

管理者コンソール › レポート

エラスティック SIEM

ヘルプセンターで表示:
<https://bitwarden.com/help/elastic-siem/>

エラスティック SIEM

Elasticは、Bitwarden組織の監視のための検索と観察可能性のオプションを提供できるソリューションです。Elastic Agentは、Elastic Bitwardenの統合を使用して、コレクション、イベント、グループ、およびポリシー情報を監視する機能を提供します。

設定

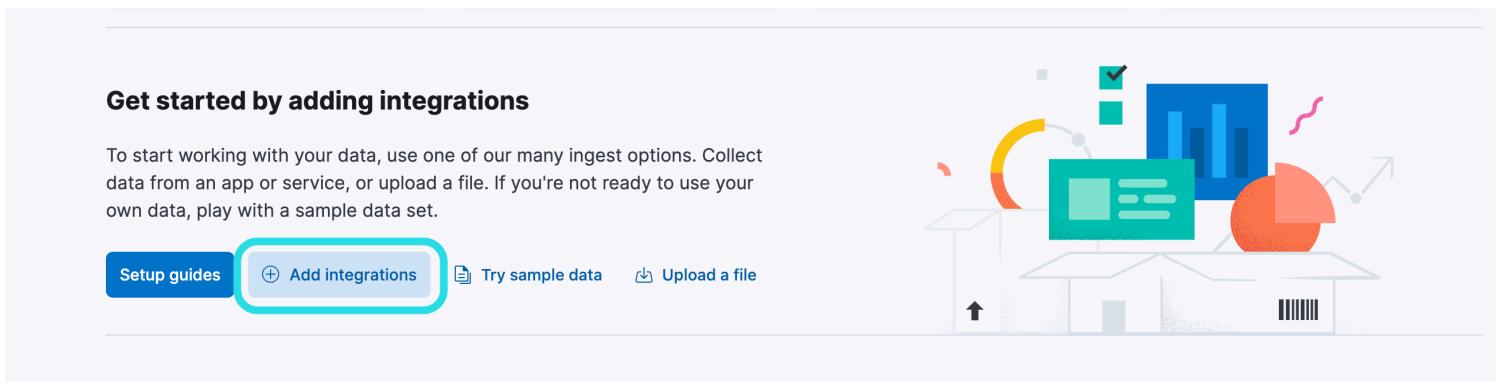
エラスティックアカウントを作成します

まず、Elasticアカウントを作成することから始めてください。このステップは、Elasticのクラウドホストサービス（推奨）またはオンプレミスサービスでデータを監視するダッシュボードを設定するために必要です。

Bitwardenの統合を追加してください

データの監視にはElastic SearchとKibanaを使用してデータを視覚化する必要があります。

1. Elasticのホーム画面で下にスクロールし、インテグレーションを追加を見つけてください。



2. 一度インテグレーションカタログに移動したら、検索フィールドにBitwardenを入力し、Bitwardenを選択してください。

Integrations

Choose an integration to start collecting and analyzing your data.

[Browse integrations](#) [Installed integrations](#)

