### 로그 스키마

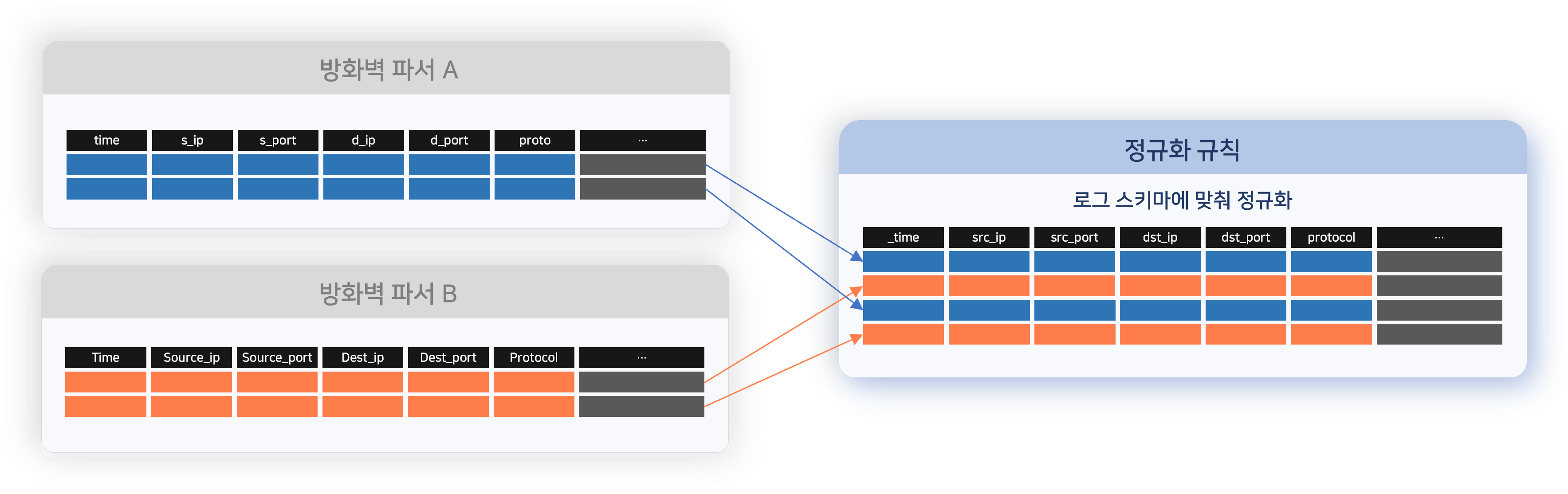
#### 개요

먼저 파서의 역할을 간단히 살펴보겠습니다. 파서는 입력 데이터로부터 레코드 단위로 필드를 추출합니다. 예를 들어, 팔로알토 네트웍스 방화벽 로그와 포티넷 포티게이트 방화벽 로그 원본에서 레코드를 단위로 필드를 식별하고 추출합니다. 그러나 이렇게 파서가 처리한 팔로알토 네트웍스 방화벽 로그와 시스코 파이어파워 방화벽 로그는 필드의 이름이나 구성, 순서가 달라 서로 대조하거나 비교하기 어렵습니다.

제대로 활용하려면 서로 다른 로그의 형식을 동일하게 맞추어야 합니다. 바로 이 지점에서 로그 스키마가 필요해집니다. 로그 스키마는 데이터베이스의 테이블 스키마와 유사하게 다음과 같은 기능을 수행합니다.

* 여러 파서가 필드 단위로 식별한 입력 데이터의 필드 이름을 표준화
* 사용 목적에 따라 필드를 재구성하고 정렬하는데 필요한 형식을 정의
* 필요하다면, 비어 있는 필드에 원본 레코드에서 추출한 값을 할당

로그 스키마는 수집 모델에 정의된 규칙에 따라 레코드를 정규화할 때 기준으로 사용됩니다. 다음 그림은 수집 모델의 정규화 규칙이 로그 스키마에 따라 로그를 정규화하는 과정을 도식화하여 나타냅니다.

