"기독교대학의 글로벌 리더"

31065 충남 천안시 동남구 백석대학로 1 / 전화 041-550-2339 / 팩스 041-550-2854
개인정보보호책임자 [illegible] 개인정보보호담당자 [illegible]

2026. 6. 1(월)

# 업 무 연 락

수 신 : 전 부서장
참 조 :
제 목 : 2025년 개인정보 유출신고 및 조사·처분 사례 분석결과 발표 배포 안내

1. 관련 :「개인정보위, 2025년 개인정보 유출 신고 및 조사·처분 사례 분석결과 발표」, 보도자료(2026.05.15.)

2. 위와 관련하여 개인정보보호위원회와 한국인터넷진흥원은 2025년 동안 접수된 개인정보 유출 신고 및 처분 사례를 분석해 원인별 예방책 및 주요 사례를 담은 「2025년 개인정보 유출 신고 동향 및 조사 · 처분 사례」를 발간하였습니다.

3. 이에 주요 내용을 다음과 같이 알려 드리오니 관련 업무에 참고하시기 바랍니다.

붙임 2025년 개인정보 유출 신고 동향 및 조사 처분 사례 1부. 끝.

**[관련 붙임자료 안내] <2026.06.01부터 확인 가능>**
1. 백석대학교 : 교내홈페이지>백석광장>IT지침/규칙>개인정보보호게시판>지침 및 서식
2. 백석문화대학교 : 교내홈페이지>개인정보처리방침>개인정보보호게시판>지침 및 서식

개인정보보호책임자 서명생략

2026. 5.

# 2 * 25

# 개인정보 유출 신고 동향 및 조사·처분 사례

개인정보보호위원회 KISA 한국인터넷진흥원

2026. 5.

# 2 * 2 5

# 개인정보 유출 신고 동향 및 조사·처분 사례

개인정보보호위원회 KISA 한국인터넷진흥원

# 2 * 2 5

# 개인정보 유출 신고 동향 및 조사·처분 사례

CONTENTS



* 본 보고서는 2025년 기준으로 작성되었으며, 개인정보 유출 신고 현황은 오신고·중복 신고 등이 포함될 수 있음
* 각 통계의 비율은 소수점 반올림을 적용하였으며, 총합계 100%를 맞추기 위해 가장 비중이 높은 항목에서 소수점 단수 조정이 반영되었음
* 개인정보 유출 사고 원인 및 예방 방법은 개인정보처리자의 시스템 운영 환경 등에 따라 안전조치 등이 다르게 적용될 수 있음
* 개인정보 유출 사고 원인은 유출 신고 당시 파악된 내용으로서 실제 조사 결과와 다를 수 있음

PART

# * 1

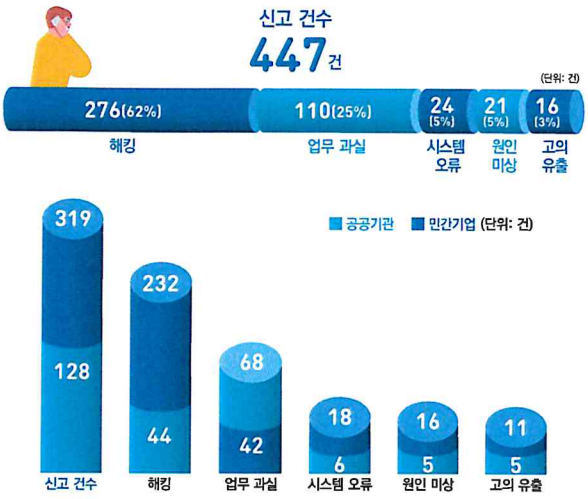
## 개인정보 유출 신고 동향



# 01 개인정보 유출 신고 현황

# 01
# 개인정보
# 유출 신고 현황

## 2025년 개인정보 유출 신고는 총 447건



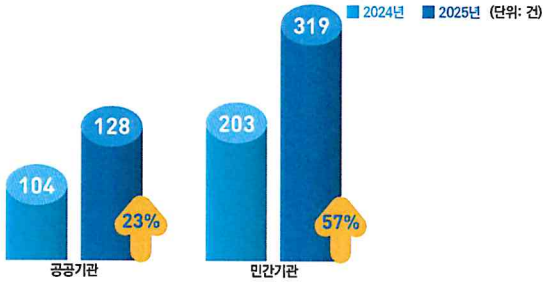

* 전년도 대비 46.6% 증가(2024년 307건 → 2025년 447건)



### 신고 기관

**공공기관[1]이 28%**(128건), **민간기업이 72%**(319건) 차지

• 전년도 대비 공공기관은 23% 증가(104건 → 128건) 하였고, 민간기업은 57% 증가(203건 → 319건)




### 사고 원인

**해킹[2] 62%(276건), 업무 과실 25%**(110건), **시스템 오류 5%**(24건), **원인 미상 5%**(21건), **고의 유출 3%**(16건) 순으로 확인

• 전년도 대비 **해킹으로 인한 신고는 61% 증가**(171건 → 276건), **업무 과실은 21% 증가**(91건 → 110건), **시스템 오류는 4% 증가**(23건 → 24건)

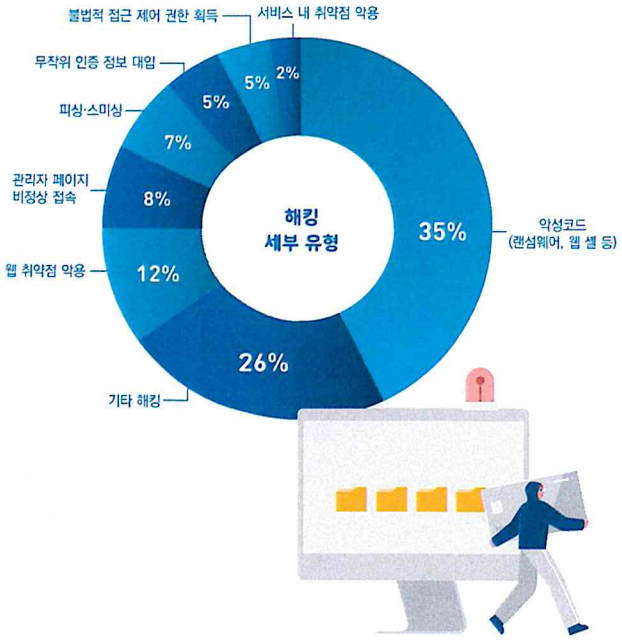

1) 중앙행정기관(소속기관), 지방자치단체(직속기관), 공공기관, 지방공기업, 각급 학교, 특수법인 등
2) 해킹 : 개인정보처리시스템 등에 대한 외부로부터의 불법적인 접근에 의해 개인정보가 유출등이 된 경우
업무 과실 : 개인정보취급자가 개인정보 처리 업무 수행 과정에서의 실수, 과실 등
시스템 오류 : 개인정보처리시스템 개발·운영·고도화 과정에서 프로그램 영향이 누락, 오류 설정 등
고의 유출 : 개인정보취급자가 개인정보를 불법 취득·제공 등
원인 미상 : 개인정보 유출 사실은 확인되었으나, 신고 시점에 그 원인이 확인되지 않은 경우 등



• 해킹 같은 경우 **악성코드(랜섬웨어, 웹 셸 등) 35%**(96건), **SQL 인젝션·파라미터 변조 등 웹 취약점 악용 12%**(32건), **관리자 페이지 비정상 접속 8%**(23건) 순으로 해킹 유형 확인

• 이외 피싱·스미싱 7%(20건), 무작위 인증 정보 대입(브루트 포스, 크리덴셜 스터핑) 5%(13건), 불법적 접근 제어 권한 획득(원격 제어, 세션 탈취, 인증 파일 탈취 등) 5%(13건), 서비스 내 취약점 악용 2%(6건), 신고 시점에서 원인을 알 수 없었던 기타 해킹* 26%(73건) 확인

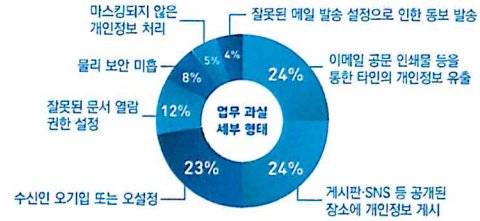
* KISA·언론, 정보주체 제보 등 제3자를 통한 개인정보 유출 인지 47건, 원인미상 15건, 알 수 없는 경위로 관리자 계정 유출 11건



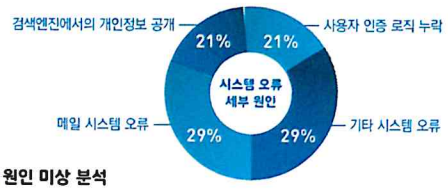



• 업무 과실은 **이메일·공문·인쇄물 등을 통한 타인의 개인정보 유출 24%** (26건), **게시판·SNS 등 공개된 장소에 개인정보 게시 24%**(26건), 수신인 오기입 또는 오설정으로 인한 개인정보 유출 23%(25건) 순으로 과실 형태 확인

• 그 밖에 잘못된 문서 열람 권한 설정 12%(13건), 물리 보안 미흡으로 인한 개인정보 유출 8%(9건), 마스킹되지 않은 개인정보 처리 5%(6건), 잘못된 메일 발송 설정으로 인한 동보 발송 4%(5건) 과실 형태 확인




• 시스템 오류의 세부 원인은 **메일 시스템 오류로 인한 유출 29%**(7건), 비공개 페이지 접근 통제 오류로 인한 **검색엔진에서의 개인정보 공개 21%**(5건), API 권한 검증 등 **사용자 인증 로직 누락 21%**(5건), 이 외 기타 시스템 오류 29%(7건) 으로 확인




### 원인 미상 분석

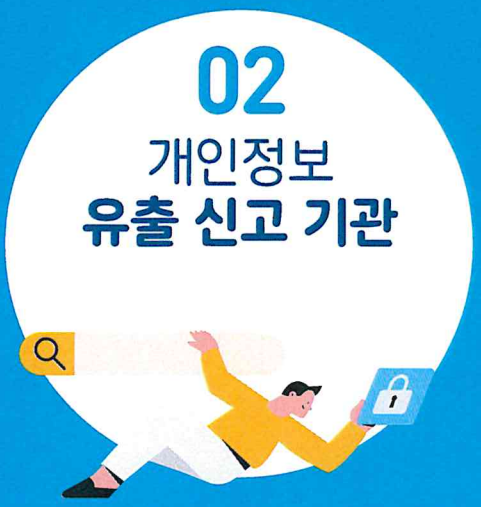
전년도 개인정보 유출 신고 당시 원인 미상 신고(17건)와 해킹으로 접수된 개인정보 유출 원인 미상 신고[3](87건) **조사를 진행하여 53%의 신고에 대한 해킹 유형 식별**(원인 미상 104건 → 원인 확인 55건)

• 관리자 페이지 비정상 접속(12건), SQL 인젝션·파라미터 변조 등 웹 서비스 관련 취약점을 악용한 공격(11건), 랜섬웨어 등 악성코드 및 웹 셸(9건), 무작위 인증 정보 대입(4건), 원격 제어(2건), 기타 해킹 기법(17건)

• 원인 미상의 신고 건은 대부분 **사고 관련 로그가 부재하여 정확한 유출 경위 파악이 어려워 여러 가설 기반으로 추정하여 조사 수행**

3) 불법적인 접근을 통한 개인정보 유출 사실을 인지하였으나, 신고 시점에 어떤 방법을 통해 접근하였는지 명확히 식별되지 않아 우선 신고한 경우

# 02
# 개인정보
# 유출 신고 기관



# 02
# 개인정보
# 유출 신고 기관

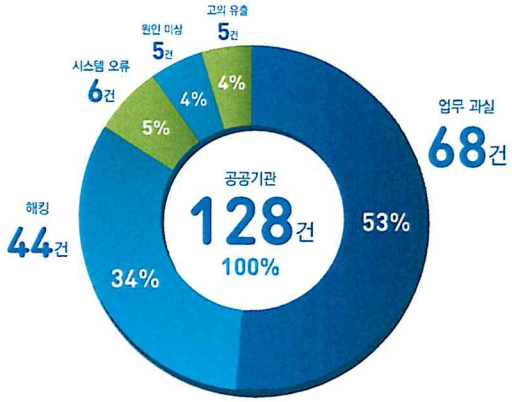
## 1.공공기관

### ○ 신고 현황

2025년 개인정보 유출 신고(447건) 중, **공공기관의 개인정보 유출 신고는 28%**(128건)을 차지

유형 **중앙행정기관·지방자치단체 등(57%), 대학교·교육청 등(30%)**, 공공기관[4]· 특수법인 등(13%)

원인 **업무 과실(53%), 해킹(34%)**, 시스템 오류(5%), 원인 미상(4%), 고의 유출(4%)