All categories

335

APM

1

AWS

36

Azure

23

Cloud

5

Containers

15

Custom

30

Database

35

Elastic Stack

35

Elasticsearch SDK

9

Bitwarden



Bitwarden

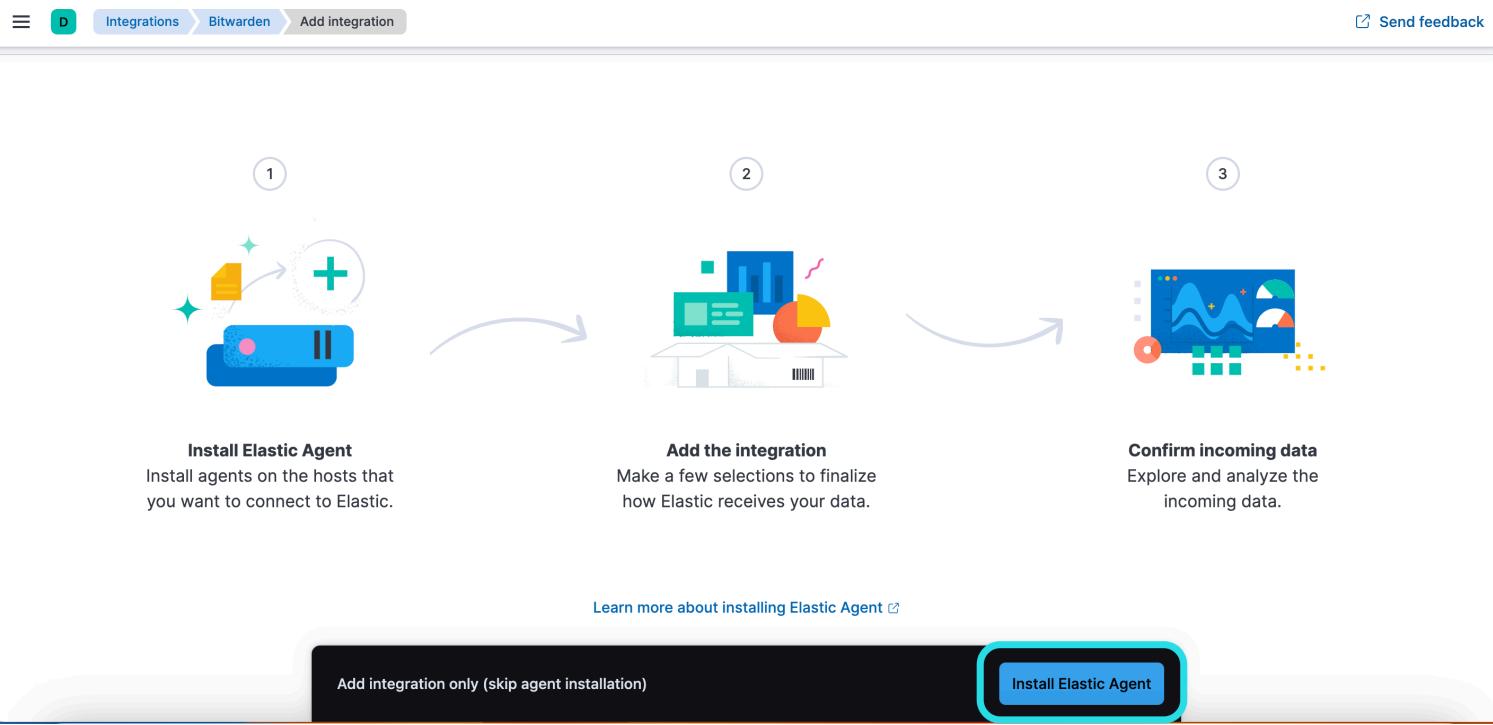
Collect logs from Bitwarden with Elastic Agent.

Don't see an integration? Collect any logs or metrics using our [custom inputs](#). Request new integrations in our [forum](#).