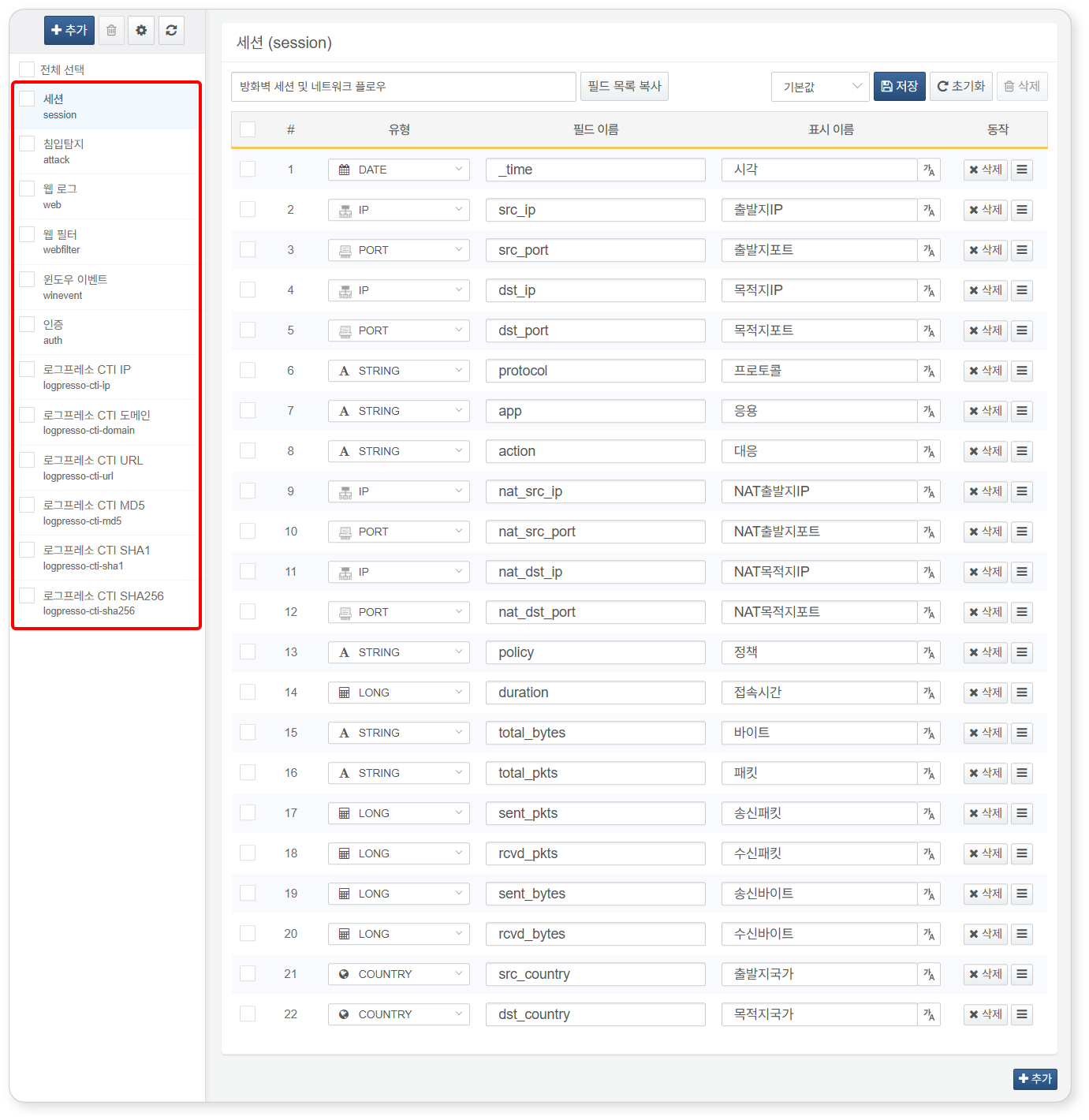


기본 스키마와 앱 스키마

스키마는 기본 스키마와 앱 스키마로 구분할 수 있습니다. 로그 스키마의 특성 상 서로 다른 이기종 로그를 정규화할 필요가 있기 때문에 앱 스키마보다 기본 스키마가 자주 사용되는 편입니다.

**기본 스키마**

일반적인 범주의 이기종 로그를 정규화하는데 사용할 수 있도록 기본 내장되어 제공하는 로그 스키마입니다. 다음 그림에서 빨간 박스 영역은 로그프레소 소나를 설치했을 때 조회할 수 있는 스키마 목록을 보여줍니다. 오른편 영역은 로그 스키마에 정의된 필드 목록으로, 세션 로그 스키마의 필드 목록을 보여줍니다.



로그프레소 소나의 기본 스키마는 다음과 같습니다.

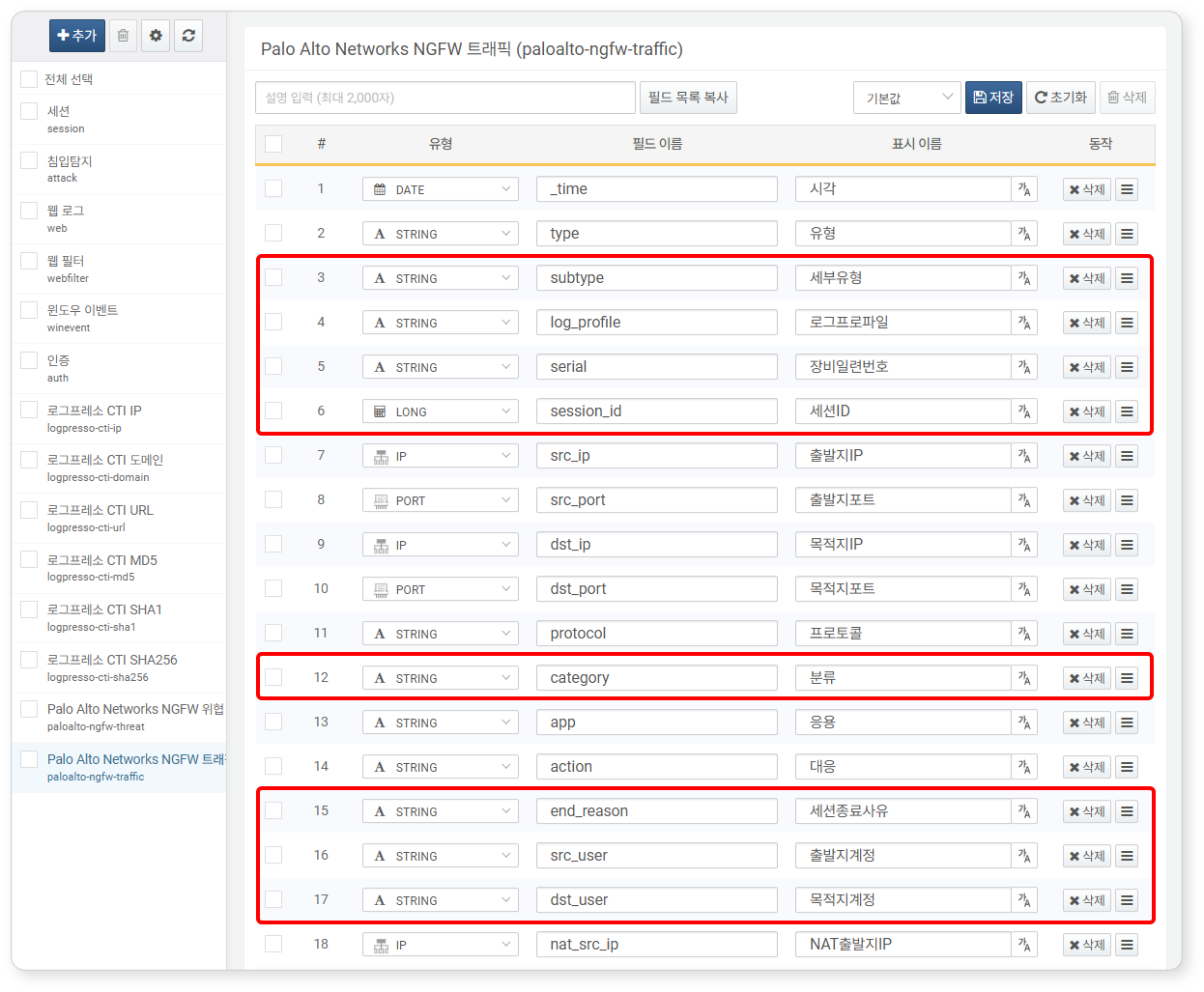
|  |  |  |
| --- | --- | --- |
| 이름 | 식별자(스키마 코드) | 설명 |
| 세션 | session | TCP/IP 세션과 관련된 로그 |
| 침입탐지 | attack | IPS, 웹 방화벽의 침입탐지 로그 |
| 웹 로그 | web | W3C 표준 웹 로그 |
| 웹 필터 | webfilter | 웹 프록시 및 유해사이트 차단 로그 |
| 윈도우 이벤트 | winevent | 윈도우 이벤트 로그 |
| 인증 | auth | 윈도우 로그온, SSH, VPN 인증 등 원격 로그인 관련 로그 |
| 로그프레소 CTI IP | logpresso-cti-ip | 로그프레소 CTI의 악성 IP 주소 및 관련 정보 |
| 로그프레소 CTI 도메인 | logpresso-cti-domain | 로그프레소 CTI의 악성 도메인 및 관련 정보 |
| 로그프레소 CTI URL | logpresso-cti-url | 로그프레소 CTI의 악성 URL 및 관련 정보 |
| 로그프레소 CTI MD5 | logpresso-cti-md5 | 로그프레소 CTI의 악성코드 MD5 해시값 및 관련 정보 |
| 로그프레소 CTI SHA1 | logpresso-cti-sha1 | 로그프레소 CTI의 악성코드 SHA-1 해시값 및 관련 정보 |
| 로그프레소 CTI SHA256 | logpresso-cti-sha256 | 로그프레소 CTI의 악성코드 SHA-256 해시값 및 관련 정보 |

로그프레소 CTI는 접속 프로파일에서 API 키를 등록한 후 이용할 수 있습니다.

