개인정보보호위원회 보도자료

보도시점 2025. 6. 12.(목) 12:00 (2025. 6. 12.(목) 석간) 배포 2025. 6. 11.(수) 18:50

안전조치 소홀로 개인정보를 유출한 2개 대학에 과징금 9억 6,600만 원 부과

- 주말·야간 포함 24시간 유출 탐지·차단 체계 운영토록 시정명령도 부과
- 교육부에 "대학 학사정보시스템의 개인정보 관리 강화 전파 및 대학 평가에 반영 검토" 요청

개인정보보호위원회(위원장 고학수, 이하 '개인정보위')는 6월 11일(수)에 개최된 제13회 전체회의에서 개인정보 보호법(이하 '보호법')을 위반하여 개인정보를 유출한 **전북대학교**와 **이화여자대학교**에 총 **9억 6,600만 원의 과징금***과 **540만 원의 과태료**를 부과하고 **시정명령, 공표명령** 및 **징계권고**를 하기로 의결하였다.

* 개인정보 유출에 따른 피해 규모 등을 고려하여 전북대학교(32만여 명 유출)는 6억 2,300만 원, 이화여자대학교(8만 3천여 명 유출)는 3억 4,300만 원을 각 부과

개인정보위는 개인정보 유출 신고에 따라 조사한 결과, 이들 대학의 **학사정보시스템**에 **구축 당시부터 취약점**이 **존재**하여 왔고, 일과시간 외 **야간 및 주말**에는 외부의 불법 접근을 탐지하여 차단하는 **모니터링이 제대로 이루어지지 않**는 등 「**개인정보 보호법**」**에 따른 안전조치의무**를 **소홀**히 한 사실을 확인하였다. 대학별 위반 내용과 처분 결과는 다음과 같다.

<전북대학교>

'24. 7. 28.(일) ~ 7. 29.(월) 해커가 에스큐엘(SQL) 인젝션(데이터베이스 명령어 주입)* 및 파라미터(입력값) 변조** 공격을 통해 전북대학교 학사행정정보시스템에 침입하여 **32만여 명**의 **개인정보(주민등록번호 28만여 건 포함)**를 **탈취**하였다.

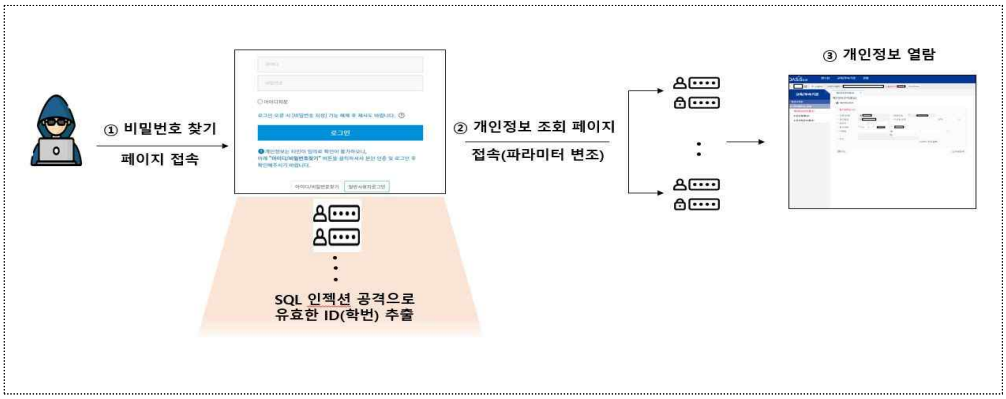
* 데이터베이스 명령어를 악의적으로 조작하여 서버를 오작동시킴으로써 접근권한 없는 정보를 열람 또는 변조하는 공격 방식

** 웹 애플리케이션에서 입력된 데이터 검증 로직의 취약점을 악용하여 입력값 조작을 통해 개인정보를 탈취하는 해킹 기법

개인정보위 조사 결과, 해커는 학사행정정보시스템의 비밀번호 찾기 페이지에 존재하는 취약점을 악용하여 학번 정보를 입수한 후 학적정보 조회 페이지 등에서 약 90만 회의 파라미터 변조 및 무작위 대입을 통해 전북대학교 학생 및 평생교육원 홈페이지 회원 총 32만여 명의 개인정보에 접근한 것으로 파악되었다. 해당 취약점은 '10. 12월 시스템 구축 당시부터 존재하였다.

※ '97~'01년 당사자의 동의를 받아 수집한 주민등록번호 233건을 주민등록번호 수집 법정주의 도입('14.8.7.) 이후에도 파기하지 않고 계속 보유한 위반사항도 확인

< 개인정보 유출사고 개요 >



아울러 전북대학교는 기본적 보안 장비는 갖추고 있었으나 외부 공격에 대한 대응이 미흡하였고, 특히 일과시간 외에는 모니터링을 소홀히 한 결과 **주말·야간에 발생한 비정상적 트래픽 급증 현상**을 **'24. 7. 29.(월) 오후에야 뒤늦게 인지**한 것으로 드러났다.

이에 따라 개인정보위는 전북대학교에 총 **6억 2,300만 원의 과징금**과 **540만 원의 과태료**를 부과하면서 이를 **대학 홈페이지에 공표**하도록 명하는 한편, 모의해킹 등 취약점 점검을 강화하고 상시 모니터링 체계를 구축하도록 **시정명령** 함과 동시에 책임자에 대한 **징계**도 **권고**하였다.