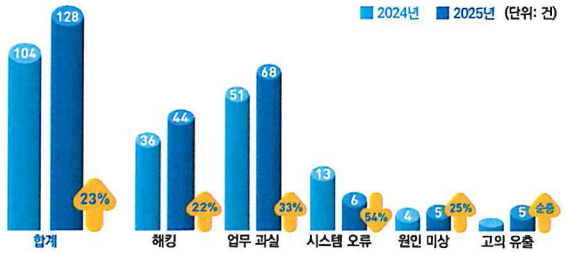

4) 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관



### ○ 신고 동향

공공기관은 전년도(104건) 대비 **23%**(128건) **증가**

- **해킹으로 인한 신고는 22% 증가**(36건 → 44건), **업무 과실은 33% 증가**(51건 → 68건), **시스템 오류는 54% 감소**(13건 → 6건)




### ○ 시사점

국민의 주요 개인정보를 대량으로 처리하는 공공기관에서 업무 과실로 인한 개인정보 유출 사고가 증가하고 있어, 공공기관장과 개인정보 보호 책임자의 개인정보 보호 수준 제고 필요

- 최근 개인정보보호위원회는 개인정보를 대량으로 처리하는 공공기관에서 유출 사고가 지속됨에 따라 공공기관이 개인정보 보호법규를 한 차례라도 위반하여 처분받은 경우,
- 모든 공공기관에 대해 위원회 **홈페이지에 처분결과*를 게시할 수 있도록 규정하는 공공기관 처분결과 전면 공표제를 도입**

  * 개선권고, 시정조치 명령, 과징금 부과, 고발 또는 징계권고, 과태료 부과
- 또한, 주요 공공시스템에 대해서는 공표명령을 도입, 공표명령을 받은 공공기관은 기관 대표 홈페이지(모바일 앱 포함), 사업장이나 신문 등에 공표지침 상 최장기간인 **10일 이상 12일 이하의 기간 동안 처분 결과를 게시하여야 함**
- 개인정보분쟁조정위에서도 공공기관 등을 대상으로 신청한 분쟁 조정 건을 분석한 결과, **정보공개 청구 업무와 홈페이지 자료실 게시물 첨부 시 개인정보가 유출되어 반복적으로 분쟁조정이 신청되는 사례를 발견**하여 재발 방지를 위한 개선의견을 통보
- **업무 과실로 인한 개인정보 유출 대부분은** 개인정보 파일을 게시하거나 타인의 개인정보 제공 등 **계속해서 유사한 형태로 발생**
- 해킹으로 인한 주 신고내용은 관리자 계정 및 관리자 페이지 접근 관리 미흡, 파라미터 변조 취약점, 비밀번호 찾기 기능 취약점 등 **장기간 동안 점검 및 개선하지 않아 개인정보 유출이 반복적으로 발생**



- 또한, 이외 해킹으로 점수된 유출 신고 중 **해외사업자가 제공하는** 학생 및 교직원 정보 관리를 위한 **클라우드 기반 서비스의 해킹 사고 여파로 국내 학교 10곳 이상 개인정보 유출 신고 접수** 되었으며,
- 공공분야에서 **해외사업자**가 제공하는 **응용프로그램** 등 **소프트웨어를 제공하는 클라우드컴퓨팅 서비스(SaaS) 도입 및 이용** 시 국외 이전 관련 사항과 **보안인증(CSAP)** 등 **반드시 보안성 검토 필요**
- 공공기관의 **순환근무제**는 조직 유연성을 높이는 장점이 있으나, **고도의 법률적·기술적 전문성이 요구되는 개인정보보호 업무에서는** 잦은 인사이동으로 인한 **업무 인수인계 미흡, 전문성 결여 등 한계 존재**
- 이를 고려하여 개인정보 보호 전문 지식과 역량을 보유한 전담 인력 및 개인정보보호책임자(CPO) 지정 등에 필요한 인력·예산 편성 필요
- 추가적으로 과도한 법적 책임 및 징계 부담과 타 업무 겸직 등 과도한 업무 부여로 인한 업무 기피 현상을 방지하기 위해
- **개인정보보호 업무에 대한 전문직위 지정 및 타 업무 겸직 금지 등 최소 필수 근무 기간과 형태를 보장**하고, 전문 수당 및 가점을 부여 하여 장기 근무가 가능하도록 개선 필요
- 최근 여러 차례 발생한 해킹으로 인한 대규모 개인정보 유출 사고를 기점으로 **관계부처 합동 범부처 정보보호 종합대책**을 발표하고, 개인정보보호위원회에서도 **「2026년 개인정보 조사업무 추진 방향」**을 수립하는 등 대대적으로 공공분야 정보보안·개인정보 보호 관리체계를 재편하고 있음
- 기반 시설, 중앙·지방 행정기관 등 **대상 대대적인 보안 취약점 점검을 즉시 추진할** 예정이며, **주요 공공시스템에 대한 모의해킹** 등 취약점 **점검 의무** 강화 및 **3대 유출 취약점**(인적 과실·웹취약점·관리 사각지대) **보완대책** 수립에 따른 사전 점검 등 대응 필요
- 정보보안·개인정보보호 예산 및 인력을 정보화 대비 일정 수준 확보 등 **장기적으로 개인정보 유출 사고를 방지하기 위한 노력 및 계획 수립 필요**

## 2. 민간기업

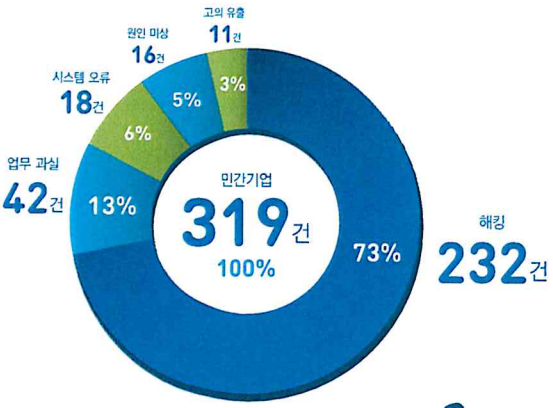
### 신고 현황

2025년 개인정보 유출 신고(447건) 중, **민간기업의 개인정보 유출 신고는 72%**(319건)을 차지

유형 **중소기업 47%**(149건), 대기업 18%(58건), 중견기업 17%(54건), 해외사업자 8%(24건), 이 외 기타 10%(34건) 순으로 확인

* 업종 : 정보통신업 22%(70건), 도매 및 소매업 19%(61건), 금융 및 보험업 15%(48건), 제조업 13%(41건), 협회 및 단체, 수리 및 기타 개인 서비스업 8%(24건), 운수 및 창고업 6%(18건), 보건업 및 사회복지 서비스업 5%(16건), 기타 12%(41건)

원인 **해킹(73%), 업무 과실(13%)**, 시스템 오류(6%), 원인 미상(5%) 등

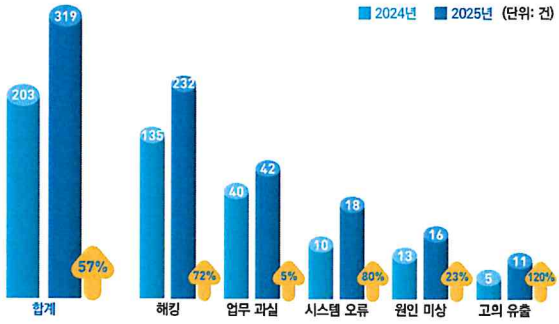





### 신고 동향

민간기업은 전년도(203건) 대비 **57%**(319건) **증가**

- **해킹으로 인한 신고는 72%**(135건 → 232건), **업무 과실은 5%**(40건 → 42건), **시스템 오류는 80%**(10건 → 18건), 신고 시점에 유출 원인이 확인되지 않은 **원인 미상은 23% 증가**(13건 → 16건), **고의 유출은 120% 증가**(5건 → 11건)






### 시사점

**전년도 대비 대규모 개인정보처리자 유출 신고가 239% 증가**(33건 → 112건) 하였으며, 정보주체의 **피해 규모가 1천만명이 넘어가는 유출 신고 건수가 여러 차례 발생**함에 따라 기업의 책임성을 강화하기 위한 **관련 법률 개정 및 행정제재 대응 필요**

- 고의 또는 **중대한** 과실로 3년 이내 반복적 위반, 고의 또는 중대한 과실로 1천만명 이상 대규모 피해 발생, 시정조치 명령에 따르지 아니하여 유출이 발생한 행위에 대해서는 **전체 매출액의 10% 범위 내에서 과징금을 부과할 수 있도록** 징벌적 형태의 과징금 제도 도입 예정
- 해킹으로 인한 개인정보 유출 신고 시 **개인정보가 유출된 정황을 인지하였음에도** 유출 사실의 인지 시점과 통지 내용의 구체성을 위한 사실관계 확인이 늦어짐에 따라
- 법령에서 정한 72시간 이내에 통지하지 않고, **홈페이지에 고객의 일부 정보가 유출된 것으로 추정된다는 내용의 전체 공지로 사회적 혼란 야기 등 문제 발생**
- 개인정보가 유출된 정보주체의 연락처를 알았음에도 유출통지를 하는 등의 후속조치를 취하지 않거나 유출항목 중 개인 식별성이 높은 항목 등을 누락하여 통지하는 등 유출 통지를 적절히 수행하지 않아 **기존 통지 대상이던 개인정보의 분실·도난·유출 뿐만 아니라 위조·변조·훼손까지 통지 법위 확대 예정**
- 대통령령으로 정하는 **유출 가능성이 있는 경우에도** 유출의 가능성이 있는 **모든 정보주체 대상 법정 통지사항을 개별적으로 통지할 것을 의무화**하여 정보주체의 권리 보호 강화 예정
- 예산·인력·설비·장치 등의 투자 및 운영 시 **과징금 감경 요소도 있어 서비스 특성에 맞는 투자전략 수립 및 적용 방안 검토 필요**
- 민간기업에서 해킹으로 접수된 유출 신고 중 **수탁사 관련 해킹 사고가 62건(11개의 수탁사)으로 수탁사 1곳당 평균 약 5.5곳의 위탁사가 영향을 받음**
- 수탁사의 주요 서비스는 NAS[5] 등 자원관리 48%(30건), CRM[6] 등 고객 정보 관리 34%(21건), 기업 내 직원 정보 관리 10%(6건), 홈페이지 유지보수 5%(3건), 구매대행 3%(2건) 으로 확인
- **수탁사가 제공하는 서비스는 작업 요청 또는 장애 발생 시 원격 등으로 비대면 형태의 기술지원을 하는 경우가 대부분이며, 비대면 업무 환경의 일상화는 역설적으로 보안의 가장 약한 고리인 인적 요소를 타겟팅한 피싱(Phishing)공격의 최적지가 되고 있음**

5) Network Access Server(NAS) : 네트워크에 접속하는 데이터 저장 장치. 사무실 따위에서 얼터미디어 데이터 등 광대한 자료나 파일을 네트워크에 부착해 사용하기 편하게 저장하는 장치 (출처 : 국립국어원)

6) Customer Relationship Management(CRM) : 기업이 고객과 관련된 각종 자료를 분석하고 통합하여 고객 중심의 자원을 극대화함으로써, 이를 바탕으로 고객의 특성에 맞게 판촉 활동을 계획하고 지원하며 평가 (출처 : 국립국어원)



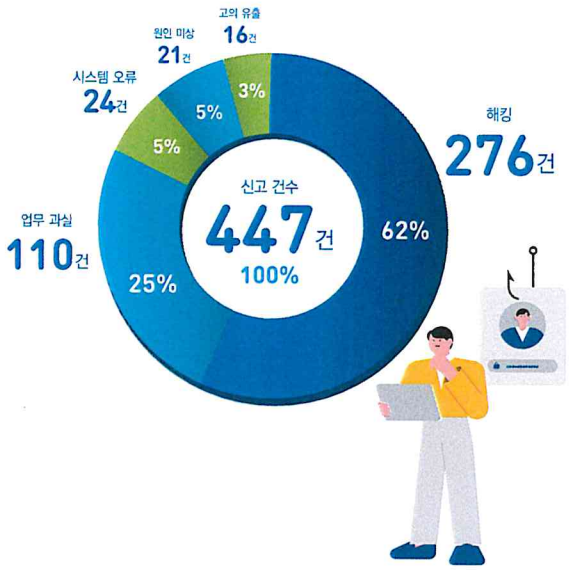
- 대면 확인이 불가능한 점을 악용한 사칭 공격은 기존 보안시스템을 무력화하며, 이는 결국 대규모 개인정보 유출 및 기업 신뢰도 하락이라는 치명적인 결과로 직결될 수 있어 대응 필요
- 내부 시스템 접근 시 두 가지 이상의 인증 요소를 이용하여 본인 여부를 인증하는 다중 인증 방식(MFA)을 도입하거나 **원격 접속 시 개인 기기가 아닌 인가된 업무용 단말기 또는 전용 가상 데스크톱(VDI) 접속 허용 등 업무 데이터 접근 통제 환경 마련 필요**
- **비밀번호나 개인정보는 어떠한 경우에도 메신저나 유선상으로 요구하지 않는다는 원칙을 명문화**하고, 이메일이나 메신저로 급박한 요청을 받을 경우 사내 메신저가 아닌 직통 내선 번호 등 **전용 연락 수단으로 직접 전화하여 본인 확인 절차를 거치도록 업무 프로세스를 개선 필요**
- 개인정보보호위원회에서도 개인정보 유출 사고 시 **개인정보 안전 조치 의무에 대한 책임이 명확하게 수탁자에게 있는 경우** 수탁자와 함께 수탁자에 대한 관리·감독을 소홀히 한 위탁자도 안전조치 의무 위반과 **수탁자 관리·감독 소홀로 모두 과징금 처분하였으며,**
- 개인정보 처리 업무 위탁 시 위탁하는 업무 내용이나 목적, **보호조치** 등을 명확히 하고, **수탁자 대상 개인정보 처리 현황 점검 및 교육 등 관리·감독을 충실히 이행 필요**
- 민간분야에서 침해사고 신고[7]로 접수된 랜섬웨어(Ransomware) 공격이 전년도 대비 40.5%로 높게 증가(195건 → 274건) 함에 따라 **랜섬웨어로 인한 개인정보 유출 신고 건수도 약 517% 증가**(12건 → 74건)
- 「개인정보 보호법」제29조는 유출 외 분실·도난·위조·변조·훼손 등 방지를 위한 안전관리 의무를 규정하고 있으며, **제64조의2는 유출 외 분실·도난·위조·변조·훼손 등에도 과징금 부과가 가능하며,**
- 이에 개인정보보호위원회는 랜섬웨어로 인해 개인정보가 암호화되어 처리가 불가능한 경우 유출 여부가 불분명하다 하더라도, **정상적인 서비스 제공 여부 등을 기준으로 개인정보 훼손을 판단**하여 처분
- **별도의 백업 정보가 없어** 시스템을 재구축하고 회원 **개인정보를 새로 수집하여 개인정보 효용 침해가 발생한 경우 과징금을 부과 하고**, 백업해 둔 정보로 신속히 복구하여 **개인정보 효용에 침해가 발생하지 않은 경우 과태료 부과**
- 이처럼 랜섬웨어 감염 시 대응에 따라 처분 형태가 달라지기에 **개인정보 데이터베이스 등 주요 파일은 주기적으로 별도 백업·보관 필요**