**앱 스키마**

앱을 설치할 때 함께 제공되는 로그 스키마입니다. 기본 스키마와 달리 원천 데이터의 고유한 필드까지 포함해 정규화할 때 사용할 수 있습니다.

다음 그림은 [팔로알토 네트웍스 방화벽](https://logpresso.store/ko/apps/paloalto-ngfw) 앱을 설치했을 때 볼 수 있는 **Palo Alto Networks NGFW 트래픽** 로그 스키마의 일부입니다. 붉은색으로 표시한 필드는 앱 스키마를 이용할 때 조회할 수 있고, 기본 스키마를 적용해 로그를 조회할 때에는 생략됩니다.



스키마의 활용

**로그프레소 쿼리문**

쿼리문에서 [schema](https://docs.logpresso.com/ko/sonar/4.0/ui/ko/query/schema-command) 명령을 이용해 입력 데이터에 로그 스키마를 적용할 수 있습니다. 다음은 팔로알토 네트웍스 방화벽 로그의 가공된 샘플에 **Palo Alto Networks NGFW 위협** 로그 스키마(paloalto-ngfw-threat)를 적용해 출력하는 예시입니다.

json "{}" | eval line="Apr 10 04:38:54 1,2012/04/10 04:38:54,012345678911,THREAT,spyware,1,2012/04/10 04:38:49,192.0.2.255,192.0.2.2,0.0.0.0,0.0.0.0,rule1,,crusher,web-browsing,vsys1,untrust,trust,ethernet1/2,ethernet1/1,forwardAll,2012/04/10 04:38:54,25466,1,80,59127,0,0,0x200000,tcp,drop-all-packets,\"habl.bin\",Trojan-Spy.Win32.Zbot.wti(12620),any,medium,server-to-client,0,0x0,United States,192.0.2.0-192.0.2.255,0," | parse overlay=t paloalto-ngfw | schema paloalto-ngfw-threat

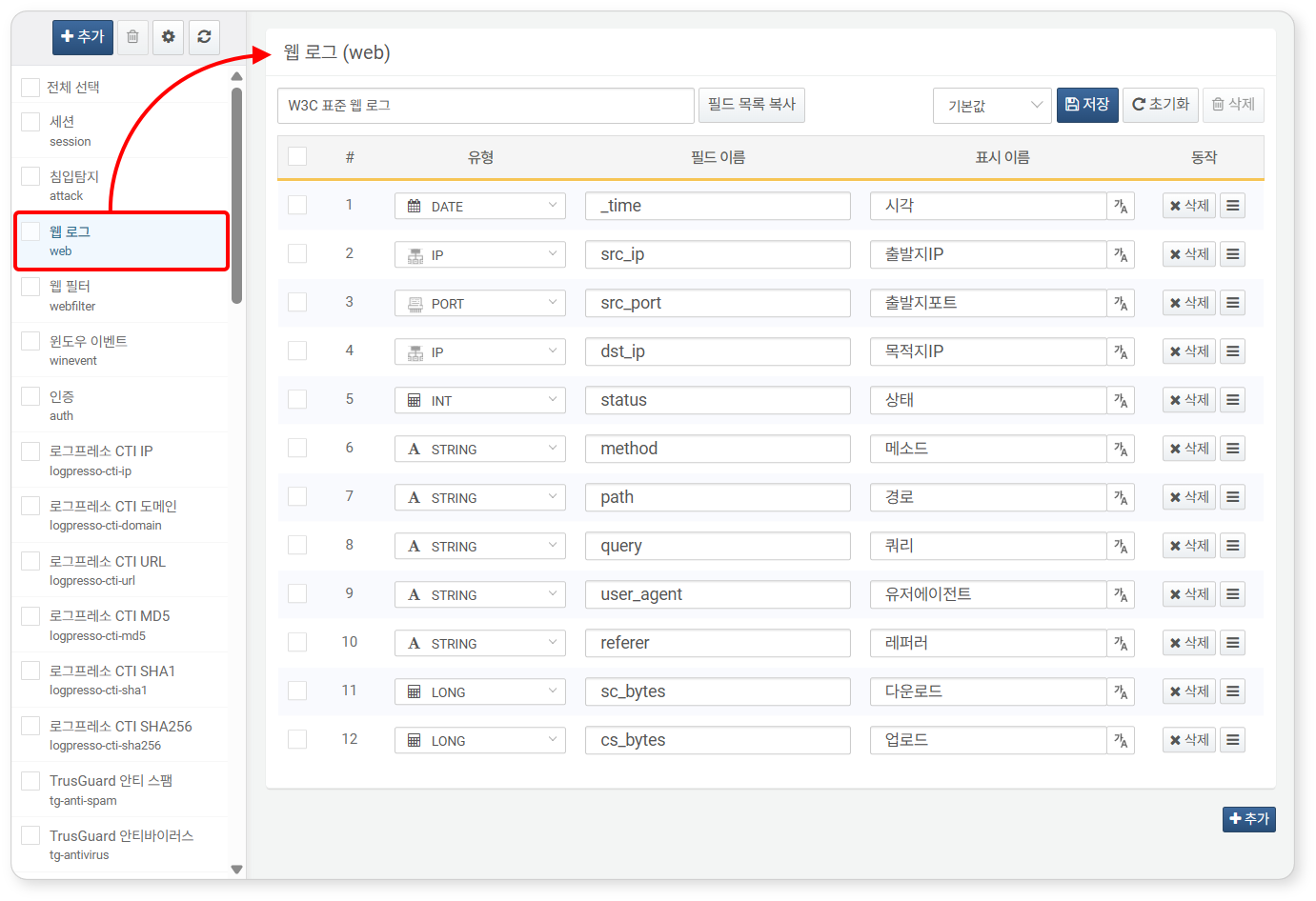
**소명 요청의 국제화 지원**

보안위반 행위가 의심되는 임직원에게 [소명](https://docs.logpresso.com/ko/sonar/4.0/ui/section-explanation)을 요청하면 해당 임직원에게 소명 요청 메일이 전송됩니다. 다국어 환경에서 임직원이 [소명 요청을 조회](https://docs.logpresso.com/ko/sonar/4.0/ui/submit-explanation)하거나 1차 검토자가 [소명을 검토](https://docs.logpresso.com/ko/sonar/4.0/ui/review-explanation)할 때 제시되는 근거 자료는 해당 [임직원](https://docs.logpresso.com/ko/sonar/4.0/ui/section-employees)이 사용하는 언어를 기준으로 제시할 필요가 있습니다. 이때 로그 스키마에 정의된 표시 이름이 사용됩니다.

