국회입법조사처 | 2025. 7. 21. | 제2387호

이슈와 논점
Issues and Perspectives

한국연구재단 해킹 사건을 계기로 본 공공기관 정보보호 강화방안

황 현 희 · 강 은 수

2025년 6월 한국연구재단의 논문투고시스템(JAMS)이 해킹되어 약 12만 명의 연구자 개인정보가 유출되었다. 이번 사건은 재단의 심각한 보안 취약성과 미흡한 초기대응은 물론, 공공기관 정보보호 체계 전반의 구조적 문제점을 드러낸 것이다. 공공기관의 사이버보안 진단·점검의 법적 근거를 상위 법률로 격상하면서 제재 수단을 도입하고, 정보보호 인증 및 공시 의무 대상을 공공기관까지 확대하는 방향으로 정보통신망법 등의 개정을 검토할 필요가 있다. 아울러, 「개인정보 보호법 시행령」 개정을 통해 고위험 정보 등이 유출된 경우에는 '인지 즉시 우선 통지'를 의무화하는 방안도 고려할 수 있다.

1 한국연구재단 해킹 사건의 시사점

2025년 6월 6일, 한국연구재단(이하 "재단")의 논문투고시스템(JAMS)[1]이 해킹되어 약 12만 명의 연구자 개인정보가 유출되었다.

지난 4월 역대 최악으로 평가된 SKT 해킹 사태가 채 수습되기도 전에, 6월에는 예스24와 재단까지 민간과 공공을 불문하고 사이버공격이 잇따르고 있다. 특히 이번 사건은 국가 R&D 지원의 핵심 공공기관이 단순 공격에 무방비로 노출되었다는 점에서 연구생태계의 신뢰를 흔들 수 있는 중대한 사안이다.

그럼에도 사회적 주목은 크지 않았고, 언론 보도도 많지 않은 편이다. 공공부문 사이버보안에 대한 사회 전반의 문제 인식이 오히려 부족함을 보여준다.

사이버공격이 갈수록 정교화 · 고도화되는 상황에서 공공기관의 정보보호는 조직의 지속가능성과 국민 신뢰 확보를 위한 필수 조건이다. 기술적 대응만으로는 한계가 있는 만큼, 법·제도적 기반을 포함한 종합적인 대응 체계 마련이 시급하다.

이 글에서는 재단 해킹 사건의 주요 경과를 살펴보고, 사전 예방 체계 및 대응 과정에서 드러난 문제점을 분석한 뒤, 공공기관의 정보보호 강화를 위한 개선과제를 제시하고자 한다.

2 사건 발생 경과 및 피해 현황[2]

2025년 6월 6일 새벽, 공격자는 기초적 수준의 해킹기법인 'URL 파라미터 변조'[3] 방식을 통해 JAMS 사용자의 비밀번호 초기화를 시도했다.

재단은 자체 조사 결과를 토대로 6월 7일, "비밀번호가 변경되지 않아 개인정보 유출은 없었다"고 공지했다. 그러나 6월 9일, 과학기술정보통신부(이하 "과기부") 소관 '사이버안전센터'[4]의 정밀 조사에서 개인정보 유출 사실이 확인되었다.

1) JAMS(Journal & Article Management System)는 학술지 논문 투고·심사·출판 업무의 통합관리 시스템으로, 주로 소규모 영세학회 대상으로 서비스를 제공한다(2025.6월 기준 1,617개 학회 가입, 약 79만 명 이용).

2) 재단 제출자료(2025.7.1.) 및 유선 확인을 토대로 작성하였으며, 현재 과기부 및 개보위 조사가 진행 중이므로, 추후 달라질 수 있다.

3) 웹사이트 URL 주소의 매개변수(Parameter) 값을 임으로 조작하여 접근 권한 없는 정보에 접근하거나 서버의 동작을 바꾸는 기초적 해킹기법이다. (예) https://example.com/user?user_id=1001에서 "user id" 값만 바꿔 접속하면 다른 사용자의 정보를 열람할 수 있다.

4) 정식 명칭은 '과학기술정보통신 사이버안전센터"로, 과기부가 설치하고 한국과학기술정보연구원(KISTI)이 수탁 운영한다. 과기부 산하 · 유관기관과 국가과학기술연구회(NST) 소관 출연연에 대해 24시간 통합관제, 취약점 점검 · 대응, 침해 대응훈련 등 정보보안을 지원한다.

