db tech showcase

ONLINE 2020

27TUE OCTOBER - 10THU DECEMBER

ようこそ！

DB tech showcase ONLINE 2020へ

ログ収集の裏側から見る データベース監査

～ MySQL Audit Plugin Internals ～

株式会社インサイトテクノロジー
プロダクト開発本部
趙　明春（チョウ　メイシュン）

自己紹介

- 趙　明春（チョウ　メイシュン）
  - データベース監査ツール PISO の開発に従事
  - 趣味
    - Apache Solr (全文検索システム)
    - Apache ManifoldCF (クローラー) コミッター

本セッションの目的

- MySQLを例に監査ログ収集のアプローチとその裏側を覗き、
- いかにデータベースの性能を担保しつつ、
- 監査に必要なデータを収集するかを考えます。

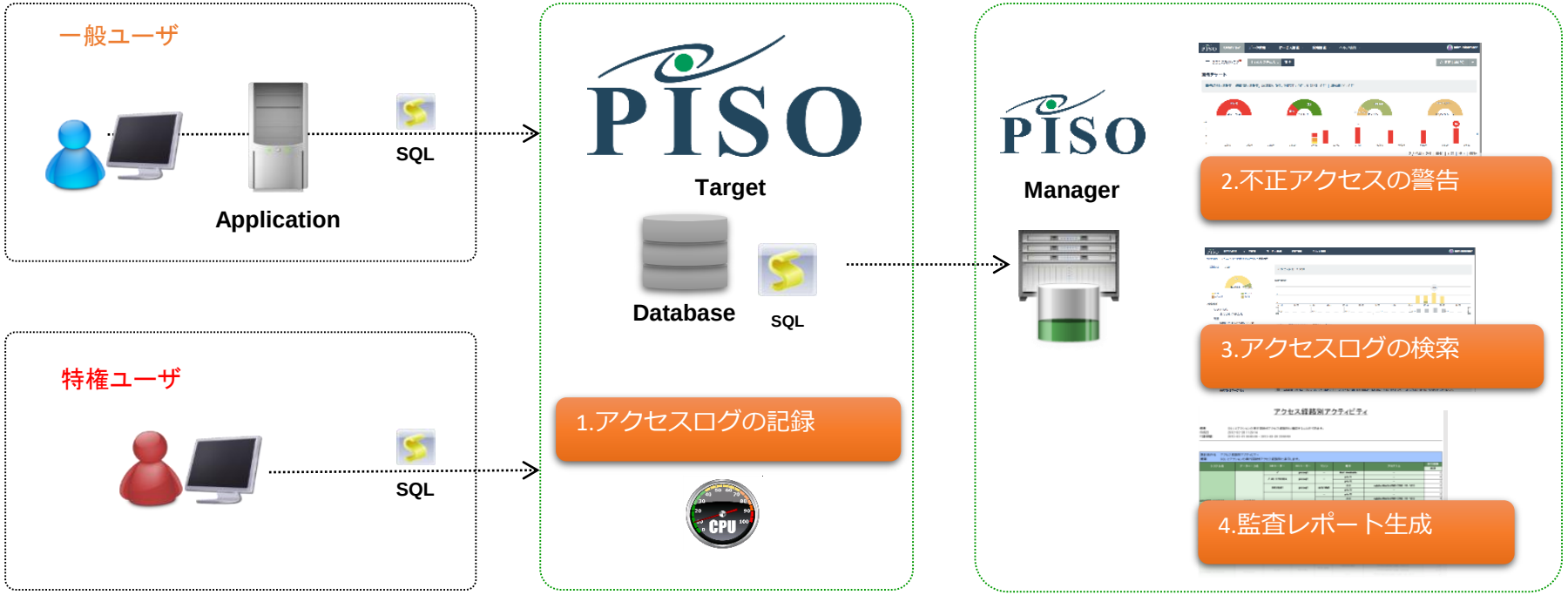
データベース監査とは

- 個人情報や企業機密の漏えい対策として、データベースセキュリティにおける「監査」
- テーブルへのアクセス履歴やSQL文の実行履歴など監査ログを記録し、不正な操作を見つける
- 監査ツールに求められる機能
  - データベースのアクセスログを取得して分析
  - 不正アクセスやポリシー違反などを検知

監査ツールの評価ポイント

- 監査に必要な正確なログを取得できるか
- ログ収集負荷によるデータベース性能低下が許容範囲内か
- 情報流出などが発生した場合、迅速に追跡調査を行えるか
- J-SOX法、HIPAA、PCI DSSなど情報保護規制に準拠するか
- 特権ユーザーによる内部犯行を追跡できるか

監査製品の構成図(PISOの例)



