキーを保存)

konekto

Auditing(監査)

Enterprise

- MySQL Enterprise Audit
  - ログオン、クエリーの情報を監査ログとして記録
  - ユーザがポリシーを設定可能：フィルタリング、ログローテーション

konekto

MySQL Enterprise Audit デモ①

ロ有効化(プラグイン設定)

- install plugin audit_log soname 'audit_log.dll';
- install plugin audit_log soname 'audit_log.so';

ロデフォルト設置内容

```
mysql> show variables like 'audit_log%';
+-------------------------------+--------------+
| Variable_name                 | Value        |
+-------------------------------+--------------+
| audit_log_buffer_size         | 1048576      |
| audit_log_connection_policy   | ALL          |
| audit_log_current_session     | OFF          |
| audit_log_exclude_accounts    |              |
| audit_log_file                | audit.log    |
| audit_log_filter_id           | 0            |
| audit_log_flush               | OFF          |
| audit_log_format              | NEW          |
| audit_log_include_accounts    |              |
| audit_log_policy              | ALL          |
| audit_log_rotate_on_size      | 0            |
| audit_log_statement_policy    | ALL          |
| audit_log_strategy            | ASYNCHRONOUS |
+-------------------------------+--------------+
13 rows in set, 1 warning (0.02 sec)
```

ログファイル名

対象ユーザID

ローテーションサイズ(なし)

konekto

MySQL Enterprise Audit デモ②

採取内容

- audit.log抜粋

```
<AUDIT_RECORD>
 <TIMESTAMP>2017-07-25T08:23:32 UTC</TIMESTAMP>
 <RECORD_ID>14_2017-07-25T08:19:56</RECORD_ID>
 <NAME>Query</NAME>
 <CONNECTION_ID>8</CONNECTION_ID>
 <STATUS>0</STATUS>
 <STATUS_CODE>0</STATUS_CODE>
 <USER>fw_user[fw_user] @ localhost [::1]</USER>
 <OS_LOGIN/>
 <HOST>localhost</HOST>
 <IP>::1</IP>
 <COMMAND_CLASS>select</COMMAND_CLASS>
 <SQLTEXT>select * from car where no=1</SQLTEXT>
</AUDIT_RECORD>
```

konekto

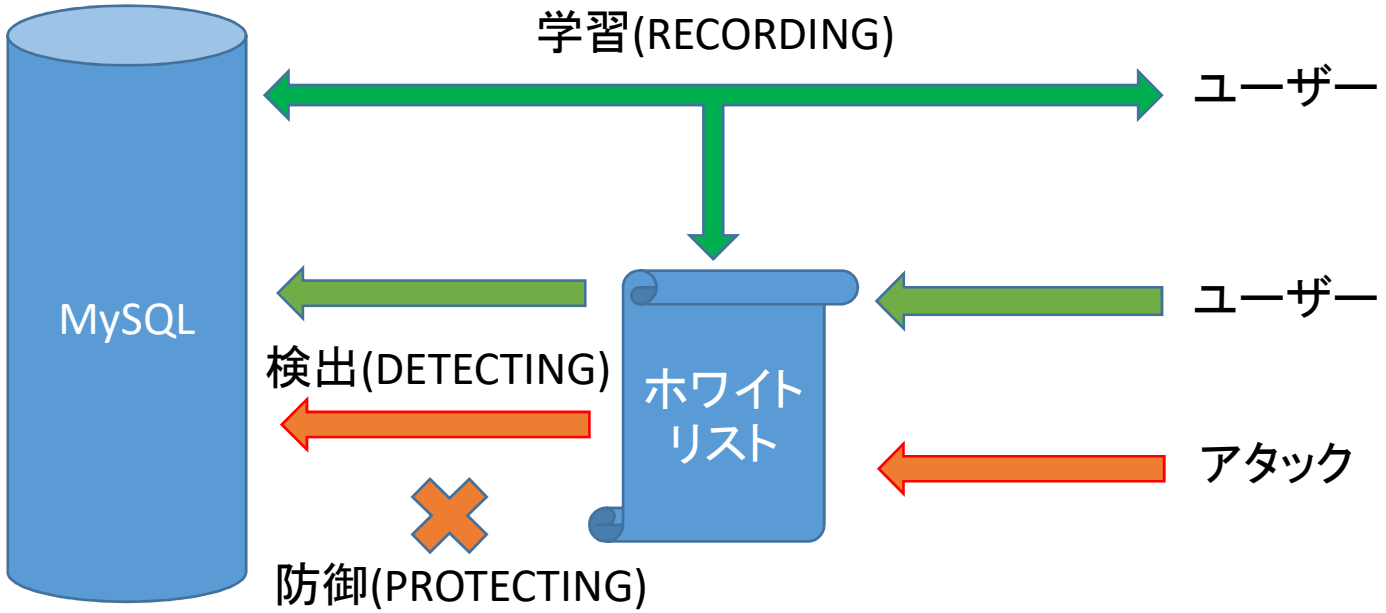
Firewall(ファイアウォール)