7) 세부내용은 「'25년 사이버 위협 하반기 동향 및 '26년 전망」(과학기술정보통신부·한국인터넷진흥원, '26.2월) 참고

# 03
# 개인정보 유출 사고 원인 및 예방방법

# 03
# 개인정보 유출 사고 원인 및 예방 방법

● 개인정보 유출 사고 유형은 해킹(62%), 업무 과실(25%) 등으로 확인






## 1.해킹으로 인한 개인정보 유출 예방·대응 방법

주요 개인정보 유출 사례 기반 예방 방법

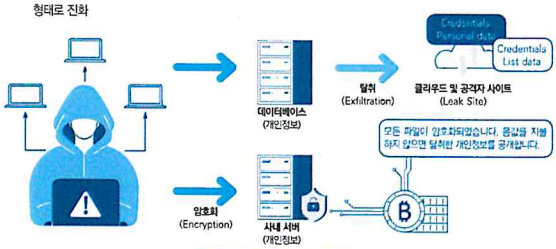
| 구분 | 사고 사례 | 예방 방법 |
|---|---|---|
| 개인정보 웹페이지 자동화 공격 탐지 | 유출된 계정 정보를 무작위로 대입하는 크리덴셜 스터핑 공격으로 개인정보 도용 | • 개인정보 조회 페이지 및 로그인 페이지에 대한 공격자의 과도한 접근 행위 분석 및 모니터링 강화<br>① 로그인 실패 비율의 급증<br>② IP 주소 또는 단말 정보의 지역간 급격한 이동<br>③ 해외 IP에서 유입되는 로그인 요청 급증<br>• 다중 인증(MFA, 패스키 등) 체계 도입 및 적용 |
| 서버 로그 파일 개인정보 주기적 점검 | 서버 로그 파일에 중요 개인정보(결제 내역, 계정 정보 등)가 평문으로 저장 | • 웹 애플리케이션 서버(WAS) 등 DB가 아닌 일반 시스템에 민감한 개인정보가 로그 형태로 저장되는지 주기적 검토<br>• 불필요한 개인정보 로그 저장을 원천 제한하고, 불가피할경우 마스킹 처리 및 파일 암호화 보관 조치, 특히, 암호키는 별도의 안전한 저장소에 관리 |
| 개인정보 조회 API 취약점 악용 방지 | 취약한 오픈 API(BOLA 취약점 등)를 악용하거나 식별 파라미터를 조작해 타인의 개인정보를 대량 스크래핑 | • API 호출 시 요청자의 권한과 접근하려는 데이터의 실소유주를 교차 검증하는 인가(Authorization) 통제 로직 필수 구현<br>• 식별 파라미터는 예측 불가능한 난수(UUID 등)를 사용하고, 비정상적 대량 API 호출 시 임계치(Rate Limit)를 설정하여 자동 차단 |
| 개인정보처리시스템 최신 보안 패치 | 라녹스 권한 상승 취약(DirtyCow 등) 악용으로 최고 권한(Root)을 획득해 데이터베이스에 침투 | • DirtyCow 등 일반 권한을 관리자 권한으로 상승시킬 수 있는 OS 보안 취약점의 상시 모니터링 및 즉시 패치 |
| | 오라클 웹로직(WebLogic), 오픈소스 게시판(CMS)의 취약점을 방치하여 해커가 웹셸을 업로드하여 개인정보 유출 | • WAS 및 웹 프레임워크의 알려진 웹 취약점을 상시 점검하여 최신 보안 패치 적용<br>• 특히 웹로직, 아파치 스트러츠, 게시판 솔루션 등에서 자주 발생하는 '파일 업로드' 및 '원격 코드 실행(RCE)' 취약점 선제적 조치 |
| 데이터베이스 보안 (접근통제 강화) | 데이터베이스에 인증 없이 접근 가능 | • 강력한 비밀번호 검증 로직 및 추가 인증(IP 접근제어 솔루션 등)을 도입하여 데이터베이스 관리자 인증 설정 강화<br>• DBMS 접속 시 비인가자가 인증 수단 없이 개인정보 테이블을 임의로 조회(Dump)할 수 없도록 통제 |
| | 편의 목적으로 서버 내 데이터베이스 계정 정보를 저장된 상태로 관리 | • DB 서버 등 시스템 계정 정보가 서버 내에 저장·노출되지 않도록 관리<br>• DB 접속 계정(ID/Password)은 일반 직원 및 서비스 사용자 계정과 철저히 분리하여 최소 권한 부여 |
| 암호키 생명주기 관리 및 분리 보관 | 해킹된 서버에 암호화된 데이터와 이를 복호화하는 암호키가 동일한 공간에 방치되어 함께 유출·복호화 | • 개인정보 암호화에 사용하는 암호화 키(대칭키, 비대칭키등)의 안전한 생명주기(생성·이용·파기) 절차 수립<br>• 암호키는 서비스 환경과 물리적·논리적으로 분리된 별도의 안전한 공간(KMS, HSM 등)에 저장하여 엄격히 관리 |
| 종단간 암호화 적용 | 패킷 스니핑 등 중간자 공격(MITM)으로 전송 중인 개인정보(로그인, 세션 정보 등)를 가로채어 탈취 | • 통신 중간에 개입하여 암호화 설정을 해제할 수 없도록 종단간(End-to-End) 및 전송 구간(TLS 1.3 이상 등) 암호화 |
| 퇴직자 접근 권한 즉시 회수 | 회수되지 않은 인증키·접근 권한을 악용하여 고객 정보에 무단 접근 | • 퇴직·전환배치 즉시 모든 시스템 계정 비활성화 및 API키·인증 토큰·SSL 인증서 등 접근 수단 일괄 폐기 절차<br>• 접근 권한 부여 현황을 주기적으로 재검토하고, 특히 개인정보처리 시스템에 대해서는 퇴직 당일 회수 완료 여부를 CPO 등에게 보고하는 체계 구축<br>• 내부자 이상행위 탐지(UEBA) 솔루션을 도입하여 비정상적 시간대 접속, 대량 조회, 비인가 IP 접근 등을 실시간 탐지·차단<br>• 인사시스템과 개인정보처리시스템을 연동하여 인사 변동 시 시스템에 즉시 반영하는 절차 마련 |



해킹 유형별 예방·대응 방법

### ◦ 랜섬웨어(Ransomware)

현상 최근 랜섬웨어는 단순 암호화를 넘어 개인정보를 유출한 후 다크웹 공개를 빌미로 금전을 요구하는 이중 협박 형태로 진화




개인정보 유출 후 암호화 이중 협박

| | 공격 경로 | 유출 사례 |
|---|---|---|
| 사례 1 | 중앙관리 시스템 취약점 악용 | 공격자가 기업 내 Active Directory(AD) 서버 권한을 장악하여 사내망 통제권을 획득. 랜섬웨어(예: LockBit 등)를 전사적으로 배포하여 시스템을 암호화하기 직전, 확보한 관리자 권한을 통해 내부 DB 및 파일 서버의 개인정보를 클라우드 스토리지 등으로 유출 |
| 사례 2 | 피싱 메일을 통한 단말기 장악 | 이력서, 공문 등으로 위장한 악성 메일 첨부파일 실행 시, 1차적으로 정보 탈취형 악성코드(Infostealer)가 설치. 이를 통해 로컬 PC에 보관된 개인정보를 C&C 서버로 탈취한 후, 2차 페이로드로 랜섬 웨어를 다운로드하여 해당 PC의 데이터를 암호화 |
| 사례 3 | 드라이브 바이 다운로드 공격 | 취약한 브라우저를 통해 악성 웹사이트 방문 시 익스플로잇 으로 자동 감염. PC에 저장된 시스템 접속 크리덴셜(ID/PW)을 통해 내부망에 침투하여 고객 데이터를 빼낸 뒤 다크웹 공개를 빌미로 랜섬웨어를 감염 |
| 사례 4 | 접근통제 설정 및 보안 패치 누락 점점 악용 | 외부망과 연결된 시스템(VPN, NAS, 웹 서버 등)의 보안 패치 누락 및 기본 관리자 패스워드 방치. 이를 통해 공격자가 내부망에 접근한 뒤, 장기간에 걸쳐 고객 개인정보 데이터를 무단 다운로드 한 뒤 최종적으로 데이터를 암호화하여 복구 비용을 요구 |

**예방·대응**[8] **랜섬웨어를 통한 개인정보 데이터 유출 예방 방법**

**☑ 최신 보안 업데이트 유지**

- 운영체제, 주요 프로그램 및 외부 접점 장비(VPN, 방화벽 등)의 알려진 취약점을 악용한 랜섬웨어 초기 침투를 예방하기 위해 신속하고 정기적인 보안 업데이트(Patch) 적용

**☑ 악성 및 피싱 이메일 클릭 금지**

- 정기적인 악성 이메일 모의 해킹 훈련을 실시하여 조직 전체의 보안 인식을 제고하고, 사회공학적 기법(Social Engineering)을 통한 최초 침투 원천 차단

**☑ 안전한 백업 체계 운영**

- 랜섬웨어 감염 시 즉시 복원할 수 있도록, 개인정보 등 중요 데이터는 서비스 운영망과 물리적/논리적으로 단절된 안전한 저장소에 정기적인 2차 백업(3-2-1 백업 룰*) 수행 및 덮어쓰기 방지 적용

  * 중요 데이터 3개 사본 보유, 2개는 서로 다른 저장매체, 1개는 오프사이트에서 백업 및 운영

**☑ 접근통제 및 데이터 암호화**

- 개인정보 취급자 외 중요 데이터 접근 원천 차단 및 최소 권한의 원칙 적용하고 개인정보 파일 및 DB는 안전한 암호 알고리즘을 적용하여 암호화 보관

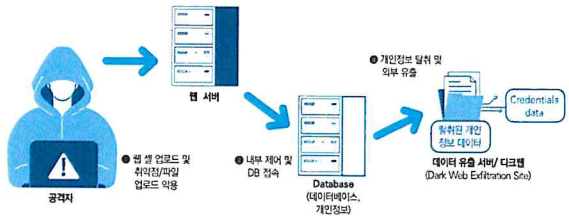
**☑ 랜섬웨어 피해 확산 방지**

- 네트워크를 통해 랜섬웨어가 확산될 가능성이 있으므로 감염 사실 확인 즉시 네트워크 및 전원 차단
- 공유폴더, PC에 연결되어 있는 이동식 저장장치(USB), 외장하드 등에 저장되어 있는 파일에도 접근해서 암호화할 수 있으므로 외부 저장 장치에 대한 연결 해제

8) 세부내용은 「랜섬웨어 악성코드 감염피해 예방을 위한 보안강화 권고」, (한국인터넷진흥원, '25.12월) 참고
「랜섬웨어 대응을 위한 데이터백업 8대 보안 수칙」, (한국인터넷진흥원, '25.7월) 참고
「랜섬웨어 대응 가이드라인」, (과기정통부, '23.8월) 참고



