최근 개인정보 유출사고 분석 및 대응

’24. 3월

KISA 한국인터넷진흥원

목차

01 개인정보 유출이란?

개정 후

표준 개인정보 보호지침 제25조, ’24.1.4. 시행

☑ **개인정보의 분실・도난・유출(이하 "유출등"**이라 한다)은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고 개인정보가 해당 **개인정보처리자의 관리・통제권을 벗어나 제3자가 그 내용을 알 수 있는 상태**에 이르게 된 것을 말한다.

개정 전

☑ 개인정보의 유출은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보처리자가 통제를 상실하거나 권한 없는 자의 접근을 허용한 것으로서 다음 각 호의 어느 하나에 해당하는 경우를 말한다.

1. 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우
2. 개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우
3. 개인정보처리자의 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이문서, 기타 저장 매체가 권한이 없는 자에게 잘못 전달된 경우
4. 기타 권한이 없는 자에게 개인정보가 전달된 경우

02 개인정보 유출 통지 및 신고

개정 후

개인정보 보호법 제34조, ’23.9.15. 시행

☑ 유출 통지

- (시점) **72시간 이내**

  * 다만, 아래에 해당하는 경우 해당 사유 해소 후 통지 가능

  1. 유출등이 된 개인정보의 확산 및 추가 유출등을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출등이 된 개인정보의 회수·삭제 등 긴급한 조치가 필요한 경우
  2. 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 통지하기 곤란한 경우

- (규모) 1명 이상

- (방법) 서면 등의 방법으로 개별 통지

  * 다만, 정보주체의 연락처를 알 수 없는 경우에는 홈페이지에 30일 이상 게시

☑ 유출 신고

- (시점) **72시간 이내**

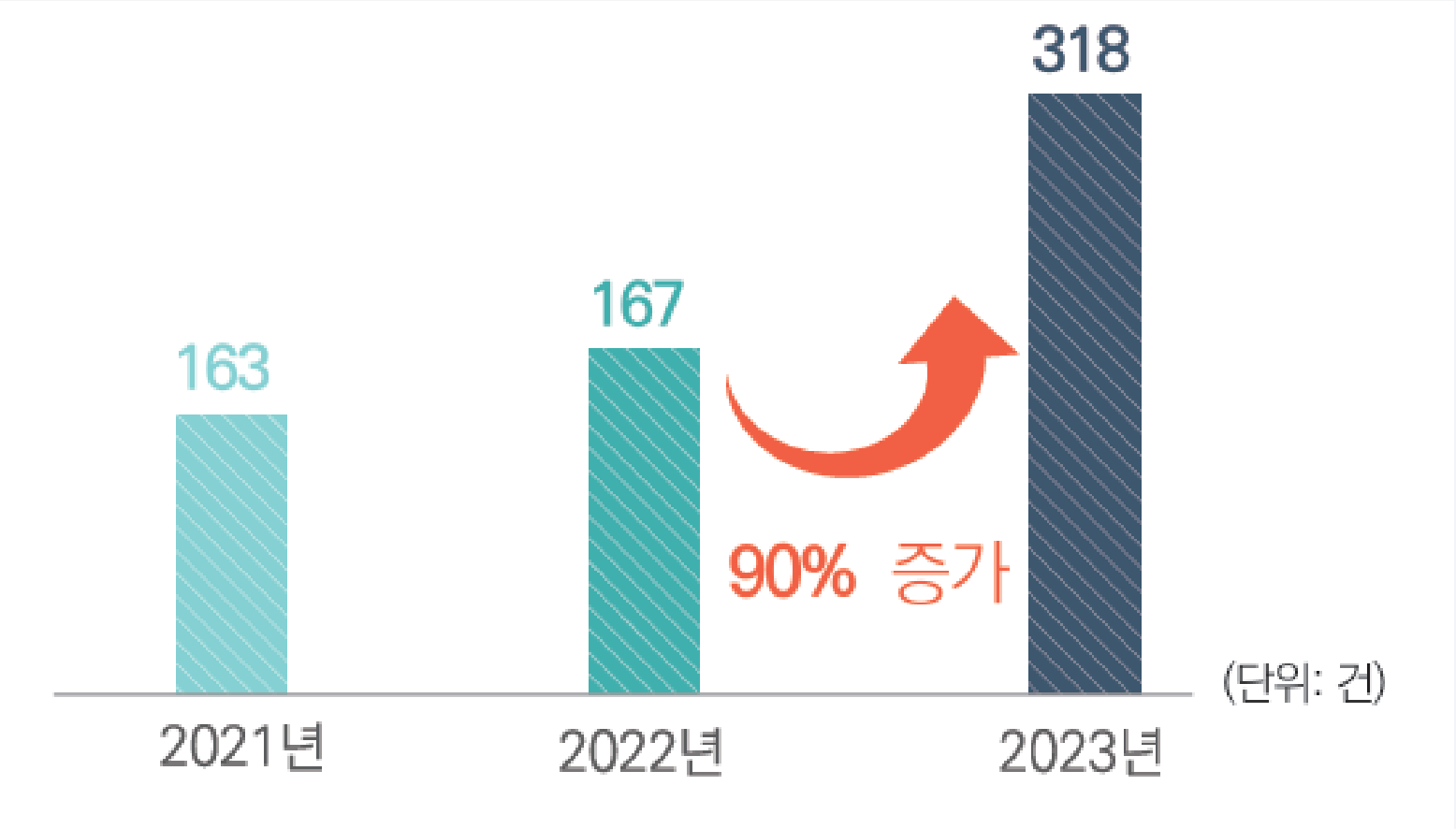
  * 다만, 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 신고하기 곤란한 경우에는 해당 사유가 해소된 후 지체 없이 신고