로그 스키마의 국제화는 4.0.2404.0 버전부터 지원합니다.

#### 로그 스키마 조회

**수집 > 로그 스키마**에서 로그 스키마 목록 및 로그 스키마의 세부 내용을 조회할 수 있습니다. 왼쪽 패널은 로그 스키마 목록을 보여줍니다. 스키마 목록은 각 스키마의 이름과 식별자를 보여줍니다. 스키마 목록에서 로그 스키마를 클릭하면 해당 로그 스키마에 정의된 필드 목록을 확인할 수 있습니다.



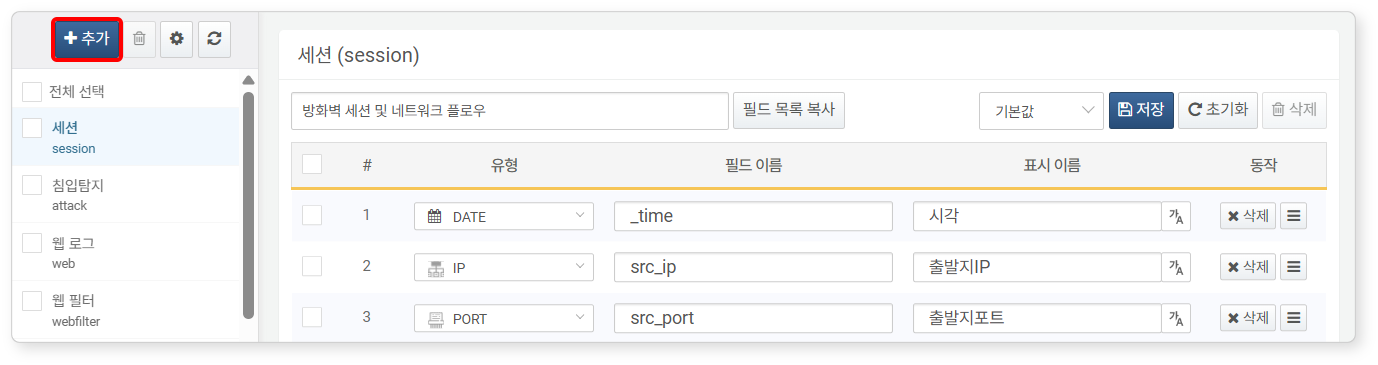
* **순서 번호(#)**: 필드의 정렬 순서
* **유형**: 필드 값의 유형
* **필드 이름**: 영문과 숫자, 밑줄(\_)로 구성되는 필드의 이름
* **표시 이름**: 웹 콘솔에서 사용하는 사용자 친화적인 이름
* **동작**: 필드의 삭제 또는 위치 이동 핸들

표시 이름은 공백문자를 허용하지 않습니다.

#### 로그 스키마 추가

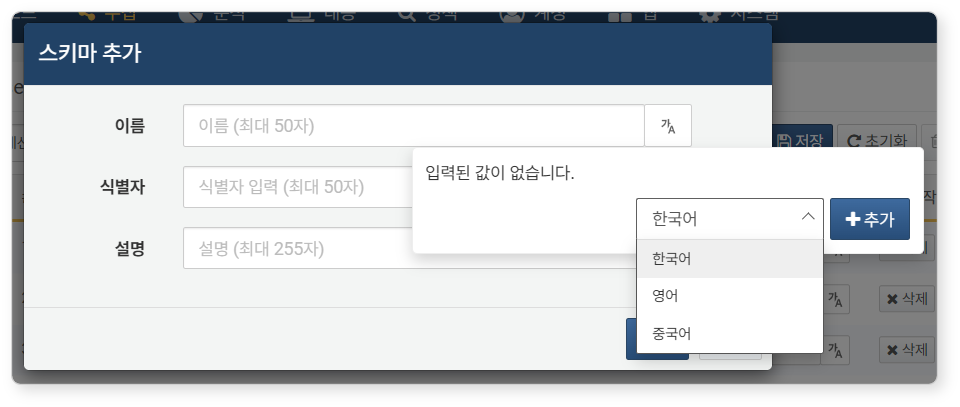
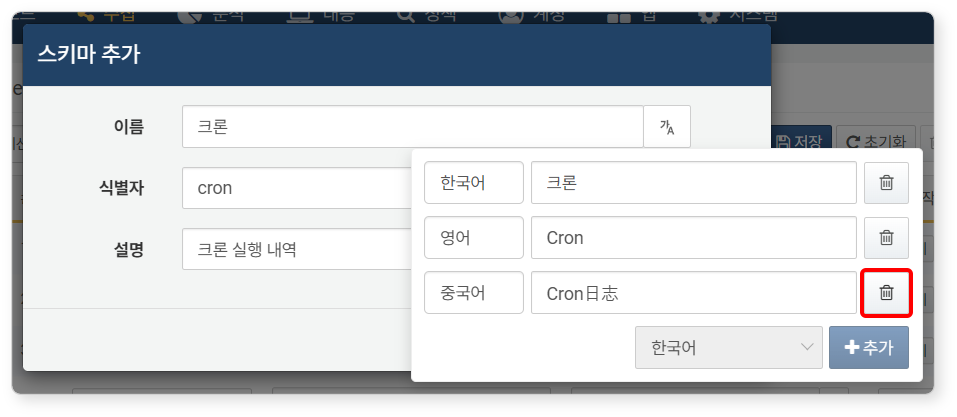
대부분의 운영 환경에서 기본 스키마나 앱 스키마를 이용하는 것으로 충분합니다. 기본 스키마나 앱 스키마로 정규화할 수 없는 경우 다음과 같이 사용자 정의 로그 스키마를 추가하세요

**수집 > 로그 스키마**에서 로그 스키마 목록 위에 있는 **추가**를 클릭하세요.



**스키마 추가** 대화상자에서 스키마 속성을 입력하세요.



* **이름**: 로그 스키마의 이름. 여기에 입력한 이름은 다국어 환경에서 기본 이름으로 쓰입니다.
* 다국어 환경에서 언어별로 이름을 입력하려면 입력상자 우측에 있는 **가A**를 클릭하세요.
* 언어(한국어, 영어, 중국어)를 선택하고 언어에 맞는 이름을 입력하세요.
* 
* 추가한 문자열의 오른쪽에 있는 휴지통을 클릭하면 해당 문자열을 삭제할 수 있습니다.
* 
* **식별자**: 로그프레소 쿼리문에서 스키마 호출에 사용할 고유 식별자. 로그 수집 시점에 **\_schema** 필드에 식별자가 지정됩니다.
* **설명**: 로그 스키마 화면 상단에 표시되는 로그 스키마에 대한 설명

모든 설정을 마쳤으면 **확인**을 클릭하세요. 스키마를 추가하지 않으려면 **취소**를 클릭하세요.

추가된 로그 스키마는 아무 필드도 없이 비어있습니다. [필드 설정](https://docs.logpresso.com/ko/sonar/4.0/ui/section-schemas)을 참고하여 추가한 스키마에 필드를 추가하고 순서를 정렬하세요.