Bitwarden Elastic Integration

3. Bitwardenを追加ボタンを選択して、インテグレーションをインストールします。

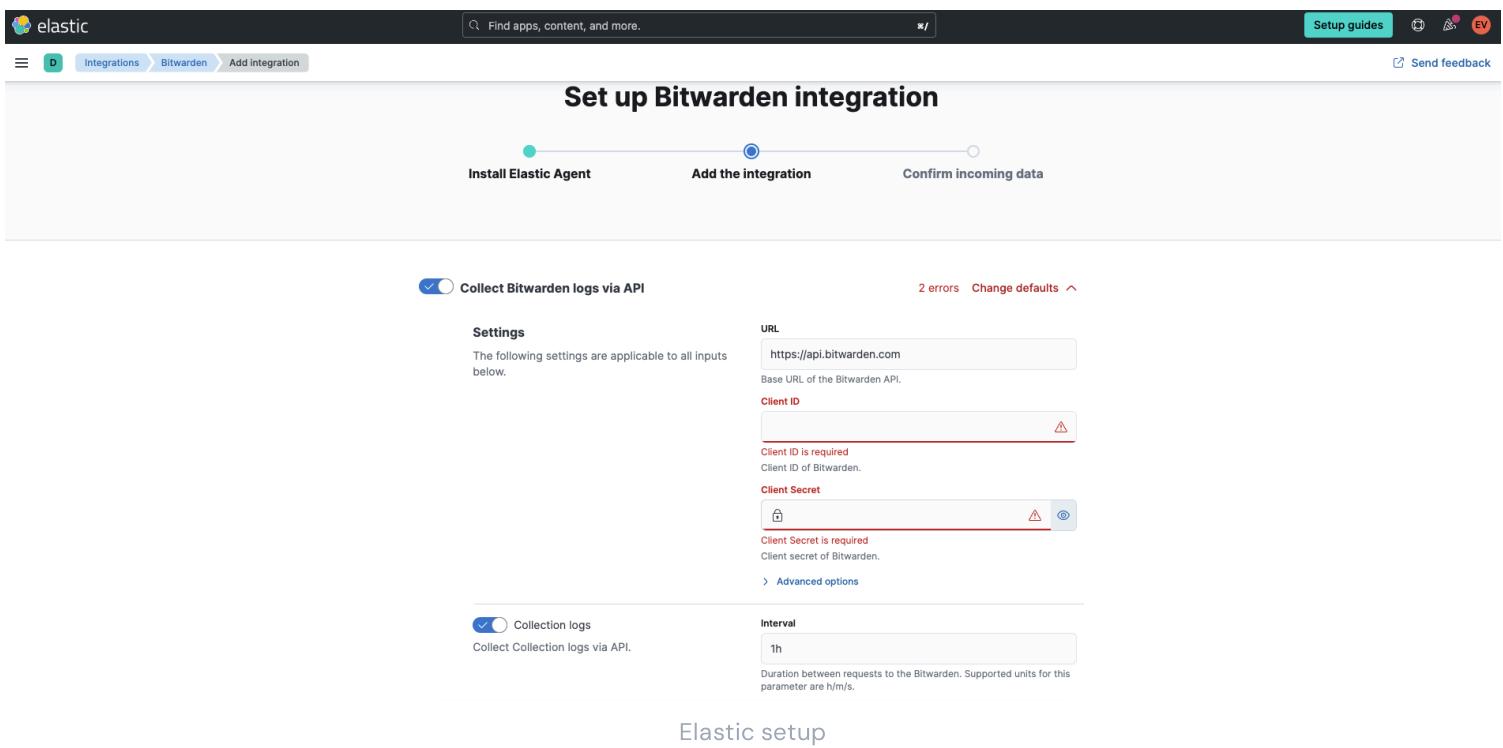
4. これがあなたの初めてのElasticの統合である場合、Elastic Agentをインストールする必要があります。次の画面で、**Elastic Agentをインストール**を選択し、インストール手順に従ってください。



The screenshot shows the Bitwarden Integrations page. On the left, there's a sidebar with categories like All categories (335), APM, AWS, Azure, Cloud, Containers, Custom, Database, Elastic Stack, and Elasticsearch SDK. In the center, there's a search bar with 'Bitwarden' typed in. Below it is the 'Bitwarden' integration card, which includes the Bitwarden logo, the name 'Bitwarden', a brief description 'Collect logs from Bitwarden with Elastic Agent.', and a note about custom inputs and forums. At the bottom of the page, there's a message 'Bitwarden Elastic Integration'. The main content area has a breadcrumb navigation: Integrations > Bitwarden > Add integration. To the right, there's a 'Send feedback' link. The main content area shows three steps: 1. Install Elastic Agent (with a sub-note: 'Install agents on the hosts that you want to connect to Elastic.'), 2. Add the integration (with a sub-note: 'Make a few selections to finalize how Elastic receives your data.'), and 3. Confirm incoming data (with a sub-note: 'Explore and analyze the incoming data.'). Below these steps is a link 'Learn more about installing Elastic Agent'. At the bottom, there are two buttons: 'Add integration only (skip agent installation)' and 'Install Elastic Agent' (which is highlighted with a blue border).