特徴

システム性能を劣化させずに監査ログを取得
DBアクセスを可視化(監視、検索、レポート)
監査ログ保全(改ざん防止)と運用自動化

導入効果

各種法規制への対応
セキュリティの向上と標準化
監査運用コスト削減

不正アクセス検知(PISOの例)

select /* PISO_Seminar */ * from app.customer;

10,000,000件 抽出

PISO

DBA

顧客情報データベース

アクセス権限を持つ人物

名簿業者

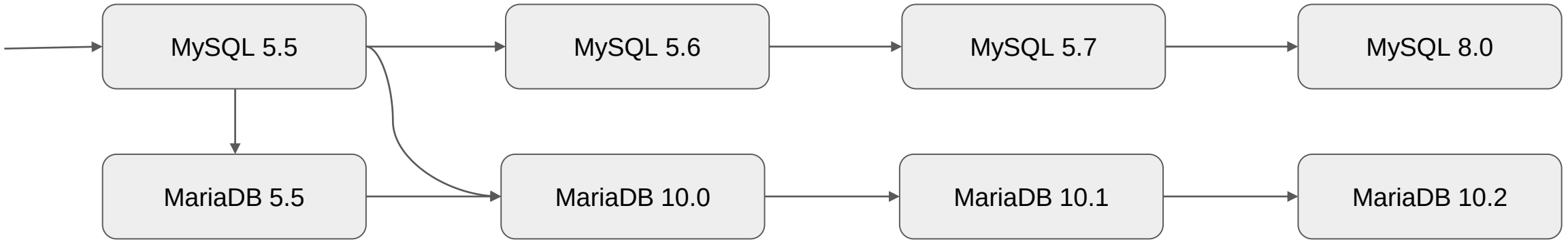
セキュリティ担当

監査ログの項目(PISOの例)

Who	ログイン
	ログアウト
	OSユーザ
	DBユーザ
When	警告日付
	ログ取得日付
Where	マシン
	端末
What	オブジェクト
	SQL開始日付
	SQL終了日付
	SQL文
How Many	実行回数
	処理行数
How	プロセスID
	実行プログラム
	アクション

ログオン	ログオン成功
	ログオン失敗
	ログオン継続時間
DDL成功・失敗	create
	drop
	alter
失敗DML	delete
	insert
	select
	update

MySQL/MariaDB のバージョンと分岐

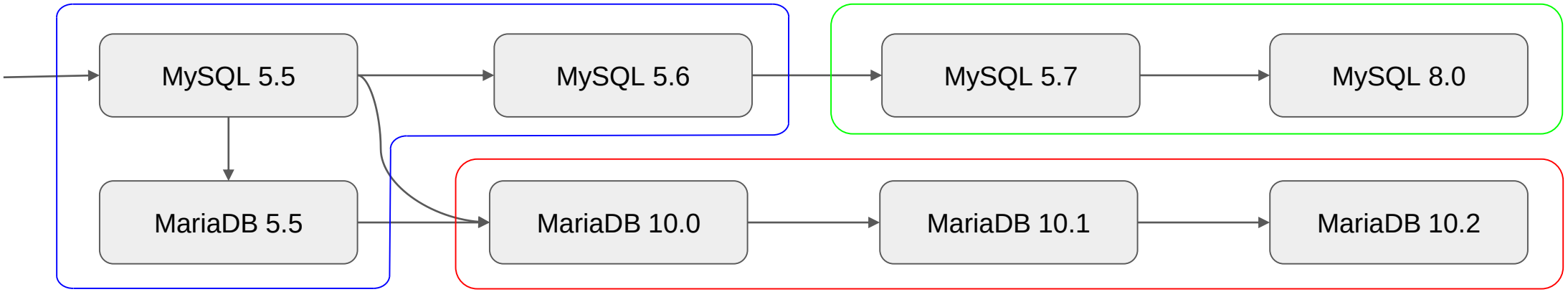


MariaDB 5.5 は MySQL 5.5 とほぼ同じ。

MariaDB 10.0 以降は MySQL とは別の道を歩む。

監査インタフェース(API)

- 監査インタフェース
  監査ログ収集用にMySQLが提供するAPI。
  DB操作に関する監査イベントの通知を受け取り、イベント情報を取得する。
- 監査インタフェースの分岐