#### 로그 스키마 수정

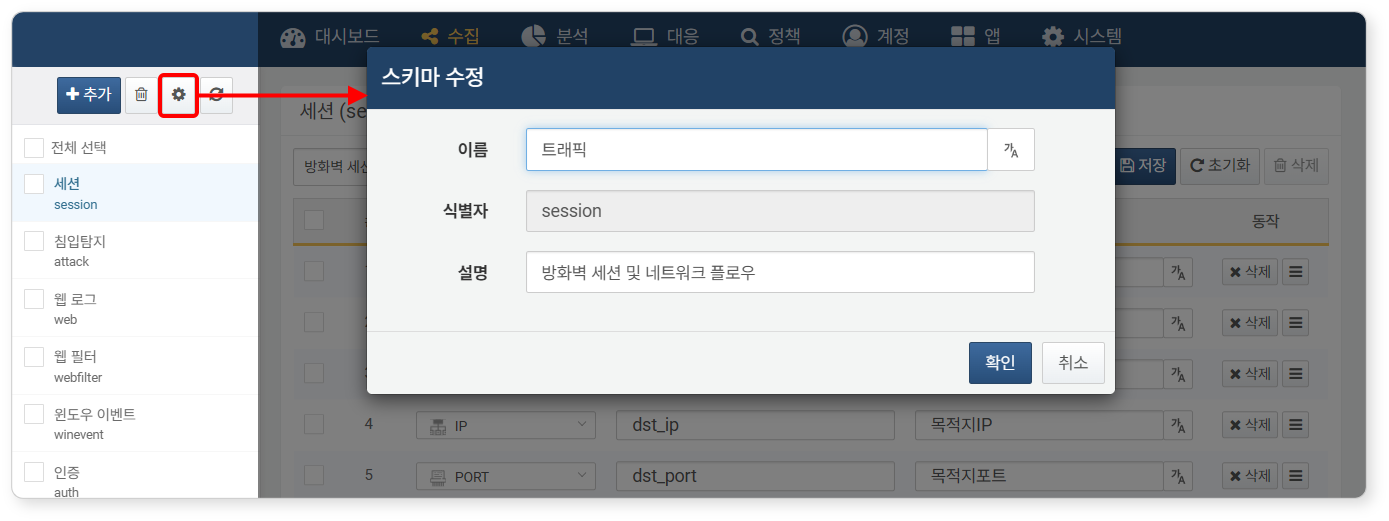
기본/앱 스키마에 필요에 따라 필드를 추가하는 것은 괜찮지만, 이미 정의되어 있는 필드를 수정하지 마세요. 수집 모델의 동작에 문제를 일으킬 수 있습니다.

이름/설명 변경

로그 스키마의 이름 또는 설명을 수정하려면,

**수집 > 로그 스키마**에 있는 로그 스키마 목록에서 수정할 스키마의 이름을 클릭한 다음, 톱니바퀴 버튼을 클릭하세요.

**스키마 수정** 대화상자에서 이름 또는 설명을 수정하고 **확인**을 클릭하세요.

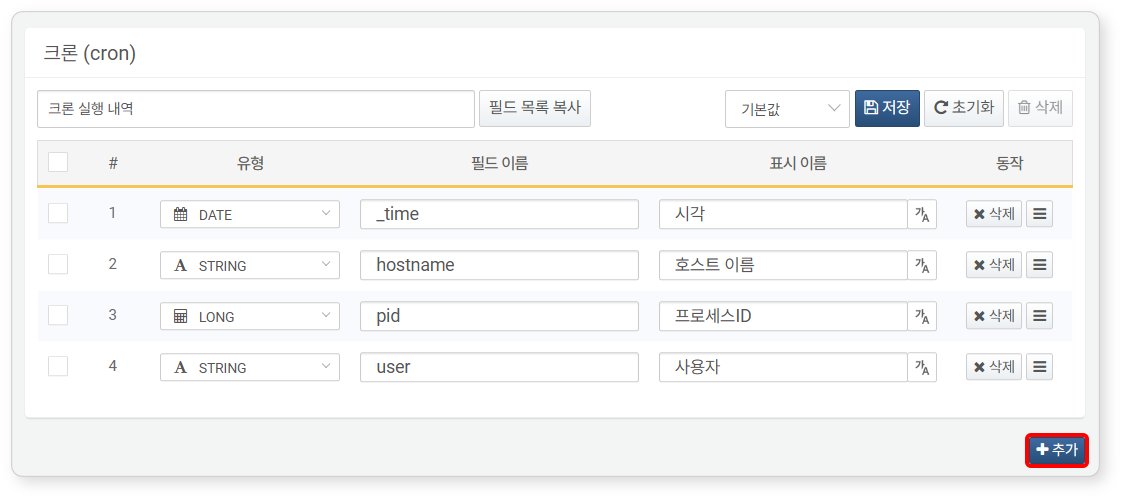


필드 설정

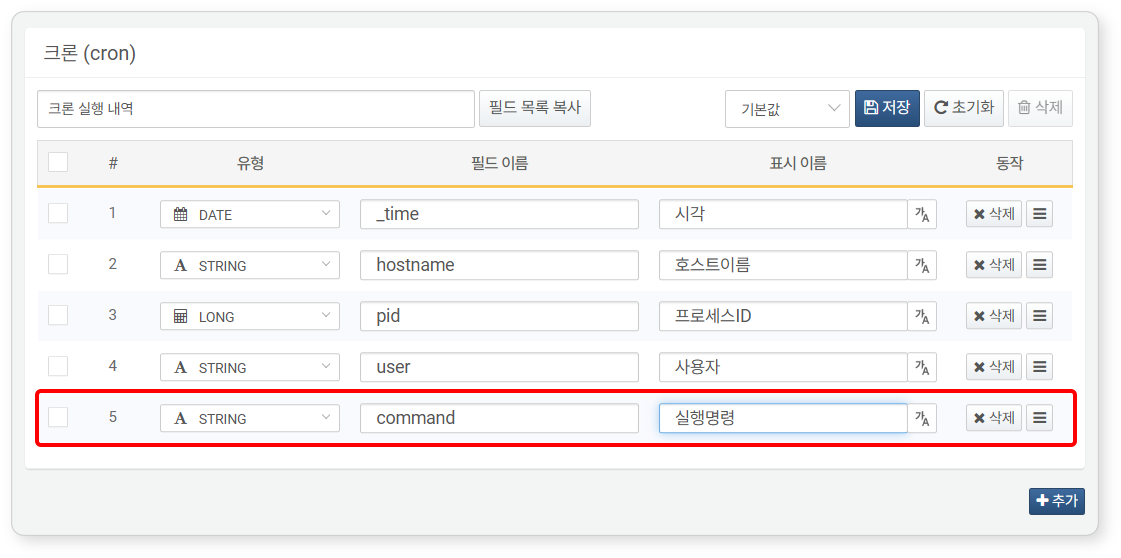
로그 스키마에 필드를 추가하거나, 이미 정의된 필드의 속성을 수정하려면,

**수집 > 로그 스키마**에 있는 로그 스키마 목록에서 수정할 스키마의 이름을 클릭하세요. 여기서는 임의로 추가된 크론 스키마를 예시로 설명합니다.

로그 스키마 화면 우측 하단에 있는 **추가**를 클릭해 필드를 추가하세요.