NARS
www.nars.go.kr

발행처 국회입법조사처
발행인 이관후 국회입법조사처장
저 자 황현희 사회문화조사실 과학방송통신팀 팀장
02-6788-4710 wonder@assembly.go.kr
강은수 사회문화조사실 과학방송통신팀 입법조사관
02-6788-4712 eunsu@assembly.go.kr

국회입법조사처
NATIONAL ASSEMBLY RESEARCH SERVICE

재단은 3일이 지난 6월 12일에서야 사과문을 통해 기존 공지 내용을 정정한 후, 개인정보보호위원회(이하 "개보위")에 유출 사실을 신고했다.

재단에 따르면, 전체 JAMS 이용자 약 79만 명 중 12만 2,954명의 개인정보가 유출되었고, 회원 가입 시 입력정보 일체(이름, ID, 생년월일, 휴대전화, 직장, 계좌 등)가 유출되면서, 116명의 경우 주민등록번호[5]까지 함께 유출된 것으로 파악된다.

또한 6월 17일 새벽에는 피해자 중 1,559명의 명의로 특정 학회에 무단 가입된 사실이 확인되었다. 재단은 즉각적인 가입 무효화 조치를 통해 추가적인 피해는 없었다는 입장이나, 중요한 건 '명의 도용'이라는 2차 피해가 현실화되었다는 점이다.

이는 회원 가입 시 이중 인증조차 적용하지 않은 채 시스템을 서둘러 재개한 것이 결정적 원인으로 보인다. 재단은 6월 20일에 이르러서야 이중 인증 기능을 도입하며 본인확인 절차를 강화했다.[6]

[표] 한국연구재단 JAMS 해킹 사건의 주요 경과

일자	주요 경과
6. 6.(금)	02:43 해킹 발생, 09:45 **의심 신고**→사고 인지, 11:47 1차 내부조사, 22:50 사고 신고(과기부), 23:47 JAMS 차단
6. 7.(토)	13:20 개인 통지(이메일 발송, '유출 불가')
6. 8.(일)	11:00 취약점 보완 및 JAMS 재개
6. 9.(월)	10:00 2차 정밀조사(과기부 주관), 16:50 유출 확인
6.12.(목)	16:00 유출 통지, 16:07 유출 신고(개보위), 16:29 사과문
6.17.(화)	02:00 2차 피해, 09:00 **의심 신고**, 09:30 JAMS 차단
6.18.(수)	08:00 취약점 보완 및 JAMS 재개(신규가입 기능 제외)
6.20.(금)	JAMS 이중 인증 절차 도입, 10:00 2차 피해 통지(카톡)

* 재단 제출자료(2025.7.1.) 및 유선 확인 토대로 재구성 (※ 이후 경과는 생략)

3 공공기관 정보보호 체계의 문제점

(1) 보안 설계의 심각한 구조적 취약성

재단은 JAMS의 근본적인 보안 취약점을 장기간 방치한 채 운영해 왔다. 2008년 최초 개통된 이후 일부 기능 보완은 이루어졌으나, 보안 구조 전반에 대한 고도화나 재설계는 전혀 진행되지 않았다.

특히 이중 인증 절차 없이도 회원 가입과 임시비밀번호 발급이 가능했고, 4가지 식별정보(이름, ID, 생년월일, 이메일) 중 '이메일'만 입력해도 시스템이 응답하도록 설계되어 있었다. 응답 과정에서 요청 범위를 넘어 개인정보 테이블 전체가 서버로부터 전송(반환)되도록 설계된 구조적 허점도 발견되었다.

개발단계는 물론 기능 보완 과정에서도 보안에 대한 고려가 없었던 전형적 사례로, 이처럼 허술한 설계 결함은 '이메일'이라는 단일 정보와 단순한 URL 조작만으로 대량의 개인정보 유출로 이어졌다.

이에 대해 재단은 5명으로 구성된 정보보안팀이 관제[7]를 제외한 자체 보안 업무를 수행 중이나, 보안 인력이 지침상 기준 인원(7명)에 못 미쳐 매년 증원(+2명)과 시스템고도화 예산을 요청하고 있음에도 반영되지 않아 대응에 한계가 있다고 설명한다.

그러나 이는 인력과 예산 부족을 이유로 근본적인 책임을 회피하는 듯한 해명으로, 실제로 보안 예산 등 내부 자원이 전략적 배분과 우선순위에 따라 적절히 편성·집행되어왔는지 점검이 필요하다.