Install Elastic Agent

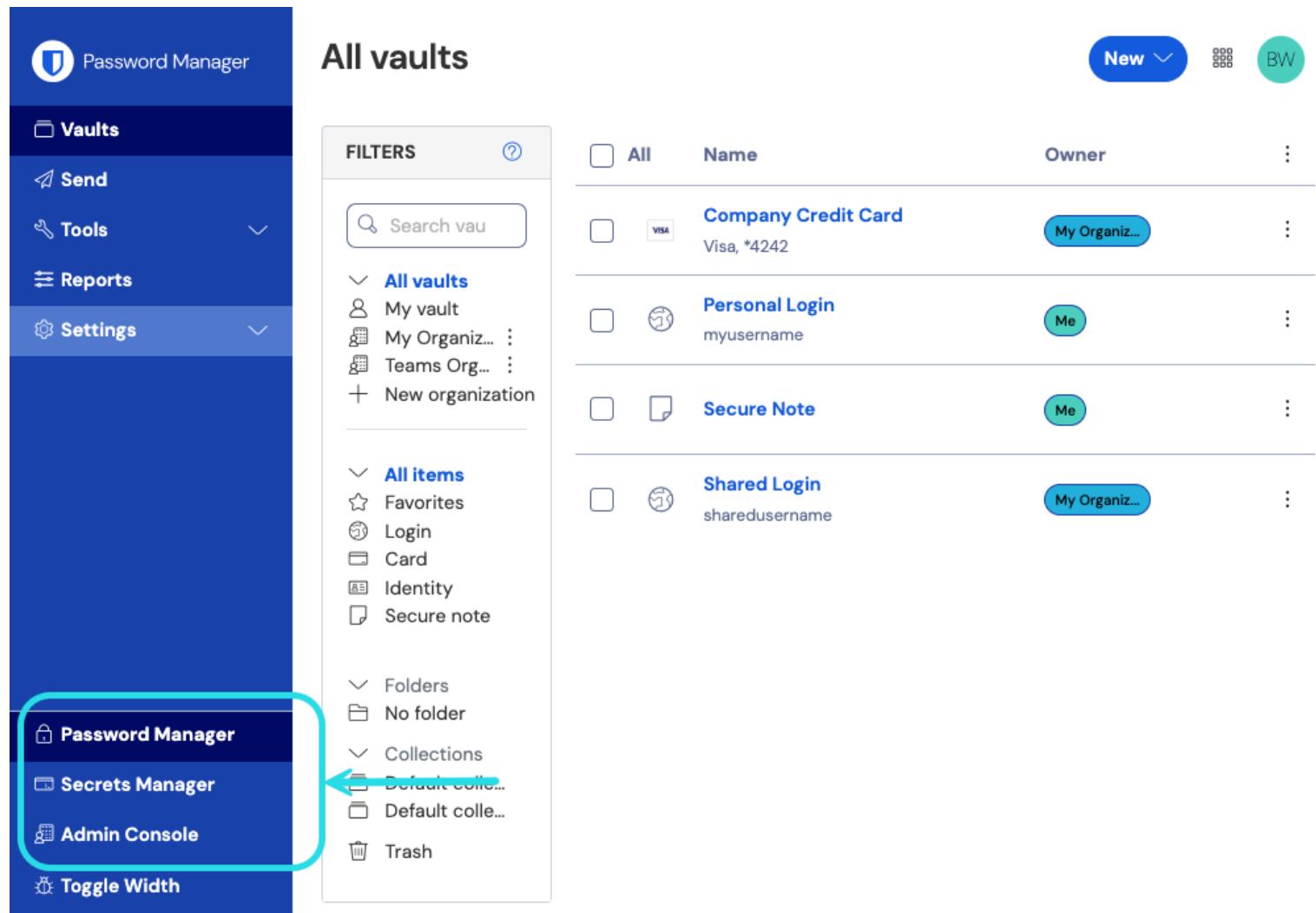
5. Bitwardenの統合を実行するためには、Elastic Agentが統合データを維持する必要があります。インストールが完了すると、Elasticは成功したインストールを検出します。エージェントの設定が成功した後、**インテグレーションを追加**を選択してください。



