MySQL 5.1.47 リリースノート（日本語翻訳）

InnoDB Plugin に関する注意事項:

- InnoDB Plugin はバージョン 1.0.8 にアップグレードされている。本バージョンは、General Availability（GA）の品質であるとみなされている。InnoDB Plugin Change History には、ここで報告した変更点に加えて情報が含まれている場合がある。

  今回のリリースでは、InnoDB Plugin は、RHEL3、RHEL4、SuSE 9（x86、x86_64、ia64）、および Linux RPM 汎用パッケージを除き、ソースおよびバイナリディストリビューションに含まれている。また、FreeBSD 6 と HP-UX、および ia64 全般の Linux では動作しない。

機能の追加と変更:

- InnoDB は、リカバリ中に REDO ログ記録をハッシュテーブルに再保存する。64 ビットシステムでは、このハッシュテーブルはバッファプールサイズの 8 分の 1 である。メモリ使用量を減らすために、ハッシュテーブルの大きさがバッファプールサイズの 64 分の 1 に縮小した（32 ビットシステムでは 128 分の 1）（Bug#53122）。

修正されたバグ:

- **セキュリティ修正**: サーバは、COM_FIELD_LIST コマンドパケットのテーブル名引数の正当性およびテーブル名の許容基準への準拠をチェックしていなかった。したがって、特別に作成されたテーブル名引数を COM_FIELD_LIST に付与することで、権限およびテーブルレベルの許可に対するほぼすべての形式のチェックを迂回することが可能であった。

  つまり MySQL 5.0 以降では、1 つのテーブルの SELECT 権限を有する認証済みユーザが、その他のすべてのデータベースのすべてのテーブルのフィールド定義を取得でき、さらにはサーバのファイルシステムからアクセス可能なその他の MySQL インスタンスも取得できる可能性があった。

  さらに MySQL 5.1 以降では、1 つのテーブルの DELETE または SELECT 権限を有する認証済みユーザが、このサーバ上にあるすべてのデータベースのすべてのテーブルのコンテンツだけでなく、サーバのファイルシステムからアクセス可能なその

Copyright © 2012 Nomura Research Institute, Ltd. All rights reserved

他の MySQL インスタンスの削除や読み取りを行うことが可能であった（Bug#53371、CVE-2010-1848）。

- **セキュリティ修正**: COM_FIELD_LIST コマンドパケットのテーブル名引数に対して境界チェックを行わないため、サーバがバッファオーバーフロー攻撃を受ける可能性があった。テーブル名に長いデータを送信することでバッファのオーバーフローが引き起こされるため、認証済みユーザが悪意のあるコードを投入する可能性があった（Bug#53237、CVE-2010-1850）。
- **セキュリティ修正**: 1 つのパケットの最大サイズよりも大きなパケットを受信した場合、サーバが無制限にパケットの読み取りを続ける可能性があった（Bug#50974、CVE-2010-1849）。
- **重要な変更**: **レプリケーション**: CHANGE MASTER TO および SET GLOBAL sql_slave_skip_counter を実行すると、ステートメント実行以前のスレーブの状態に関する情報がエラーログに書き込まれるようになった。CHANGE MASTER TO の場合は、MASTER_HOST、MASTER_PORT、MASTER_LOG_FILE、MASTER_LOG_POS の以前の値などが書き込まれる。SET GLOBAL sql_slave_skip_counter の場合は、sql_slave_skip_counter の以前の値、グループのリレーログ名、グループのリレーログ位置などが書き込まれる（Bug#43406、Bug#43407）。
- **レプリケーション**: REVOKE ステートメントの失敗が間違ったエラーコードで記録されていたため、マスター上での失敗が予測されていた場合でもレプリケーションスレーブが停止した（Bug#51987）。
- 一部のパス名が LOAD_FILE()に渡された場合に、サーバクラッシュを引き起こす可能性があった（Bug#53417）。
- INSERT 中の外部キー制約違反を報告する際に、InnoDB は DB_TRX_ID および DB_ROLL_PTR システムカラムに、初期化されていないデータを表示する可能性があった（Bug#53202）。
- 圧縮テーブルを使用している場合、InnoDB ページ分割が無限ループに陥ることがあった（Bug#52964）。
- カラム値のプレフィックスのインデックスを含む DYNAMIC または COMPRESSED フォーマットの InnoDB テーブルから削除マークの付いたレコードを消去している間に、厳密すぎる表明が失敗する可能性があった（Bug#52746）。
- InnoDB は、レコードヘッダに“オフページストレージ”フラグがあることを確認せずにオフページストレージの選択を試みていた。これを修正するために、DYNAMIC および COMPRESSED フォーマットにおいて、InnoDB は長さの上限が 256 バイトを超えない非 BLOB カラムをローカルに保存するようになった。これは、長さの上

Copyright © 2012 Nomura Research Institute, Ltd. All rights reserved

限が 255 バイト以下の場合は、“外部ストレージ”フラグが入る余地がないからである。REDUNDANT および COMPACT フォーマットにおいては、InnoDB は local_len = 788 バイトまでの長さのカラムは常にローカルに保存するため、この制限は当然適用される（Bug#52745）。

