개인정보보호위원회 KISA

Information

Countermeasure

Controls

개인정보 관련 판례 및 사례 소개

CONTENTS

Ⅰ 개인정보 유출 등에 대한 사업자의 책임

1. 행정처분

- 과태료/과징금
- 시정명령
- 징계권고/고발
- 위반행위 공표

행정처분

- 상당인과관계X (유출사고)
- **위탁자책임**
  처리자책임 vs. 관리 · 감독책임
- **수탁자책임**
  과징금 부과 가능, 과태료는 적용 안됨

[현행법] 수탁자에 과징금 부과 조항(제64조의2) 준용(제26조 제8항)

- **과태료**: 행정처분의 일종. 행정법규 위반의 정도가 비교적 경미하여 간접적으로 행정 목적 달성에 장애를 줄 위험성이 있는 정도의 단순한 의무 태만에 대해 과하는 금전벌
- **과징금**: 행정처분의 일종. 경제적 이익 환수 과징금은 불법행위로 얻어진 경제적 이익을 확실히 환수하기 위해 도입. (1)경제적 이익 환수 (2)영업정지 대체 (3)순수한 금전적 제재(과태료와 비슷하지만 금액이 큼)
- (참고) 유럽연합 개인정보보호법(GDPR) 제83조의 **Administrative fine**은 벌금? **과징금**?

1. 행정처분

개인정보에 대한 안전성 확보조치 위반

과징금(행정처분)

제64조의2(과징금의 부과)

① 보호위원회는 다음 각 호의 어느 하나에 해당하는 경우에는 해당 개인정보처리자에게 전체 매출액의 100분의 3을 초과하지 아니하는 범위에서 과징금을 부과할 수 있다.

5. 개인정보처리자가 처리하는 개인정보가 분실·도난·유출·위조·변조·훼손된 경우. 다만, 개인정보가 분실·도난·유출·위조·변조·훼손되지 아니하도록 개인정보처리자가 제29조(제26조제8항에 따라 준용되는 경우를 포함한다)에 따른 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다.

② 보호위원회는 제1항에 따른 과징금을 부과하려는 경우 전체 매출액에서 위반행위와 관련이 없는 매출액을 제외한 매출액을 기준으로 과징금을 산정한다

vs.

과태료(행정처분)

제75조(과태료)

② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다.

5. 23조 제2항·제24조 제3항·제25조 제6항(제25조의2 제4항에 따라 준용되는 경우 포함) ·제28조의4 제1항·제29조(제26조 제8항에 따라 준용되는 경우 포함)를 위반하여 안전성 확보에 필요한 조치를 하지 아니한 자

제76조(과태료에 관한 규정 적용의 특례) 제75조의 과태료에 관한 규정을 적용할 때 제64조의2에 따라 과징금을 부과한 행위에 대하여는 과태료를 부과할 수 없다.

2. 형사책임

제74조(양벌규정)

① 법인의 대표자나 법인 또는 개인의 대리인, 사용인, 그 밖의 종업원이 그 법인 또는 개인의 업무에 관하여 제70조에 해당하는 위반행위를 하면 그 **행위자를 벌하는 외에 그 법인 또는 개인을 7천만원 이하의 벌금에 처한다.** 다만, 법인 또는 개인이 그 위반행위를 방지하기 위하여 해당 업무에 관하여 상당한 주의와 감독을 게을리하지 아니한 경우에는 그러하지 아니하다.

3. 민사책임

- 과실책임주의
- 입증책임전환
- 법정손해배상
- 징벌손해배상

민사 책임

- 상당인과관계
- 사용자 책임(연대책임)
  위탁자+수탁자
- 단체소송
  - 침해 금지 · 중지
  - 조정전치주의

Ⅱ

해킹으로 인한 개인정보 유출 사례

1. 클라우드에서 2차 인증 미적용 사례(개인정보위 2022.3.23. 의결, 제2022-005-014호)

사건 개요 | 주요 쟁점 | 의결 내용 | 의결 결과

피심인 C
(호주 기업)

개발자가 실수로 **테스트 목적으로 생성한**
Buildkite 프로그램의 소스코드에
개인정보처리시스템에 접근할 수 있는
AWS 루트 Access Key를 저장

크리덴셜 스터핑 공격

2019.5.18

신원 미상자

Buildkite의 취약점을 이용해
크리덴셜 스터핑 공격 시도

크리덴셜 스터핑(Credential Stuffing)
다른 곳에서 유출된 아이디 · 비밀번호 등의 로그인 정보를 무작위로 대입하여 로그인하는 수법

1. 클라우드에서 2차 인증 미적용 사례(개인정보위 2022.3.23. 의결, 제2022-005-014호)

사건 개요 | 주요 쟁점 | 의결 내용 | 의결 결과

2019.5.24 Buildkite 접속에 성공하여 시스템 접속 정보 및 AWS 루트 Access Key를 탈취하고 이용자 데이터베이스에 무단 접속

⇒ 한국 이용자들의 개인정보(계정정보, 이름, 국가, 이메일 주소, 도시, 결제정보 등)가 유출

2019.5.25 시스템 모니터링 과정 중 침입 사실을 탐지,
같은 날 개인정보 유출 사실을 인지하고 즉시 웹사이트에 유출 사실을 영어로 공지

2019.5.27 한국어 이용자에게 **유출 통지**

2019.6.13 개인정보보호 포털에 개인정보 **유출 신고**함

1. 클라우드에서 2차 인증 미적용 사례(개인정보위 2022.3.23. 의결, 제2022-005-014호)

사건 개요 | **주요 쟁점** | 의결 내용 | 의결 결과

개인정보처리시스템 구축·운영을 위해 클라우드서비스 이용 시 2차 인증을 적용해야 하는지 여부

Buildkite 프로그램의 소스코드에 개인정보처리시스템에 접근할 수 있는 AWS Access Key를 저장한 것이 기준 제4조 제9항 위반에 해당하는지 여부

19. 5. 25. 유출 사실을 인지하고 **18일 만**인 '19. 6. 13.에 개인정보보호 포털에 신고한 것이 신고 지연에 해당하는지 여부

(심결외 이슈) 국내 정보통신서비스 이용자에게 서비스를 제공하는 **해외 사업자**에게 과태료 부과 가능 여부

1. 클라우드에서 2차 인증 미적용 사례(개인정보위 2022.3.23. 의결, 제2022-005-014호)

사건 개요 | 주요 쟁점 | **의결 내용** | 의결 결과

1 2차 인증 위반 여부

구 개인정보의 기술적 관리적 보호조치 기준('15.5.19.) 제4조 제4항은 정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 **개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하여야 한다**고 규정

➡ 외부에서 개인정보처리시스템에 접속하려는 경우 안전한 인증수단을 적용하여야 하나 피심인이 이를 적용하지 않아 개인정보가 유출된 것은 정보통신망법 제28조 제1항 위반에 해당

피심인 C (호주 기업)

