### matchfeed()

脅威インテリジェンスフィードにおいて、対象式の評価値が検出された場合は true、検出されなかった場合は false を返します。

#### 構文

matchfeed(STR\_FEED, STR\_EXPR)

必須パラメータ

**STR\_FEED**

脅威インテリジェンスフィード文字列。フィード文字列には以下のタイプを指定できます。無効なフィード文字列定数を使用した場合、クエリは失敗します。

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | STR\_FEED | タイプ | 説明 |
| ログプレッソ・ソナー CTI IP | logpresso\_cti\_ip | IP | サイバー攻撃に関連する悪性IPアドレス情報 |
| ログプレッソ・ソナー CTI ドメイン | logpresso\_cti\_domain | DOMAIN | マルウェア配布サイト、C&Cサーバー等の悪性ドメインアドレス情報 |
| ログプレッソ・ソナー CTI URL | logpresso\_cti\_url | URL | ログプレッソ・ソナー CTI URL インジケーター情報 |
| ログプレッソ・ソナー CTI MD5 | logpresso\_cti\_md5 | MD5 | ログプレッソ・ソナー CTI MD5 ハッシュインジケーターフィード |
| ログプレッソ・ソナー CTI SHA1 | logpresso\_cti\_sha1 | SHA1 | ログプレッソ・ソナー CTI SHA1 ハッシュインジケーターフィード |
| ログプレッソ・ソナー CTI SHA256 | logpresso\_cti\_sha256 | SHA256 | ログプレッソ・ソナー CTI SHA256 ハッシュインジケーターフィード |

上記以外にも、ソナーにインストールされたアプリが提供するフィードを利用できます。アプリが提供するフィード識別子については、該当アプリのドキュメントを参照してください。

**STR\_EXPR**

脅威インテリジェンスフィード内で検索する文字列