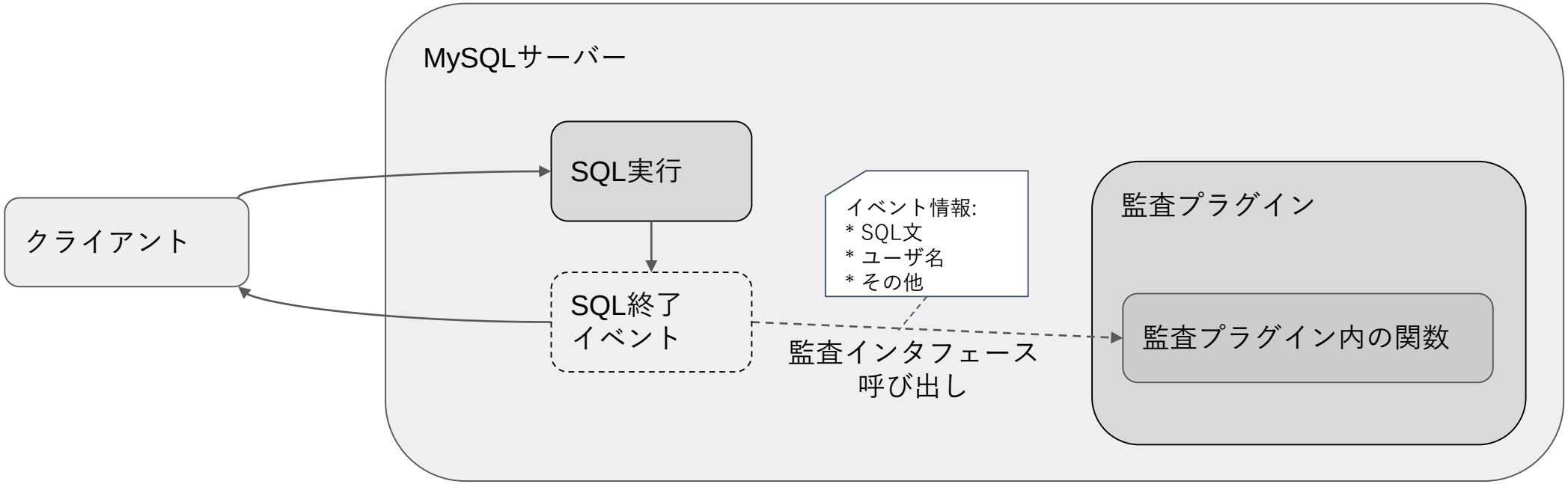
1 「MySQL 5.5, 5.6 & MariaDB 5.5」監査インタフェースは MySQL 5.5 に追加され、MySQL 5.6 と MariaDB 5.5 の監査インタフェースはほぼ同じ。

2 「MySQL 5.7 以降」 MySQL 5.7 は監査インタフェースに独自の拡張を行う。

3 「MariaDB 10.0 以降」 MariaDB 10.0 も監査インタフェースに独自の拡張を行う。ただし拡張の方向はかなり異なる。

監査プラグイン(共有ライブラリ)

- 監査プラグイン
  監査インタフェースを用いて、監査イベントを取得・加工する共有ライブラリ。
  事前登録の監査イベント通知を受け、自前関数でカスタマイズ処理を実行。
- 監査プラグインはイベントドリブンでログ収集



MySQL 内部で特定のイベントが起こったときに、
イベント情報とともにプラグインの関数を呼び出す。

監査インタフェースのイベント種類

- イベントの種類は様々

5.5以降の MySQL & MariaDB 全て

クラス	サブクラス
General	Log
	Error
	Result
	Status
Connection	Connect
	Disconnect
	Change User

MariaDB 5.5.37 で追加

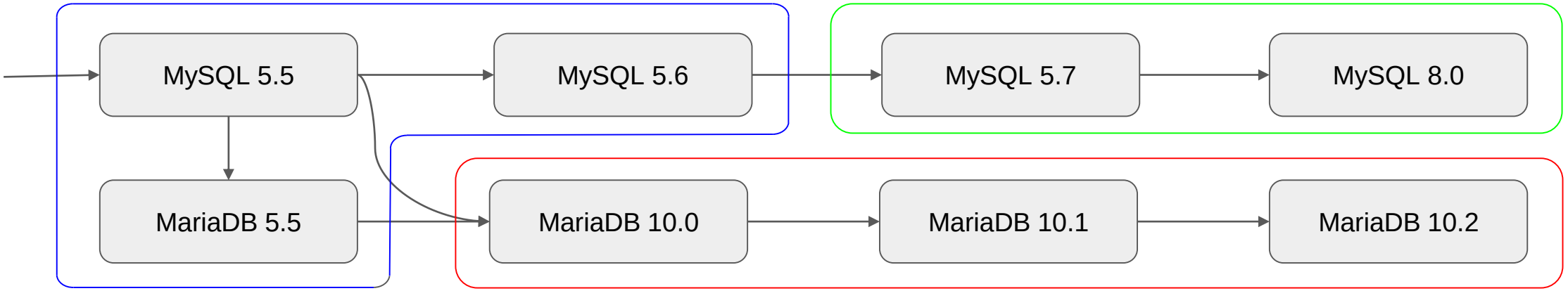
クラス	サブクラス
Table	Lock
	Create
	Drop
	Rename
	Alter

MySQL 5.7 で追加

クラス	サブクラス
Parse	...略...
Authorization	...略...
Table Access	...略...
Command	...略...
Query	...略...
Stored Program	...略...
...略...	...略...