- Bug#3300 に対処するために、InnoDB に半一貫的読み込みが実装された。半一貫的読み込みは、一致しないレコードが既に他のトランザクションによってロックされている場合は、そのトランザクションをブロックしない。レコードがロックされていない場合はロックを取得するが、そのレコードが WHERE 条件に合致しない場合はロックをリリースする。しかし、pk_col1=constant1, ..., pk_colN=constantN 形式の WHERE 条件を有する UPDATE ステートメントについても半一貫的読み込みを試みており、半一貫的読み込みはテーブルスキャンの際のみ試行される、という前提のもとに設計されたいくつかのコードの実行が失敗していた（Bug#52663）。
- 空文字列に@@GLOBAL.debug を設定すると、現行のデバッグ設定をクリアできなかった（Bug#52629）。
- コンパレータアレイ（Arg_comparator クラスのメンバ）の割り当ての解除をしなかったことによりメモリリークが発生した（Bug#52124）。
- デバッグビルドにおいて、照合順序の調整が必要な可能性のあるサブクエリを含むビューを作成すると表明が発生した。例えば、照合順序の異なる複数のアイテムがあり、結果の照合順序をその内のどれか 1 つに調整できる場合に表明が発生する可能性があった（Bug#52120）。
- InnoDB の行ロックを待機している接続は、行ロックの待機が終了するまで KILL を無視していた。ロック待機中に KILL が実行されると“lock wait timeout exceeded”ではなく“query interrupted”エラーになるようになった（Bug#51920）。
- LOCK_plugin、LOCK_global_system_variables、LOCK_status mutex などでロックを実行した場合に、デッドロックが発生する可能性があった（Bug#51591）。
- InnoDB は、高速インデックス作成の際に間違ってテーブルコピーを使用する場合があった（Bug#50946）。
- トリガのリストを作成する際に、構文的に間違ったトリガにより、サーバがクラッシュする可能性があった（Bug#50755）。
- InnoDB Plugin は、すべてのカラムが埋まっている場合、ある行が最大サイズをオーバーすることが可能かどうかチェックする。そのため、組み込み InnoDB で作成できるテーブルについて、Row size too large エラーが生じる場合があった。したがって、innodb_strict_mode がオンになっている場合、または動的テーブルもしくは圧縮テーブルの場合のみチェックが行われるようになった（Bug#50495）。
- --secure-file-priv に空白文字に設定しても有効にならなかった（Bug#50373）。

Copyright © 2012 Nomura Research Institute, Ltd. All rights reserved

- MySQL 5.1 では、行ベースのバイナリログの制限により READ COMMITTED によるロックの使用を減らすように変更された（Section 12.3.6「SET TRANSACTION Syntax」の「READ COMMITTED」の Note を参照）。しかし、READ UNCOMMITTED はそのように変更されなかったため、より高く設定されたアイソレーションレベルを超えるロックを使用していた。これは予想していなかったことである。したがって、READ UNCOMMITTED についてもロックの使用を減らし、READ COMMITTED と同様のバイナリログの制限を設けるように変更された（Bug#48607）。
- サブクエリを含むクエリで EXPLAIN を実行すると、サーバがクラッシュする可能性があった（Bug#48419）。
- Windows では、サーバが Event ID 100 の記述を見つけることができなかった（Bug#48042）。
- InnoDB テーブルの更新の際に、値の変更がない場合でも TIMESTAMP カラムが更新される可能性があった（Bug#47453）。
- *mysqld_safe* が *mysqld* に--open-files-limit を渡さない場合があった。また、*mysqld_safe* は、ダッシュやアンダースコアをオプション名と同等に扱わなかった（Bug#47095）。
- --skip-grant-tables でサーバを起動する場合、プラグインのロードおよびアンロードは許可されるべきではないが、サーバは INSTALL PLUGIN および UNINSTALL PLUGIN ステートメントを拒否しなかった（Bug#46261）。
- InnoDB は、NULL カラムにユニークインデックスを作成できない場合があった（Bug#41094）。
- time_t の定義が、サーバ側で想定したものと違った場合でも、Windows 上のストレージエンジンプラグインをビルドすることができてしまった。その違いにより、影響を受けたプラグインがクラッシュする可能性があった。さらに、ストレージエンジンの API 層において time_t 型の使用が強制されていた（Bug#39802、Bug#40092）。
- UNINSTALL PLUGIN を使用してロードされたプラグインを削除する際に、オープンテーブルおよび接続が原因で、オープン接続が切断されるまで *mysqld* がハングしていた（Bug#39053）。
- 1）FLUSH PRIVILEGES 操作中にスレッドが中断された場合、不適切な診断エリアの設定により、後にデバッグ表明が発生することがまれにあった。2）KILL 操作を行うと、診断エリアの状態に関するコンソールエラーメッセージが、そのような状態の存在を確認せずに発生する可能性があった（Bug#33982）。

※本翻訳は、理解のための便宜的な訳文として、オラクルが著作権等を保有する英語原文を NRI の責任において翻訳したものであり、変更情報の

Copyright © 2012 Nomura Research Institute, Ltd. All rights reserved

正本は英語文です。また、翻訳に誤訳等があったとしても、オラクルには一切の責任はありません。

Copyright © 2012 Nomura Research Institute, Ltd. All rights reserved