2026.9.29.

국회예산정책처 | 나보포커스 | 제177호

nabo Focus

개인정보 유출사고 관련 재정사업의 효과성 분석과 개선과제

산업예산분석과 김지수 분석관

분석 배경 및 현황

▪ **2026년 상반기 개인정보 유출신고는 432건[1]으로 반년 만에 2025년 연간 신고건수(447건)에 육박하였으며, 국민 다수의 개인정보를 처리하는 주요 사업자에서 대규모 유출사고가 잇따라 발생하면서 개인정보 보호 사업의 실효성 점검 필요성이 증대**

- 티빙(3,954만 계정), 쿠팡(3,756만 명), 듀오(43만 명)[2] 등 국민 생활과 밀접한 서비스를 제공하는 기업에서 대규모 개인정보 유출사고 발생

※ 유출 신고건수: ('21) 163건 → ('25) 447건 → ('26 上) 432건

▪ **개인정보보호위원회 주요 사업비는 2022년 347.2억원에서 2026년 549.7억원으로 202.5억원(58.3%) 증가하였으며, 2027년도 정부안에는 전년 대비 251.3억원(45.7%) 증가한 801억원이 편성됨**

- 주요 사업에는 정책·교육 및 인증제 운영 등 개인정보 보호기반을 조성하는 '개인정보보호강화'와, 유출·침해사고 조사 및 디지털 포렌식 랩 운영 등을 통해 사고 조사역량을 강화하는 '개인정보이슈대응' 등이 있음

- 이외에도 '신뢰기반의 AI 개인정보 보호활용 기술개발(R&D)' 등 개인정보 보호 관련 기술개발(R&D) 사업이 추진되고 있으며, 2027년도 정부안에는 181.6억원이 편성됨

[표 1] 개인정보 보호 관련 주요 사업 현황(2022~2027년)

(단위: 백만원, %)

구분	2022	2023	2024	2025	2026	2027(안)	증감률 ('26대비)
주요 사업비 예산	34,719	42,721	49,364	48,995	54,967	80,095[1]	45.7
(1031) 개인정보보호강화	8,925	9,231	9,639	9,693	8,478	8,792	3.7
(2034) 개인정보이슈대응	8,044	11,139	9,832	10,887	10,815	14,454	33.6

주: 1) 2027년 예산안 합계에는 공익신고장려기금(기획예산처 소관) 사업이 포함되어 있음
1. 2022~2026년은 예산현액, 2027년은 정부안 기준이며, 2027년도 과목구조 기준으로 작성함
자료: 개인정보보호위원회

▪ **이에 본고는 유출사고 급증에 대응한 재정투입 확대가 개인정보 사고조사 처리성과 제고와 유출사고 예방으로 이어지고 있는지, 관련 재정사업의 운영성과를 점검하고 개선과제를 제시하고자 함**

1) 개인정보보호위원회 보도자료(26.7.16), "AI 혁신을 뒷받침하고 국민 권익을 증진하는 예방중심 개인정보 보호 실현"
2) 듀오와 쿠팡은 각각 2026년 4월 22일 및 6월 10일 개인정보보호위원회 제재처분 의결 기준이며, 티빙은 2026년 6월 확인된 유출규모이다.