추가된 필드의 **유형**, **필드 이름**, **표시 이름**을 선택/입력하세요.

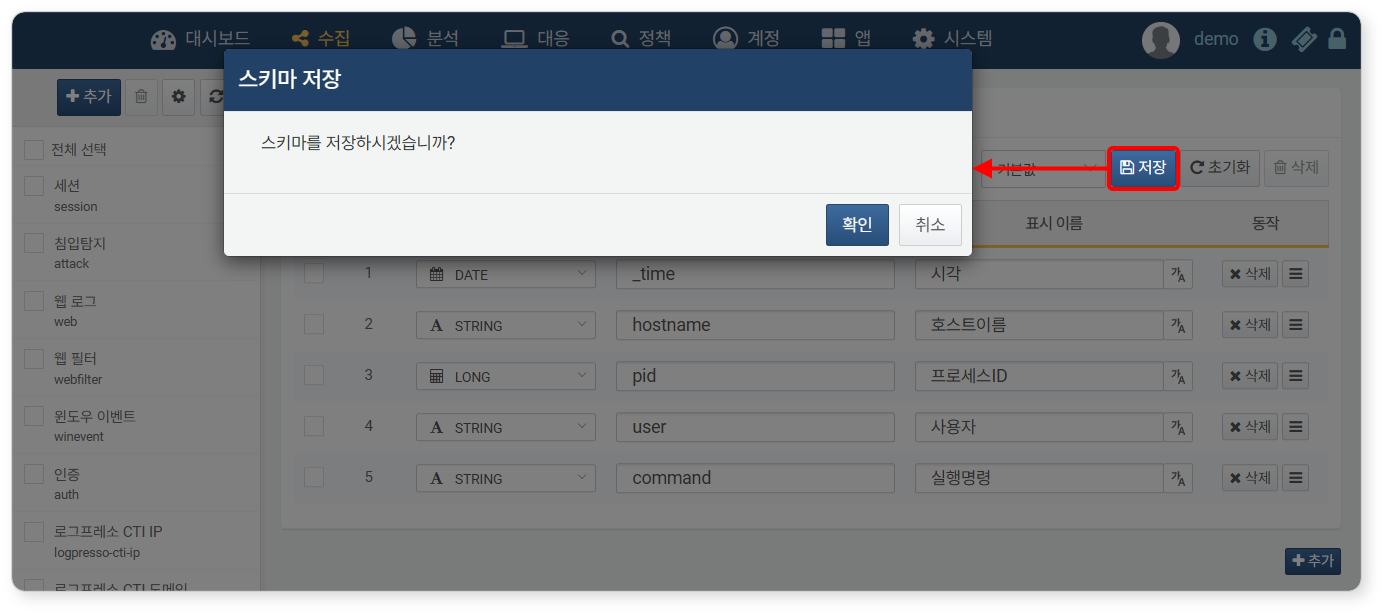


* **순서 번호(#)**: 필드의 정렬 순서. 새 필드를 추가할 때마다 순차적으로 증가합니다.
* **유형**: 필드 값의 유형. 다음 중 하나를 선택하세요.

|  |  |
| --- | --- |
| 유형 | 설명 |
| STRING | 문자열 |
| BOOL | 불리언 값(true, false) |
| SHORT | 16비트 정수(-32,768 ~ 32,767) |
| INT | 32비트 정수(-2,147,483,648 ~ 2,147,483,647) |
| LONG | 64비트 정수(-9,223,372,036,854,775,808 ~ 9,223,372,036,854,775,807) |
| DOUBLE | 64비트 소수 |
| DATE | 날짜/시간. 밀리초 단위의 해상도를 갖습니다. |
| COUNTRY | ISO 3166-1 alpha-2 국가코드 (예: KR) |
| PORT | 포트 번호 (0 ~ 65535) |
| IP | IPv4 또는 IPv6 주소 |
| MD5 | MD5 해시 |
| SHA1 | SHA-1 해시 |
| SHA256 | SHA-256 해시 |
| URL | URL |
| DOMAIN | 도메인 주소 |
| BLOB | 바이너리 데이터 |

* **필드 이름**: 영문과 숫자, 밑줄(\_)로 구성되는 필드의 이름
* **표시 이름**: 웹 콘솔에서 사용하는 사용자 친화적인 이름
* **동작**: 필드의 삭제 또는 위치 이동 핸들
* **삭제**를 클릭해서 해당 필드를 로그 스키마에서 삭제할 수 있습니다. 여러 개의 필드를 한꺼번에 삭제하려면 삭제할 필드의 좌측 체크박스를 클릭한 다음 로그 스키마 화면 우측 상단에 있는 **삭제**를 클릭하세요.
* **위치 이동 핸들**을 드래그해 다른 위치에 놓음으로써 필드 순서를 변경할 수 있습니다.
* 

모든 필드 설정을 마쳤으면 로그 스키마 화면 우측 상단에 있는 **저장**을 클릭한 다음, **스키마 저장** 대화상자에서 **확인**을 클릭하세요.



* **초기화**를 클릭하면 마지막으로 저장된 로그 스키마로 초기화됩니다.
* 필드 설정을 변경하다가 다른 화면으로 이동하려 할 때에도 **스키마 저장** 대화상자가 나타납니다.

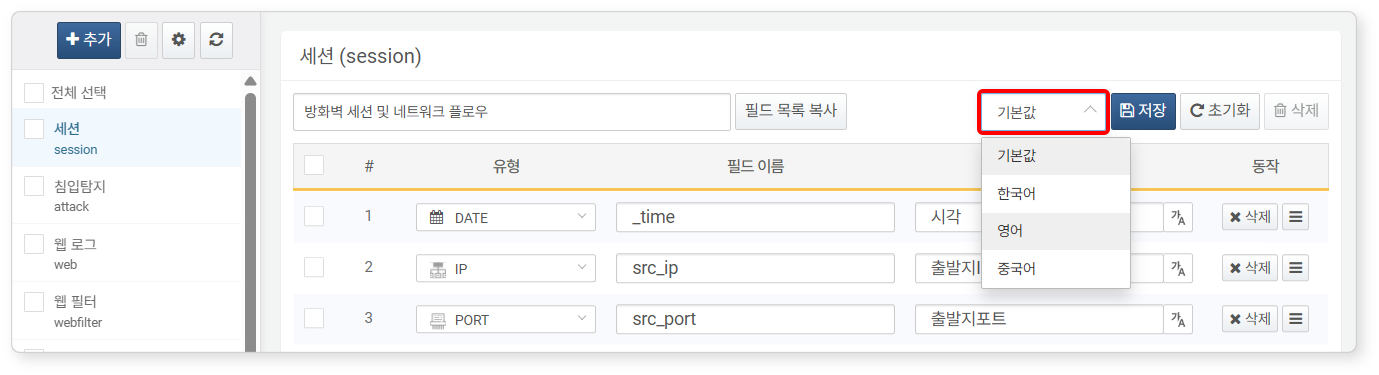
국제화 지원

[소명 요청](https://docs.logpresso.com/ko/sonar/4.0/ui/submit-explanation)의 국제화를 지원할 수 있도록 로그 스키마 필드를 언어별로 설정할 수 있습니다.