또한 사이버안전센터의 24시간 통합관제에도 불구하고, 1·2차 피해 모두 '의심 신고'로 인지된 점은 관제 체계가 제대로 기능하지 않았음을 보여준다. 재단의 주무 부처이자 통합관제를 총괄하는 과기부 역시 이번 사고의 책임에서 자유로울 수 없다.

(2) 초기대응 부실과 유출 통지체계의 한계

현행 「개인정보 보호법 시행령」 제39조는 개인정보 유출 사실을 인지한 경우 72시간 이내에 통지하되, 확인된 사실만 우선 통지하고 추가로 확인되는 내용은 확인 즉시 통지하도록 규정하고 있다.

그러나 실제 현장에서는 이 규정이 최대 72시간까지 통지를 미룰 수 있는 근거로 오용되는 경향이 있다. 재단 역시 2차 정밀 조사에서 유출 사실을 확인하고도 '피해 규모 미확정'을 이유로 3일간 '유출 없음'을 유지하여 공공기관으로서의 책임성과 신뢰성을 훼손했다는 비판을 받고 있다.

5) 계좌정보(은행, 계좌번호, 명의자) 중 계좌번호는 암호화된 상태였고, 주민등록번호는 사용자가 '비고' 란에 임의로 입력한 경우였다.

6) 이중 인증은 로그인 등에 우선 적용, 신규 가입에는 6.30.부터 적용 후 기능 재개

7) 24시간 관제는 '과학기술정보통신 사이버안전센터'에서 통합 수행한다 (※ 1쪽 '각주 4번' 참조).

이러한 통지 지연은 국민의 알 권리를 침해하고 2차 피해 가능성을 높이는 결과로 이어질 수 있다.

또한 시행령과 개보위 가이드라인[8]에 규정된 단계별 통지절차 및 72시간 초과 통지가 허용되는 '정당한 사유'의 기준 등이 불명확해 대응 과정에서 판단의 어려움을 겪는 것으로 보인다. 실제로 재단 관계자 역시 통지 시점과 방법 등에 관한 판단이 가장 어려웠다고 언급한 바 있다.[9]

아울러 6월 12일에 발송된 피해자 통지 메일도 문제점으로 지적된다. 해당 메일은 수신자가 실제 유출 대상자인지를 명확히 적시하지 않아, 본인의 개인정보가 유출된 것인지, 단순한 사고 공지인지 혼란을 초래했다. 또한 휴대폰 문자 등 즉시 확인 가능한 수단이 아닌 이메일로만 통지함으로써 통지의 실효성이 떨어졌다는 비판도 제기된다.[10]

(3) 공공기관 정보보호 인증의 사각지대

재단은 정부가 부여하는 정보보호 관리체계 인증(이하 'ISMS 인증'[11])을 보유하고 있지 않다.

현행 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법') 제47조는 전년도 정보통신서비스 부문 매출액(100억 원 이상) 또는 일일 평균 이용자 수(100만 명 이상)를 기준으로 ISMS 인증을 의무화하고 있다.

이에 따라 대다수 공공기관은 의무 대상에서 제외된다.[12] 재단과 같이 국가 R&D 등 고도의 정보자산을 다루는 기관조차 ISMS 인증 없이 정보시스템을 운영하고 있다. 일부 공공기관이 자율적으로 취득한 사례도 있으나 소수에 그쳐,[13] 공공부문 전반이 정보보호 인증의 구조적 사각지대에 놓여 있다.

(4) 공공기관의 정보보호 공시 의무 배제

'정보보호 공시'는 정보보호 투자·인력·인증 현황 등을 공개함으로써 정보보호 투자를 유도하고 이용자 보호를 강화하기 위한 제도이다.

그러나 재단을 포함한 공공기관은 「정보보호산업의 진흥에 관한 법률」(이하 '정보보호산업법') 제13조 및 같은 법 시행령 제8조에 따라 공시 의무 대상에서 제외된다. 이는 공공기관이 국가정보원의 사이버보안 실태평가를 받고 있으며, 「공공기관의 운영에 관한 법률」에 따른 경영공시·평가 등 다른 제도와의 중복규제 우려가 반영된 결과로 보인다.[14]

하지만 이들 제도는 경영관리 중심이거나 결과 공개가 제한적이어서[15] 대체 수단으로는 한계가 있고, 기관별 정보보호 수준을 외부에서 파악하기 어렵다. 특히 국가 R&D 및 과학기술 정보를 다루는 기관은 정보 유출이 국가적 피해로 직결될 수 있는 만큼 보다 높은 수준의 보안 체계와 함께 정보보호에 대한 책임성과 외부 점검 가능성을 높일 필요가 있다.

