概要

Firepower システム® データベース アクセス機能により、シスコ Firepower Management Center では、JDBC SSL 接続をサポートしているサードパーティ クライアントを使用して、侵入、検出、ユーザ アクティビティ、相関、接続、脆弱性、アプリケーション、および URL 統計のデータベース テーブルを照会できます。

Crystal Reports、Actuate BIRT、JasperSoft iReport などの業界標準のレポート作成ツールを使用してクエリを作成し、送信することができます。また、独自のカスタム アプリケーションを設定してプログラム制御下にある シスコ データを照会することもできます。たとえば、侵入およびディスカバリ イベント データについて定期的にレポートしたり、アラート ダッシュボードをリフレッシュしたりするサーブレットを構築することが可能です。

1 つのクライアントで複数の Firepower Management Center に接続できますが、それぞれへのアクセスを個別に設定する必要があることに注意してください。

接続するアプライアンスを決定する際には、シスコ アプライアンス上のデータベースを照会すると、使用可能なアプライアンス リソースが減少する点に注意してください。クエリを慎重に設計し、組織の優先度に対応した適切な時点でクエリを送信する必要があります。

詳細については、次の項を参照してください。

バージョン 6.3 でのデータベース アクセスの重要な変更

Firepower システム展開をバージョン 6.1 から バージョン 6.3 にアップグレードする場合、次に示す変更に注意してください。これらの変更の一部では、クエリを更新する必要があります。

バージョン 6.3 の新規テーブルおよび変更されたテーブル

次の表に、バージョン 6.3 のデータベース アクセス テーブルに対する変更を示します。

表 1-1　　でのテーブルの変更の概要バージョン 6.3

テーブル	変更の説明
rule_documentation	テーブルが廃止されました

前提条件

データベースアクセス機能を使用する前に、以降の項で説明する前提条件を満たしている必要があります。

ライセンス

いずれかの シスコ ライセンスがインストールされている場合には、外部データベースを照会できます。ただし、一部のテーブルは、ライセンスされている機能に関連付けられています。これらのテーブルにデータが取り込まれるのは、関連付けられている機能を使用できるようにライセンスが設定されており、そのデータが生成されるように展開が適切に設定されている場合だけです。ライセンスされていない機能に関連付けられているテーブルを照会することはできません。ライセンスの詳細については、『*Firepower Management Center Configuration Guide*』の「Understanding Licensing」を参照してください。

Firepower システム 機能と用語

このマニュアルの情報を理解するには、Firepower システム の機能と名称、そのコンポーネントの機能について理解しておく必要があります。これらのコンポーネントにより生成される各種イベント データについて理解しておく必要があります。『*Firepower Management Center Configuration Guide*』では、聞き慣れない用語や製品固有の用語の定義を頻繁に確認できます。この構成ガイドには、このマニュアルで説明するフィールドのデータに関する追加情報も収録されています。

通信ポート

Firepower システム では、内外のアプライアンス間で通信を行い、ネットワーク展開内で特定の機能を有効にするために、特定のポートを使用する必要があります。

Firepower Management Center でデータベース アクセスを有効にすると、クライアントとアプライアンスの間で JDBC トラフィックを伝送する接続にポート 1500 と 2000 が使用されます。

クライアント システム

Firepower システム データベースへの接続に使用するコンピュータに、Java ソフトウェア（Java Runtime Environment（JRE）とも呼ばれます）または Java 仮想マシン（JVM）をインストールする必要があります。最新バージョンの Java を `http://java.com/` からダウンロードできます。

Firepower Management Center から、データベースへの接続に使用する JDBC ドライバ ファイルが含まれているパッケージをダウンロードして解凍する必要があります。このパッケージには、Firepower Management Center との暗号化通信用の SSL 証明書のインストールに使用する実行可能ファイルや、これらのユーティリティのその他のソース ファイルも含まれています。