  * 다만, 개인정보 유출등의 경로가 확인되어 해당 개인정보를 회수·삭제하는 등의 조치를 통해 정보주체의 권익 침해 가능성이 현저히 낮아진 경우에는 신고하지 않을 수 있음

- (규모) **1천명 이상, 민감정보/고유식별정보 유출 등, 외부로부터의 불법적인 접근에 의해 개인정보가 유출 등**

- (방법) 개인정보 포털(privacy.go.kr)에서 신고

03 개인정보 유출 신고 현황



04 개인정보 조사 및 처분 규정

개정 후

개인정보 보호위원회의 조사 및 처분에 관한 규정, ’23.10.16. 시행

☑ **조사·처분 과정의 적법절차 강화**

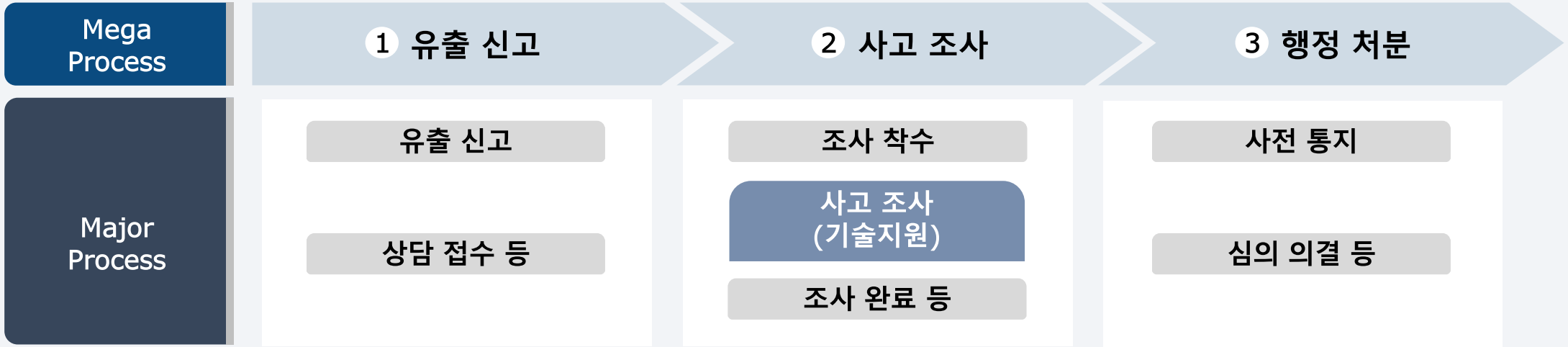
- 사건에 대한 안내를 강화하여 현장조사를 할 때 긴급사항 시에도 구두 통지가 아닌 조사공문을 교부
- 조사 종료 후에는 이후의 사건처리절차를 안내
- 사건이 종료되었을 때에는 조사대상자에게 처리결과를 안내 등

