### 꼭 읽어주세요

#### 데이터 수집/처리 과정

로그프레소 소나가 다루는 데이터의 최소 단위는 레코드입니다. 레코드는 "하나의 완결된 논리적 단위로서의 기록"을 의미합니다. 예를 들어, 방화벽이나 웹 서버의 로그 한 줄, 시스로그 메시지 한 줄, SNMP 트랩 메시지 한 줄, 관계형 데이터베이스 테이블에 저장된 하나의 행(row), 몽고DB 컬렉션에 저장된 하나의 문서, PCAP 장치를 통해 수집된 파일에서 확인할 수 있는 하나의 패킷, 외부 REST API를 호출하고 응답으로 받은 JSON 객체(중괄호에 감싸여 있는 이름-값 쌍의 집합) 등이 로그프레소 소나가 다루는 "레코드"입니다.

수집 메뉴를 훑어보면 수집기, 파서, 로그 스키마, 수집 모델로 구성되어 있습니다. [앱](https://docs.logpresso.com/ko/sonar/4.0/ui/chapter-apps)을 설치하면 데이터 원천에서 데이터를 수집해서 처리하는데 필요한 파서, 로그 스키마, 수집 모델이 제공되므로 관리자가 (필요에 따라 접속 프로파일과 함께) 수집기만 구성하면 동작하는 데에는 아무 문제가 없습니다. 그러나 각 기능들이 수행하는 동작과 상호관계를 이해해야 수집 기능을 제대로 이해하고 활용할 수 있습니다.

다음 그림은 로그프레소 소나에서 데이터가 처리되는 과정을 보여줍니다(그림을 클릭해서 큰 그림을 볼 수 있습니다).



데이터 원천이 보낸 데이터를 수집기가 받거나, 수집기가 주기적으로 직접 데이터 원천에 접속해 데이터를 수집합니다.

* 그림에서 화살표는 TCP/IP 또는 애플리케이션 수준에서 통신의 방향을 의미합니다.

수집 모델에 정의된 파서를 이용해 원본 데이터를 레코드 단위로 식별하고, 각 레코드에서 필드를 식별하고 추출합니다.

수집 모델에 정규화 규칙이 있는 경우, 파서를 통해 추출된 필드와 필드 값을 로그 스키마의 필드 이름과 유형에 맞게 변환합니다.

정규화된 레코드를 테이블에 저장합니다. 이 때 저장되는 레코드는 정규화된 필드와 원본 로그를 모두 포함하고 있습니다.

이러한 일련의 데이터 처리 과정은 일관된 정책을 수립하고 데이터를 분석하는데 꼭 필요한 절차입니다. 이기종 장비에서 발생하는 로그는 각각 다른 형식으로 구성되지만, 공통된 속성을 가지고 있으므로 필드 정규화를 통해서 정책 설정 및 분석을 단순화할 수 있습니다. 예를 들어, 이기종 방화벽의 로그는 모두 형식이 다르지만, 동일한 필드 이름으로 정규화해두면 전체 방화벽을 대상으로 출발지 IP 주소에 대해 [주소 그룹](https://docs.logpresso.com/ko/sonar/4.0/ui/section-address-group)에 구성해둔 차단 목록과 대조할 수 있습니다.

#### 간소화된 수집 설정 절차

관리자가 일일이 설정해야 했던 로그/데이터 수집 설정 과정을 **[앱](/ko/sonar/4.0/ui/chapter-apps)** 시스템을 도입하면서 간소화했습니다. 앱을 설치하면 연동할 시스템에서 데이터 수집에 필요한 파서, 로그 스키마, 수집 모델을 모두 제공합니다. 수집 설정 절차는 다음과 같이 바뀌었습니다.

|  |  |
| --- | --- |
| 4.0.2308.0 이전 | 4.0.2308.0 이후 |
| 1. 로그 스키마 구성 | 1. [로그프레소 스토어](https://logpresso.store)에서 앱 다운로드 |
| 2. 원본 로그 파서 구성 | 2. 앱 설치 |
| 3. 정규화 파서 구성 | 3. 접속 프로파일 등 데이터 원천 연결 설정 |
| 4. 수집 모델 구성 | 4. 수집기 생성 |
| 5. 추출 모델 구성 | - |
| 6. 수집기 생성 | - |

여전히 관리자가 [파서](https://docs.logpresso.com/ko/sonar/4.0/ui/section-parsers), [로그 스키마](https://docs.logpresso.com/ko/sonar/4.0/ui/section-schemas), [수집 모델](https://docs.logpresso.com/ko/sonar/4.0/ui/section-logger-models)을 직접 설정할 수 있지만, 일반적인 상황에서 관리자가 모든 것을 일일이 구성하지 않고 앱이 제공하는 것들을 사용하는 것만으로도 충분합니다.

#### 국제화된 로그 스키마

[로그 스키마](https://docs.logpresso.com/ko/sonar/4.0/ui/section-schemas)는 한국어, 영어, 중국어를 지원할 수 있도록 개선되었습니다. 이제 임직원에게 소명을 요청할 때, 근거 자료로 제시되는 로그의 필드 이름도 임직원이 사용하는 언어로 표시됩니다.

#### 데이터 수집이 불가능할 때

앱 개발 요청

[로그프레소 스토어](https://logpresso.store)에서 데이터 원천으로부터 데이터를 수집에 사용할 앱이 제공되지 않는 경우, 로그프레소에 앱 제작을 요청하세요. 앱 제작을 요청하실 때에는 다음과 같은 정보가 필요합니다.

* 앱을 요청하는 고객사 정보
* 연동할 제품의 제조사, 제품 이름 및 버전
* 로그 수집 방식
* 로그 정의서(데이터베이스와 연동하는 경우 데이터베이스 정보 및 테이블 스키마 정보)
* 샘플 로그

자체 앱 개발

로그프레소는 로그프레소 소나/마에스트로와 연동할 시스템을 위해 직접 앱을 개발할 수 있도록 앱 SDK를 제공합니다. 앱 개발에 필요한 정보는 [로그프레소 앱 개발 가이드](https://docs.logpresso.com/ko/sonar/4.0/ui/ko/app-sdk)를 참고하세요.