개발자등이 Buildkite에 접속할 때 모든 계정에 대해서 ID/PW와 추가적 2차 인증을 의무화하였으나, **Buildkite를 API로 접속하는 경우** 2차 인증을 우회할 수 있는 취약점이 존재하였다고 소명

1. 클라우드에서 2차 인증 미적용 사례(개인정보위 2022.3.23. 의결, 제2022-005-014호)

2 유출신고 지연 책임

구 정보통신망법 제27조의3 제1항은 정보통신서비스 제공자등은 개인정보의 유출 사실을 안 때 지체 없이 한국인터넷진흥원에 신고하여야 하며 정당한 사유 없이 그 사실을 안 때부터 **24시간을 경과하여 신고해서는 아니 된다**고 규정

➠ 개인정보 유출 사실을 안 때에는 지체 없이(24시간) 이내 한국인터넷진흥원에 신고하여야 하나 **피심인이 24시간을 경과하여 신고한** 피심인의 행위는 정보통신망법 제27조의3 제1항 위반에 해당

1. 클라우드에서 2차 인증 미적용 사례(개인정보위 2022.3.23. 의결, 제2022-005-014호)

사건 개요 | 주요 쟁점 | 의결 내용 | 의결 결과

3 공개·유출 방지 조치의무 위반

개인정보위는 피심인이 Buildkite 프로그램의 소스코드에 개인정보처리시스템에 접근할 수 있는 AWS Access Key를 저장한 것에 대하여 **보호조치 기준 제4조 제9항 위반은 적용하지 않음**

➠ 개인정보위는 **AWS S3 버킷에 저장된 일부 파일의 접근통제를 공개로 설정**하여 운영한 것과 관련하여 보호조치 기준 제4조 제9항을 적용, 과징금/과태료 부과 및 형사 고발 등의 조치를 취한 바 있음(소개팅앱 G사, T사)

1. 클라우드에서 2차 인증 미적용 사례(개인정보위 2022.3.23. 의결, 제2022-005-014호)

사건 개요 | 주요 쟁점 | 의결 내용 | **의결 결과**

1. **과태료 1,000만 원**
2. **시정명령(재발방지조치)**
3. **행정처분 결과 공표**

✓ **유사 사례(Z사(아일랜드), F사(미국), H사(한국), G사(한국), T사(한국) 등**

AWS Access Key를 직원 등이 실수로 소스코드에 저장해 두거나 해커가 미상의 방법으로 탈취, 2차 인증 미적용 등 다수 발생

1. 클라우드에서 2차 인증 미적용 사례(개인정보위 2022.3.23. 의결, 제2022-005-014호)

사건 개요 | 주요 쟁점 | 의결 내용 | **의결 결과**

구 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제27조의3(개인정보 유출등의 통지·신고)

① 정보통신서비스 제공자등은 개인정보의 분실·도난·유출(이하 "유출등"이라 한다) 사실을 안 때에는 지체 없이 다음 각 호의 모든 사항을 해당 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다. 다만, 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다.

③ 정보통신서비스 제공자등은 제1항 본문 및 단서에 따른 정당한 사유를 방송통신위원회에 소명하여야 한다.

구 개인정보의 기술적 관리적 보호조치 기준 제4조(접근통제)

④ 정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용하여야 한다.

⑨ 정보통신서비스 제공자등은 처리중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.

2. SQL 인젝션 공격으로 인한 해킹 사례(방통위, 2017. 9. 8.)

사건 개요 | 주요 쟁점 | 의결 내용 | 의결 결과

피심인 W사

여행숙박앱 서비스
정보통신서비스 제공자

2017. 3. SQL Injection 공격을 받아 숙박예약정보, 제휴점정보, 회원정보 등 약 99만여 건 유출

해커는 먼저 여행숙박앱의 '마케팅센터 웹페이지'에 SQL 인젝션 공격을 통해 DB 구조를 파악하고, 이를 통해 DB에 저장되어 있던 고객센터 상담직원용 관리자페이지를 관리하는 관리자의 인증 세션 값(Session ID) 탈취

탈취한 관리자 인증 세션 값을 도용하여 외부에 노출된 '서비스 관리자 웹페이지'를 관리자 권한으로 우회하여 인증·접속(세션 변조 공격)

관리자페이지의 '엑셀 다운로드' 기능을 이용하여 예약정보, 제휴점정보, 회원정보 등의 숙박 예약정보 총990,584건을 유출

해커 일당은 W사측에 수십억 원 요구, 공갈 과정에서 피해자들에게 문자 발송, 2017. 6. 1. 해커 일당 경찰에 검거

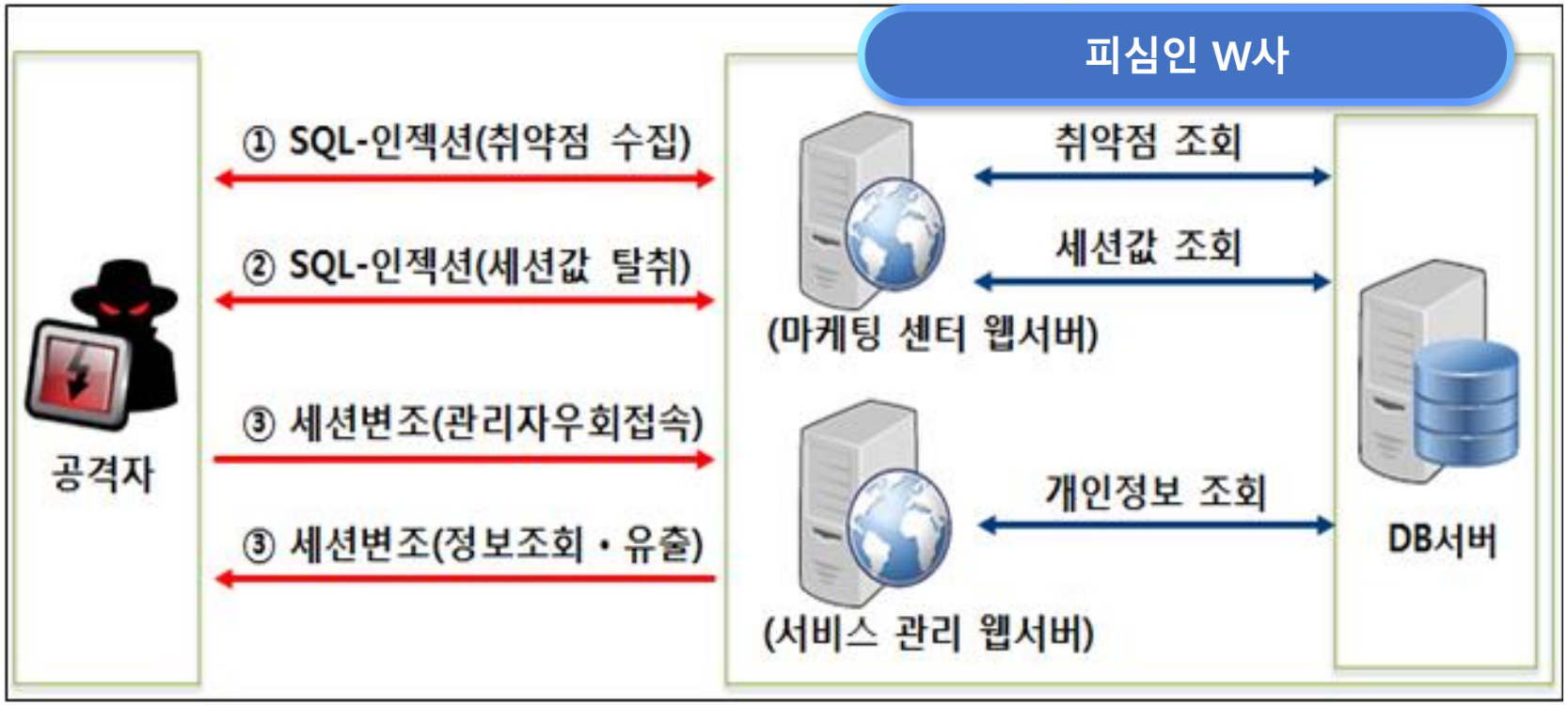
※ Session ID : 웹 통신에서 접속 또는 로그인한 사용자를 구분하기 위해 서버에서 할당하는 사용자 고유 식별값