☑ **업무 프로세스 및 체계 개선**

- 단계별 처리기한을 명확화(신고 접수 후 14일 이내 조사 착수, 조사기간 6~12개월 등)
- 경미한 사건은 간소화 절차를 마련하였고, 소재불명, 연락두절 등 조사중지 사유를 신설
- 개인정보 침해를 선제적·예방적 점검할 수 있는 사전 실태점검(법 제63조의2) 세부 기준 마련 등

05 개인정보 유출사고 처리 절차

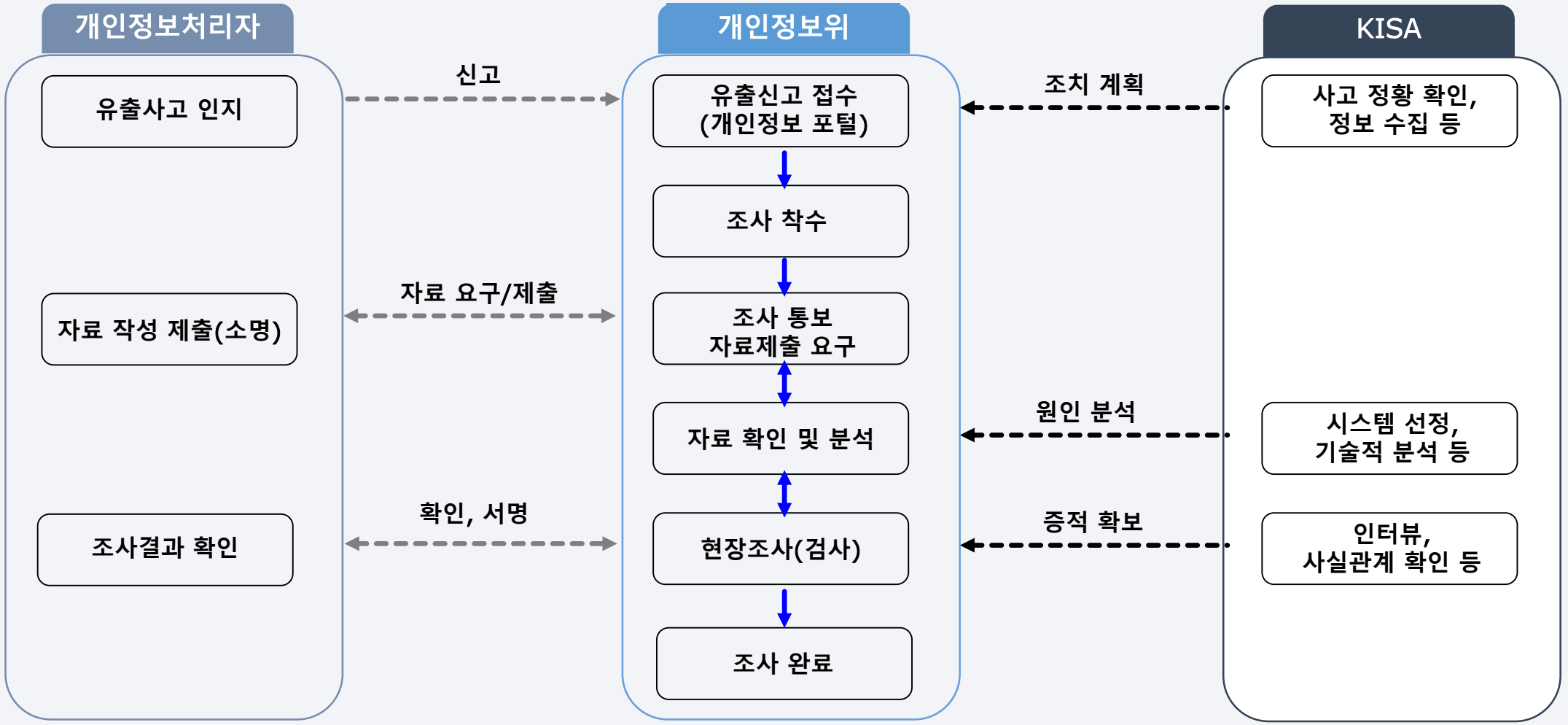
사건별 상이할 수 있음



- ☑ 개인정보처리자 : 개인정보 유출 신고
- ☑ 개인정보보호위원회 : 개인정보 유출 신고 접수(KISA 공통), 사고 조사, 행정 처분 등
- ☑ **KISA :** 개인정보위의 사고조사에 대한 **기술적 사항을 자문**하는 등 필요한 지원을 수행(법 63조)
  - 사고 경로 및 원인, 사고 규모 및 항목, 사고 대응 경위 등