※ MySQL 5.7 に追加されたイベント多数

MySQL/MariaDB の監査インタフェースの差異



1

Table : Lock (PISO不使用)を除くと MySQL 5.5, 5.6, MariaDB 5.5 の違いはない。
プロシージャ内部のSQLは取れない。

2

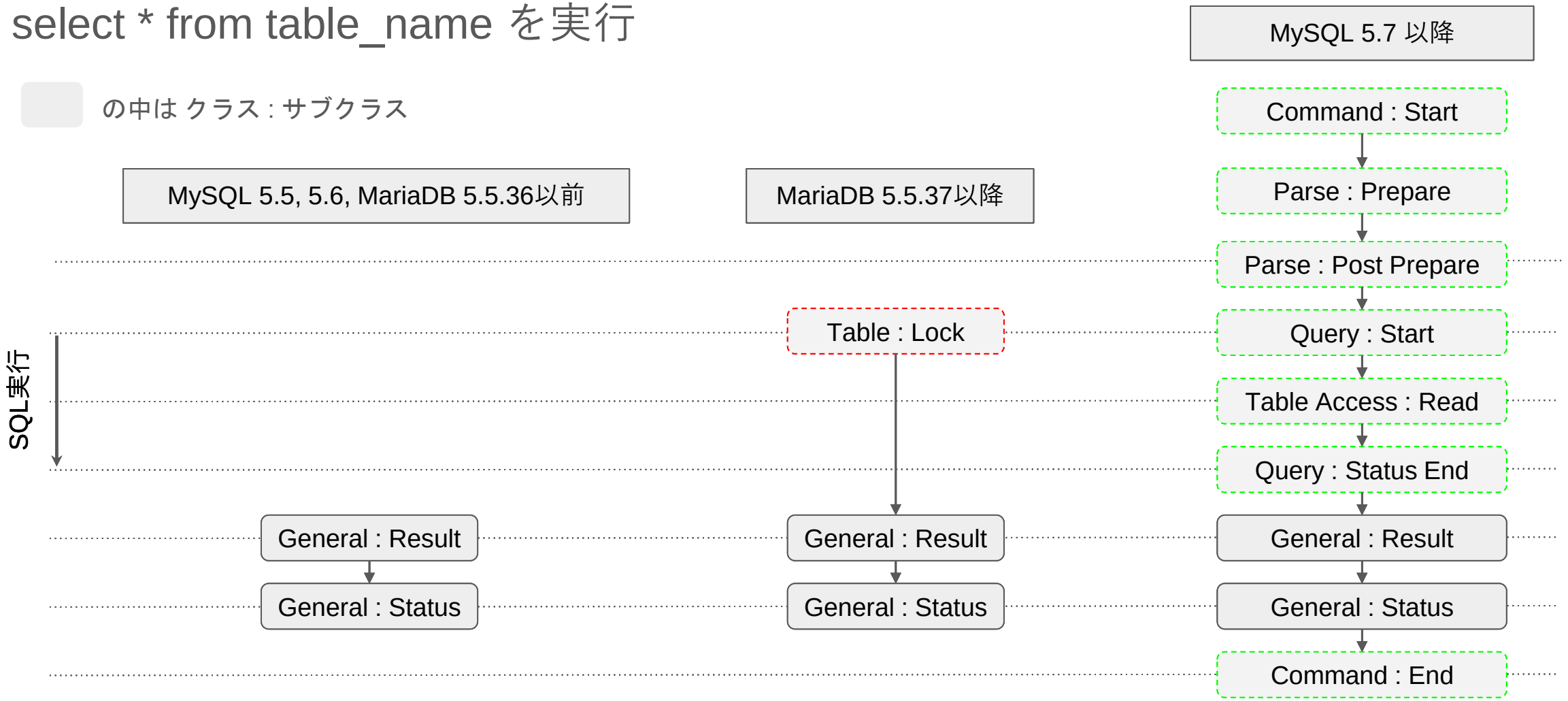
MySQL 5.7 は既存のイベントの発行タイミングに変化なし。
プロシージャ内部で実行されたSQLは新規追加のイベントで取得。

3

MariaDB 10.0 は新規のイベントの追加なし。
プロシージャ内部で実行されたSQLは既存のイベントで取得。
トップレベルのSQLなのか、内部のSQLなのか区別できない。