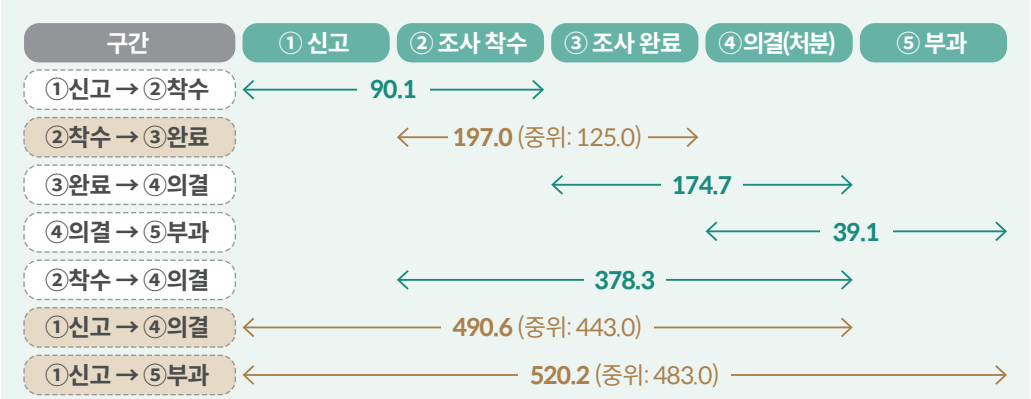
재정사업 문제점①
: 사고조사 처리 장기화

▪ **개인정보 유출 신고일부터 의결일까지 평균 490.6일이 소요되는 등 사고조사 처리가 전반적으로 장기화[3)]**

- 2020년 11월부터 2026년 4월까지 의결서가 공개된 사건(약 700건) 중 주요 사고조사 처리일자 확인이 가능한 사건을 분석
- 분석 결과, 평균적으로 신고 → 조사 착수 90.1일, 조사 착수 → 조사 완료 197.0일, 조사 완료 → 의결(처분) 174.7일이 소요되며, 신고 이후 의결까지 평균 490.6일, 과태료·과징금 부과까지 평균 520.2일이 소요

[그림 1] 개인정보 사고조사 구간별 평균 소요 일수 (분석기간: 2020년 11월 ~ 2026년 4월)

(단위: 일)



주: 1. 개인정보보호위원회 누리집에 공개된 2020년 11월~2026년 4월 의결 완료 사건 중 각 구간의 일자가 확인되는 사건을 분석대상으로 하며, 구간별로 확인 가능 건수의 차이로 인해 분석대상 건수가 상이할 수 있음
2. 기획조사 및 사전 실태점검 사건은 제외하고, 신고·제보 등에 기반한 사고조사만을 대상으로 산정
3. 각 구간은 신고일·조사 착수일·조사 완료일(또는 사전통지)·의결(처분)일·과태료 및 과징금 부과일을 기준으로 산정

자료: 개인정보보호위원회 공개 의결서 및 보도자료를 바탕으로 국회예산정책처 자체 분석

- 그러나 개인정보보호위원회는 신고·착수·조사 완료·의결 등 단계별 처리통계를 활용하여 지연 구간과 장기계류 원인을 분석하고, 사건별 처리상황을 체계적으로 관리하는 데 미흡한 측면이 있는 것으로 파악됨

▪ **개인정보 유출신고 증가에 대응하여 조사인력 증원과 디지털 포렌식 랩 구축 등 조사 지원 인프라에 대한 투자가 확대되었으나, 사건 처리 실적 및 처리기간 단축 등 이에 상응하는 실질적인 성과 개선은 제한적인 것으로 보임**

[표 2] 개인정보 유출신고 접수·의결 및 조사인력 1인당 처리 현황(2021~2025년)

(단위: 건, 명, 일)

구분	2021	2022	2023	2024	2025
유출신고 접수 건수	163	167	318	307	447
사고조사 의결 건수	264	162	272	318	360
조사인력 수	30	34	37	37	38
조사인력 1인당 의결 건수	8.8	4.8	7.4	8.6	9.5
신고→의결(처분) 평균 소요일수	357.7	436.8	528.3	589.1	508.2

주: 1. 유출신고 접수 건수는 접수연도 기준이며, 사고조사 의결 건수는 의결(처분)연도 기준으로 비공개 안건을 포함하여 유출신고 외에 인지 조사·타부처 이관 사건 등을 포함함. 단, 기획조사·사전실태점검은 제외함
2. 조사인력 수는 해당 연도 말 현원(실제 사고조사 수행 인력) 기준이며, 조사인력 1인당 의결 건수는 의결 건수를 조사인력 수로 나눈 값임
3. 신고→의결(처분) 평균 소요일수는 공개된 의결서([그림 1] 참조)를 바탕으로 자체 분석한 결과로, 기획조사·사전실태점검을 제외하고 신고일과 의결(처분)일이 모두 확인되는 사건만을 대상으로 산정함