06 개인정보 유출사고 조사 절차

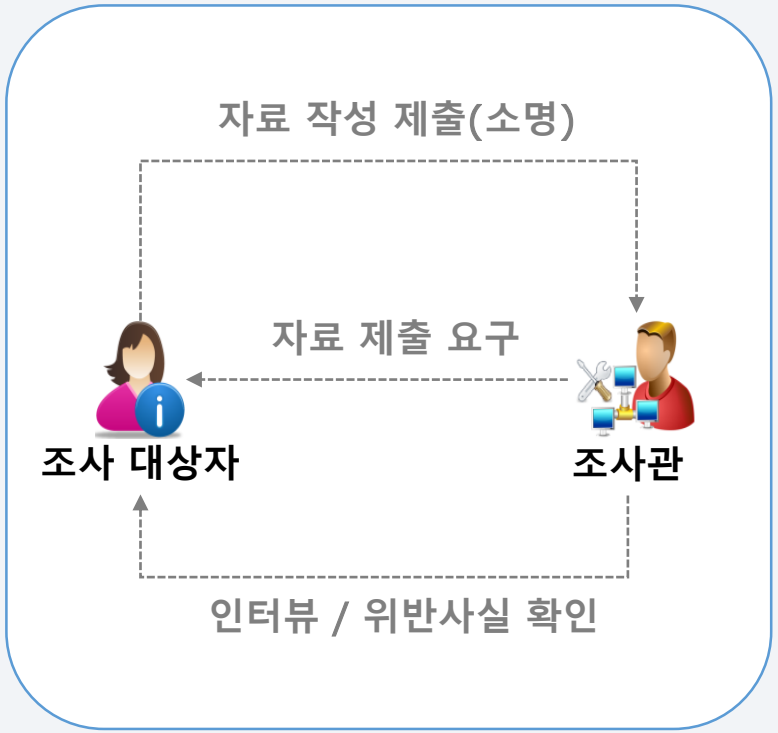
사건별 상이할 수 있음



07 개인정보 유출사고 분석 절차

사건별 상이할 수 있음

☑ 자료확보 → 제출자료·시스템·로그 등 분석 → 유출 경로·원인 확인 및 증거 자료 확보 → 피해규모·사실관계 확인 → 보고서 작성 등




제출 자료 분석


현장조사 (검사)


디스크 분석


로그 분석

유출 경로 파악


증적 수집

피해 규모 확인


보고서 작성

08 개인정보 유출사고 분석 사례(관리적)

09 개인정보 유출사고 분석 사례(기술적)

10 개인정보 유출사고 대응 조치

외부 공격

유출된 **시스템 분리·차단 조치**, 관련 로그 등 **증거자료 확보**, 유출 **경로 및 원인 분석**,
이용자 및 개인정보취급자 **비밀번호 변경** 등 안전조치 강화, 시스템 개선 및 복구 등