SQL 인젝션(Structured Query Language Injection)

데이터베이스에 대한 질의 값(SQL 구문)을 조작하여 정상적인 자료 이외에 해커가 원하는 자료까지 데이터베이스로 부터 유출 가능한 공격기법

2. SQL 인젝션 공격으로 인한 해킹 사례(방통위, 2017. 9. 8.)

사건 개요 | 주요 쟁점 | 의결 내용 | 의결 결과



- 발생일: 2017.3.7~3.17
- 유출 정보
  - ✓ 개인정보 99만 명, 340만 건
  - ✓ 예약정보: 숙박일수, 예약일시, 예약자, 휴대폰번호, 결제방법, 금액 등
- 적용법규: (옛) 정보통신망법 제28조 제1항 및 시행령, 하위 고시
- 규제기관: 방송통신위원회

출처: 민관합동조사단 발표, 2017.4.26.

2. SQL 인젝션 공격으로 인한 해킹 사례(방통위, 2017. 9. 8.)

사건 개요 | 주요 쟁점 | 의결 내용 | 의결 결과

- 다수의 상담원에게 파일 다운로드 권한을 부여한 것이 접근권한 제한에 위반한 것인지 여부
- 조직개편 및 인사이동 후 관리자 페이지의 접근권한을 미변경한 것이 접근권한 변경 및 말소 의무 위반에 해당하는지 여부
- 전문 서비스 외에 OS에서 제공하는 기본방화벽 및 오픈소스만 이용한 침입탐지가 접근통제 의무 위반에 해당하는지 여부
- 시큐어 코딩 미수행 및 마케팅센터 웹페이지 취약점 점검 미수행이 홈페이지 등 개인정보 유출 방지 의무 미조치에 해당하는지 여부
- (심결외 이슈) 조치 의무 위반과 개인정보 유출 사이에 인과관계가 인정되어야 하는지 여부(과태료 vs. 과징금 vs. 형사처벌)

2. SQL 인젝션 공격으로 인한 해킹 사례(방통위, 2017. 9. 8.)

사건 개요 | 주요 쟁점 | **의결 내용** | 의결 결과

Y 홈페이지에는 비정상적인 DB 질의에 대한 검증절차가 없어 SQL 인젝션 공격에 취약한 웹페이지가 존재하였으며,

탈취된 관리자 세션값을 통한 우회접속(세션변조 공격)을 탐지·차단하는 체계가 없는 것으로 확인됨

1. 고객센터 상담직원 무려 35명에게 고객정보 파일 다운로드 권한을 부여함으로써(그 중 한 명의 권한을 해커가 도용), 필요한 범위를 넘어 접근권한을 과다 부여	기준 §4 ① 위반
2. 조직개편에 따른 인사이동 후 관리자페이지 접근권한 미변경(그 중 한 명의 권한을 해커가 도용)	기준 §4 ② 위반
3. OS에서 제공하는 기본방화벽(iptable) 및 오픈소스(Snort)를 이용한 침입탐지 이외에 전문기업이 제공하는 시스템 미설치, 외부에서 파일 다운로드 시도 등 시스템에 접속한 IP 주소 재분석 미실시	기준 §4 ⑤ 위반

2. SQL 인젝션 공격으로 인한 해킹 사례(방통위, 2017. 9. 8.)

사건 개요 | 주요 쟁점 | **의결 내용** | 의결 결과

Y 홈페이지에는 비정상적인 DB 질의에 대한 검증절차가 없어 SQL 인젝션 공격에 취약한 웹페이지가 존재하였으며, 탈취된 관리자 세션값을 통한 우회접속(세션변조 공격)을 탐지·차단하는 체계가 없는 것으로 확인됨

4. SQL 인젝션 공격 등을 방지할 수 있는 시큐어 코딩 미수행 및 마케팅센터 웹페이지 취약점 점검 미수행	기준 §4 ⑨ 위반
5. 관리자페이지에서 내보내는 개인정보 엑셀파일에 비밀번호를 설정하지 않은 행위	기준 §6 ④ 위반

2. SQL 인젝션 공격으로 인한 해킹 사례(방통위, 2017. 9. 8.)

사건 개요 | 주요 쟁점 | 의결 내용 | 의결 결과

1. 과징금 3억100만원
2. 과태료 2,500만원

※ 기타 진행사항

- 형사 – 법인 및 전 '실질적' 개인정보관리책임자 벌금 2000만 원(2심, 2022. 10.)
- 민사 – 원고 312명, 인당 최대 40만 원 배상(1심, 2022. 9.)

2. SQL 인젝션 공격으로 인한 해킹 사례(방통위, 2017. 9. 8.)

사건 개요 | 주요 쟁점 | 의결 내용 | **의결 결과**

위 반 내 용	관련 규정
▪ **개인정보 보호조치 (접근통제)**	법 §28①제2호
- 개인정보처리시스템 접근권한 최소부여 원칙 위반 ※ 고객센터 상담직원 35명에게 개인정보처리시스템 파일다운로드 권한 부여 (상담사 권한을 해커가 도용)	시행령§15②제1호, 고시 §4①
- 취급자 인사이동 시 지체없이 개인정보처리시스템 접근권한 변경하여야 하나 이를 위반 (이들 직원의 최고관리자 권한을 해커가 도용)	시행령§15②제1호, 고시 §4②
- 취급자가 외부에서 인터넷을 통해 개인정보처리시스템 접속 시 안전한 인증수단(OTP 등) 미적용	시행령§15②제1호, 고시 §4④
- 개인정보 다운로드·파기 가능한 취급자의 컴퓨터 망분리 미적용	시행령§15②제3호, 고시 §4⑥

- 정보통신망법 제28조 제1항
- 시행령 제15조
- 개인정보의 기술적·관리적 보호조치 기준(방송통신위원회 고시)

