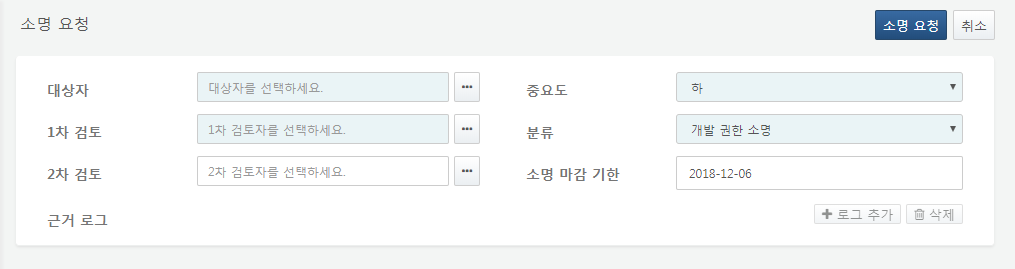
#### 소명 추가

소명은 실시간 탐지나 배치 탐지에서 자동으로 생성되도록 설정할 수 있고, 티켓 화면에서 소명 요청을 할 수도 있으며, 소명 화면에서 추가 버튼을 눌러 직접 추가할 수 있습니다. 여기서는 티켓 화면과 소명 화면에서 소명 요청을 추가하는 방법을 알아보도록 하겠습니다.



단계 1

대상자 할당

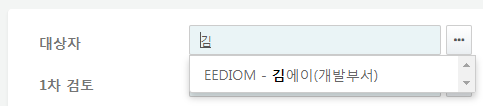
가장 먼저 대상자를 할당합니다. 대상자를 지정하면 1차 검토자는 대상자의 부서의 부서장으로 자동 지정됩니다. 2차 검토자는 필요한 경우 같이 할당합니다. 인풋 상자에서 직접 대상자/검토자 이름을 입력하는 방법이 있고, ... 버튼을 눌러 조직도에서 대상자/검토자를 선택하는 방법이 있습니다.

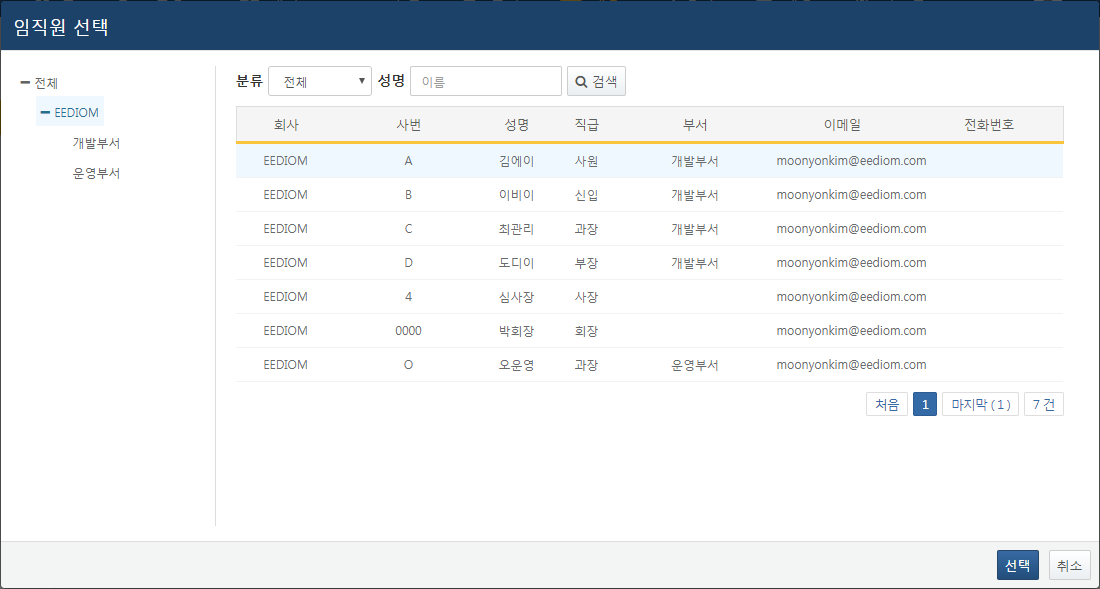
1차 검토자 자동 지정

* 소명 대상자의 부서에 부서장이 1차 검토자로 지정
* 소명 대상자의 부서에 부서장이 없는 경우 상위 부서의 부서장이 1차 검토자로 지정
* 최상위 부서까지 올라가도 부서장이 없는 경우, 관리자 권한의 임직원이 1차 검토자로 지정