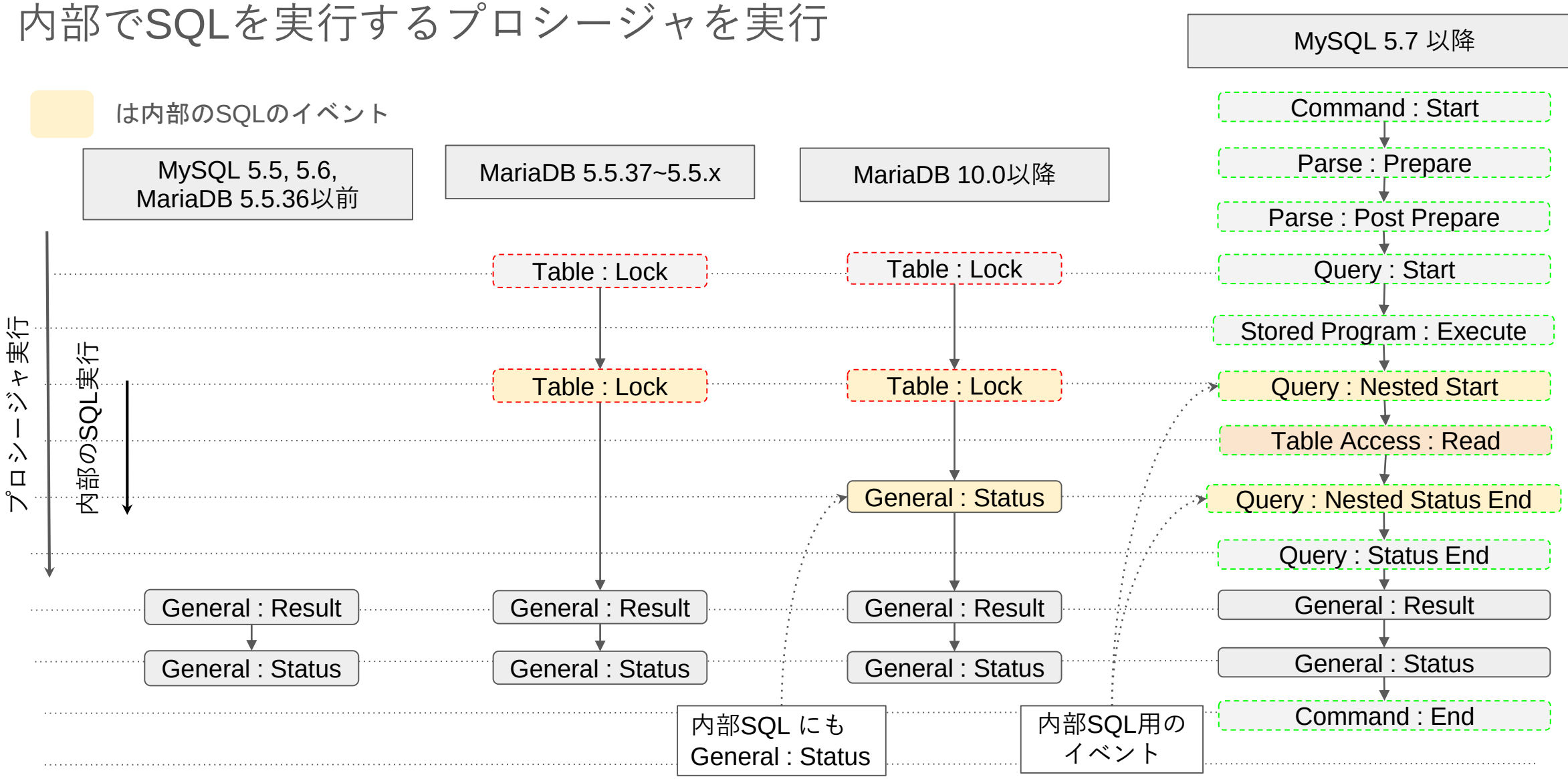
単純なSQLを実行したときのイベント

- select * from table_name を実行

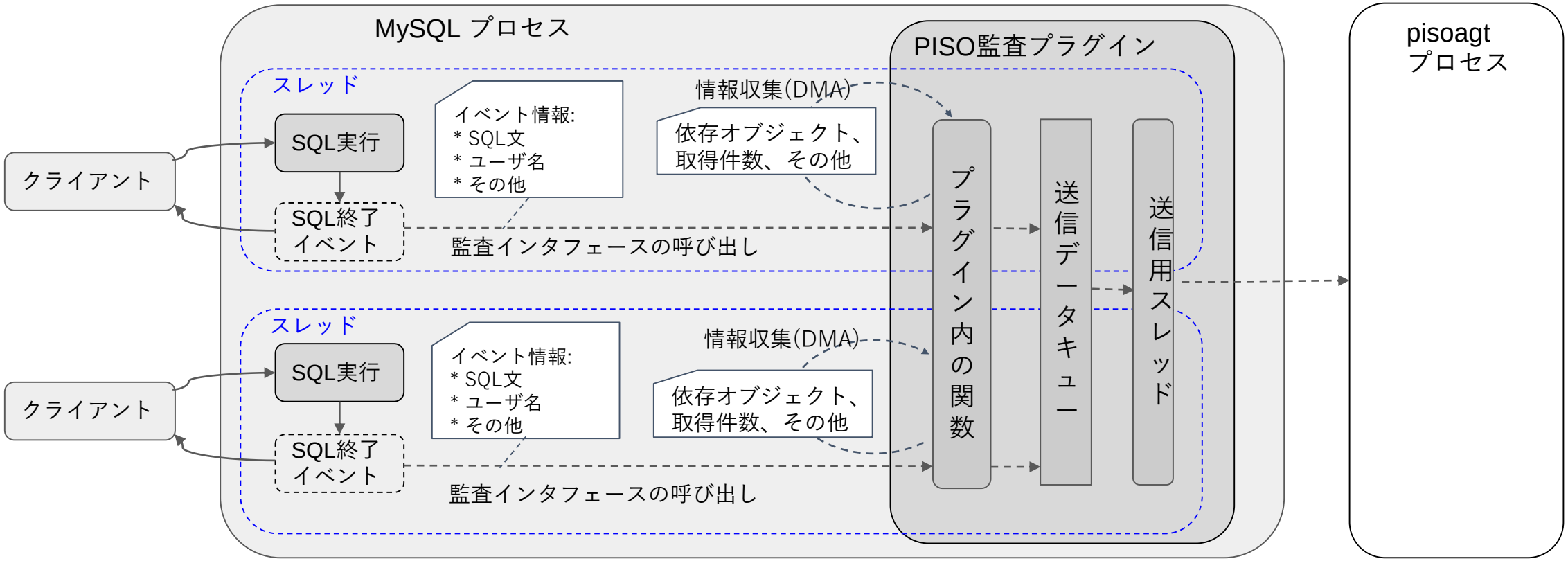


プロシージャを実行したときのイベント

- 内部でSQLを実行するプロシージャを実行

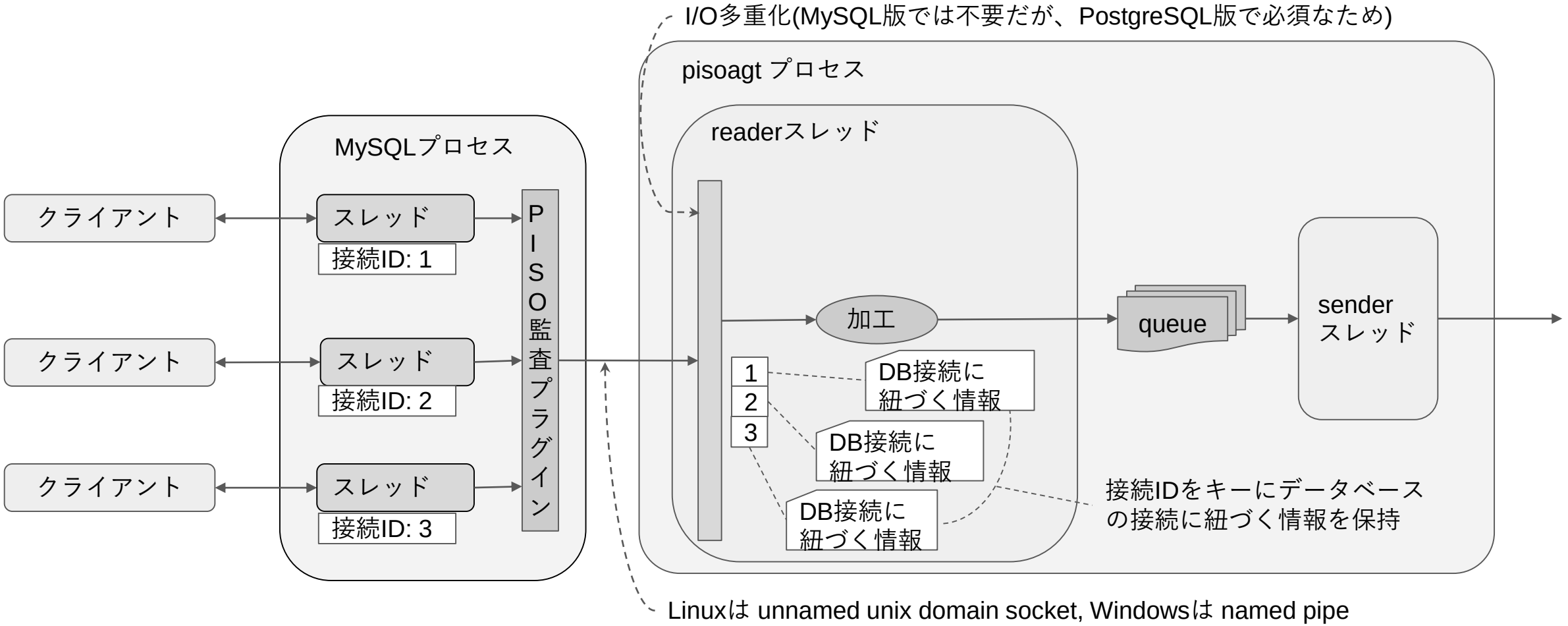


監査プラグインの内部構造(PISOの例)



- MySQL内部で発行するイベントをトリガーに、イベント情報とともに監査インタフェース (API)を呼び出す。