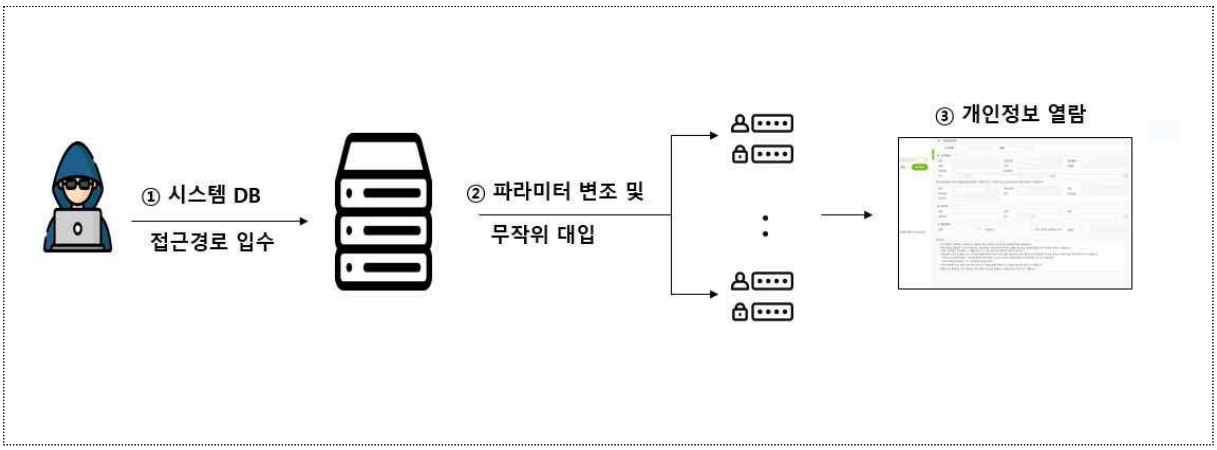
<이화여자대학교>

'24. 9. 2.(월) ~ 9. 3.(화) 해커가 시스템의 데이터베이스(DB) 조회 기능의 취약점*을 악용한 파라미터 변조 공격으로 이화여자대학교 통합행정시스템에 침입하여 **8만 3천여 명**의 주민등록번호를 포함한 **개인정보**를 **탈취**하였다.

* 개인정보 조회 시, 세션값(사용자 식별값)과 조회 대상 정보가 불일치하는 경우에도 파라미터(학번) 변조를 통해 다른 사용자의 개인정보 조회가 가능한 취약점 존재

개인정보위 조사 결과, 해커는 통합행정시스템에 접근하여 약 10만 회의 파라미터 변조 및 무작위 대입을 통해 이화여자대학교 학부생 및 학부 졸업생 8만 3천여 명의 개인정보를 탈취한 것으로 드러났다.

< 개인정보 유출사고 개요 >



이화여자대학교 역시 이러한 **취약점**이 **'15. 11월 시스템 구축 당시부터 존재**해 왔던 것으로 나타났으며, 마찬가지로 기본적인 보안 체계는 갖추고 있었으나 외부 공격(예: 동일한 아이피(IP)에서 타인의 개인정보를 반복적으로 조회 시도하는 경우 등)에 대한 대응이 미흡하였고, 특히 일과시간 외에는 **주말·야간 모니터링**을 **소홀**히 하는 등 외부의 불법적인 접근 통제 조치가 미흡했던 것으로 밝혀졌다.

이에 따라 개인정보위는 이화여자대학교에 총 **3억 4,300만 원의 과징금**을 부과하면서 이를 **대학 홈페이지에 공표**하도록 명하는 한편, 모의해킹 등 취약점 점검을 강화하고 상시 모니터링 체계를 구축하도록 **시정명령** 함과 동시에 책임자에 대한 **징계**를 **권고**하였다.

<이번 조사·처분의 의의>

대학의 경우 대개 생성규칙이 단순한 '학번' 등을 기준으로 개인정보를 관리하고 있어 파라미터(입력값) 변조 공격에 취약한 측면이 있고, 대규모 고유식별정보를 처리하고 있어 유출 사고 발생 시 정보주체의 막대한 피해가 예상된다. 이에 따라 파라미터 변조 공격에 대비하고, 외부의 불법적인 접근 시도를 24시간 철저히 모니터링하는 등 각별한 주의가 필요하다.

개인정보위는 최근 대학에서 개인정보 유출 사고가 잇따르는 점*을 감안하여, **교육부에 “전국 대학 학사정보관리시스템의 개인정보 관리가 강화될 수 있도록 전파해 줄 것과 관련 내용을 대학 평가 등에 반영될 수 있도록 검토해 줄 것”**을 **요청**할 예정이다.

* 지난해부터 ’25. 5월말까지 전국 대학에서 21건의 개인정보 유출 신고

[붙임] 대학별 위반 및 시정조치 내역

담당 부서 <총괄>	개인정보보호위원회 조사총괄과	책임자	과 장	김대현 (02-2100-3101)
		담당자	공공조사팀장	방선욱 (02-2100-3106)
			조사관	송영아 (02-2100-3105)
<공동>	한국인터넷진흥원 탐지조사팀	책임자	팀 장	문홍식 (061-820-2810)
		담당자	선 임	장웅태 (061-820-2817)

붙임 | **대학별 위반 및 시정조치 내역**

사업자명	위반 내용	위반 조항 (보호법)	시정조치(안)
전북대학교	• 안전조치 의무 위반 • 주민등록번호 처리 제한 위반	• 법 §29 • 법 §24의2①	**• 과징금 6억 2,300만 원** **• 과태료 540만 원** **• 시정명령** **• 공표명령** **• 징계권고**
이화여자대학교	• 안전조치 의무 위반	• 법 §29	**• 과징금 3억 4,300만 원** **• 시정명령** **• 공표명령** **• 징계권고**