시스템 오류

시스템 **영향도 분석, 소스코드, API 설정 및 연동, 서버 설정** 개선, **형상관리**(기록, 보관) 등

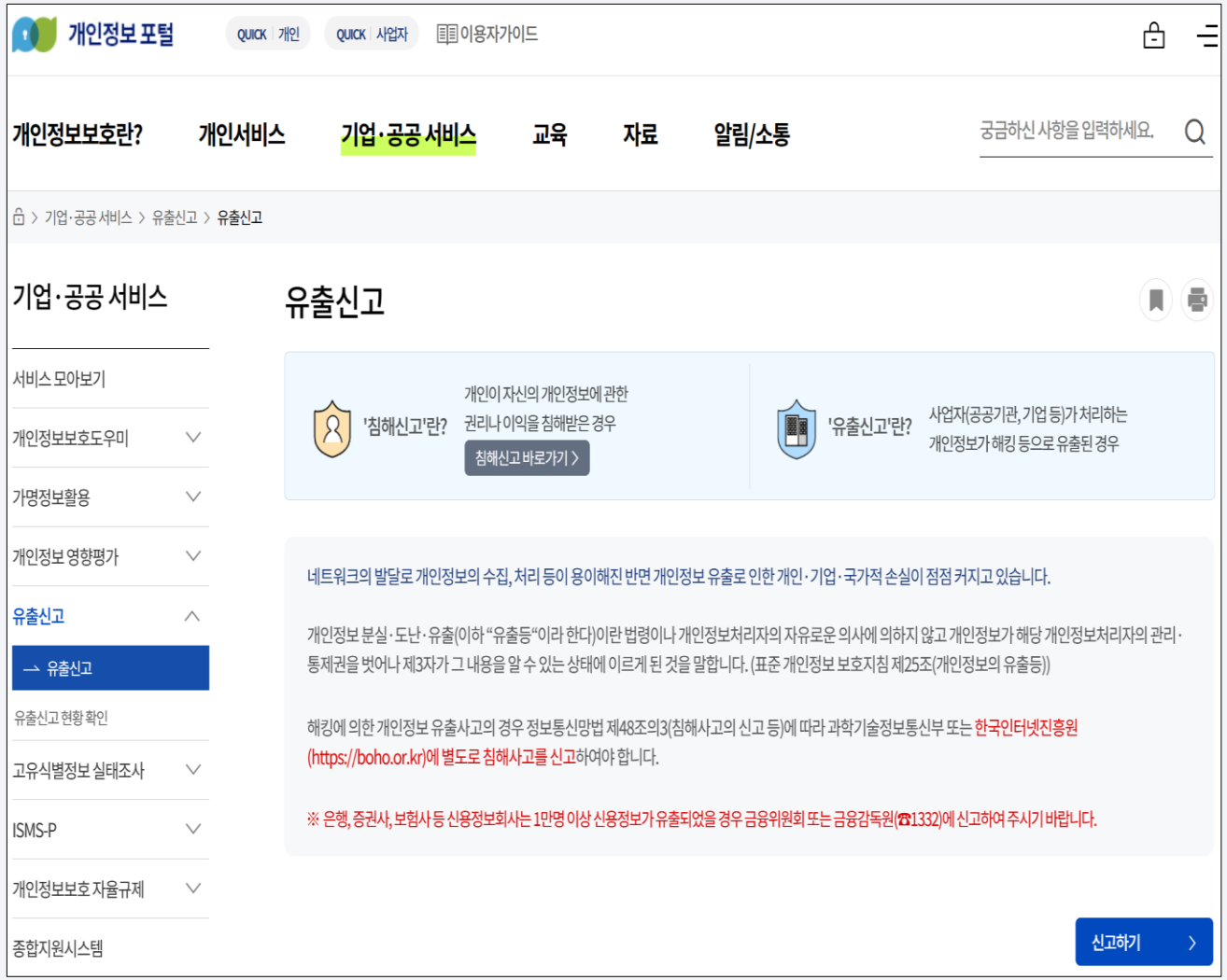
검색 노출

검색엔진에 **노출된 개인정보 삭제** 요청, 관리자 계정 **로그인 추가 인증, 소스코드** 점검
(개인정보 포함시 삭제), **웹페이지 전송방식** 확인(GET방식이 아닌 POST방식 사용) 등

11 개인정보 유출사고 통지 및 신고(1/2)

적용 대상		개인정보처리자
적용 범위		개인정보 유출 등
의무 사항		통지 및 신고
벌칙 규정		3천만원 이하의 과태료
유출통지	규모	1명 이상
	시점	72시간 이내
	방법	홈페이지, 서면 등의 방법으로 개별 통지
	항목	유출 등이 된 개인정보 항목, 유출 등이 된 시점과 그 경위, 유출 등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보, 개인정보처리자 대응조치 및 피해 구제절차, 피해 신고·상담 부서 및 연락처 등
유출신고	규모	1. 1천명 이상 2. 민감정보, 고유식별정보 유출 등 3. 외부로부터의 불법적인 접근에 의해 개인정보가 유출 등
	시점	72시간 이내
	기관	개인정보보호위원회 또는 한국인터넷진흥원(KISA)

11 개인정보 유출사고 통지 및 신고(2/2)