Enterprise

MySQL

MySQL Enterprise Firewall

- ユーザ別に設定したSQLステートメント以外の実行制限する
- 不審な動作の検出(記録)/ブロックを実施
- 実行可能なSQLステートメントを学習して自動的にホワイトリスト作成



konekto

MySQL Enterprise Firewall デモ①

有効化(SQL実行)

- mysql -u root -p < C:¥mysql¥share/win_install_firewall.sql
- mysql -u root -p < /usr/local/mysql/share/linux_install_firewall.sql

制御

- 学習 CALL sp_set_firewall_mode('fw_user@localhost','RECORDING');
- 防御 CALL sp_set_firewall_mode('fw_user@localhost','PROTECTING');
- 検出 CALL sp_set_firewall_mode('fw_user@localhost','DETECTING');
- 停止 CALL sp_set_firewall_mode('fw_user@localhost','OFF');
- 消去 CALL sp_set_firewall_mode('fw_user@localhost','RESET');

MySQL Enterprise Firewall デモ②

◘学習状態

```
mysql> select * from car where no=1;
+----+--------+
| No | Name   |
+----+--------+
|  1 | TOYOTA |
+----+--------+
1 row in set (0.00 sec)

mysql> select * from moto;
+----+----------+
| No | Name     |
+----+----------+
|  1 | HONDA    |
|  2 | YAMAHA   |
|  3 | SUZUKI   |
|  4 | KAWASAKI |
+----+----------+
4 rows in set (0.00 sec)
```

◘防御状態

```
mysql> select * from car;
ERROR 1045 (28000): Statement was blocked by Firewall
mysql> select * from car where no=1;
+----+--------+
| No | Name   |
+----+--------+
|  1 | TOYOTA |
+----+--------+
1 row in set (0.00 sec)

mysql> select * from moto;
+----+----------+
| No | Name     |
+----+----------+
|  1 | HONDA    |
|  2 | YAMAHA   |
|  3 | SUZUKI   |
|  4 | KAWASAKI |
+----+----------+
4 rows in set (0.00 sec)

mysql> select * from airplane;
ERROR 1045 (28000): Statement was blocked by Firewall
```

konekto

MySQL Enterprise Firewall デモ③

ロ検出状態(エラーログ)

```
2017-07-27T08:06:35.404519Z 14 [Note] Plugin
 MYSQL_FIREWALL reported: 'SUSPICIOUS STATEMENT from
 'fw_user1@localhost'. Reason: No match in whitelist.
 Statement: SELECT * FROM `moto` ‘
```

```
2017-07-27T08:06:59.233011Z 14
[Note] Plugin MYSQL_FIREWALL
reported: 'SUSPICIOUS STATEMENT from 'fw_user1@localhost'.
Reason: No match in whitelist.
Statement: SELECT * FROM `airplane` '
```

konekto

MySQL Enterprise Firewall デモ④

□稼働状況

```
show status like 'Firewall%';
+--------------------------+-------+
| Variable_name            | Value |
+--------------------------+-------+
| Firewall_access_denied   | 3     |   ブロック数
| Firewall_access_granted  | 4     |   非ブロック数
| Firewall_access_suspicious | 0   |   検知数(ブロックを除く)
| Firewall_cached_entries  | 5     |   記録した数
+--------------------------+-------+
```