2. SQL 인젝션 공격으로 인한 해킹 사례(방통위, 2017. 9. 8.)

사건 개요 | 주요 쟁점 | 의결 내용 | **의결 결과**

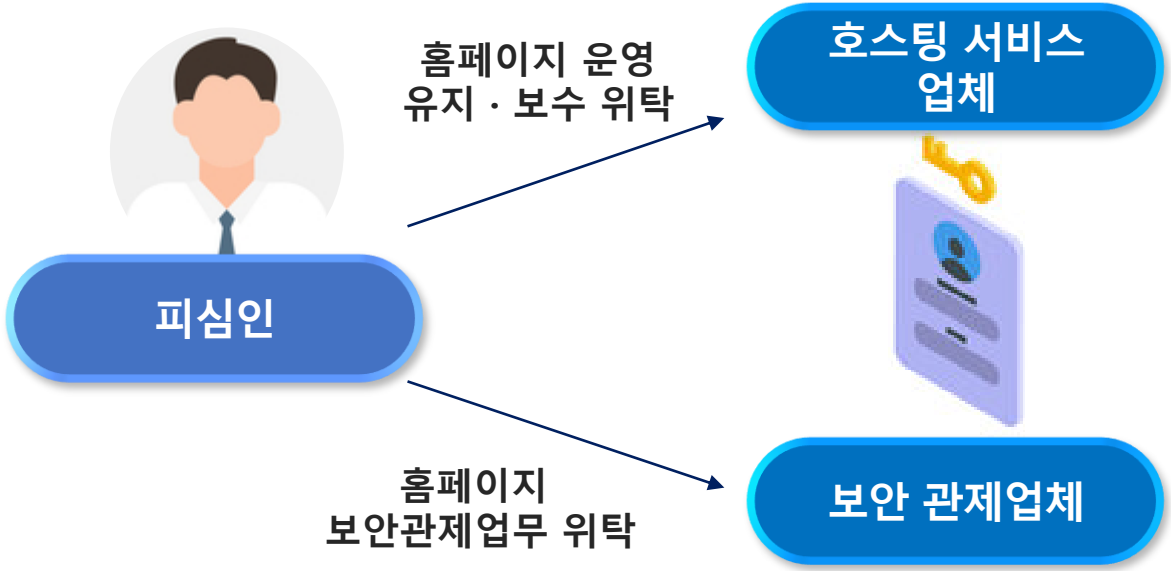
위 반 내 용	관련 규정
•**개인정보 보호조치 (접근통제)**	법 §28①제2호
- 웹페이지 취약점 점검 미수행 (해당 웹페이지 해커 공격)	시행령§15②제5호, 고시 §4⑨
•**개인정보 보호조치 (접속기록)**	법 §28①제3호
- 개인정보취급자의 접속기록 보관(6개월), 정기 정검(월 1회 이상) 의무 위반	시행령§15③, 고시 §5①④
•**개인정보 보호조치 (암호화)**	법 §28①제4호
- 관리자페이지 접근권한 변경이력의 관리자 비밀번호 평문 저장	시행령§15④제1호, 고시 §6①
- 직원 개인용PC에 이용자개인정보(20,462건) 미암호화 저장	시행령§15④제4호, 고시 §6④

- 정보통신망법 제28조 제1항
- 시행령 제15조
- 개인정보의 기술적·관리적 보호조치 기준(방송통신위원회 고시)

출처: 방통위 보도자료, "방통위, ㈜위드이노베이션 개인정보 유출사고 엄정 제재", 2017.9.8

3. 웹쉘 공격으로 인한 해킹 사례(개인정보위 2022.3.23. 의결, 제2022-005-020호)

사건 개요 | 주요 쟁점 | 의결 내용 | 의결 결과



웹쉘(Web Shell) 공격
웹셸은 시스템에 명령을 내릴 수 있는 코드로서, 간단한 서버 스크립트로 만드는 방법이 널리 사용되고 있으며 웹서버 취약점을 통해 스크립트가 업로드되면 해커들은 보안 시스템을 피해서 별도 인증 없이 시스템에 접속 가능하여 원격으로 해당 웹서버를 조종할 수 있음

20.10.17~'21.4.20

다수의 외부 IP가 동일한 행위로 접근한 이력이 발견되었으며, 보안관제업체가 모니터링 중 웹쉘 탐지

2020.8.13

신원미상자(중국 IP)가 알 수 없는 경로로 웹쉘 파일을 업로드

2021.7.3

신원 미상자가 **홍콩 IP**로 홈페이지 취약점을 이용해 **웹쉘(Web Shell) 공격**을 통해 서버 접근

⇒ 홈페이지 관리자페이지에 접속하여 회원 정보를 조회하고, **관리자페이지의 메일보내기 기능을 이용하여 회원들에게 스팸메일 전송**

3. 웹쉘 공격으로 인한 해킹 사례(개인정보위 2022.3.23. 의결, 제2022-005-020호)

사건 개요 | **주요 쟁점** | 의결 내용 | 의결 결과

홈페이지 관리자페이지가 개인정보처리시스템에 해당하는지 여부

인가받지 않은 외부 IP주소 등의 접근 탐지, 제한, 차단 등을 하지 아니한 것이 접근통제조치 위반에 해당하는지 여부

(심결외 이슈) 홈페이지 유지 · 보수 · 보안관제 등을 위탁받은 보안관제 업체 또는 호스팅 서비스 업체의 책임 범위

3. 웹쉘 공격으로 인한 해킹 사례(개인정보위 2022.3.23. 의결, 제2022-005-020호)

사건 개요 | 주요 쟁점 | **의결 내용** | 의결 결과

1 **호스팅 서비스 업체가 제공하는 솔루션 기능을 통해 개인정보처리시스템에 대한 접속 권한을 특정 IP주소로 일부 제한하는 조치는 하였으나, 인가하지 않은 외부 IP주소의 적절한 차단 조치는 하지 않음**

- 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하지 아니한 것은 **안전성 확보조치 기준 제6조 제1항 위반**

2 **개인정보처리시스템에 접속한 IP주소를 분석해 불법적인 개인정보 유출 시도를 탐지하고 접근 제한·차단 등 적절한 대응조치를 하지 않음**

- 시스템 운영 정책에 IP주소 등을 분석하여 불법적인 개인정보 유출 시도의 탐지 및 대응 기능을 포함하지 않은 것은 **안전성 확보조치 기준 제6조 제1항 위반**

3. 웹쉘 공격으로 인한 해킹 사례(개인정보위 2022.3.23. 의결, 제2022-005-020호)

사건 개요 | 주요 쟁점 | 의결 내용 | **의결 결과**

처분내용 : 과태료 300만원

개인정보의 안전성 확보조치 기준 제6조(접근통제)

① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol) 주소 등으로 제한하여 인가받지 않은 접근을 제한

2. 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응

Ⅲ 개인정보취급자 부주의로 인한 유출 사례

1. 수탁자 부주의로 회원명단 홈페이지 게시판 공개(개인정보위 2022.3.23. 의결, 제2022-005-026호)