- イベントの提供する情報から収集した監査情報のみではPISO仕様を満たせないため、
プラグイン内の関数でメモリを参照しから必要な情報を取得し補完する(Direct Memory Access)。

PISOログ収集モジュールの構成



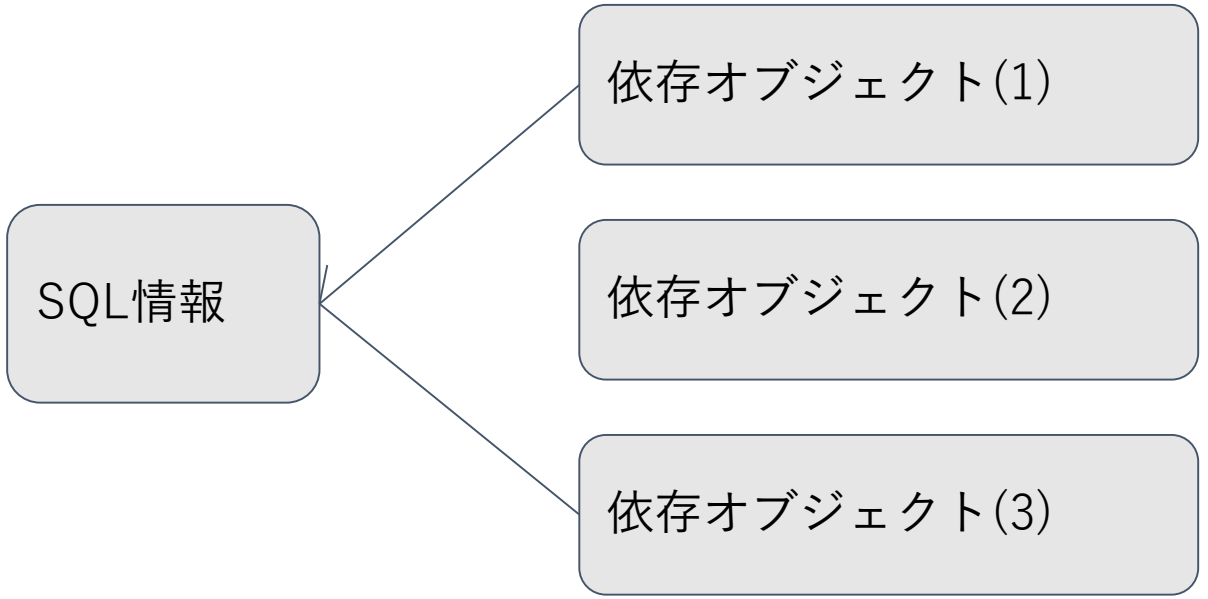
- MySQLは1プロセスで複数のクライアントの処理を行う、デフォルトで1接続につき1スレッドが使用される。
- PISOは監査プラグインを用いたメモリ参照型、PISO監査プラグインはMySQLプロセスにロードされる。

PISO監査プラグインの特徴

- 収集ログにおいて
  - 取得項目を拡張
  - 情報を分類し正規化
    - セッション
    - SQL
    - 参照オブジェクト
    - 統計情報
- 性能において
  - ファイル出力せずディスクI/Oなし
  - ログ量抑制(※ 詳細は右サイド)
  - 送信回数抑制(※ 詳細は後続)
  - マルチスレッド(※ 詳細は後続)
- マルチデータベースにおいて
  - 1つの監査プラグインでMySQLとMariaDB両方に対応
  - データ正規化により異種DBを同一の監査項目に落とし込んで一括管理