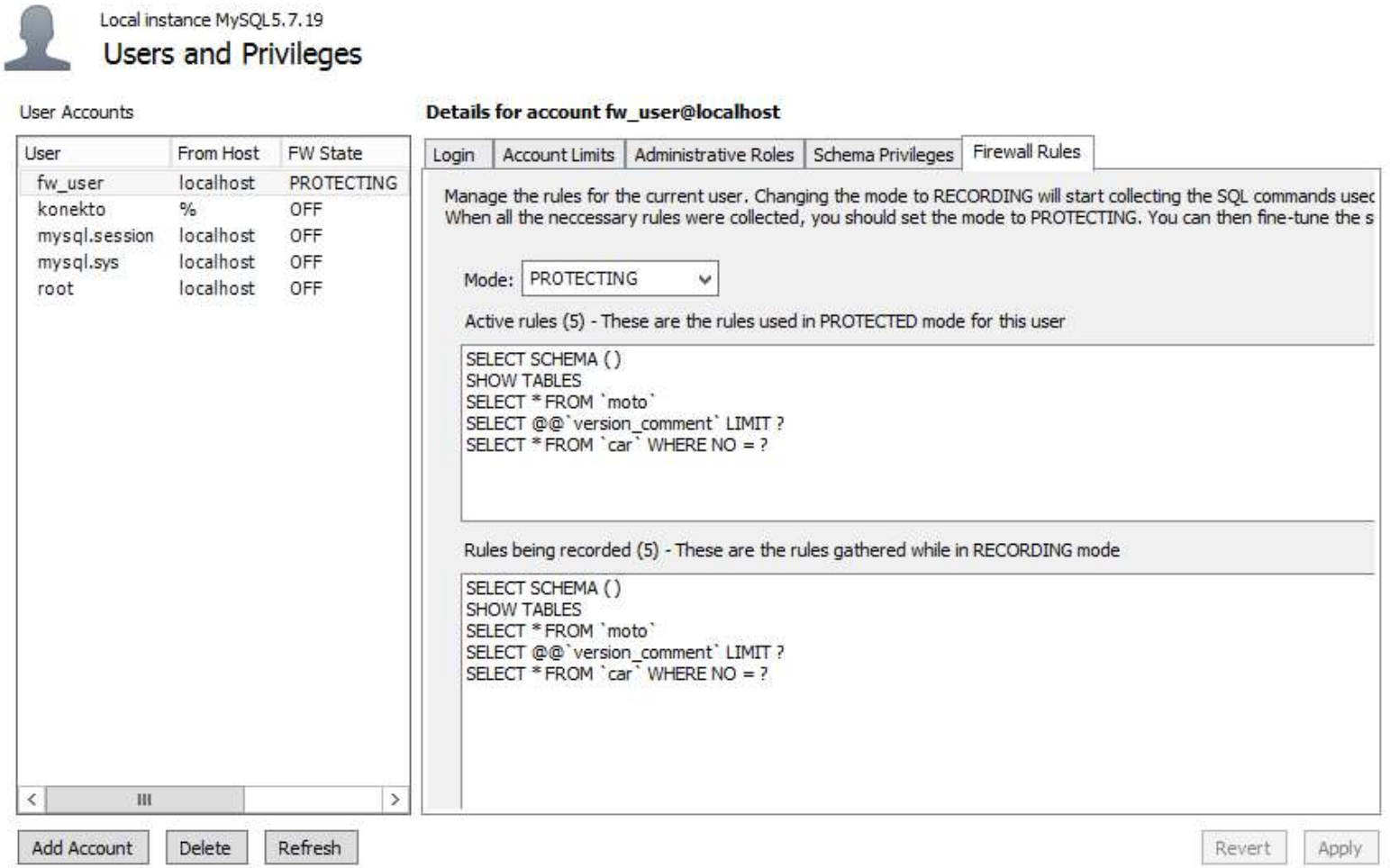
新たに学習後、検知状態に切替

```
mysql> show status like 'Firewall%';
+--------------------------+-------+
| Variable_name            | Value |
+--------------------------+-------+
| Firewall_access_denied   | 3     |
| Firewall_access_granted  | 9     |
| Firewall_access_suspicious | 2   |
| Firewall_cached_entries  | 12    |
+--------------------------+-------+
```

konekto

MySQL Enterprise Firewall デモ⑤

◘MySQL Workbenchによる学習内容(ルール)表示/設定



konekto

まとめ

- MySQLには、様々なセキュリティ機能が実装されています。
- MySQL Enterprise Editionには、さらに強力なセキュリティ機能が搭載されています。
- MySQLは、ニーズとコストに応じて、後付けでセキュリティ強化が可能です。
  これぞ、デュアルライセンスの醍醐味です。

- MySQL 8には、ロールが実装されます。

konekto

since 2001

コネクト株式会社

ORACLE Gold Partner
Specialized
MySQL 5

佐藤栄一 satou@konekto.jp

ORACLE Certified Professional
MySQL 5.0 Database Administrator

ORACLE Certified Professional
MySQL 5.0 Database Administrator

konekto