## ○ 웹 셸(Web Shell)




**현상** 웹 서버에 업로드되거나 취약점을 통해 삽입되는 스크립트 형태의 악성 파일로 공격자가 파일 업로드 취약점을 이용하여 악성 파일을 업로드한 뒤 홈페이지와 연동된 내부 데이터베이스에 접근 및 개인정보를 탈취하는 형태로 발생

| | 공격 경로 | 유출 사례 |
|---|---|---|
| 사례 1 | 웹서버 파일 업로드 기능 악용 | 홈페이지의 파일 업로드 기능을 악용하여 악성 파일을 업로드한 후 연동된 데이터베이스에 접근하여 개인정보 탈취 |
| 사례 2 | 웹 애플리케이션 취약점 | 웹 애플리케이션(Weblogic, Apache struts 등) 취약점을 악용 하여 서버에 웹 셸을 설치, 원격으로 서버를 제어하여 개인정보 탈취 |

**예방·대응** **웹 셸을 통한 개인정보 유출 예방 방법**

**☑ 의심 정황 탐지 및 초기 대응**

- 비정상적 트래픽 탐지 등 웹 셸 의심 정황 발견 시 방화벽 등을 통한 네트워크 차단 및 웹 서버 로그·시스템 로그 등 의심 행위 관련 정보 보존

**☑ 안전한 파일 업로드 기능 구현**

- 사용자가 서버에 업로드하고자 하는 파일에 대하여 허용된 특정 확장자(png, gif, pdf 등)만 제한적으로 업로드할 수 있도록 설정 하거나 업로드되는 파일의 이름을 난수화 후 서버에 저장 등



**☑ 웹 애플리케이션 최신 보안 패치**

- 최근 웹 셸 감염은 웹 서버 자체의 업로드 로직 결함뿐만 아니라 Log4j 사태처럼 오픈소스 라이브러리의 취약점을 통해 이루어지는 사례가 많아 웹 애플리케이션, 구동 인프라(웹 서버, WAS) 및 오픈 소스 라이브러리에 존재하는 알려진 취약점(CVE)에 대해 신속하고 정기적인 보안 업데이트(Patch) 적용

**오픈소스 및 주요 프레임워크 웹 셸 취약점 사례**

| 발생연도 | 애플리케이션 | 취약점 명칭 | 내용 |
|---|---|---|---|
| 2022 | Spring Framework | Spring4Shell (CVE-2022-22965) | 데이터 바인딩 과정의 취약점을 악용하여 ClassLoader를 조작, 이를 통해 Tomcat 웹 서버의 특정 경로에 악성 JSP 파일(웹 셸)을 직접 생성하고 실행 권한 획득 |
| 2021 | Apache Log4j 2 | Log4Shell (CVE-2021-44228) | 로그를 기록할 때 JNDI 기능을 통해 외부 악성LDAP 서버의 자바 객체를 로드 및 실행. 직접적인 파일 업로드 기능이 없어도, 이 RCE를 통해 후속 페이로드로 웹 셸을 서버에 다운로드 하고 구동시키는 데 광범위 하게 악용 |
| 2021 | Microsoft Exchange Server | ProxyLogon (CVE-2021-26855 등) | APT 공격 그룹이 Exchange 서버에 'China Chopper' 웹 셸을 일괄 설치, 이를 통해 최고 관리자 권한을 획득하고, 서버에 저장된 개인의 이메일 서신, 연락처 등 민감한 개인 정보를 탈취 |
| 2020 | WordPress | WP File Manager | 플러그인 내부의 특정 라이브러리 (elFinder)에 접근 통제가 누락됨. 인증되지 않은 외부 공격자가 이를 통해 PHP 확장자를 가진 악성 웹 셸 파일을 서버에 직접 업로드하고 실행 하여 사이트 권한 장악 |
| 2017 | Oracle WebLogic | CVE-2017-10271 | 웹로직 서버의 SOAP 보안 구성 요소(WLS Security Component)처리 과정에서 입력값 검증이 제대로 이뤄지지 않아 발생 |

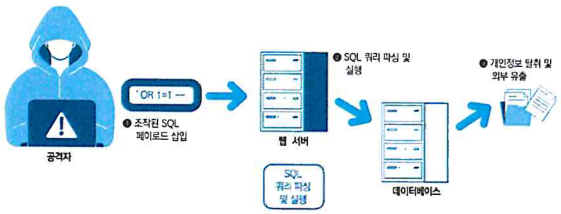


- (취약점 점검 정례화) 정기적인 웹 취약점 스캐닝을 통해 파일 업로드 검증 로직의 결함을 식별·조치하고, 보안 업데이트 지원이 중단된 EoL(End-of-Life) 소프트웨어의 선제적 교체 진행

**☑ 웹 방화벽(WAF, Web Application Firewall) 도입 및 운영**

- 방화벽의 파일 업로드 통제 및 악성 페이로드 탐지 정책을 적용하여, 공격자가 취약점을 통해 웹 셸을 서버에 무단 삽입하거나 실행하는 시도를 네트워크 단에서 선제적으로 탐지 및 차단

## ○ SQL 인젝션(SQL Injection)




**현상** 공격자가 웹 애플리케이션의 입력 폼(로그인, 검색창, 게시판 등)이나 파라미터 검증 취약점을 악용하여 조작된 악의적 SQL 구문을 삽입 하고, 이를 통해 백엔드 데이터베이스(DB)의 정보를 비정상적으로 조회 하여 저장된 개인정보를 무단으로 열람, 변조 및 외부로 탈취

| | 공격 경로 | 유출 사례 |
|---|---|---|
| 사례 1 | 취약한 입력 폼 (검색창 등) 악용 | 구직 웹사이트의 검색 기능 등에 악의적인 SQL 쿼리를 삽입하여 내부 DB 구조를 파악하고, 이용자의 이름, 전화 번호, 이력(경력) 등 민감한 개인정보를 대량 탈취 |
| 사례 2 | 관리자 페이지 인증 우회 | 관리자 웹 서비스의 로그인 또는 URL 파라미터 입력 필드에 SQL 구문을 주입하여 관리자 인증을 우회한 후, DB 접근 권한을 획득하여 고객 개인정보 테이블 전체를 덤프(Dump)하여 유출 |

**예방·대응** SQL 인젝션으로 인한 개인정보 유출 예방 방법

**☑ 안전한 시큐어 코딩(Secure Coding) 적용**

- 로그인 페이지, 게시글 검색 등 데이터베이스와 연동된 사용자 입력 값에 대한 형식, 길이 검증을 수행하고, SQL 쿼리(Union, Select 등) 및 특수문자( ' , " , -- , ; 등)에 대한 필터링 적용

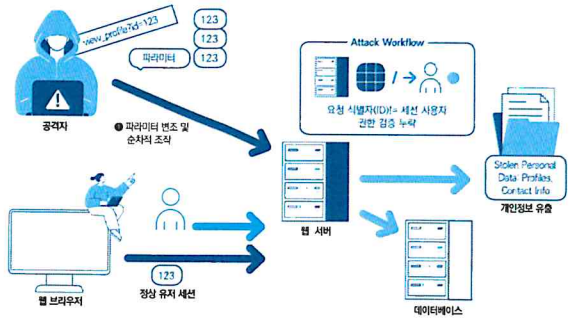
**☑ 관리자 페이지 접근 통제 강화**

- 관리자 페이지에 접근할 수 있는 IP 주소를 관련 담당자, 특정 VPN 등 허가된 주소로만 한정하여 외부에서의 SQL 인젝션으로 인해 무단 인증 시도를 네트워크 레벨에서 차단

**☑ 정기적인 취약점 점검 및 모니터링 체계 강화**

- 소스코드 취약점 진단 및 정기적인 모의해킹을 통해 잠재적인 SQL인젝션 취약점을 사전에 식별하고 조치
- 악의적 SQL 구문 탐지 시, 웹 서버 로그 보존 및 악성 IP 차단 등 추가 공격 방어하고 웹 애플리케이션과 DB 서버 사이에 웹 방화벽(WAF)를 사용하여 악의적인 SQL 질의문 등 관련 공격을 차단 등

## ○ 파라미터(Parameter) 변조




**현상** 웹 브라우저(Client)와 웹 서버(Server) 간에 데이터를 교환할 때 사용되는 파라미터 값(URL 쿼리스트링, Hidden Field, 쿠키 등)을 공격자가 임의로 변조하여 타인의 개인정보나 민감한 데이터를 무단으로 열람·유출



| | 공격 경로 | 유출 사례 |
|---|---|---|
| 사례 1 | URL 파라미터 순차적 증가 | 마이페이지 접속 URL(예: view_profile?user_no=100)에서 회원 식별 번호(user_no)를 101, 102 등으로 순차적으로 조작하여, 인가받지 않은 다른 고객들의 개인정보(이름, 연락처, 주소 등)를 대량으로 열람 및 탈취 |
| 사례 2 | 히든 필드 및 식별자 변조 | 1:1 문의 게시판이나 개인정보 조회 페이지에서, 화면에 노출되지 않은 숨겨진 파라미터(Hidden Field)의 '작성자 ID'나 '주문 번호' 값을 타인의 값으로 변조하여, 다른 사용자가 남긴 민감한 정부파일이나 개인 정보를 무단 조회 |

**예방·대응** 파라미터 변조를 통한 개인정보 유출 예방 방법

**☑ 서버 단에서의 파라미터 유효성 검증**

- 클라이언트(브라우저)에서 전달되는 파라미터 값을 절대 신뢰 하지 않고, 요청한 객체(게시글, 개인정보 페이지 등)의 소유자와 현재 로그인된 세션(Session)의 사용자가 정확히 일치하는지 서버 단에서 교차 검증하는 로직 구현

**☑ 예측 불가능한 식별자(난수화) 사용**

- 사용자 번호, 주문 번호, 게시물 번호 등에 '1, 2, 3'과 같이 순차적으로 증가하는 예측 가능한 정수형 인덱스 대신 유추가 불가능한 무작위 식별자(UUID, 난수화된 해시값 등)를 사용

**☑ 비정상 요청 탐지 및 안전한 예외 처리**

- 유효한 파라미터가 입력되지 않았거나 파라미터 처리 과정 중 예외 발생 시, 개인정보를 처리하지 않는 별도 페이지를 출력 하는 절차 구현 등(작성자와 수정자 일치 여부 확인 등)
- 파라미터 변조를 통한 대량의 데이터 스크레핑(Scraping) 정황 발견 시, 즉각적인 IP 차단 조치 및 추후 원인 분석을 위한 웹/WAS 접근 로그 안전하게 보존



## ○ 관리자 페이지 비정상 접속


**현상** 관리자 페이지 주소가 추측하기 쉬운 주소(admin, administrator 등)로 되어있거나 관리자 페이지 인증 정보(ID/PW 등)가 단순한 경우, 공격자가 이를 악용해 개인정보 탈취 및 위변조 등 공격 수행

| | 공격 경로 | 유출 사례 |
|---|---|---|
| 사례 1 | 인증 페이지 | 사전에 획득한 관리자 계정(단순 ID/PW 등)을 사용하여 MFA(다중 인증)가 미적용된 관리자 페이지에 접속 |
| 사례 2 | | 접속이 가능한 상태로 노출된 관리자 페이지에 무단으로 접근하여 개인정보 탈취 |

**예방·대응** 관리자 페이지 개인정보 유출 예방 방법

**☑ IP 기반 접근 통제**

- 특정 IP 또는 내부 네트워크/VPN에서만 관리자 페이지 접근이 가능하도록 IP주소 기반 접근 통제 설정

**☑ 관리자 인증 체계 강화**

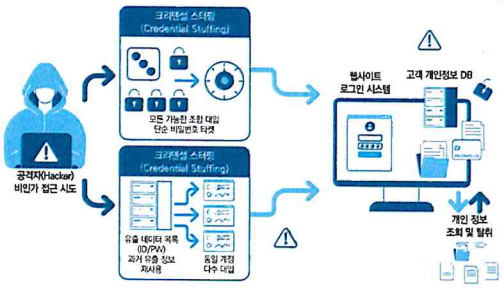
- 관리자 페이지에 접근하기 위해서는 OTP 등 암호 이외의 추가 정보를 요구하는 다중 인증 도입 등
- 관리자 페이지의 접근 주소·경로 변경 및 관리자 계정에 대한 인증 정보 변경을 통한 추가 공격 차단

**☑ 서버 설정을 통한 도메인 분리 및 내부 관리계획 수립**

- 관리자 페이지에 대한 별도 도메인 또는 서브 도메인을 사용할 수 있도록 애플리케이션에 대한 서버 설정을 별도로 구성
- 유출 발생 시점에 접속한 관리자 계정 정보 확인 및 관련 웹 로그를 보존하고 관리자 계정을 안전하게 보관하는 등 접근권한 및 접근 통제 관련 내부 관리계획을 수립하고 시행



## ○ 브루트 포스(Brute Force) 및 크리덴셜 스터핑(Credential Stuffing)




**현상** 계정의 비밀번호를 해독하기 위해 조합 가능한 모든 문자열을 하나씩 대입(브루트 포스)하거나 과거 다른 웹사이트의 데이터 유출사고 등을 통해 확보한 사용자의 인증정보(ID/PW 등)를 악용하여 무작위 또는 지속적으로 접속을 시도(크리덴셜 스터핑)하는 공격 현상

| | 공격 경로 | 유출 사례 |
|---|---|---|
| 사례 1 | 비밀번호 무작위 대입 | 이용자가 설정한 비밀번호의 보안강도가 낮거나 다수가 사용하는 비밀번호(ex. 1234, love 등)를 무작위로 대입 |
| 사례 2 | 유출된 계정정보 공격 | 로그인 페이지 대상 크리덴셜 공격으로 이용자 계정으로 접속하여 개인정보 조회·탈취 |

