### お読みください

#### データの収集および処理方法

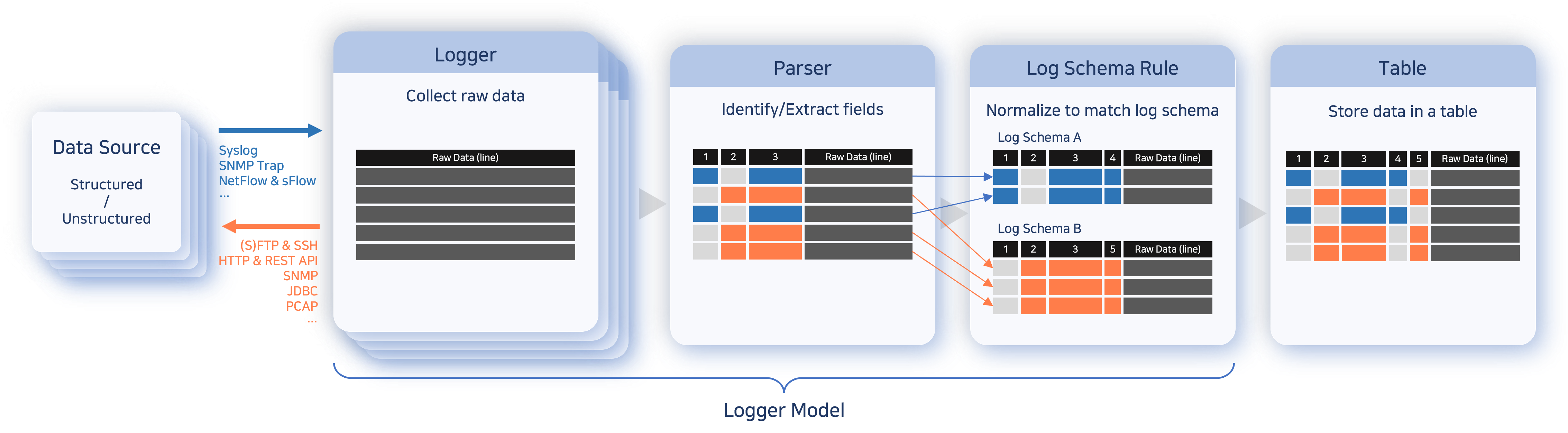
ログプレッソ・ソナーで処理されるデータの最小単位は**レコード**であり、「単一かつ完全な論理データ単位」と定義されます。具体例は以下の通りです。

* ファイアウォールやWebサーバーからのログの1行
* 1件のSyslogメッセージ
* 1件のSNMPトラップメッセージ
* リレーショナルデータベーステーブルに格納された1行
* MongoDBコレクションに格納された1ドキュメント
* PCAPデバイスで収集されたファイル内の1パケット
* 外部REST API呼び出しの応答として受信した1つのJSONオブジェクト（波括弧で囲まれた名前と値のペアの集合）

上記のすべてが、ログプレッソ・ソナーでは**レコード**として扱われます。

ロガーメニューは、ロガー、パーサー、ログスキーマ、ロガーモデルの4つのコンポーネントで構成されています。ログプレッソストアからアプリをインストールすると、データソースからのデータ収集および処理に必要なパーサー、ログスキーマ、ロガーモデルが自動的に提供されます。管理者はロガー（および必要に応じて接続プロファイル）の設定のみでデータ処理を開始できます。ただし、各コンポーネントの役割や相互作用を理解することで、収集機能をより効果的に活用できます。

以下の図は、ログプレッソ・ソナーにおけるデータ処理の流れを示しています。



ロガーがデータソースからデータを受信、または定期的に接続してデータを収集します。

* 図中の矢印は、TCP/IPまたはアプリケーションレベルでの通信方向を示しています。

ロガーモデルで定義されたパーサーが、レコードごとにデータを処理し、フィールドを抽出・識別します。

正規化ルールが定義されている場合、抽出されたフィールドや値はログスキーマで定義されたフィールド名や型に変換されます。

正規化されたレコードは、正規化フィールドと元のログの両方を保持したままテーブルに保存されます。

このプロセスは、一貫したポリシーの確立や効率的なデータ分析のために不可欠です。異種システムからのログはフォーマットが異なりますが、多くの場合共通の属性を持っています。これらの属性を正規化することで、シームレスなポリシー設定や分析が可能となります。

例えば、異なるファイアウォールからのログが異なるフォーマットで出力されていても、共通スキーマに正規化することで、すべてのファイアウォールに対して[アドレスグループ](https://docs.logpresso.comnull)で定義されたブロックリストと送信元IPアドレスの比較が可能となります。

#### ログ・データ収集メカニズムの簡素化

**[アプリ](/ja/sonar/4.0/ui/chapter-apps)** システムの導入により、ログおよびデータ収集のセットアップ作業が大幅に簡素化され、管理者の手間が最小限に抑えられました。アプリをインストールするだけで、対象システムからのデータ収集・処理に必要なパーサー、ログスキーマ、インジェストモデルがすべて自動的に構成されます。

新しいデータ収集セットアップ手順は以下の通りです。

|  |  |
| --- | --- |
| 4.0.2308.0以前 | 4.0.2308.0以降 |
| 1. ログスキーマの設定 | 1. [ログプレッソストア](https://logpresso.store)からアプリをダウンロード |
| 2. ログパーサーの設定 | 2. アプリをインストール |
| 3. 正規化パーサーの設定 | 3. 接続プロファイルなどのデータソース接続を設定 |
| 4. ロガーモデルの設定 | 4. ロガーを作成 |
| 5. 抽出モデルの設定 | - |
| 6. ロガーの作成 | - |

管理者は引き続き[パーサー](https://docs.logpresso.comnull)、[ログスキーマ](https://docs.logpresso.comnull)、[ロガーモデル](https://docs.logpresso.comnull)を手動で構成することも可能ですが、アプリシステムの導入により、ほとんどの場合手動設定の必要性が大幅に削減されました。多くの場合、アプリで提供される事前構成済みコンポーネントを利用することで、より迅速かつ効率的なセットアップが可能です。

#### ログスキーマの多言語対応

[ログスキーマ](https://docs.logpresso.comnull)は、現在、韓国語・英語・中国語に対応しています。従業員に弁明を依頼する際、サポートログ内のフィールド名はユーザーの言語設定に応じて表示されるため、より明確で分かりやすくなっています。

#### 標準でデータ収集が提供されていない場合

アプリ開発の依頼

ご利用のデータソースに対応するアプリが[ログプレッソストア](https://logpresso.store)に存在しない場合は、ログプレッソにカスタム開発を依頼できます。ご依頼の際は、以下の情報をご提供ください。

* 貴社の情報
* 連携対象システムのメーカー、製品名、バージョン
* ログ収集方法
* ログ仕様（データベースの場合はスキーマおよびテーブル定義を含む）
* サンプルログ

独自アプリの開発

ログプレッソは、ログプレッソ・ソナーおよびログプレッソ・マエストロ向けの統合アプリを開発できるアプリSDKを提供しています。詳細なガイドについては、[ログプレッソアプリ開発ガイド](https://docs.logpresso.comnull)をご参照ください。