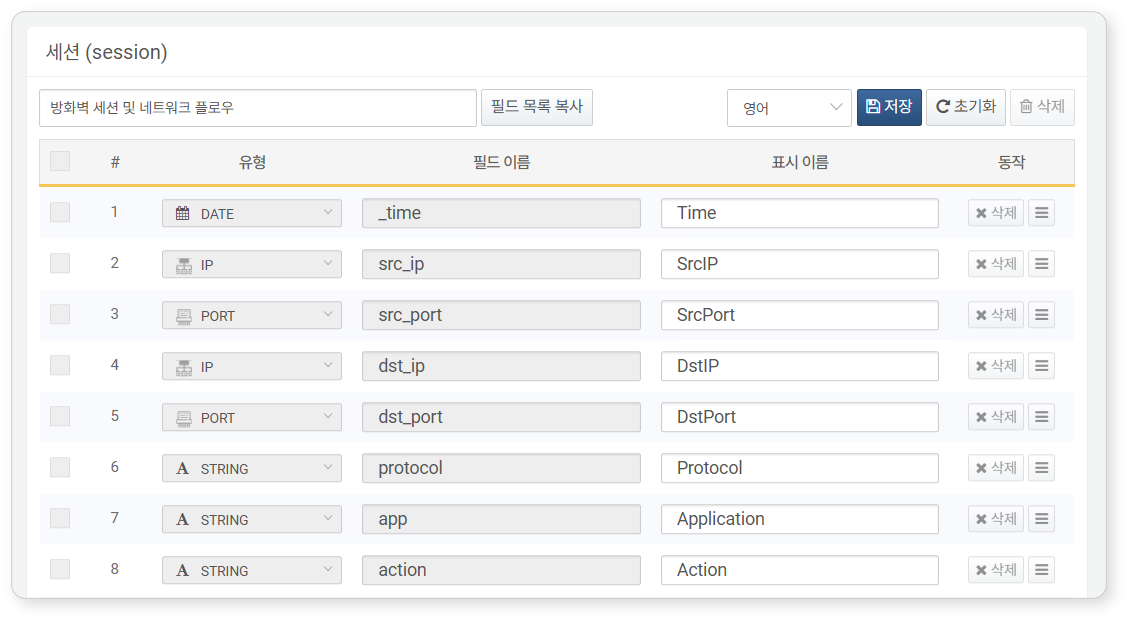
언어별 로그 스키마 표시 이름을 설정하려면,

**수집 > 로그 스키마**에 있는 로그 스키마 목록에서 국제화를 설정할 스키마의 이름을 클릭하세요.

로그 스키마 화면 우측 상단에서 다음 그림을 참고해 언어를 선택하세요.



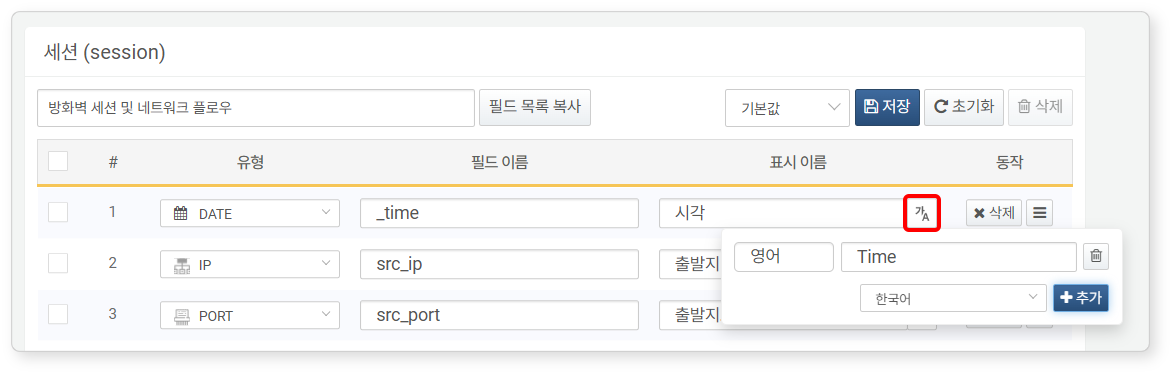
선택한 언어로 표시 이름을 입력하세요.



모든 표시 이름을 입력한 후, 화면 우측 상단에 있는 **저장**을 클릭하세요.

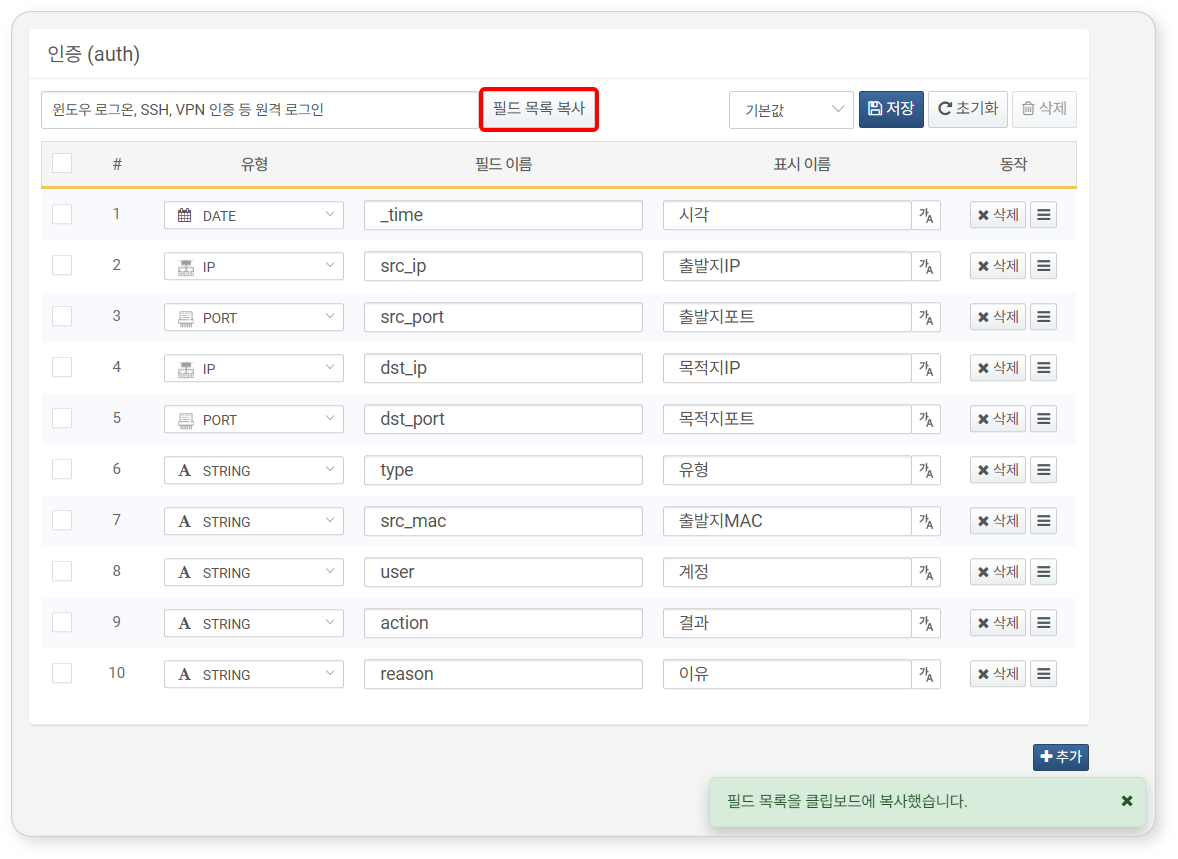
**스키마 저장** 대화상자에서 **확인**을 클릭하세요.