**예방·대응** 브루트 포스 및 크리덴셜 스터핑 예방 방법

- 비정상적 로그인 시도 탐지 시, 공격자 IP와 해당 대역에 해당하는 IP에 대한 즉각적인 접근 차단 및 로그인 시도 결과 등을 확인할 수 있는 웹 서버 및 애플리케이션 로그 자료 보존
- 로그인 성공 후 사용자 정보를 확인할 수 있는 페이지에 마스킹 등을 적용하여 개인정보 최소화 조치
- 새로운 IP에서 로그인 요청 또는 동일한 IP에서 다수의 로그인 요청 시, 로그인 실패에 대한 IP 차단 조치 또는 SMS, 이메일, OTP 등의 추가 인증수단을 적용

### ○ 크로스 사이트 스크립팅(XSS, Cross Site Scripting)

현상 웹사이트 관리자 권한이 없는 자가 웹페이지에 악성 스크립트를 삽입하여 공격

| | 공격 경로 | 유출 사례 |
|---|---|---|
| 사례 1 | 게시판내 악성 스크립트 삽입 | 공격자가 홈페이지 내 게시판에 XSS 공격 스크립트를 삽입하여 게시글을 작성, 직원이 해당 글을 확인 하면서 관리자 로그인 세션 탈취 |
| 사례 2 | 취약점 결합 및 우회 공격 | 공격자가 XSS 취약점과 SSO 취약점을 결합하여 사용자의 인증 토큰을 탈취 후, 웹 애플리케이션 방화벽 설정을 우회 접속 |

**예방·대응 크로스 사이트 스크립팅 개인정보 유출 예방 방법**

**☑ 시큐어 코딩 및 입력값 검증 (Secure Coding & Validation)**

- 외부 입력값 또는 출력값에 스크립트가 삽입되지 못하도록 &<>" '/() 등을 & > " ' / ( ) 등으로 인코딩하여 처리
- 웹 방화벽(WAF)을 사용하여 비정상적인 트래픽 분석 및 주요 공격 패턴 차단
  * <script>, onerror=, onload=, javascript:: 등의 문자열을 포함한 요청 차단 및 OWASP CRS(Core Rule Set)을 적용하여 웹 애플리케이션 공격 패턴 차단
- 이용자 입력값에 대해 서버에서 검증
  * 클라이언트에서 검증하는 경우, Web Proxy(Paros, Burp Suite) 등 도구를 이용해 쉽게 우회 가능
- 컨텐츠 보안 정책(Context Security Policy, CSP)을 통해 입력값이 스크립트 코드로 해석되지 않도록 조치 등

**☑ 사후 대응 및 증거 보존**

- 크로스 사이트 스크립팅 취약점이 존재하는 페이지에 대한 접근 차단 및 해당 페이지 관련 웹 서버 로그 등 증거 보존
- 악성 스크립트가 서버에 남아있는 Stored XSS 공격의 경우, DB서버 등에 남아있는 악성 스크립트를 즉시 제거하여 추가 피해 방지

**참고 다크웹(Dark Web)과 해킹포럼(Hacking Forums)**

- 다크웹은 일반적인 검색엔진으로 접근할 수 없고, 특수한 소프트웨어를 통해서만 접근할 수 있는 웹사이트와 서비스로 구성되어 있으며, Tor(The Onion Router)와 I2P(Invisible Internet Project) 같은 익명화 네트워크를 사용
- 해킹포럼은 해킹 기술과 정보를 공유하는 커뮤니티로 최신 해킹 기술, 보안 취약점, 익스플로잇 등을 공유하며 해킹 툴, 악성코드, 스크립트 등을 거래하거나 무료로 배포



## 2.업무 과실로 인한 개인정보 유출 예방·대응 방법

### ○ 개인정보를 처리하는 과정에서 **개인정보취급자의 과실, 실수 등으로 발생**

**사례 1** 개인정보를 다수에게 이메일·문자메세지로 동보 발송하거나 이메일 주소 등을 잘못 기재하여 다른 사람에게 발송

- 가능한 경우, 개인정보 수신인으로부터 해당 자료를 즉시 회수하거나 파기 요청하여 유출 피해 가능성을 최소화
- 다수에게 동시에 메일을 발송해도 수신자별로 개별 확인이 가능하도록 개인별 발송 기능을 기본 설정 등

**사례 2** 개인정보 파일을 홈페이지 공지사항, 게시판 등에 게시(업로드)

- 추가 확산을 방지하기 위해 해당 게시글을 삭제
- 마스킹 등의 방법을 통해 최소한의 개인정보를 기재
- 가능한 경우, 개인정보 필터링 솔루션을 통해 개인정보 포함 여부 사전 탐지
- 부득이 개인정보를 기재해야 하는 경우 해당 게시물 및 댓글을 비공개로 전환, 첨부파일이 공개되지 않도록 접근 제어[9] 등

**사례 3** 개인정보파일이 저장된 업무용 기기(노트북, 휴대전화 등) 및 이동형 저장매체 등을 분실

- 기기 분실을 인지한 즉시 관리자 또는 관련 부서에게 보고(기기의 종류와 분실 위치, 관련 정보 등)
- 기기에 원격제어나 관리 기능이 있는 경우, 기기 비활성화 및 데이터 초기화
- 업무용 기기, 일반 USB 사용 시 반드시 반입·반출대장을 작성하고 기기 비밀번호 설정 및 디스크 암호화 등

**사례 4** 온라인 설문조사 플랫폼 등을 통해 개인정보를 수집하였으나, 열람 권한을 잘못 설정하여 타인의 개인정보가 공개

- 타 플랫폼을 통해 개인정보 수집 및 처리 시, 수집 결과에 대한 열람 권한을 개인정보 취급자에게만 부여 등

9) 세부내용은 「홈페이지 개인정보 노출방지 안내서」(개인정보위, '24. 4월) 참고



## 3.시스템 오류로 인한 개인정보 유출 예방·대응 방법

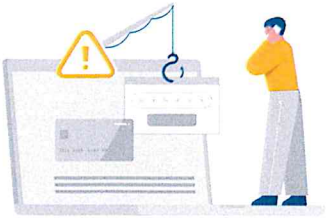
### ○ 시스템 오류는 개인정보처리시스템 **개발·운영·고도화 과정에서 프로그램 명령어 누락, 오류 설정** 등으로 발생

**사례 1** 잘못된 캐시 설정으로 인한 개인정보 유출

- 개인정보를 처리하는 페이지 또는 시스템에 대하여 CDN(Content Delivery Network)[10] 설정을 해제하거나 캐시된 민감 한 데이터 무효화 및 재설정 등

**사례 2** 검색엔진(Google, Bing 등)에서 개인정보를 조회 가능한 관리자 페이지가 검색

- 검색엔진에 관리자 페이지가 노출됨을 인지한 즉시, robots.txt 수정 및 검색엔진 제공사에 문의하여 캐시 페이지 삭제 요청
- 관리자 페이지가 외부에서 접근되지 않도록 제한하고, 접속 시 안전한 인증수단 도입
- 개인정보 조회 페이지는 인증 후 접속 가능하도록 보호조치 적용



10) 네트워크에서 이용자에게 콘텐츠를 효율적으로 전달하기 위해서 저장되는 콘텐츠 전달용 네트워크 (출처 : TTA표준)



PART

# *2

## 개인정보 조사·처분 사례

개인정보 조사·처분 현황

주요 개인정보 조사·처분 사례

# 01
# 개인정보
# 조사·처분 현황

# 01
# 개인정보
# 조사·처분 현황

## 개요

현황 **2025년 조사·처분* 건수는 총 227건**이며, **과징금은 40건**으로 총 167,797,874천원, **과태료는 125건** 총 587,200천원 부과

*과징금, 과태료, 개선권고, 시정명령, 시정권고, 고발, 징계권고, 공표, 공표명령

※ 경고 · 종결 등 조사 관련 의결 건수를 모두 포함 시 **425건**

접수 **인지 조사 33%**(76건), **신고 조사 67%**(151건)

*인지 : 기획조사, 언론보도, 사전실태점검, 조사중인지

*신고 : 침해신고, 유출신고, 민원신고, 공익신고, 타기관 이첩

유형 **유출 51%**(115건), **침해 49%**(112건)

기관 **공공기관 34%**(77건), **민간기업 66%**(150건)


## 전년도 비교·분석

증감 전년도 대비 **처분 건수 48%**(110건) **감소, 과징금·과태료 172%**(1,083억원) **증가**

※ ('24·'25) 337건 → 227건, 619억원 → 1683억원

※ 다만, **조사 관련 의결 건수는** ('24) 370건 → ('25) **425건으로 소폭 상승(14%)**

유형 전년도 대비 **유출 처분 비중 19% 증가**

※ ('24년) 337건 중 유출 처분 32%(110건) → ('25년) 227건 중 유출 처분 51%(115건)

기관 전년도 대비 **민간기관 처분 비중 21% 증가**

※ ('24년) 337건 중 민간 처분 45%(157건) → ('25년) 227건 중 민간 처분 66%(150건)



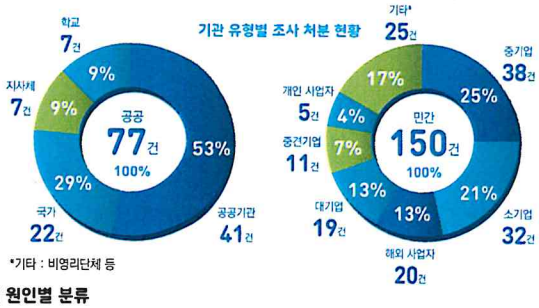

## 기관별 세부 분류

공공 **총 77건** 중 **공공기관 53%**(41건), **중앙행정기관·헌법기관 등 29%**(22건), 지방자치단체/학교 각 9%(각 7건) 순으로 확인

※ 과징금 기준 : 학교(대학 등) 9.6억(71%), 국가 2.2억(16%), 산하 공공기관 1.9억(14%)

민간 **총 150건** 중 **중기업·소기업·개인사업자 등 중소기업 50%**(75건), **대기업·중견기업 20%**(30건), **비영리 단체 등 기타 17%**(25건) 순으로 확인

※ 과징금 기준 : 대기업 1,550억(94%), 해외사업자 42.2억(3%), 중견기업 38.4억(2%)




*기타 : 비영리단체 등

## 유출 원인별 분류

현황 **총 115건** 중 **해킹 45%**(52건) 및 **업무 과실 46%**(53건)로 거의 동일한 비중을 차지하고 있으나, 주요 유출 원인이 **공공부문은 업무과실 64%, 민간부문은 해킹 49%**로 차이가 있음을 확인

※ 과징금·과태료 부과액 기준으로는 공공 · 민간 모두 해킹이 압도적 비중 차지(공공:97%, 민간:91%)

공공 **총 25건** 중 **업무 과실 64%**(16건), **해킹 32%**(8건) 순으로 확인

민간 **총 90건** 중 **해킹 49%**(44건), **업무 과실 41%**(37건), **시스템 오류 등 기타 10%**(10건) 순으로 확인

**기관 유형별 유출 원인 현황**

단위 : 백만원

| 구분 | 공공 | | | | 민간 | | | | 총 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 건수 | % | 과징금·과태료 | % | 건수 | % | 과징금·과태료 | % | 건수 | % | 과징금·과태료 | % |
| 해킹 | 8건 | 32% | 1,392 | 97% | 44건 | 49% | 142,587 | 91% | 52건 | 45% | 143,980 | 91% |
| 업무 과실 | 16건 | 64% | 35 | 3% | 37건 | 41% | 14,131 | 9% | 53건 | 46% | 14,167 | 9% |
| 시스템 오류 | 1건 | 4% | 2 | - | 7건 | 8% | 109 | - | 8건 | 7% | 112 | - |
| 고의 유출 | 0건 | - | 0 | - | 1건 | 1% | 3 | - | 1건 | 1% | 3 | - |
| 기타(원인 미상 등) | 0건 | - | 0 | - | 1건 | 1% | 0 | - | 1건 | 1% | 0 | - |
| 총 | 25건 | 100% | 1,429 | 100% | 90건 | 100% | 156,830 | 100% | 115건 | 100% | 158,262 | 100% |