자료: 개인정보보호위원회 제출자료를 바탕으로 국회예산정책처 재작성

3) 개인정보보호위원회 공개 의결서 및 보도자료를 바탕으로 국회예산정책처 자체 분석

- 조사인력 1인당 의결 건수는 2021년 8.8건에서 2025년 9.5건으로 소폭 증가하는 데 그침
- 신고일부터 의결일까지 평균 소요일수는 ('21년) 357.7일 → ('24년) 589.1일 → ('25년) 508.2일로 높은 수준이 지속
- 포렌식 랩은 2025년 12월 구축되었으나, 2026년 9월 현재까지 전담인력 채용이 진행되는 등 운영인력 확보가 지연되어 본격적인 사고조사 활용을 위한 운영기반이 충분히 갖춰지지 못함

▪ **사건의 조사 및 처리에 관한 기간을 규정하고 있음에도, 신고 이후 실제 조사 착수까지 상당한 기간이 소요되는 것으로 확인되어 조사 및 처분의 적시성이 저하될 우려[4)]**

- 신고일·조사착수일이 모두 확인되는 310건 중, 신고 후 14일 이내에 착수한 사건은 102건(32.9%)에 불과한 반면, 180일 이상 경과 후 착수한 사건은 58건(18.7%)으로 나타남

▪ **2021~2025년 유출신고는 총 1,402건인 반면, 같은 기간 의결이 확인되는 유출신고 사건은 538건으로, 미의결·진행 중 사건이 누적되고 있을 가능성을 시사**

- 본고의 처리기간 분석은 공개된 의결 완료 사건만을 대상으로 하므로, 미의결·진행 중인 장기계류 사건을 포함할 경우 실제 소요기간은 분석값보다 길어질 가능성

재정사업 문제점②

: 공공·민간 부문별 사고 특성을 고려한 조사·대응 체계 미흡

▪ **공공부문은 업무과실, 민간부문은 해킹이 주요 유출원인으로 나타나나, 조사·예방 사업의 운영은 이러한 부문별 위험요인의 차이를 충분히 반영하지 못하고 있음**

- 2025년 공공부문은 업무과실이 53.1%(68건)로 가장 높은 반면, 민간부문은 해킹이 72.7%(232건)를 차지함
  - 세부 유형을 보면 업무과실은 수신인 오기입, 열람권한 설정 오류, 공개된 장소에의 개인정보 게시 등 처리절차 준수와 관련된 유형이며, 해킹은 악성코드(랜섬웨어·웹셸 등) 감염, SQL 인젝션 등 웹 취약점 악용 등 기술적 침해경로를 통한 유형임

[표 3] 공공·민간 부문별 개인정보 유출사고 원인별 신고 현황

(단위: 건, %)

구분	공공 부문			민간 부문		
	유출원인	건수	비중	유출원인	건수	비중
1	업무과실	68	53.1	해킹	232	72.7
2	해킹	44	34.4	업무과실	42	13.2
3	시스템 오류	6	4.7	시스템 오류	18	5.6
4	원인 미상	5	3.9	원인 미상	16	5
5	고의 유출	5	3.9	고의 유출	11	3.4

자료: 개인정보보호위원회·한국인터넷진흥원, 「2025년 개인정보 유출 신고 동향 및 조사·처분 사례」

- 이에 따라 공공부문은 내부통제·접근권한·처리절차 점검이, 민간부문은 침해경로·보안취약점 분석이 상대적으로 중요한 것으로 보임

4) 「개인정보 보호위원회의 조사 및 처분에 관한 규정」
제5조(사전검토 등)
② 조사관은 제4조 등에 따른 신고의 경우에는 사건을 지정받은 날부터 14일 이내에 해당 국장에게 조사착수 여부의 보고를 마쳐야 한다. 다 만, 사실관계의 확인 등 부득이한 사유가 있는 경우에는 필요한 범위에서 기간을 연장할 수 있다.
제7조(조사기간)
① 사건의 조사개시일은 제6조에 따른 조사착수 보고일로 한다.
② 조사관은 조사개시일로부터 6개월(조사내용이 복잡하고 전문성이 요구되는 사건의 경우 12개월) 이내에 제15조 제1항에 따른 조사결과 보고를 마쳐야 한다. 다만, 부득이한 사유로 조사기간의 연장이 필요한 경우에는 연장기간을 정하여 해당 국장에게 보고하여야 한다.

