MySQL 5.1.46sp1 リリースノート （日本語翻訳）

これは MySQL Enterprise Server 5.1 の *サービスパック*リリースです。

> **重要**
>
> InnoDB のプラグインバージョンを使用する場合は、5.1.46sp1 ではなく、MySQL 5.1.48 以降を使用することをお勧めします。これは、5.1.46sp1 には最初のプロダクションレディバージョンが含まれており、その後のバージョンではより広範囲にわたるプロダクションユースで見つかったバグがいくつか修正されているためです。

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）。
- ALTER DATABASE `#mysql50#<*special*>` UPGRADE DATA DIRECTORY NAME の<*special*>が「.」、「..」、または「./」あるいは「../」で始まるシーケンスの場合、MySQL はこのステートメントを正しく処理しなかった。MySQL はサーバデータディレクトリ（他の通常のデータベースが含まれている）をデータベースディレクトリとして使用していた（Bug#53804、CVE-2010-2008）。
- 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）。
- 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）。
- 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）。
- INFORMATION_SCHEMA.ROUTINES または INFORMATION_SCHEMA.PARAMETERS から選択を行うと、メモリリークが発生した（Bug#48729）。
- 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）。

※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。