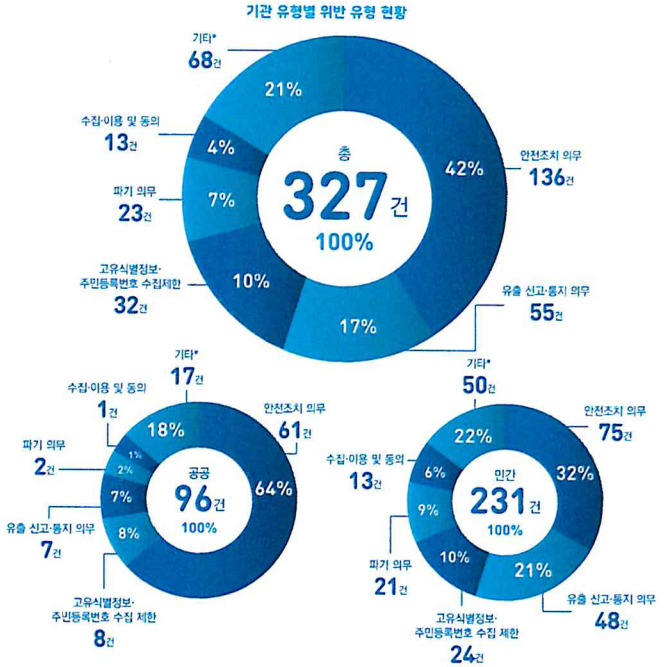
## 위반 유형별 분류

현황 **총 327건(중복포함)** 중 모든 부문에서 **안전조치의무 위반 42%**(136건)이 제일 높은 비중을 차지하고 있으며, 그 다음으로 **공공**은 **고유식별정보·주민등록번호 수집 제한**, **민간**은 **유출 신고·통지의무 위반** 순으로 확인

공공 **총 96건** 중 **안전조치의무 64%**(61건), **고유식별정보·주민등록번호 수집 제한 8%**(8건) 순으로 확인

민간 **총 231건** 중 **안전조치의무 32%**(75건), **유출 신고·통지 의무 21%**(48건) 순으로 확인

**기관 유형별 위반 유형 현황**




*기타 : 영상정보처리기기 제한, 열람요구, 국외이전, 처리방침, 가명정보 등

※ 개선권고, 사전실태점검, 경고, 조사중지, 종결 등 위반사항이 없는 경우 제외

### 시정조치 유형별 분류

현황 총 415건 중 모든 부문에서 **과태료 30%**(125건)가 제일 높은 비중을 차지하고 있으며, **공표 15%**(65건), **개선권고 12%**(51건) 순으로 확인

공공 **공표 30%**(47건), **시정권고 25%**(40건), **과태료 17%**(27건) 순으로 확인

민간 **과태료 38%**(98건), **개선권고 15%**(38건), **과징금/시정명령 13%**(34건)순으로 확인

**총 처분 시정조치 현황**

| 구분 | 총 | 과징금 | 과태료 | 개선권고 | 시정명령 | 시정권고 | 고발 | 징계권고 | 공표 | 공표명령 |
|---|---|---|---|---|---|---|---|---|---|---|
| 공공 | 158건 | 6건 | 27건 | 13건 | 9건 | 40건 | 0건 | 3건 | 47건 | 13건 |
| | 100% | 4% | 17% | 8% | 6% | 25% | 0% | 2% | 30% | 8% |
| 민간 | 257건 | 34건 | 98건 | 38건 | 34건 | 2건 | 1건 | 0건 | 18건 | 32건 |
| | 100% | 13% | 38% | 15% | 13% | 1% | 1% | 0% | 7% | 12% |
| 총 | 415건 | 40건 | 125건 | 51건 | 43건 | 42건 | 1건 | 3건 | 65건 | 45건 |
| | 100% | 10% | 30% | 12% | 10% | 10% | 1% | 1% | 15% | 11% |

### 유출 건수 및 과징금 TOP 5

2025년도 유출 건수 TOP 5

공공

| 순위 | 구분 | 기관명 | 유출 항목 수(건) |
|---|---|---|---|
| 1 | 학교 | 전북대학교 | 322,130 |
| 2 | 학교 | 이화여자대학교 | 83,352 |
| 3 | 학교 | 영남사이버대학교 | 57,367 |
| 4 | 국가 | 법원행정처 | 17,998 |
| 5 | 공공기관 | 국립항공박물관 | 11,029 |

민간

| 순위 | 규모 | 기업명 | 유출 항목 수(건) |
|---|---|---|---|
| 1 | 대기업 | SK텔레콤㈜ | 23,244,649 |
| 2 | 중기업 | 인크루트㈜ | 7,275,843 |
| 3 | 중견기업 | ㈜모두투어 | 3,064,862 |
| 4 | 중기업 | ㈜클래스유 | 1,601,890 |
| 5 | 중견기업 | ㈜동행복권 | 749,114 |

2025년도 과징금 TOP 5 (유출·침해 포함)

공공

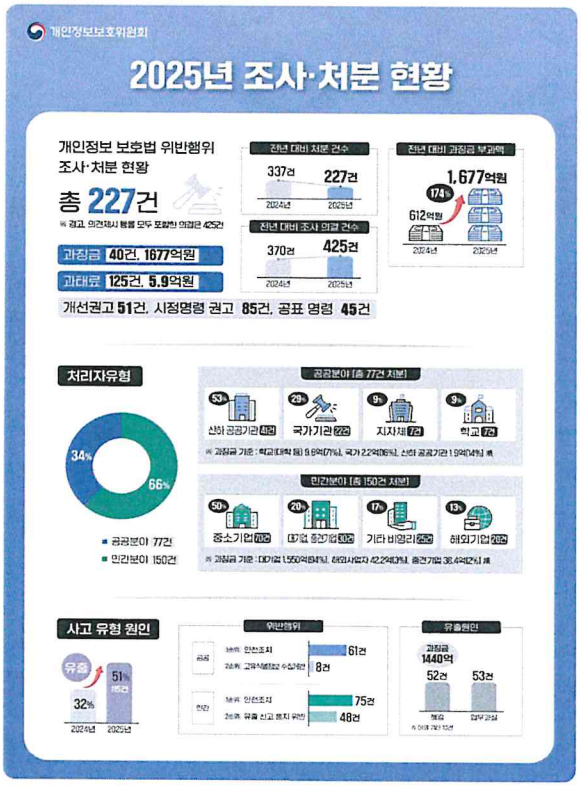
| 순위 | 구분 | 기관명 | 과징금(천원) |
|---|---|---|---|
| 1 | 학교 | 전북대학교 | 623,000 |
| 2 | 학교 | 이화여자대학교 | 343,000 |
| 3 | 국가 | 법원행정처 | 207,000 |
| 4 | 공공기관 | (재)전남테크노파크 | 98,000 |
| 5 | 공공기관 | 국립항공박물관 | 98,000 |

민간

| 순위 | 규모 | 기업명 | 과징금(천원) |
|---|---|---|---|
| 1 | 대기업 | SK텔레콤㈜ | 134,791,000 |
| 2 | 대기업 | ㈜우리카드 | 13,451,000 |
| 3 | 대기업 | ㈜카카오페이 | 5,968,000 |
| 4 | 대기업 | 애플 | 2,405,000 |
| 5 | 중견기업 | ㈜센타나인 | 1,477,000 |



참고 2025년 조사·처분 현황






# 02
# 주요 개인정보 조사·처분 사례

# 02
# 주요 개인정보 조사·처분 사례

## 1. 개인정보 수집·이용·제공 관련

### 가. 온라인 사기 피해 조회 서비스에 관한 보호법 해석

**사건의 개요**

중고거래 사기 및 보이스피싱 등 온라인 사기 피해 시례를 등록·조회할 수 있는 서비스를 운영하는 사업자 A는 온라인 사기 피해자가 피해 사례를 등록하는 과정에서 사기 행위를 의심 받는 자(사기 의심자)의 개인정보(계좌번호, 휴대전화번호 등)를 피해자(등록자)로부터 수집·처리하고 있었다.

**조사결과 및 시정조치**

사업자 A는 정보주체의 개인정보를 제3자를 통해 수집하였으나, 개인정보 보호법 제15조제1항제5호에 따라 "명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우"에 해당하여 개인정보의 수집·이용이 가능한 것으로 보고, 개인정보 보호법 상 제한된 행위로 판단하지 않았다.

- 다만, 개인정보처리자가 수집한 개인정보를 사기 피해 방지 목적으로만 제한적으로 이용·제공하고, 개인정보의 보유 및 공개기간을 필요 최소한으로 설정하며, 사기 의심자가 실제 사기 피해가 없는 것을 소명한 이후 자신의 개인정보 삭제를 요청하면 등록 정보 삭제 등 필요한 조치를 마련하도록 개선권고 하였다.
- 아울러, 개인정보처리자가 회원가입 및 피해사례 등록 시 이용자로부터 동의를 구분해서 받아야 하는데 이를 개인정보처리방침 및 피해사례 등록 약관으로 포괄 동의를 받고 있던 점과 개인정보 처리방침의 일부 항목이 누락된 사실이 확인되어, 개인정보위는 과태료 480만 원 부과 및 시정조치를 명령하고, 향후 이행 여부를 확인하기로 하였다.

**조사·처분 의의**

국민이 널리 이용하는 서비스에 대해 개인정보 처리근거를 명확히 해석함으로써 사업자가 법적 리스크 없이 사업을 지속할 수 있도록 하되, 보호법 위반행위는 처분하고, 정보주체의 개인정보 자기결정권을 강화하는 방향으로 서비스 개선을 유도한 데 의의가 있다.

### 나. 카드사의 개인정보 목적 외 이용·제공 위반 제재

**사건의 개요**

개인정보위는 '24년 4월 카드사의 신고와 함께 "카드사 가맹점대표자(이하 '가맹점주')의 개인정보가 카드 신규 모집에 이용된다"는 언론보도 등에 따라 조사에 착수하였다.

**조사결과 및 시정조치**

카드사가 가맹점주의 개인정보를 동의 없이 신규 카드발급 마케팅에 활용한 행위와 영업센터 직원이 이를 카드 모집인에게 전달한 사실을 확인하였다.

- 카드사 지역영업센터는 신규 카드발급 마케팅을 통한 영업실적 증대를 위해 카드가맹점의 사업자등록번호를 가맹점관리 프로그램에 입력하여 가맹점주 개인정보를 조회하였고, 카드발급심사 프로그램에서 가맹점주의 주민등록번호를 입력하여, 해당 가맹점주가 카드사에에서 발급한 신용카드를 보유하고 있는지 확인한 후, 출력된 가맹점 문서에 이를 기재 및 촬영하여 카드 모집인 등이 참여한 SNS 단체 채팅방에 공유하였다.
- 특히, 가맹점주 및 카드회원의 개인정보를 처리하는 데이터베이스를 이용하여 가맹점주의 개인정보 및 신용카드 보유 여부를 개인정보 파일로 생성하였으며, 가맹점주들의 개인정보를 카드 모집인에게 이메일로 전달하였고, 해당 정보는 신용카드 발급을 위한 마케팅에 활용되었다.
- 이에 따라, 개인정보위는 카드사가 가맹점주의 개인정보를 목적 외로 이용한 행위 등에 대해 과징금 134억 5,100만 원을 부과하는 한편, 개인정보 오·남용을 방지하기 위한 내부통제 강화, 접근권한 최소화 및 점검 등 안전조치의무 준수, 개인정보취급자에 대한 관리·감독 강화 등을 시정명령하고, 처분받은 사실을 홈페이지 등에 공표하도록 하였다.

**조사·처분 의의**

당초 개인정보의 수집·이용 목적을 벗어난 개인정보의 처리는 위법이라는 점을 강조하는 한편, 직원 등 개인정보 취급자의 개인정보 접근권한을 주기적으로 점검하고, 불필요한 개인정보 조회나 이용이 없는지 점속기록도 확인하는 등 내부통제 시스템을 잘 갖추어야 한다고 강조하고, 금융회사 또한 보호법이 적용될 수 있으므로, 보호법 준수 여부를 다시 한번 점검할 필요가 있음을 시사하였다.



### 다. 신규 AI 서비스의 개인정보 처리실태 신속한 시정·개선조치

**사건의 개요**

해외 생성형 신규 AI 서비스가 '25년 1월 출시하면서 당시 국내에서 일평균 5만여 명이 이용하였고, 이용자로부터 개인정보(계정, 프롬프트 등 이용자 입력 정보 등)를 수집하고 있었다.

- 한편, 신규 AI 서비스의 개인정보 과다 수집 소지, 국내법 미준수등 개인정보 침해 우려 제기와 함께 국내·외 정부기관의 서비스 차단 소식이 다수 보도되었다. 이에, 개인정보위는 개인정보 처리 과정에서의 침해 위험을 사전에 예방하고자 그 즉시 사전 실태점검에 착수하였다.

**조사결과 및 시정조치**

첫째, 한국 앱 마켓에 서비스를 출시하면서 외국어로만 처리방침을 공개하였고, 해당 처리방침에서도 개인정보 파기 절차 및 방법, 안전조치, 개인정보 보호책임자의 성명 · 연락처 등 우리 보호법이 요구하는 사항을 누락하였으며, 키 입력 패턴·리듬과 같은 광범위한 정보를 수집한다고 명시하고 있었다.