사건 개요
주요 쟁점
의결 내용
의결 결과

피심인은 지역 의사들로 구성된 의사회로 전임 회장 임기만료에 따른 제39대 선거 실시를 위해
선거인단의 개인정보를 수집 · 보관

2021.1.25

피심인의 홈페이지 유지·보수 업무를 위탁받은 관리업체가 **홈페이지 게시판에 대한 테스트 작업 과정에서**
위 선거인명단 엑셀파일(유출파일)을 실수로 다른 지역 의사회 홈페이지 게시판에 게시

회원들의 면허번호, 성명, 소속의사회명, 주소, 우편번호, 근무처명, 직장전화번호, 팩스번호, 생년월일, 휴대전화번호 등이 포함된 개인정보 유출

1. 수탁자 부주의로 회원명단 홈페이지 게시판 공개(개인정보위 2022.3.23. 의결, 제2022-005-026호)

사건 개요

주요 쟁점

의결 내용

의결 결과

실수로 홈페이지 게시판에 선거인단명단을 게시한 것이 안전성 확보조치 기준 제6조(접근통제) 제3항 위반에 해당하는지 여부

(심결외 이슈) 수탁사의 실수로 인한 개인정보 유출에 대해서 **위탁사에게 과태료 처분**이 가능한지 여부
- 위탁자의 책임은 관리·감독책임인가 자기책임인가?

(심결외 이슈) 홈페이지 유지 · 보수 업무를 위탁받은 **관리업체의 직원이 개인정보취급자에 해당**하는지 여부

개인정보 처리 위탁 범위 내에서 발생한 수탁자의 개인정보보호법규 위반에 따른 사고는 책임이 위탁자에 있음

1. 수탁자 부주의로 회원명단 홈페이지 게시판 공개(개인정보위 2022.3.23. 의결, 제2022-005-026호)

**수탁사의 업무 실수로 홈페이지의 게시판에 엑셀파일을 잘못 첨부하였고,
그 사실을 알고 해당 게시물이 삭제 조치('21.8.26)될 때까지 개인정보가 노출된 상태로 다운로드된 것이 확인됨**

➡ 개인정보처리자는 취급 중인 개인정보가 인터넷 **홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여** 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근통제 등에 관한 조치를 하여야 함(**안전성 확보조치 기준 제6조 제3항 위반**)

1. 수탁자 부주의로 회원명단 홈페이지 게시판 공개(개인정보위 2022.3.23. 의결, 제2022-005-026호)

처분내용 : 과태료 300만원

개인정보의 안전성 확보조치 기준 제6조(접근통제)

③ 개인정보처리자는 취급중인 개인정보가 **인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록** 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 한다.

2. 개발자 과실로 인한 관리자페이지 접근 통제 누락(개인정보위 2022. 3.23. 의결, 제2022-005-027호)

사건 개요
주요 쟁점
의결 내용
의결 결과

집합투자업체로 고객사를 대상으로 연금상품 판매에 관한 온라인 세미나 참가 신청을 받기 위해
성명, 휴대전화번호, 이메일 주소, 직장명 등의 개인정보 수집

2021.9.23 온라인 세미나 신청자로부터 인터넷 검색엔진(구글)에서 본인의 개인정보가 검색되고 있다는 전화를 받음

접속 로그기록 확인 결과 검색엔진(구글)이 최초 접근일('21.7.26)부터 차단 조치 확인일('21.9.26)까지 약 2개월간 총 257회(다운로드, 성공 152회/ 실패 105회) 외부 접근이 허용된 사실 확인

홈페이지 관리자페이지에 대한 접근 통제가 이루어지지 않아 온라인 토론회(세미나) 참가자 2,932명의 명단이 인터넷에서 검색

2. 개발자 과실로 인한 관리자페이지 접근 통제 누락(개인정보위 2022. 3.23. 의결, 제2022-005-027호)

사건 개요
주요 쟁점
의결 내용
의결 결과

웹페이지 개발자 과실로 일부 관리자페이지에 대한 접근 통제를 누락한 것이 홈페이지등 개인정보 유출 방지 위반에 해당 여부

(실결외 이슈) 개발업체 실수로 인한 개인정보 유출에 대해서 **본사에게 과태료 처분**이 가능한지 여부 (관리·감독 책임 vs. 자기책임)

(심결외 이슈) 웹페이지 개발 업무를 위탁받은 **개발업체의 직원이 개인정보취급자에 해**당하는지 여부

- 개인정보취급자: 임직원, 파견근로자, 시간제근로자 등 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 자(법 제28조 제1항)

2. 개발자 과실로 인한 관리자페이지 접근 통제 누락(개인정보위 2022. 3.23. 의결, 제2022-005-027호)

사건 개요
주요 쟁점
의결 내용
의결 결과

웹페이지 개발 과정에서 개발자의 실수로 일부 관리자페이지가 비인가자의 접근 통제가 허용된 상태(세션값 누락)로 설정되어 있었으며, 검색엔진(구글 IP)의 정보수집(크롤링)을 통해 개인정보가 검색되었던 것으로 확인

개인정보처리자는 취급중인 개인정보가 **인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출**되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 함**(안전성 확보조치 기준 제6조 제3항 위반)**

2. 개발자 과실로 인한 관리자페이지 접근 통제 누락(개인정보위 2022. 3.23. 의결, 제2022-005-027호)

처분내용 : 과태료 300만원

개인정보의 안전성 확보조치 기준 제6조(접근통제)

③ 개인정보처리자는 취급중인 개인정보가 **인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록** 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 한다.

Ⅳ 최근 쟁점이 된 주요 판례 (해킹 관련 주요 관심 판례)

1. SQL 인젝션 공격으로 인한 해킹 사례

사건 개요

원고 P사
(온라인 커뮤니티 사이트)

주요 수입원 : 사이트의 배너와 텍스트 광고
전체 회원 수 : 1,956,835명(2015.9.12 기준)