The screenshot shows the 'Set up Bitwarden integration' step in the Bitwarden integration setup process. The progress bar indicates three steps: 'Install Elastic Agent' (green dot), 'Add the integration' (blue dot, currently active), and 'Confirm incoming data' (grey dot). The main configuration area is titled 'Collect Bitwarden logs via API'. It includes fields for 'URL' (https://api.bitwarden.com), 'Client ID' (empty field with error message 'Client ID is required'), 'Client Secret' (empty field with error message 'Client Secret is required'), and 'Interval' (1h). A note states 'The following settings are applicable to all inputs below.' A 'Collection logs' checkbox is checked. At the bottom right, there's a link to 'Elastic setup'.

Bitwardenにインテグレーションを接続する

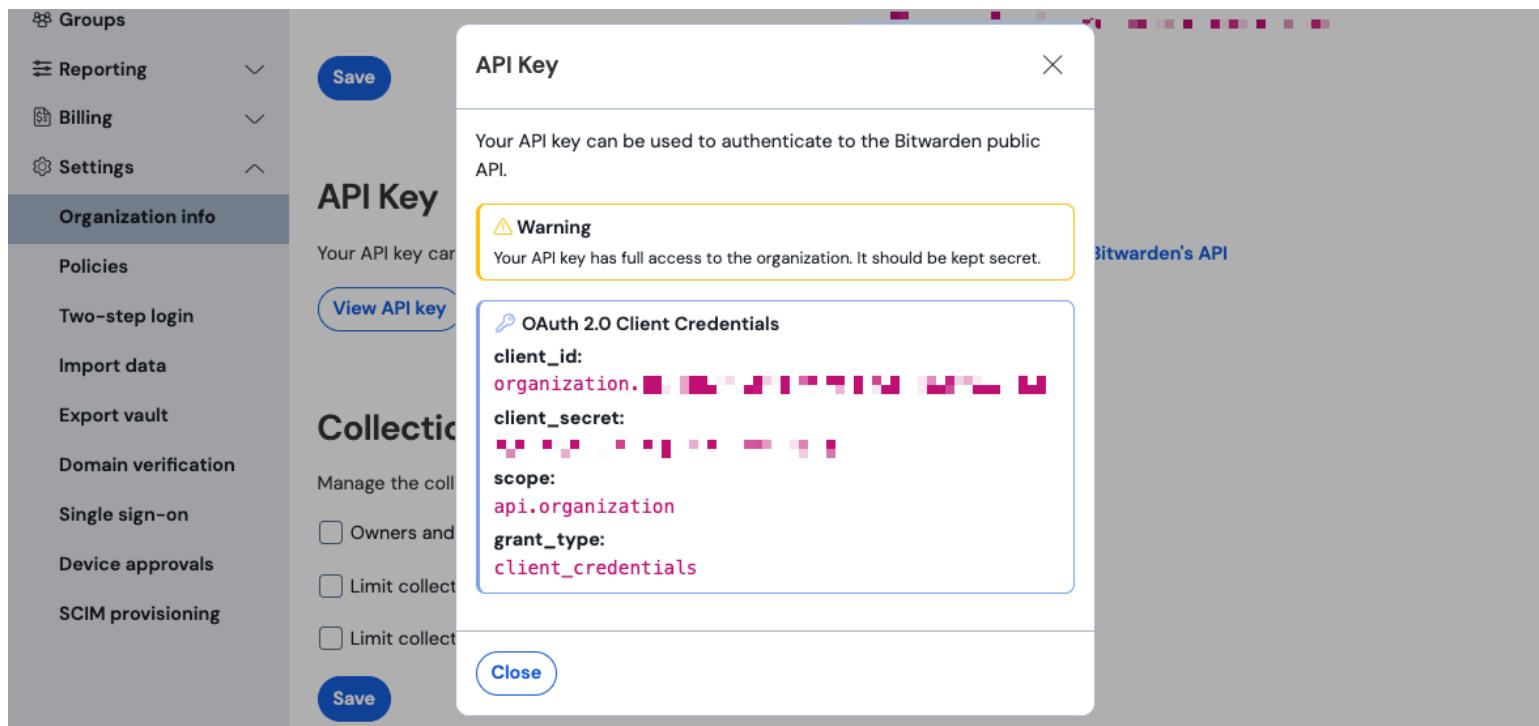
Bitwardenの統合を追加したら、統合を設定するための設定画面に移動します。この画面を開いたまま、別のタブでBitwardenのウェブアプリにログインし、製品切り替えを使用して管理者コンソールを開きます(��片)：