- 둘째, 서비스 개선 등을 위해 개인정보를 해외 소재 회사로 이전 하면서 이용자로부터 국외 이전에 대한 동의를 받지 않고 있었다. 셋째, 이용자가 프롬프트에 입력한 내용을 AI(인공지능) 개발 · 학습에 이용하고 있었으나, 이용자가 이를 거부할 수 있는 기능이 없었다. 그 외, 14세 미만 아동의 개인정보를 수집하지 않는다면서도 서비스 가입시 아동 여부를 확인하는 절차가 없었다.
- 개인정보위는 이상의 위반행위에 대하여 시정 및 개선권고를 하였다. 이에, 신규 AI 서비스 사업자는 이를 이행하여 개인정보 수집 항목을 정비 후 국외이전 사항을 포함하여 한국어로 된 처리방침, AI개발·학습 활용과 관련해 이용자가 거부할 수 있는 기능(opt-out) 및 연령 확인 절차 등을 마련하였다. 특히, 개인정보위 지적에 따라 불필요하게 타 회사로 이전된 '이용자의 프롬프트 입력 내용'에 대해서는 해당 행위를 중지하고, 이미 이전된 정보에 대해서는 파기 조치를 하였다.

**조사·처분 의의**

세계 최초로 해외 생성형 AI 서비스 처리실태에 신속한 시정·개선조치를 유도하여, 글로벌 서비스의 국내법 준수와 한국 이용자 권리보장을 강화하였다. 즉, 신규 AI 서비스 기능 보완 등 시정사항은 한국뿐만 아니라 전세계 이용자의 개인정보 권리보장을 강화한 데 의의가 있다.

- 한편, 본 사전 실태점검을 계기로 해외사업자가 보호법 준수에 필요한 기본적인 사항을 미리 점검하도록 체크리스트를 마련·배포하였다. 이를 활용하여 해외사업자가 기본적인 사항을 미리 점검함으로써 보다 더 한국 정보주체의 권리를 충실히 보장하고 개인정보를 안전하게 보호하며 서비스를 출시·운영할 것으로 기대한다.



## 2. 개인정보 국외 이전 관련

### 가. 해외 플랫폼 사업자의 개인정보 국외 이전 등 제재

**사건의 개요**

사업자 A는 해외 전자상거래 플랫폼을 운영하면서 상품 배송을 위해 우리나라를 포함해 중국, 싱가포르, 일본 등의 다수 사업자에게 국내 이용자(구매자)의 개인정보(성명, 주소, 개인통관 고유부호 등) 처리를 위탁하거나 보관하고 있었으며, '25. 2월부터 한국에서 직접 상품을 판매·배송할 수 있는 서비스를 제공하기 위해 판매자를 시범 모집하면서, 판매자의 신원확인을 위해 개인정보(신분증, 얼굴 동영상, 주민등록번호)를 수집·처리하고 있었다.

**조사결과 및 시정조치**

사업자 A가 상품 배송을 위해 국내·외 사업자(수탁사)에게 개인정보 처리를 위탁·보관하면서 해당 사실을 개인정보 처리방침에 공개하거나 이용자에게 알리지 않고, 수탁사에 대해 개인정보 안전관리 방안 교육, 개인정보 처리현황 점검 등의 관리·감독을 실시하지 않았다.

- 또한, '23년 말 기준 일일 평균 290만 명의 한국 이용자가 사업자A의 서비스를 이용하고 있음에도 보호법에서 요구하는 국내 대리인을 지정하지 않았고, 회원 탈퇴 절차를 7단계로 복잡하게 구현하여 이용자의 권리행사를 어렵게 하였다. 마지막으로, 신원 확인을 위해 사업자 A는 판매자의 신분증과 얼굴 동영상을 수집 하고 법적 근거 없이 주민등록번호를 처리하였다.
- 이에, 개인정보위는 국외이전 위반와 개인정보 및 주민등록번호 처리 제한 위반 행위에 대해 과징금 13억 6,900만 원을 부과하고, 업무 위탁사실 미공개 및 수탁자 교육·관리를 하지 않은 행위에 대해 1,760만 원의 과태료를 부과하고 위반 행위에 대해 시정을 명령하고, 국내대리인을 지정하도록 개선권고하였다.

**조사·처분 의의**

개정된 보호법상 국내대리인 규정('25. 10. 2. 시행) 취지에 따라 사업자 A의 국내 법인을 국내대리인으로 지정하도록 하여 해외사업자가 정보주체의 피해 구제 등 우리 국민의 개인정보를 효과적으로 보호할 수 있도록 하였다.

- 아울러, 해외 사업자의 국내 진출이 증가함에 따라, 본 건 처분을 계기로 「해외사업자의 개인정보 보호법 적용 안내서」 번역본을 마련·배포하였다. 이에, 해외 사업자가 보호법을 충실히 준수할 수 있도록 기준 및 참고 사례 제시 등을 통해 국내 정보주체의 개인정보를 보호하는 기반을 마련했다는 점에서 의의가 있다.



### 나. 간편 결제 사업자, 플랫폼 사업자의 개인정보 국외 이전 제재

**사건의 개요**

국내 간편결제 사업자 A는 플랫폼 사업자 C내 결제시스템 통합서비스를 제공하는 해외 간편결제 사업자 B의 중계를 통해 결제 정보 등을 플랫폼 사업자 C에게 전송하고 있었으며, 플랫폼 사업자는 결제평가지수 산출을 포함한 결제 처리에 수반된 개인정보 처리업무를 해외 간편결제 사업자 B에게 위탁하고 있었다.

- 이 과정에서 국내 간편결제 사업자 A는 플랫폼 사업자 C의 수탁사인 해외 간편결제 사업자 B가 결제평가지수 점수산출 모델 구축을 할 수 있도록 전체 국내 간편결제 사업자 A 이용자의 개인정보를 동의(제3자 제공 및 국외이전 별도 동의)없이 해외 간편결제 사업자 B에게 전송하였으며, 해외 간편결제 사업자 B가 이용자별 결제평가지수를 산출할 수 있도록 국내 간편결제 사업자 A 전체 이용자의 개인정보를 동의없이 해외 간편결제 사업자 B에 전송하였다.
- 특히, 국내 간편결제 사업자 A 전체 이용자 중 국내 간편결제 서비스를 결제 수단으로 등록한 이용자는 20% 미만에 불과함에도 국내 간편결제 사업자 A는 플랫폼 사업자 이용자뿐만 아니라 플랫폼 사업자 미이용자까지 포함된 전체 이용자의 정보를 해외 간편결제 사업자 B에게 전송하였다.

**조사결과 및 시정조치**

국내 간편결제 사업자 A가 플랫폼 사업자가 사용하는 결제평가지수 모델 구축 및 점수 산출 등을 위해 전체 이용자의 개인정보를 동의(제3자제공 동의 및 국외이전 동의)없이 플랫폼 사업자(수탁자: 해외 간편결제 사업자 B)에 제공한 행위에 대하여 적법처리 근거 없는 국외이전으로 보아 과징금 59억 6,500만 원을 부과하고, 국외 이전 적법 요건을 갖추도록 시정명령 하였다. 또한, 홈페이지에 관련 사실을 공표하도록 명하였다.

- 또한, 플랫폼 사업자가 개인정보를 국외로 처리위탁하면서 국외 수탁자 등을 개인정보처리방침 등을 통해 정보주체에게 공개하거나 고지하지 않은 행위에 대해서는 과징금 24억 500만원을, 위탁 사실을 밝히지 않은 행위에 대해서는 과태료 220만원을 부과하고, 개인정보 처리 수탁자인 해외 간편결제 사업자 B에 대한 국외이전(위탁) 사실을 개인정보처리방침 등에 공개하도록 시정명령하였다. 또한 플랫폼 사업자의 홈페이지에 관련 사실을 공표하도록 명하였다.
- 한편, 해외 간편결제 사업자 B가 구축한 국내 간편결제 사업자 A 이용자의 결제평가지수 산출 모델은 위법하게 제공 및 국외 이전된 개인정보를 활용해 구축된 것으로, 개인정보의 침해상태를 근본적으로 해소하기 위해 해외 간편결제 사업자 B에는 결제평가지수 산출 모델을 파기하도록 시정명령하였다.
- 참고로 국내 간편결제 사업자 A는 해외 간편결제 사업자 B에게 자사의 개인정보 처리업무를 위탁했고 수탁자에 대한 이전은 제3자 제공에 해당하지 않는다는 의견을 제출하였으나, 수용되지 않았다. 결제평가지수 관련 개인정보 처리 이익의 귀속주체가 플랫폼 사업자 C이고(단건청구·일괄청구 판단용, 플랫폼사업자 C FDS 구동용), 정보주체에게 책임을 부담(일괄청구 시 사유 설명요청에 대응, 플랫폼 사업자 C FDS 탐지 시 후속조치)하는 주체 또한 플랫폼 사업자이며, 이는 국내 간편결제 사업자 A의 이익·책임을 벗어난 것이므로 국내 간편결제 사업자 A가 위탁할 수 있는 업무가 아니라고 판단되었다.

**조사·처분 의의**

동 조사는 최근 글로벌 플랫폼 서비스의 확대로 개인정보 국외이전이 증가하고 있는 상황에서, 개인정보 국외 이전의 범위를 명확히 하고, 사업자가 국외 이전의 적법 요건을 반드시 준수해야 함을 재확인한 점에서 의의가 있다. 사업자는 개인정보 국외 이전이 수반되는 서비스 제공 시 정보주체의 별도 동의를 받거나, 국외 수탁자에게 개인정보 처리를 위탁하는 경우 개인정보 처리방침 등을 통해 개인정보가 국경을 넘어 이전되는 사실을 반드시 알려야 한다

- 또한, 개인정보 처리를 외부에 위탁하는 경우 위탁자가 정보주체에 대한 책임을 부담해야 한다. 위탁자의 책임 영역을 떠나 제3자의 책임 영역으로 개인정보를 이전하는 것은 제3자 제공에 해당하므로 정보주체의 동의 등 적법 근거를 구비해야 한다.

## 3. 개인정보 안전조치 관련

### 가. 대학교의 파라미터 변조 웹 취약점에 의한 개인정보 유출 제재

**사건의 개요**

해커가 SQL 인젝션(데이터베이스 명령어 주입) 및 파라미터(입력값) 변조 공격을 통해 A 대학교 학사행정정보시스템에 침입하여 32만여 명의 개인정보(주민등록번호 28만여 건 포함)를 탈취하였다.

- 해커가 시스템의 데이터베이스(DB) 조회 기능의 취약점*을 악용한 파라미터(입력값) 변조 공격으로 B 대학교 통합행정시스템에 침입하여 8만 3천여 명의 주민등록번호를 포함한 개인정보를 탈취하였다.

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

**조사결과 및 시정조치**

해커는 A 대학교 학사행정정보시스템의 비밀번호 찾기 페이지에 존재하는 취약점을 악용하여 학번 정보를 입수한 후, 학적정보 조회 페이지 등에서 약 90만 회의 파라미터 변조 및 무작위 대입을 통해 A 대학교 학생 및 평생교육원 홈페이지 회원 총 32만여 명의 개인정보에 접근한 것으로 파악되었다.

- 해당 취약점은 '10. 12월 시스템 구축 당시부터 존재하였으며, A 대학교는 기본적 보안 장비는 갖추고 있었으나 외부 공격에 대한 대응이 미흡 하였고, 특히 일과시간 외에는 모니터링을 소홀히 한 결과 주말·야간에 발생한 비정상적 트래픽 급증 현상을 뒤늦게 인지하였다.
- 이에 따라 개인정보위는 A 대학교에 총 6억 2,300만 원의 과징금과 540만 원의 과태료를 부과하면서 이를 대학 홈페이지에 공표하도록 명하는 한편, 모의해킹 등 취약점 점검을 강화하고 상시 모니터링 체계를 구축하도록 시정명령 함과 동시에 책임자에 대한 징계도 권고하였다.
- B 대학교의 경우, A 대학교와 동일하게 해커가 악용한 웹 취약점이 '15. 11월 시스템 구축 시점부터 존재해 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 모니터링을 소홀히 하는 등 외부의 불법적인 접근 통제 조치가 미흡했던 것으로 밝혀졌다.
- 이에 따라 개인정보위는 B 대학교에 총 3억 4,300만 원의 과징금을 부과하면서 이를 대학 홈페이지에 공표하도록 명하는 한편, 모의 해킹 등 취약점 점검을 강화하고 상시 모니터링 체계를 구축하도록 시정명령 함과 동시에 책임자에 대한 징계를 권고하였다.

**조사·처분 의의**

대학의 경우 대개 생성규칙이 단순한 '학번' 등을 기준으로 개인정보를 관리하고 있어 파라미터(입력값) 변조 공격에 취약한 측면이 있고, 대학 등 공공부문 특성상 주민등록번호 등 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 점을 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 병행하는 등 공공 교육부문 전반의 보호법 준수 책임성과 경각심을 제고하는 계기가 되었다.



### 나. 통신사의 대규모 개인정보 유출 관련 안전조치 위반 제재

**사건의 개요**

개인정보위는 2025년 4월 22일 통신사 A가 비정상적 데이터 외부 전송 사실을 인지하고 유출 신고해옴에 따라 조사에 착수하였고, 사건의 중대성을 감안하여 신고 당일 한국인터넷진흥원과 함께 집중조사 TF를 구성하여 유출 관련 사실관계, 개인정보 보호 법령 위반 여부 등을 중점 조사하였다.