4 입법 및 제도 개선 과제

(1) 사이버보안 진단·점검의 실효성 강화

「사이버안보 업무규정」(대통령령) 제12조는 공공기관의 장 등에게 사이버보안 자체 진단·점검을 연 1회 이상 실시하고, 취약 요소가 발견되면 시정조치를 하도록 의무화하고 있다.

재단도 이에 따라 자체 점검을 실시한 것으로 파악되나, 보안 설계상의 기초적 취약점이 장기간 방치된 채 운영되었고, 결국 해킹 사고로 이어졌다.

따라서 보안 점검의 근거를 「전자정부법」 등 상위 법률로 격상[16]하고, 일정 기한 내 시정조치를 의무화하며, 미이행 시 과태료 등 제재 수단을 도입함으로써 법적 구속력과 실효성을 강화할 필요가 있다.

8) 「개인정보 유출 등 사건 대응 매뉴얼」(개인정보위 가이드라인)

9) 재단 해킹 사건 관련 간담회(국회입법조사처 주관, 2025.7.1.)

10) 단, 주민등록번호 유출자에겐 가능한 전화 통지를 시도했다는 설명이다.

11) 정보통신망의 안정성·신뢰성 확보를 위해 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계를 수립·운영하는 자에 대한 인증 제도

12) 한국인터넷진흥원에 따르면, 현재 공공기관 중 정보통신서비스 부문 매출액 100억 원 이상인 한국교육방송공사, 서울올림픽기념국민체육진흥공단, 한국철도공사, ㈜에스알만이 인증 의무자에 포함된다.

13) 국가·공공분야 자율 인증 취득기관은 문화체육관광부, 중소기업중앙회 등 총 26개 기관이다(한국인터넷진흥원 제출자료, 2025.6.19.).

14) 정보통신망법 개정안(의안번호 2104486)에 대한 검토보고서(과학기술정보방송통신위원회), 과기부 제출자료(2025.6.23.) 등 참고

15) 국정원 평가는 기관별 평가등급(우수, 보통, 미흡)만 공개되고 있다.

16) 다만, 법률 격상 시 어느 법(전자정부법, 국가정보원법 등)에 포함할지, 별도 제정법을 마련할지에 대한 충분한 검토와 부처 간 조율이 요구된다.

특히 정보보호는 단순 전산 관리가 아닌 고도의 전문성이 요구되는 핵심 기능으로, '보안 투자'라는 인식 전환과 함께 인력 확충과 시스템 개선 등 역량 강화를 위한 적극적인 노력이 병행되어야 한다.

아울러 최근 SKT, 예스24, 외식·명품업계 등에서도 해킹 피해가 잇따른 만큼, 산하 공공기관은 물론 민간의 정보보호정책을 관장하는 과기부의 보다 능동적이고 책임 있는 역할 수행이 요구된다.

(2) 개인정보 유출 통지체계의 실효성 강화

현행 '72시간 이내 통지' 규정은 정보 주체의 권리 보호를 위한 최소한의 기준이지만, 실제 현장에서는 통지 지연의 근거로 오용되거나 해석상 논란의 소지가 있다. 이에 대해 개보위는 현실적으로 '인지 즉시 통지'를 강제하기는 어렵고, 72시간 안에 통지를 완료하면 법적 의무는 충족된다는 입장이다.[17]

그러나 2차 피해 최소화 및 신뢰 확보를 위해서는 신속히 우선 통지한 후 단계적 보완이 바람직하다. 특히 주민등록번호·금융정보 등 고위험 정보는 유출 즉시 대응하지 않으면 회복이 어려운 피해로 이어질 수 있어, 보다 엄격한 통지 기준이 요구된다.[18]

따라서 「개인정보 보호법 시행령」에 일정 요건의 고위험 상황[19]인 경우에는 '인지 즉시 우선 통지'를 의무화하는 예외 조항을 신설해 개인정보 자기결정권의 실질적 보장을 강화할 필요가 있다. 이때 '인지 즉시'는 예컨대 '24시간 이내'로 명시하는 방안을 고려할 수 있다. 다만 현장의 부담을 고려해 충분한 의견수렴을 거치는 것이 바람직할 것이다.