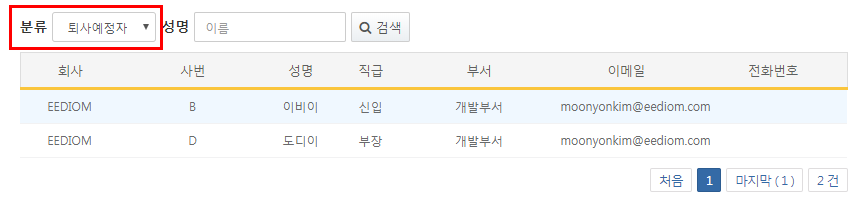
소명 대상자가 부서장인 경우, 1차 검토자 자동 지정

* 대상자(부서장)의 상위 부서에 부서장이 있는 경우, 상위 부서의 부서장이 1차 검토자로 지정
* 대상자(부서장)의 상위 부서가 없거나, 최상위 부서까지 올라가도 부서장이 없는 경우, 관리자 권한의 임직원을 1차 검토자로 지정





대상자 선택 화면에서 분류를 퇴사예정자로 검색하면 퇴사 일자가 정해진 임직원들만 표시합니다.



단계 2

소명 분류 설정

소명 분류와 중요도를 설정합니다. 소명 분류 관리 페이지에서 소명 분류를 추가/삭제/편집할 수 있습니다.



단계 3

근거 로그 추가

소명 근거 로그 데이터를 검색합니다. 소명 대상자가 보안 위반 의심 행위를 했다는 근거 자료를 로그프레소 소나 수집기가 수집한 데이터에서 검색해서 소명 요청에 추가합니다.

근거 로그 조회 시 소명 대상에 관련된 레코드만 표시합니다. 이는 검색 시 조회 대상 테이블에 emp\_key 필드가 소명 대상의 사번과 일치하는 값만 출력하도록 구현되었기 때문입니다. 그렇기 때문에 수집기를 생성할 때 수집한 데이터에 사번을 매핑해서 테이블에 저장하도록 해야 소명 요청 시 수집 데이터를 근거로 삼을 수 있습니다. 예를 들면 수집한 데이터에서 IP주소나 계정명을 매핑 테이블이나 룩업을 통해 사번과 매핑해서 함께 저장하는 방법을 활용할 수 있습니다.

**조회 대상**

근거 자료가 수집된 테이블을 선택합니다.

**데이터 유형**

근거 자료를 수집한 수집기의 스키마를 선택합니다. 조회 대상 테이블에서 해당 스키마로 저장된 데이터를 검색하게 되고, 조회 결과 또한 해당 스키마로 표시합니다.

**조회 기간**

조회할 기간을 입력합니다. 해당 기간 내에 수집된 데이터를 출력합니다.

**검색 키워드**

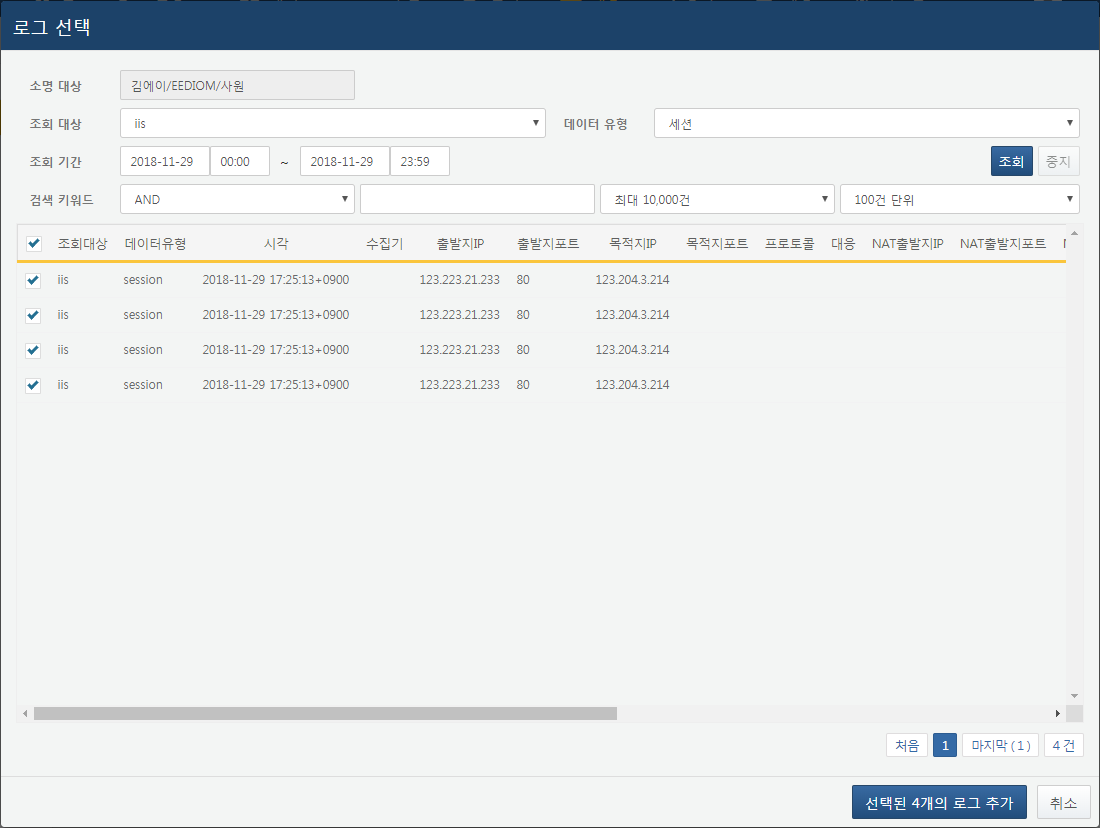
데이터 내용 중 검색할 키워드를 입력합니다. AND 조건으로 검색하면 모든 키워드가 존재하는 경우만, OR 조건은 하나의 키워드라도 존재하는 경우만 출력합니다. 쿼리 표현식 조건을 선택하면 데이터 검색에 사용할 fulltext 검색 불리언 표현식 쿼리를 직접 입력합니다.