**조사결과 및 시정조치**

통신사 A의 개인정보 처리·운영 실태와 개인정보 보호법 준수 여부를 조사한 결과, 해당 사고는 통신사 A의 기본적인 보안 조치 미비와 관리 소홀로 인해 발생한 것으로 확인되었다.

- 통신사 A는 기본적인 접근 통제조차 이행하지 않아 인터넷과 내부망 사이의 보안 운영 환경이 해커의 불법적인 침입에 매우 취약한 상태로 관리·운영되고 있었으며, 다수 서버의 계정 정보가 저장된 파일을 관리망 서버에 암호 설정 등 제한 없이 저장·관리하고, 가입자 인증 서버에서 비밀번호 입력 등 인증 절차 없이도 개인정보를 조회할 수 있도록 운영하였다.
- '25. 4월까지 각종 상용 백신 프로그램을 설치하지 않았을 뿐만 아니라 백신 미설치를 대체하는 보안 조치마저도 소홀히 하였고, 인증정보에 해당하는 유심 인증키를 암호화하지 않고 평문으로 DB 등에 저장하는 등 안전조치 의무를 소홀히 하였다.
- 한편, 유출 사고가 발생한 인프라 영역은 CPO가 개인정보 처리 실태조차 파악하지 못하는 등 CPO의 관리·감독이 사실상 이루어지지 않은 것으로 확인되었으며, 법령에서 정한 72시간 내 유출된 이용자를 대상으로 유출 사실을 통지하지 않아 이로 인한 사회적 혼란이 가중되었다.
- 개인정보위는 통신사 A가 국내 최상위의 이동통신사업자로서 안전조치의무를 소홀히 하여 유심정보를 비롯한 개인정보가 유출된 행위에 대해 과징금 1,347억 9,100만 원을 부과하는 한편, 정보 주체에 대한 유출 통지를 지연하여 신속한 피해 확산방지를 소홀히 한 행위에 대해 과태료 960만 원을 부과하기로 결정하였다.
- 아울러, 유출 사고 재발 방지를 위해 이동통신 서비스 전반의 개인정보 처리 현황을 면밀히 파악하여 안전조치를 강화하고, 개인정보 보호책임자가 회사 전반의 개인정보 처리 업무를 총괄할 수 있도록 거버넌스 체계를 정비할 것을 시정명령하였으며, 현재 일부 고객 관리시스템에 대해서만 획득한 정보보호 및 개인정보보호 관리 체계 인증(ISMS-P) 범위를 이동통신 네트워크 시스템으로 확대하여 회사 시스템 전반의 개인정보 안전성 확보조치 수준을 제고하도록 개선 권고하였다.

**조사·처분 의의**

개인정보보호위원회 출범('20.8.) 이후 발생한 최대 규모(약 2,300만 명)의 유출 사고라는 사안의 중대성을 고려하여, 착수 즉시 집중조사 TF를 구성하는 등 위원회의 조사 역량을 집중하여 신속·정밀한 조사('25.4.~7.)로 사고원인 및 개인정보 보호법 위반 사항을 규명하였다.

- 이와 함께 사업자의 개인정보 보호 및 관리 과실에 대해 역대 최고 금액인 약 1,348억 원의 과징금을 부과함으로써, 개인정보 보호가 불필요한 비용이 아니라 기업 책임과 직결된 필수 투자라는 확고한 메시지를 남겼다.



### 다. 크리덴셜 스터핑 해킹 공격에 의한 개인정보 유출 제재

**사건의 개요**

신원 미상의 해커는 멤버십 서비스 사업자 A가 운영 중인 앱 서비스에 '크리덴셜 스터핑*' 공격을 시도하여 로그인에 성공 및 개인정보를 탈취하였고, 일부 이용자의 포인트가 무단 사용 되는 2차 피해가 발생하였다.

* 사전에 확보한 다수의 아이디, 비밀번호 정보를 무차별 대입하여 접속(로그인)을 시도하는 공격 방식으로 로그인 시도 횟수와 로그인 실패율이 급증하는 특징을 보임

**조사결과 및 시정조치**

멤버십 서비스 사업자 A는 짧은 시간 동안 동일 IP 주소에서 대규모 로그인 시도 등 이상행위가 발생하는 경우 이를 탐지·차단할 수 있는 대책을 마련하지 않았고, 응용 프로그램 인터페이스(API) 응답값에 포함된 개인정보를 보호하기 위한 암호화 조치를 소홀히 하는 등 고객정보 보호를 위한 충분한 조치를 하지 않았다. 또한, 최초 유출 사고('22.10월) 이후에도 재발방지 대책을 충분히 마련하지 않아 동일한 방식으로 유출 사고('23.11월)가 또다시 발생하였다.

- 이에 개인정보위는 멤버십 서비스 사업자 A에 개인정보 보호법에 따른 안전조치 의무를 소홀히 하고 유출 통지·신고를 지연한 사실에 대하여 과징금 14억 7,700만 원과 과태료 720만 원을 부과하고, 사업자 홈페이지에 처분받은 사실을 공표하도록 명령하였다.

**조사·처분 의의**

일반적인 해킹 사고와 다른 타 사이트에서 유출된 계정 정보를 이용한 크리덴셜 스터핑 공격에 대해서도 서비스 제공자의 능동적인 방어 책임을 명확히 규정하여 기업의 보안 의무 범위를 확장하였다. 아울러, 사고가 이미 발생한 경우에도 동일 수법에 대한 재발 방지 대책을 면밀히 수립하여 유출사고가 재발 하지 않도록 엄중한 처분을 내렸다.

### 라. 보안 취약점을 노린 해킹 공격에 의한 개인정보 유출 제재

**사건의 개요**

신원 미상의 해커가 제조사 A가 운영 중인 가상 사설망 장비의 취약점을 악용하여 가상 사설망에 로그인 후, 사내망에 접근하여 내부 파일서버에 저장되어 있던 73,975명의 개인정보(주주정보, 임직원 정보, 협력사 직원 정보 등)를 외부로 유출하고, 내부 파일 서버 등에 랜섬웨어 파일을 배포 및 감염시켰다.

**조사결과 및 시정조치**

제조사 A가 사용하던 가상 사설망 장비의 취약점이 발견되어 보안 업데이트가 필요하다는 사실이 해당 장비 제조사 및 한국인터넷진흥원 등에 의해 공지되었음('23.6.12.)에도, 제조사 A는 해킹 사고 당시까지 취약점*에 대한 조치를 하지 않은 사실이 확인되었다.

* 인증되지 않은 공격자가 웹에 노출된 가상 사설망 인터페이스를 통해 취약한 장치에서 원격으로 코드를 실행할 수 있는 취약점

- 아울러, 해커가 유출을 진행하던 '23.10.11.~10.29. 기간 동안 제조사 A의 일부 시스템은 백신 동작 이력이 존재하지 않는 등, 악성 프로그램 방지·치료 기능 운영 소홀 사실도 확인되었다.
- 개인정보위는 안전조치 의무 위반으로 개인정보가 유출된 제조사 A에 과징금 3억 4,300만 원을 부과하고, 처분받은 사실을 운영 중인 홈페이지에 공표할 것을 명령하였다.

**조사·처분 의의**

제조사 A의 사례처럼 가상 사설망 등 보안 장비의 취약점을 악용한 해킹 및 제조업 등을 중심으로 랜섬웨어 감염 및 개인정보 유출이 증가하고 있는 만큼, 개인정보를 처리하는 사업 자들은 운영 중인 서비스에 대한 취약점 점검 및 보안 업데이트를 실시하여야 하고, 개인정보 DB 등 주요 파일을 별도 백업·보관하는 등 각별한 주의가 필요하다.



### 마. SQL 인젝션 해킹 공격에 의한 개인정보 유출 제재

**사건의 개요**

해커는 '24. 7.~8. 법률 서비스 사업자 A의 관리자 계정정보(아이디, 비밀번호)를 획득한 뒤, 내부 인트라넷 시스템에 접속하여, '사건 관리 리스트 웹페이지'에서 43,892건의 사건관리 리스트(의뢰인명, 소송상대자, 사건명, 사건번호 등)를 내려받아 유출하였다.

- 소송자료가 저장된 디렉토리에서는 185,047건(약 1.59TB 규모)의 소송관련 문서를 내려받아 유출하였다. 해당 문서는 소장, 판결문, 진술조서, 증거서류, 금융거래내역서, 범죄일람표, 신분증, 진단서, 통장 사본 등으로, 문서에는 이름, 연락처, 주소, 주민등록번호, 계좌번호, 범죄 정보, 건강에 관한 민감정보 등의 개인정보가 다수 포함되어 있었다.

**조사결과 및 시정조치**

법률 서비스 사업자 A는 내부 시스템에 대한 접속 권한을 IP 주소 등으로 제한하지 않는 등, 개인정보 유출시도를 탐지·대응하기 위한 접근 통제 조치를 소홀히 하였다. 외부에서 시스템 접속 시 안전한 인증수단 없이 아이디와 비밀번호만으로 접속이 가능하도록 운영했고, SQL 인젝션 공격을 예방하기 위해 웹페이지에 대한 취약점 점검·조치를 소홀히 하였던 것으로 밝혀졌다.

- 주민등록번호, 계좌번호, 비밀번호 등을 암호화하지 않고 저장 하였으며, 보관 중인 개인정보의 보유기간이나 구체적인 파기 기준도 마련하지 않은 사실을 확인하였다.
- 이에 개인정보위는 법률 서비스 사업자 A의 위반사항을 매우 중대한 위반으로 판단하고, 과징금 5억 2,300만 원과 과태료 600만 원을 부과하고, 위반사항에 대한 시정명령 및 처분받은 사실을 운영 중인 홈페이지에 공표할 것을 명령하였다.

**조사·처분 의의**

개인정보위는 법률 서비스 사업자 A가 소송 대리를 위해 민감한 개인정보를 대량으로 보관·관리하는 점을 고려하여, 보다 엄격한 개인정보 보호 및 관리 체계를 갖추고, 관련 법령을 준수하여야 함에도, 다수의 안전조치의무를 위반하여 대규모의 개인정보 유출로 이어진 점을 지적했다. 아울러, 유출사고 재발 방지를 위한 안전조치 강화, 주요 개인정보 암호화 및 명확한 파기 지침 수립, 사고 대응 체계 정립 등 전반적인 개인정보 보호 및 관리 체계를 강화할 것을 요구하고 향후 이행 여부를 점검하도록 하였다.

### 바. 웹 셸 해킹 공격에 의한 개인정보 유출 제재

**사건의 개요**

신원미상의 해커는 '24년 6월 여행사 A가 운영 중인 웹페이지의 파일 업로드 취약점을 이용해 다수의 웹 셸 파일을 업로드하였고, 해당 파일에 존재하는 악성코드를 실행하여 고객 정보 데이터 베이스(DB)에서 회원·비회원 306만여 명의 개인정보를 탈취하였다.

**조사결과 및 시정조치**

여행사 A는 해커의 웹 셸 공격을 예방하기 위해 업로드된 파일에 대한 파일 확장자 검증 및 실행권한 제한 등 보안 취약점 점검·조치를 취해야 했지만 이를 소홀히 했다. 아울러, 개인정보 유출 시도를 탐지·대응하기 위한 접근통제 조치도 미흡했던 것으로 밝혀졌다.

- 또한, 여행사 A는 '13년 3월부터 수집한 비회원 316만여 건(중복 포함)의 개인정보를 보유기간이 경과되었음에도 파기하지 않고 보유하고 있어, 대규모 유출에 영향을 끼쳤다. '24년 7월 개인정보 유출 사실을 인지했음에도 정당한 사유 없이 2개월이 지난 '24년 9월에야 개인정보 유출사실을 통지한 것도 개인정보 침해 우려를 키우게 된 한 원인으로 보인다.
- 이에, 개인정보위는 여행사 A에 과징금 7억 4,700만 원과 과태료 1,020만 원을 부과하고, 사업자 홈페이지에 처분받은 사실을 공표 하도록 명령하였다. 이와 함께 향후 유출등지 지연 행위 등이 재발 하지 않도록 내부 개인정보 보호 관리체계 개선을 요구하였다.

**조사·처분 의의**

주요 원인이 된 웹 셸 공격은 잘 알려진 웹 취약점 공격이지만 데이터베이스(DB)에 접근이 가능하여 피해 정도가 큰 특징을 가지고 있는 만큼, 개인정보 탈취 위험에 대한 사전 탐지·차단 정책 강화 및 파일 업로드 취약점 점검·조치 등 각별한 주의와 예방이 필요하다.

- 또한, 여행사 등 대규모 개인정보 처리 사업자는 보유기간 경과, 처리목적 달성 등 수집한 개인정보가 불필요하게 되었을 때는 이를 지체없이 파기하여 혹시 모를 개인정보 유출사고 발생 시 피해 규모를 최소화해야 한다. 아울러, 정보주체의 2차 피해 예방 등을 위해 개인정보 유출 사실 인지 즉시 통지가 이루어질 수 있도록 내부 개인정보 보호 체계를 정비할 것을 요구하고 이행 결과를 점검하도록 하였다.



2 * 2 5
개인정보
유출 신고 동향 및
조사·처분 사례

개인정보보호위원회 KISA 한국인터넷진흥원