아울러 실무 기준이 모호하다는 현장의 의견을 반영하여 단계별 통지방식, '정당한 사유' 및 '예외 사유(신설 시)'의 범위, 개별 통지 원칙과 예외 적용 등의 판단 기준 등을 예시를 들어 구체화한 가이드라인 정비도 요구된다. 또한 이메일·문자·카카오톡 등을 병행하는 다중채널 통지를 권장하되, 고위험 정보 유출 시에는 이를 의무화하는 방안도 검토할 수 있다. SKT 해킹 당시에도 개별 통지 없이 홈페이지 공지로 갈음해 비난받은 바 있다. 형식적 통지를 통한 책임 회피가 반복되지 않도록 명확한 기준이 필요하다.

(3) 공공기관 정보보호 인증 및 공시 의무화

정보통신망법 개정을 통해 공공기관에도 ISMS 인증을 의무화하고, 정보보호산업 법령을 개정해 정보보호 공시 의무 대상에 공공기관을 포함하는 방안을 검토할 필요가 있다. 이를 통해 공공기관의 보안 위험을 사전에 식별하고 대응 역량을 강화하는 동시에, 정보보호 투자 확대를 유도하여 실질적인 정보보호 수준 향상에 기여할 것으로 기대된다.

다만 기관의 규모나 보유정보의 특성에 따라 이행 부담이 상이한 만큼, 국가 R&D·과학기술 정보 등 고위험 정보를 다루는 기관부터 우선 적용하고, 단계적으로 확대하는 방안도 고려할 수 있다.[20]

한편, 「개인정보 보호법」 제39조의7에 따른 '개인정보 손해배상책임 보장제도' 역시 공공기관을 원칙적으로 의무 대상에서 제외하고 있다.[21] 이는 별도 보장제도 없이도 책임 이행이 가능하다는 점이 고려된 결과로 보이나,[22] 피해자 대응이 지연되거나 형식적 보상에 그치는 경우가 많아 실효성에 대한 비판도 제기된다. 재단 관계자 역시 예산 확보의 문제로 직접 보상은 어렵다고 언급한 바 있다.[23]

개인정보 유출은 민간·공공을 불문하고 동일한 피해로 이어지며, 공공기관은 신뢰 훼손으로 인한 파장이 더 클 수 있다. 차제에 공공부문에도 실효성 있는 손해배상체계 마련을 검토할 필요가 있다.

『이슈와 논점』은 국회의원의 입법활동을 지원하기 위해 최신 국내외 동향 및 현안에 대해 수시로 발간하는 보고서입니다.

17) 개인정보보호위원회 담당자 유선 통화 확인(2025.7.4.)

18) 그러나 현재 유출 정보의 민감도나 위험도에 따라 통지 기준을 달리 하는 규정은 없다. 72시간 초과 통지를 허용하는 '정당한 사유'(긴급조치, 천재지변 등)만 있을 뿐이다. 이번 사건도 주민등록번호가 유출됐음에도, 유출 사실 자체를 부인하다 72시간 만에 통지했으나 위법으로 보기는 어렵다.

19) 예컨대, 주민등록번호·금융정보 등이 유출된 경우, 온라인 유포 또는 실시간 악용 정황이 포착된 경우 등을 들 수 있다.

20) 예컨대, 개인정보 대량 보유기관은 인증·공시를 의무화하되, 소규모 기관은 자율점검이나 일부 항목 공시 등 차등 적용을 고려할 수 있다.

21) '연매출 1500억 원 이상 & 100만 명 이상의 개인정보를 처리하는 자', '공공시스템운영기관' 등이 의무대상에 해당한다(시행령 제32조제4항).

22) 개인정보보호법 개정안(2112723) 검토보고서(정무위, 2021.11.)

23) 재단 해킹 사건 관련 간담회(국회입법조사처 주관, 2025.7.1.)에서 재단 관계자는 "예산 확보에 어려움이 있으며, 논문 심사료 인하 등 간접적 방식의 보상 방안을 논의 중"이라고 했다.

07233 서울시 영등포구 의사당대로 1 국회입법조사처
Tel. 02-6788-4510
발간등록번호 31-9735044-001340-14
ISSN 2005-744X