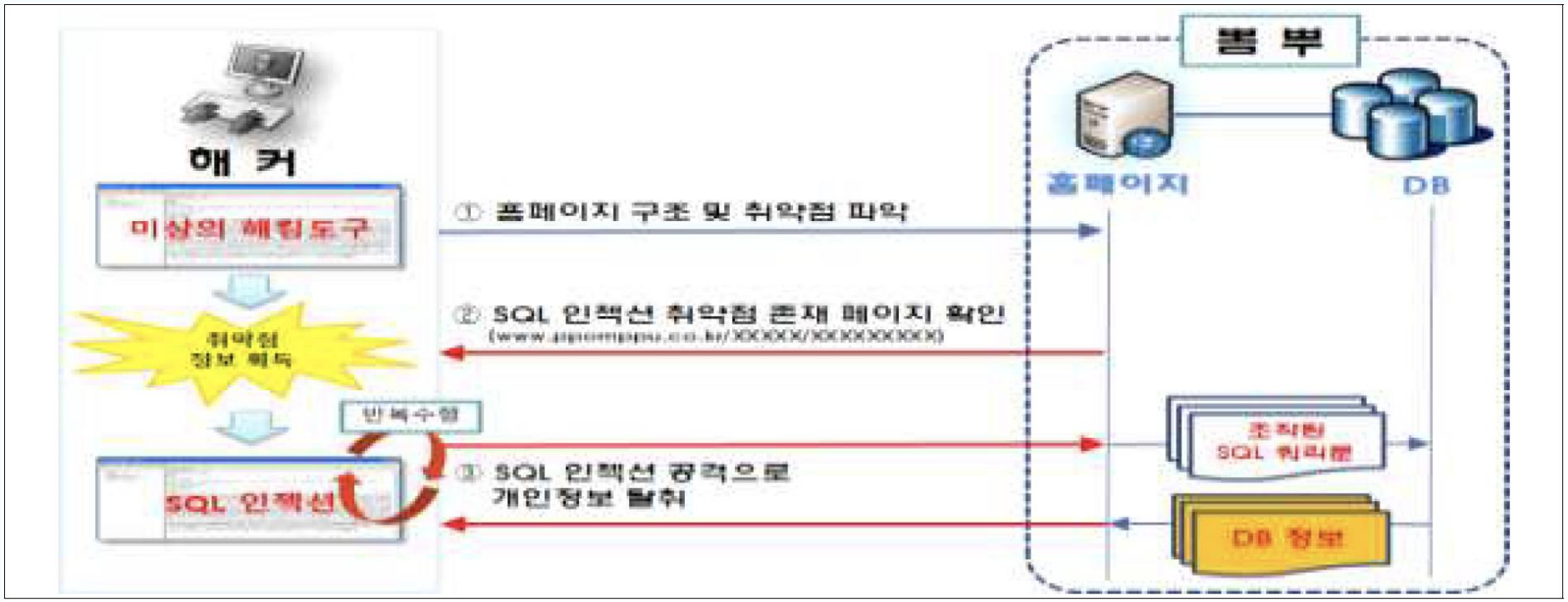
신원 불상 해커

1차 2015. 9. 10 19:11~20:40 / 2015. 9. 10 22:22~2015. 9. 11 01:13까지 2차례에 걸쳐 취약한 웹 페이지 등을 파악하기 위하여 무작위로 인터넷 사이트에 접속 시도

2차 **로또 당첨번호 알림 게시판의 취약점을 발견**하고 이를 대상으로 2015. 9. 11 01:04~02:10까지 SQL 인젝션 공격 감행

데이터베이스(DB) 서버에 저장되어 있던 원고의 회원정보 약 195만 건을 유출 (회원의 아이디, 암호화된 비밀번호, 생년월일, 이메일주소, 닉네임, 암호화된 장터 비밀번호, 가입일, 회원점수 등)

1. SQL 인젝션 공격으로 인한 해킹 사례



1. SQL 인젝션 공격으로 인한 해킹 사례 - 민사소송

서울중앙지방법원 2018나84531

정보통신망법 제32조의2(법정손해배상의 청구)에 따른 손해배상책임은 정보통신서비스 제공자의 정보통신망법상 개인정보보호 의무 위반 사실과 개인정보 유출 사실만 있으면 성립하는 법정손해배상책임으로, 이용자가 별도로 손해를 증명할 필요가 없다.

피고(회사)는, 위 규정이 손해액에 대한 증명책임을 완화할 것일 뿐 손해 발생에 대한 증명 책임까지 면제한 것은 아니므로 여전히 현실적인 손해가 발생하였다는 증명이 있어야 한다고 주장하나, 그렇게 볼 수 없음은 법문상 명백하다.

나아가 살펴보더라도, 뒤에서 보는 바와 같이 원고가 이 사건 사고로 정신적 고통을 겪었다는 점을 충분히 인정할 수 있으므로, 피고의 주장은 받아들이지 않는다.

방송통신위원회도 피고에게 고의 중과실이 있다고 보아 피고의 개인정보 보호조치 위반이 '매우 중대한 위반행위'에 해당한다고 평가하고... (하략)

이 사건 사고로 원고의 개인정보인 아이디, 암호화된 비밀번호, 생년월일... 유출됨으로써 원고로서는... (동일한 아이디, 비밀번호를 사용한 다른 사이트의) 아이디 등을 바꾸어야 하는 불편을 겪게 되었다. 이로 말미암아 원고가 정신적 고통을 받았으리라는 점은 경험칙상 충분히 인정할 수 있다.

다만 개인정보가 신원확인에 직접 관련된 민감한 정보라고 보기는 어렵고, 명의도용 등 추가적인 법익침해가 발생한 것으로 보이지는 않는다.

- 1심과 같은 20만 원 및 지연손해금 지급 판결(2심)

출처: 서울중앙지방법원 항소심 판결문 (2018나84531, 2019.05.15)

1. SQL 인젝션 공격으로 인한 해킹 사례 - 민사소송

서울중앙지방법원 2018나84531

[옛 정보통신망법] 제32조의2(법정손해배상의 청구)

① 이용자는 다음 각 호의 모두에 해당하는 경우에는 대통령령으로 정하는 기간 내에 정보통신서비스 제공자등에게 제32조에 따른 손해배상을 청구하는 대신 300만원 이하의 범위에서 상당한 금액을 손해액으로 하여 배상을 청구할 수 있다. 이 경우 해당 정보통신서비스 제공자등은 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.

1. 정보통신서비스 제공자등이 고의 또는 과실로 이 장(제4장)의 규정을 위반한 경우
2. 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우

② 법원은 제1항에 따른 청구가 있는 경우에 변론 전체의 취지와 증거조사의 결과를 고려하여 제1항의 범위에서 상당한 손해액을 인정할 수 있다.

③ 제32조에 따라 손해배상을 청구한 이용자는 사실심의 변론이 종결되기 전까지 그 청구를 제1항에 따른 청구로 변경할 수 있다.

[개인정보보호법] 제39조의2(법정손해배상의 청구)

① 제39조제1항에도 불구하고 정보주체는 개인정보처리자의 고의 또는 과실로 인하여 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우에는 300만원 이하의 범위에서 상당한 금액을 손해액으로 하여 배상을 청구할 수 있다. 이 경우 해당 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.

② 법원은 제1항에 따른 청구가 있는 경우에 변론 전체의 취지와 증거조사의 결과를 고려하여 제1항의 범위에서 상당한 손해액을 인정할 수 있다.

③ 제39조에 따라 손해배상을 청구한 정보주체는 사실심(事實審)의 변론이 종결되기 전까지 그 청구를 제1항에 따른 청구로 변경할 수 있다.