다음과 같이 언어가 기본값인 상태에서 특정한 필드의 **표시 이름** 우측에 있는 **가A** 버튼을 클릭하는 방법으로 언어별 표시 이름을 설정할 수도 있습니다.



#### 필드 목록 복사

**필드 목록 복사**를 클릭하면 조회 중인 로그 스키마의 필드 이름 목록이 클립보드에 복사됩니다.



예를 들어, 인증(auth) 스키마 조회 화면에서 필드 목록을 복사하면 클립보드에 다음과 같은 형태로 저장됩니다. 클립보드에 복사된 필드 목록을 [fields](https://docs.logpresso.com/ko/sonar/4.0/ui/ko/query/fields-command), [sort](https://docs.logpresso.com/ko/sonar/4.0/ui/ko/query/sort-command) 등 쿼리 명령어를 이용할 때 활용하세요.

\_time, src\_ip, src\_port, dst\_ip, dst\_port, type, src\_mac, user, action, reason

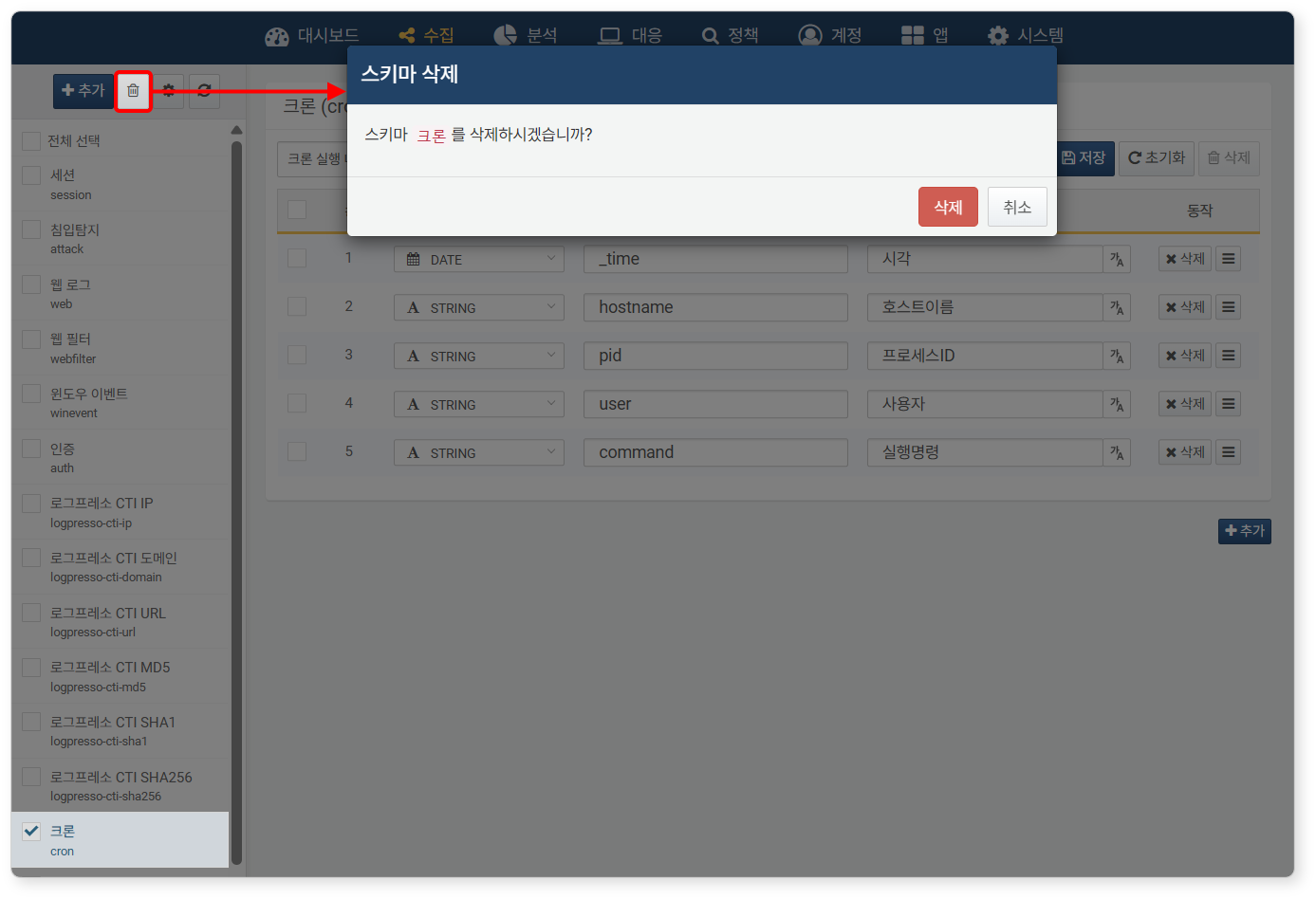
#### 로그 스키마 삭제

기본/앱 로그 스키마를 임의로 삭제하지 마세요. 수집 모델의 동작에 문제를 일으킬 수 있습니다.

로그 스키마를 삭제하려면,

**수집 > 로그 스키마**에 있는 로그 스키마 목록에서 삭제할 스키마의 이름 좌측에 있는 체크박스를 클릭한 다음, 휴지통 버튼을 클릭하세요.

**스키마 삭제** 대화상자에서 이름 또는 설명을 수정하고 **확인**을 클릭하세요.



로그 스키마를 삭제하지 못하는 경우, **스키마 삭제 실패** 대화상자에서 실패 원인을 확인할 수 있습니다.