재정사업 문제점③

: 사고조사 결과의 예방환류 및 현장 개선 연계 미흡

▪ **동일 기관에서 유출사고가 반복되는 가운데, 사고조사·처분에서 확인된 취약요인이 예방제도로 환류되는 체계가 미흡하여 재발방지 효과가 제한적**

- 분석 결과, 2회 이상 유출사고가 확인된 기관은 47개, 관련 사건은 128건으로 나타나, 반복사고 발생 기관의 보호체계 개선 여부를 점검할 필요

  • 반복사고는 종전 사건과 동일한 취약점뿐만 아니라 다른 법적 의무 위반이나 관리적·기술적 취약요인에서도 발생할 수 있어, 개별 위반사항에 대한 시정조치만으로는 기관 전반의 보호체계 개선을 담보하기 어려울 수 있음

  • 사고 조사·처분과 공공부문 집중관리시스템 점검[5], 개인정보 보호수준 평가[6], (공공부문) ISMS-P 인증 및 사후관리[7]가 각각 개별적으로 운영되고 있어, 조사에서 확인된 취약요인과 개선 결과를 예방제도의 점검기준·평가지표에 연계·반영하는 체계가 미흡

개선과제

▪ **사고조사 처리의 신속성 제고를 위해 사건관리 절차와 조사 지원 인프라 등의 운영체계 정비 필요**

- 신고 이후 조사 착수 지연이 확인되는 만큼, 유출 규모·피해 확산 가능성 및 사건 난이도에 따라 조사 우선순위를 설정하고, 신고부터 의결까지 단계별 소요기간과 지연 사유를 관리할 필요

- 의결(처분)이 완료되지 않은 사건이 다수 존재하는 점을 감안하여 연도별 신고처리·미처리 사건 현황을 구분 관리하고, 장기 계류 사건에 대해서는 지연 사유 확인과 향후 처리계획 수립 등 별도의 관리절차를 마련할 필요

- 포렌식 랩의 전담인력 등 운영기반을 확보하고, 사건 지원 실적과 분석 소요기간 등을 점검하여 실제 사고조사 역량 강화로 이어지도록 관리할 필요

▪ **공공·민간 부문별 사고 원인을 고려한 조사·예방사업 설계 필요**

- 공공부문은 업무과실 비중이 상대적으로 높은 점을 고려하여 내부통제·접근권한·처리절차 점검과 개선조치 이행관리를 강화하고, 기관평가 연계 등 책임성 확보수단을 병행할 필요

- 민간부문은 해킹 비중이 상대적으로 높은 점을 고려하여 침해경로 분석·디지털 포렌식 등 기술적 조사역량을 강화하고, 조사과정에서 확인된 주요 보안취약점이 예방·점검사업에 환류될 수 있도록 할 필요

▪ **사고조사·처분 결과가 사전예방체계로 연결되도록 환류체계 구축 필요**

- 대규모 유출사고나 반복사고가 발생한 기관에 대해서는 개별 사건의 위반사항에 대한 시정조치에 그치지 않고, 사고의 반복 원인과 관리적·기술적 취약요인을 종합적으로 점검하여 기관 차원의 보호체계 개선으로 이어질 수 있도록 할 필요

- 사고조사에서 반복적으로 확인된 취약요인을 유형별로 축적·관리하여, 공공기관 보호수준 평가, ISMS-P 인증 관리, 집중관리시스템 점검 등 예방제도의 점검기준에 반영되도록 할 필요

☞ 보다 구체적인 내용은 「2025회계연도 결산 총괄분석 III」 "개인정보 유출사고 대응체계 및 개인정보 보호정책 운영 개선과제" 참조

5) 「개인정보보호법 시행령」 제30조의2, 「개인정보의 안전성 확보조치기준」 제14조제1항에 따라 대규모·민감 개인정보를 처리하는 공공시스템을 지정하여 안전조치 이행을 중점 관리하는 제도

6) 「개인정보 보호법」 제11조의2에 따라 공공기관의 개인정보 보호 정책·업무 수행 및 법상 의무 준수 여부를 매년 평가

7) 「개인정보 보호법」 제32조의2 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조에 따라 정보보호·개인정보보호 관리체계가 인증기준에 적합함을 인증하는 제도

발간등록번호 | 31-9700484-001731-14 ISSN | 2672-0280
발행처 | 국회예산정책처 발행인 | 국회예산정책처장 지동하 담당 | 예산분석실 산업예산분석과 문의 | 02-6788-4630