**최대 건수**

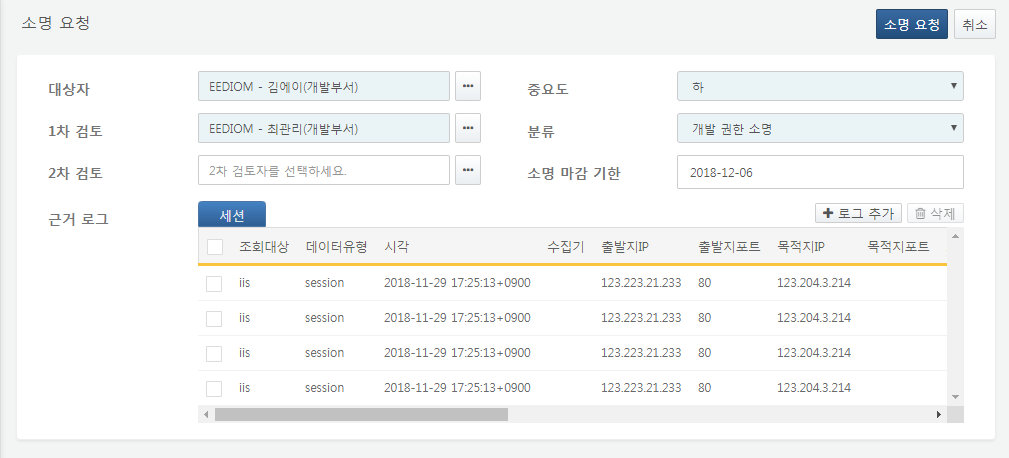
가져올 데이터의 최대 건수를 지정합니다.

**표시 단위**

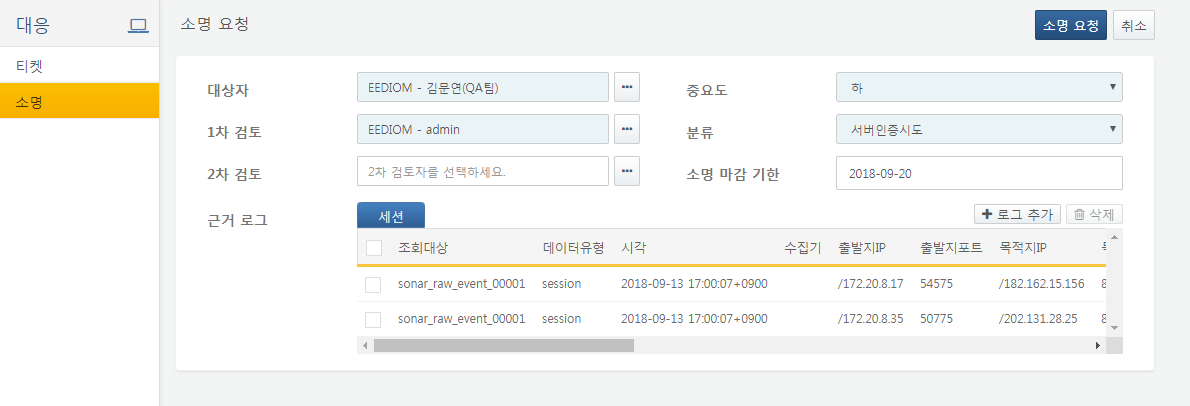
한 화면에 표시할 데이터 최대 건수를 지정합니다.



선택된 로그 추가 버튼을 누르면 선택한 로그 목록과 세션 유형이 소명 요청에 추가됩니다.



티켓 화면에서 소명 요청을 할 경우, 해당 티켓의 근거 자료가 소명의 근거 로그로 자동 추가됩니다.



단계 4

소명 요청

소명에 필요한 모든 내용을 작성했으면 화면 오른쪽 위 소명 요청 버튼을 눌러 소명 요청을 생성합니다.