대상	◯ 개인정보처리자
신고 기준	※ 아래 어느 하나에 해당하는 경우에 신고하여야 함 - 1천명 이상의 정보주체에 관한 개인정보가 유출등이 된 경우 - 민감정보 또는 고유식별정보가 유출등이 된 경우 - 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의해 개인정보가 유출등이 된 경우
신고 기한	72시간 이내
신고 내용	1. 정보주체에의 통지 여부 2. 유출등이 된 개인정보의 항목과 규모 3. 유출등이 된 시점과 경위 4. 유출등에 따른 피해 최소화 대책·조치 및 결과 5. 정보주체가 할 수 있는 피해 최소화 방법 및 구제절차 6. 담당부서·담당자 및 연락처
근거 조항	개인정보 보호법 제34조

12 개인정보 유출사고 안전조치 예시

기술적 안전조치 예시

01 | 파일 업로드 취약점 예방

- 웹서버 내 이용자가 첨부하는 파일의 확장자를 제한
- 첨부할 수 있는 파일의 최대 크기를 제한
- 사용자가 파일 업로드 시 파일명을 임의로 변경하여 저장
- 사용자·업로드 폴더는 권한이 있는 사용자만 업로드 가능하도록 변경 등

02 | SQL 인젝션 취약점 예방

- 사용자가 입력한 데이터에 대해 특수 문자가 SQL 문법으로 인식되지 않도록 보안 조치 적용
- 에러 메시지가 노출되지 않게 설정하거나 일반적인 오류 메시지만 표시하여 정보를 추출하는 것을 방지
- 사용자 입력 데이터 중, 특수 문자가 SQL 문법으로 인식되지 않도록 조치
- 웹 취약점 점검(연 1회 이상) 및 웹 에디터 등 게시판 도구 업데이트(상시)
- 웹 방화벽을 사용하고 정기적으로 보안 업데이트 실시 등

03 | 크리덴셜 스터핑 예방

- 서버 및 보안장비에 접속을 시도하는 데이터를 분석하여 접근 임계치를 설정
  ※ (예시) 동일한 IP에서 O분간 ㅁㅁ회 이상 접속을 시도하는 경우 등
- 임계치를 초과하여 접속하는 경우 해당 IP에서 서버 접근을 일정 시간 차단하고, 보안 담당자에게 알림 기능 등 활성화
- 개인정보처리시스템 모니터링으로 불법적이거나 비정상적인 접속 시도 등을 탐지 및 차단 필요
- 일정 횟수 이상 로그인 실패 시 로그인 절차에 추가적으로 2차 인증수단 또는 CAPTCHA 등을 추가하여 인증 강화 등
  ※ 이외에도 비인가 접근통제 강화, 접근권한 최소화 관리, 지속적인 모니터링 등의 안전조치 필요

관리적 안전조치 예시

업무 과실 예방

- 다수의 수신자에게 메일 발송 시에는 '개별 발송' 또는 '숨은 참조' 기능을 활용하거나 발송 버튼 클릭 시 팝업 등으로 수신자 재 확인
- 구글, 네이버 폼 등 설문조사 서비스 이용 시 설문 참여자·편집자의 정보 공개범위를 '비공개(제한됨)'로 설정하는 등 공개범위 설정
- 개인정보가 포함된 엑셀 파일을 외부 공개 시 개인정보를 '숨김'으로 처리하지 않고 삭제 후 게시
- 개인정보취급자의 개인정보 처리실태 점검 등 지속적인 관리·감독 실시 등

13 개인정보 주요 안전조치

접근권한

- ☑ 시스템 접근권한을 차등 부여
- ☑ 인사이동 시 접근권한 변경, 말소
- ☑ 일정횟수 이상 인증 실패시 접근 제한 등

접근통제

- ☑ IP 주소 등으로 인가받지 않은 접근을 제한
  IP 주소 등을 분석하여 탐지 및 대응
- ☑ 안전한 접속수단, 인증수단 적용
- ☑ 취약점 점검 등으로 취약점 제거 조치 등

암호화

- ☑ 안전한 암호 알고리즘으로 암호화 저장
- ☑ 안전한 암호 알고리즘으로 암호화 송신 등

접속기록

- ☑ 접속기록을 최소 1년 이상 안전하게 보관
- ☑ 접속기록을 월 1회 이상 점검 등

백신

- ☑ 백신 SW 등의 보안 프로그램 설치, 운영
- ☑ 보안 업데이트 실시 등

감사합니다

KISA 한국인터넷진흥원