また、ご使用のコンピュータで該当するシステム設定（環境変数など）を変更する方法も理解しておく必要があります。

クエリ アプリケーション

Firepower システム データベースを照会するには、商用のレポート ツール（Actuate BIRT、JasperSoft iReport、または Crystal Reports など）や、JDBC SSL 接続をサポートするその他の任意のアプリケーション（カスタム アプリケーションを含む）を使用できます。このマニュアルでは、データベースに接続するために必要な情報（JDBC URL、ドライバ JAR ファイル、ドライバ クラスなど）について説明します。ただし、JDBC SSL 接続の詳しい設定手順については、ご使用のレポート ツールのドキュメントを参照してください。

シスコ には、RunQuery と呼ばれるサンプル コマンドライン Java アプリケーションもあります。このアプリケーションを使用して、データベース接続のテストやスキーマの表示を実行できるほか、基本クエリまたはアドホック クエリを手動で実行することができます。RunQuery のソース コードは、カスタム Java アプリケーションでデータベース接続を設定する際のリファレンスでもあります。RunQuery ソース コードは、Firepower Management Center からダウンロードする ZIP パッケージに含まれています。

RunQuery はサンプル クライアントであり、フル機能のレポート ツール**ではありません**。シスコでは、データベース照会の主な手段として、このツールを使用しないことを**強く**推奨します。RunQuery の使用法については、ZIP パッケージに含まれている README ファイルを参照してください。

データベース アクセス機能が使用する JDBC 機能は次に示すものだけである点に注意してください。

- データベース メタデータ（スキーマ、バージョン、およびサポートされている機能などの情報を含みます）。
- SQL クエリの実行

データベース アクセスではその他の JDBC 機能（ストアド プロシージャ、トランザクション、バッチ コマンド、複数の結果セット、挿入/更新/削除機能など）は使用されません。

データベース クエリ

データベースを照会するには、結合条件を使用した 1 つまたは複数のテーブルに対する `SELECT` ステートメントの記述方法と実行方法を理解している必要があります。

ユーザを支援するため、このマニュアルでは、サポートされている MySQL クエリの構文、Firepower システム データベース スキーマ、許可されている結合、およびクエリに関連するその他の重要な要件と制約事項について説明します。

最初に行う作業

前提条件（1-2 ページ）で説明する前提条件を満たしていることを確認したら、最初に Firepower Management Center に接続するようにクライアント システムを設定できます。

データベース アクセスのセットアップ（2-1 ページ）では、アクセスを許可するようにアプライアンスを設定する方法、アプライアンスに接続するようにクライアント システムを設定する方法、およびアプライアンスに接続するようにレポート アプリケーションを設定する方法について説明します。また、いくつかの基本的なクエリの手順と、サポートされている MySQL 構文について説明します。

このマニュアルの残りの部分には、データベースのスキーマと結合に関する情報とサンプル クエリを収録しており、次の章で構成されています。

- スキーマ：システム レベル テーブル（3-1 ページ）では、システム レベル テーブル（監査ログやヘルス イベントなど）のスキーマと結合について説明します。
- スキーマ：侵入テーブル（4-1 ページ）では、侵入関連テーブルのスキーマと結合について説明します。
- スキーマ：統計情報追跡テーブル（5-1 ページ）では、アプリケーション、URL、およびユーザ統計情報のテーブルのスキーマと結合について説明します。
- スキーマ：検出イベントおよびネットワーク マップのテーブル（6-1 ページ）では、検出イベントとネットワーク マップ情報（ネットワーク資産に関する情報）が格納されているテーブルのスキーマと結合について説明します。
- スキーマ：接続ログ テーブル（7-1 ページ）では、接続イベントと接続サマリ イベントの情報が格納されているテーブルのスキーマと結合について説明します。
- スキーマ：ユーザ アクティビティ テーブル（8-1 ページ）では、ユーザ検出およびアイデンティティ データが格納されているテーブルのスキーマと結合について説明します。
- スキーマ：相関テーブル（9-1 ページ）では、相関関連テーブル（ホワイト リスト イベントおよび違反、修復ステータス データなど）のスキーマと結合について説明します。
- スキーマ：ファイル イベント テーブル（10-1 ページ）では、ファイル イベントが格納されているテーブルのスキーマと結合について説明します。