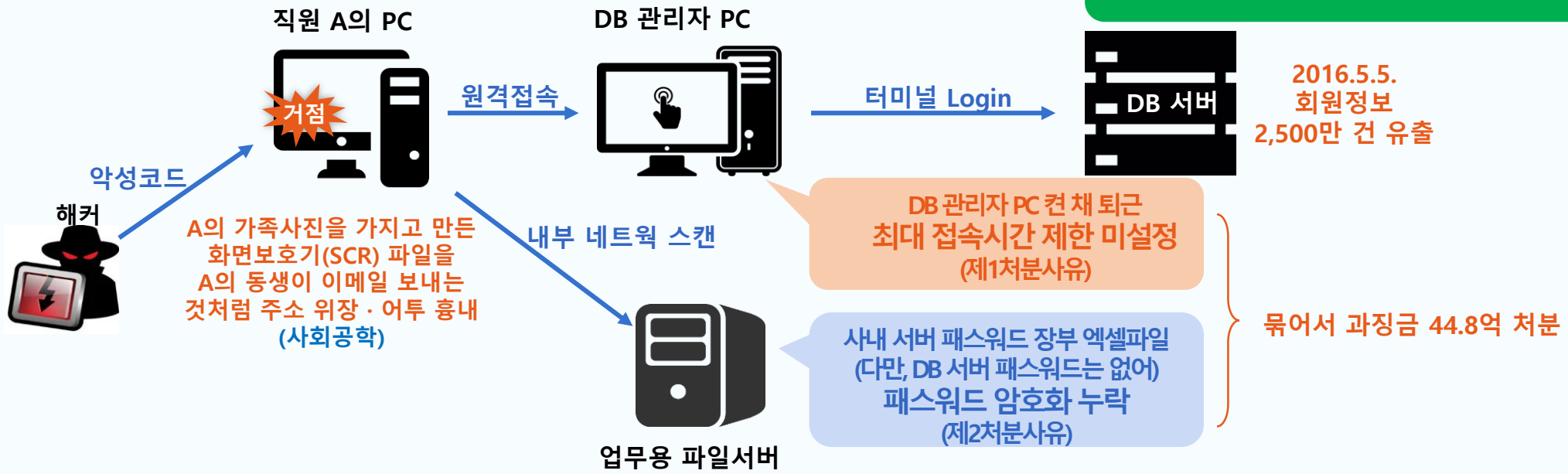
2. 지능형 표적 공격(APT 공격)에 의한 해킹 사례

서울행정법원 2018.7.5. 선고 2017구합53156,
서울고법 2019.11.1. 2018누56291, 대법원 심리불속행 확정

사건 개요

* APT: Advanced Persistent Threat

I사가 방통위의 행정처분에 불복하여 제기한 과징금 등의 취소를 위한 행정소송



- 방통위는 민관합동조사단을 구성하여 I사 개인정보처리시스템 등에 남아있는 접속기록 등을 토대로 정보통신망법 위반 여부 확인을 위한 개인정보 처리·운영 실태 조사
- 방통위는 2016.12.6 I사에 대하여 구 개인정보의 기술적·관리적 보호조치 기준 제4조 제10항(최대 접속시간 제한 적용) 및 제6조 제1항(비밀번호 암호화)을 위반하였다고 판단하고 시정명령, 시정명령을 받은 사실의 공표, 교육 및 대책 수립 후 보고, **과징금 44억 8,000만 원, 과태료 2,500만 원** 등을 명하는 행정처분

  >> 이에 원고는 고시 위반행위와 개인정보 유출 사이에 인과관계가 없다는 취지로 다투며 과징금 처분의 취소를 구하는 행정소송 제기

2. 지능형 표적 공격(APT 공격)에 의한 해킹 사례

서울행정법원 2018.7.5. 선고 2017구합53156,
서울고법 2019.11.1. 2018누56291, 대법원 심리불속행 확정

사건 개요

개인정보 유출 경과

- ✓ 해커는 I사 전산실 직원 甲을 대상으로 삼아 불상의 방법(스피어 피싱 방법으로 추정)으로 甲의 개인용 네이버 이메일 계정 ID/PW 탈취

> **스피어 피싱(Spear Phishing)**
> 불특정 다수의 개인정보를 빼내기 위한 공격이 아니라 특정인의 정보를 캐내기 위한 공격 방법. 목표물을 특정한 다음 목표물에 관련된 정보를 수집해 이를 바탕으로 맞춤형 해킹을 시도. 특정 개인 또는 회사에 악성코드를 감염시킬 것을 목표로 한다면 그 개인 또는 회사에 관한 정보를 수집해 친구, 가족, 거래처 등을 가장하여 이메일을 발송함

- ✓ 이후 甲의 메일함을 분석하여 甲이 동생과 메일을 주고받은 것을 보고 동생이 쓰는 말투와 이모티콘 등 습득
- ✓ 해커는 甲에게 스피어 피싱 메일을 보내면서 甲의 동생이 보내는 것처럼 **발신자의 이메일 주소를 변조**하고 동생의 어투까지 흉내
- ✓ 해당 이메일의 제목은 "잊지못할 상도동!"으로 되어 있고 甲의 가족사진으로 만든 **화면보호기 파일(SCR 파일)로 위장한 악성코드 첨부**
- ✓ 화면보호기 파일로 속은 甲은 해커가 보낸 첨부파일을 열어보았고, 그 결과 甲의 PC가 악성코드에 감염되어 해커가 甲의 PC에 대한 제어권 확보
- ✓ 甲은 이상함을 느끼고 사내 백신을 이용하여 악성코드 감염 여부를 점검하였으나 해당 백신은 악성코드를 감지하지 못함 (확장자가 SCR 또는 EXE로 된 파일은 백신으로 탐지 곤란)

2. 지능형 표적 공격(APT 공격)에 의한 해킹 사례

서울행정법원 2018.7.5. 선고 2017구합53156,
서울고법 2019.11.1. 2018누56291, 대법원 심리불속행 확정

사건 개요

개인정보 유출 경과

- ✓ 甲의 PC에 대한 제어권을 획득한 해커는 다수의 단말기에 악성코드를 확산시키고 내부정보 수집
- ✓ 해커는 보안이 취약한 HQ DB 관리자 乙의 PC를 발견하고 미상의 방법으로 비밀번호를 탈취하여 사내 네트워크 공유를 통해 원격으로 乙의 PC에 접속해 제어권 획득
- ✓ 접속 당시 乙의 PC에는 망분리 프로그램과 서버 접속 터미널이 로그아웃되지 않은 채 그대로 띄워져 DB 서버와의 접속이 유지되고 있었음
- ✓ I사는 **HQ DB서버에는 2시간 경과시 자동적으로 연결이 종료되는 기능을 적용하고 있다고 주장하였으나 이를 입증하지 못함**
- ✓ 해커는 망분리 프로그램 및 서버 접속 터미널의 ID/PW를 추가로 탈취하는 수고를 덜 수 있었고,
DB 서버에서 **외부 IP로 총 20회에 걸쳐** I사 회원들의 개인정보 2,540만 건(2,050만 명)을 유출(제1 처분 사유, 제4조 제10항)
- ✓ 한편, 甲의 PC에는 **내부 서버 및 업무용 PC 등에 접속할 수 있는 공용관리계정의 비밀번호가 평문으로 저장**되어 있었고,
업무용 파일공유 서버(NAS 서버)의 패스워드관리대장 엑셀 파일에는 암호가 설정되어 있기는 하나, 엑셀 파일의 비밀번호가 평문으로 저장되어 있어 실질적으로 패스워드관리대장 엑셀 파일이 암호화되어 있다고 보기는 어려움(제2 처분 사유, 기준 제6조 제1항)
- ✓ 다만, 엑셀 파일에는 개인정보가 유출된 DB 서버의 접속 패스워드는 기재되어 있지 않아 고객정보 유출의 직접적인 원인을 제공한 것은 아님