The screenshot shows the Bitwarden web interface. On the left, a sidebar menu includes 'Vaults', 'Send', 'Tools', 'Reports', 'Settings', 'Password Manager' (which is highlighted with a teal box), 'Secrets Manager', 'Admin Console', and 'Toggle Width'. A teal arrow points from the 'Default colle...' item in the 'Collections' section of the sidebar to the same item in the list on the right. The main content area is titled 'All vaults' and displays a table of vaults with columns for 'Name', 'Owner', and three vertical dots. The table lists four vaults: 'Company Credit Card' (owner 'My Organiz...', Visa card), 'Personal Login' (owner 'Me', myusername), 'Secure Note' (owner 'Me'), and 'Shared Login' (owner 'My Organiz...', sharedusername). A search bar and filter options are also visible.

製品-スイッチャー

あなたの組織の設定→組織情報画面に移動し、APIキーを表示ボタンを選択してください。あなたのAPIキー情報にアクセスするために、マスターpasswordを再入力するように求められます。



Your API key can be used to authenticate to the Bitwarden public API.

Warning
Your API key has full access to the organization. It should be kept secret.

OAuth 2.0 Client Credentials

client_id: organization.[REDACTED]
client_secret: [REDACTED]
scope: api.organization
grant_type: client_credentials

Close

組織API情報

以下の情報を対応するフィールドに入力してください。

エラスティックフィールド	値
URL	Bitwardenクラウドのユーザーのために、デフォルトのURLは https://api.bitwarden.com になります。 自己ホスト型Bitwardenのユーザーの方は、自己ホスト型のURLを入力してください。 URLの末尾に余分なスラッシュ「/」が含まれていないことを確認してください。
クライアントID	Bitwarden組織APIキーのウィンドウからclient_idの値を入力してください。
クライアントシークレット	Bitwarden組織APIキーのウィンドウからclient_secretの値を入力してください。

 Note

あなたの組織のAPIキー情報は、機密データです。これらの値を非セキュアな場所で共有しないでください。

必要なフィールドをすべて完了したら、ページを下にスクロールし続けて、希望のデータコレクション設定を適用してください。終了したら、**受信データを確認する**を選択してください。

① Note

Additional **Advanced options** are available for configuration at this point. The minimum required fields are highlighted above to add the Bitwarden integration. To access the integration at a later point to edit the setup, go to the menu and select **Integrations** → **Installed integrations** → **Bitwarden** → **Integration policies**.

すべてのデータが正しく入力された場合、Elasticは受信データを確認し、受信データのプレビューを提供します。**表示アセット**を選択して、あなたのデータを監視します。

データの監視を開始します

設定が完了したら、Bitwarden組織のデータのレビューを開始できます。ダッシュボードに関連するデータを監視するために、Bitwardenダッシュボードのいずれかを選択してください。各ダッシュボードが監視しているデータの簡単な概要は次のとおりです：

丸太	説明
[Bitwarden]にログイン ポリシー	組織のポリシー変更をレビューしてください。これには、組織のポリシーを有効にする、無効にする、または更新するなどが含まれます。
[Bitwardenログ] グループとコレクション	組織に関連するグループとコレクションのための記録されたイベントを監視します。
[Bitwardenログ] イベント	組織のイベントログを監視します。イベントログについての詳細は こちらをご覧ください 。

ダッシュボードの理解

質問

エラスティックデータモニタリングは、データのフィルタリングにKibana Query Language (KQL) を使用しました。クエリと検索について詳しく知るには、[Elasticクエリのドキュメンテーション](#)をご覧ください。