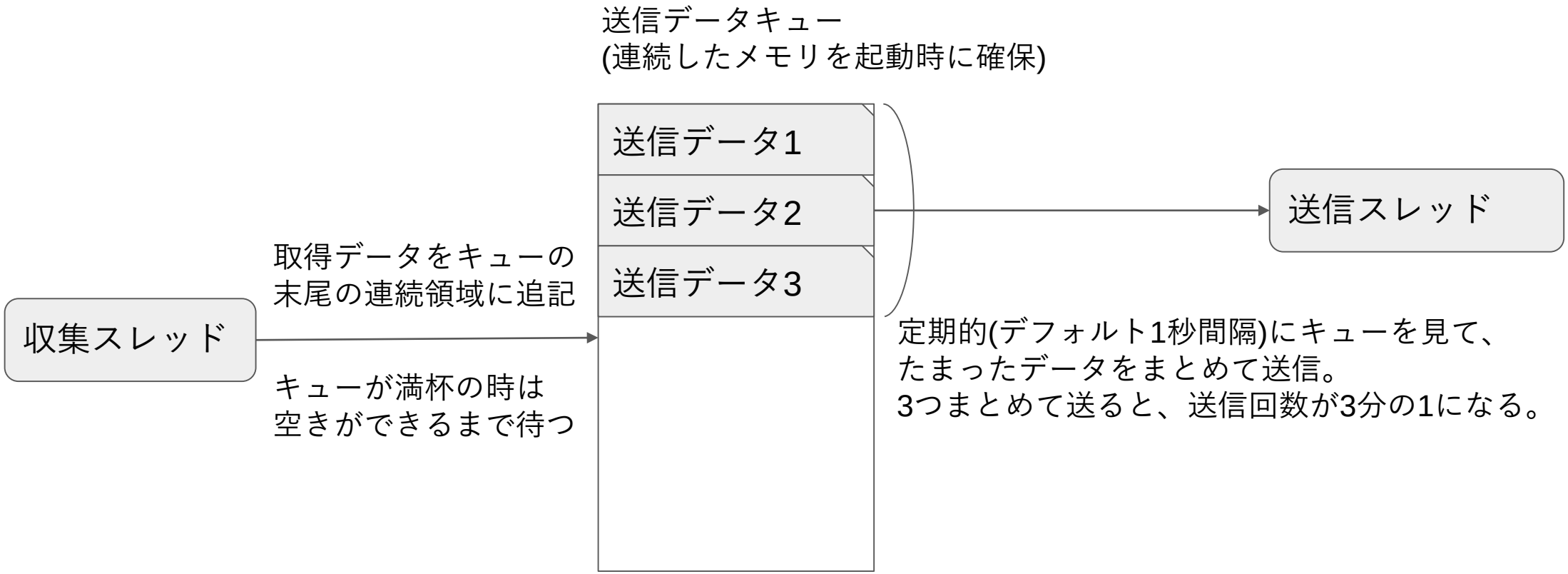
- ログ量抑止のアプローチ
  - 指定オブジェクトへアクセスしたSQLのみ記録(蓄積設定)
  - 指定ユーザが実行したSQLのみ記録(蓄積設定)
  - SQL文をハッシュ値に変換して記録し、同じSQLを重複蓄積しない
  - ノイズデータの除外
    - 指定条件に該当するアクセスを記録除外(除外設定)
      - 時間帯
      - プログラム名
      - マシン名
      - DBユーザ名
      - OSユーザ名(一部制限あり)
    - 活用例
      - バッチジョブを監査対象外とする

性能改善(エピソード1): データ送信回数抑制



- SQLが実行されたとき、SQLの情報と依存オブジェクトを別々に送信していた。
  例えば、依存オブジェクトが3つあるSQLが実行されたとき、計4回のデータ送信数。
- 1回で送信するように修正し送信数を減らす。
- その結果、TPM低下率が35%から17%に改善
  - 監査なし：32808 TPM
  - 監査あり：27305 TPM

性能改善(エピソード2) マルチスレッド処理



- その結果、TPM低下率 7% まで改善
  - 監査なし： 24001 TPM
  - 監査あり： 20804 TPM

まとめ

- 監査ログのみならず、ログ収集による
  データベース性能劣化も考慮すべき
- 監査目的や要件に合わせ、データを絞り込み、
  ログ量を抑制すべき
- 性能検証を行い、監査あり・なしの状態で
  TPM低下率とリソース使用率を比較すべき

アンケートのご記入をお願いします

https://docs.google.com/forms/d/e/1FAIpQLSdaAXrj_bBk6Xt2t-kS0-4Sz9sWY7nC88pEyivYdSH6g8jquQ/viewform?usp=sf_link

db tech showcase

ONLINE 2020

27TUE OCTOBER - 10THU DECEMBER

Thank You!