2. 지능형 표적 공격(APT 공격)에 의한 해킹 사례

서울행정법원 2018.7.5. 선고 2017구합53156,
서울고법 2019.11.1. 2018누56291, 대법원 심리불속행 확정

주요 쟁점

개인정보유출과 **인과관계가 없는 의무위반 행위**(Idle timeout 미적용, 비밀번호 암호화 저장 의무 위반)에 대하여 과징금 처분이 가능한지 여부

Idle timeout을 설정하지 아니한 것이 이건 **개인정보 유출과 인과관계**가 있는지 여부, 개인정보 유출을 방지할 수 있었는지 여부

2. 지능형 표적 공격(APT 공격)에 의한 해킹 사례

서울행정법원 2018.7.5. 선고 2017구합53156,
서울고법 2019.11.1. 2018누56291, 대법원 심리불속행 확정

법원 판단 1심 법원의 판단

- 개정 전의 법률(2015.5.19. 개정)은 **'개인정보보호조치를 하지 아니하여 이용자의 개인정보를 분실·도난, 누출·변조 또는 훼손한 경우'**라고 규정하여 명시적으로 인과관계를 요구하고 있는 반면,
  개정된 정보통신망법은 **'이용자의 개인정보를 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손한 경우로서 개인정보보호조치를 하지 아니한 경우'**라고 규정하여 이와 다른 규정 형식을 취하였음을 알 수 있고, 이용자의 개인정보를 분실·도난·유출·위조·변조 또는 훼손되었더라도 정보통신서비스제공자 등이 정보통신망법 제28조 제1항 제2호부터 제5호까지의 조치를 하였다면 과징금을 부과하지 않겠다는 취지로 보이며, 별도로 **이용자 개인정보의 분실·도난·유출·위조·변조 또는 훼손과 정보통신망법 제28조 제1항 제2호부터 제5호까지의 조치를 하지 아니한 행위 사이에 인과관계가 요구된다고 보이지는 아니한다.**

- 이 사건 제1, 2처분사유와 이 사건 개인정보 유출 간에 인과관계가 요구된다고 하더라도, 원고가 앞서 본 바와 같이 최대 접속시간 제한 등의 조치를 취하지 않아 이 사건 해커는 망분리 프로그램과 서버 접근제어 프로그램의 접속이 종료되지 않은 乙의 PC를 통하여 HQ DB 서버에 접속하였는바, 이 사건 해커가 위 프로그램의 암호를 입력하지 않고도 HQ DB 서버에 접속하였으므로 **이 사건 제1처분 사유와 이 사건 개인정보 유출 간에 상당한 인과관계도 존재하는 것으로 보인다.**

  ➡ **I사 청구(주장) 기각 (방통위 주장 수용)**

2. 지능형 표적 공격(APT 공격)에 의한 해킹 사례

서울행정법원 2018.7.5. 선고 2017구합53156,
서울고법 2019.11.1. 2018누56291, 대법원 심리불속행 확정

법원 판단 2심 법원의 판단

- 위와 같은 규정의 형식과 내용, 개정이유 등을 종합해 보면, 위 개정 이후에는 이용자 **개인정보의 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손과 정보통신망법 제28조 제1항 제2호부터 제5호까지의 조치를 하지 아니한 행위 사이의 인과관계는 요구되지 않는다**고 할 것이다.
- 헌법상 자기책임의 원칙에는 특수한 입법목적을 달성하기 위해 일정한 예외가 설정될 수 있다.
  개인정보 누출사고가 지속적으로 발생하고 있고, 특히 정보통신망을 통한 개인정보 유출은 그 피해 정도가 지대하며,
  유출된 개인정보는 2차 피해 발생 가능성도 높아 사전에 개인정보가 유출되지 못하도록 법적·제도적 장치를 마련할 필요성이 있는
  점에 비추어 볼 때, **위와 같이 인과관계가 요구되지 않는 것으로 해석하는 것이 헌법상 자기책임 원칙에 반한다고 할 수 없다.**

  ➡ **I사의 항소 기각(방통위 주장 수용)**

2. 지능형 표적 공격(APT 공격)에 의한 해킹 사례

서울행정법원 2018.7.5. 선고 2017구합53156,
서울고법 2019.11.1. 2018누56291, 대법원 심리불속행 확정

판결 결과

1심 법원	I사 청구 기각(I사 패소, 방통위 승소)
2심 법원	I사 항소 기각(I사 패소, 방통위 승소)
서울중앙지방검찰청	무혐의 처분 (I사의 개인정보보호책임자 및 개인정보관리책임자)

2. 지능형 표적 공격(APT 공격)에 의한 해킹 사례

서울행정법원 2018.7.5. 선고 2017구합53156,
서울고법 2019.11.1. 2018누56291, 대법원 심리불속행 확정

I사 개인정보 보호책임자와 개인정보 관리책임자에 대한 고소 사건

판결 결과

서울중앙지방검찰청 무혐의 처분 사유(증거불충분)(2017. 8. 14.)

피의자인 개인정보보호책임자 丙과 개인정보관리책임자 丁이 고객의 개인정보에 대하여 불법적인 접근을 차단하기 위한 기술적·관리적 조치를 다하지 못하였다는 고소 사건과 관련하여, 당시 피의자들이 도입한 망분리 프로그램 실행 환경에서 개인정보취급자의 단말기에서 외부 인터넷 접속이 가능하였다는 점에서 실질적인 망분리가 이루어지지 아니한 것으로 판단되나, **2013년 KISA로부터 ISMS 인증을 받았고 2015년에는 PIMS 인증도 받은 바 피의자들의 개인정보 보호조치 위반에 대한 고의가 없었다는 점이 인정**되며, 丙과 丁의 범의를 인정할 증거가 없는 한 I사의 피의사실도 인정할 증거가 없다.

2. 지능형 표적 공격(APT 공격)에 의한 해킹 사례

서울행정법원 2018.7.5. 선고 2017구합53156,
서울고법 2019.11.1. 2018누56291, 대법원 심리불속행 확정

관련 법령

구 개인정보의 기술적·관리적 보호조치 기준 제4조(접근통제)

⑩ 정보통신서비스 제공자등은 개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 최대 접속시간 제한 등의 조치를 취하여야 한다.

구 개인정보의 기술적·관리적 보호조치 기준 제6조(개인정보의 암호화)

① 정보통신서비스 제공자등은 비밀번호는 복호화 되지 아니하도록 **일방향 암호화하여 저장**한다.

개인정보보호위원회 KISA

감사합니다

※ 본 교재의 저작권은 한국인터넷진흥원에 있으며 교육 목적 외 상업적 등의 목적으로 재편집 사용을 금합니다.