G사 사건을 비롯한 개정 개인정보 보호법 적용 사례들의 함의와 기업·기관의 대응방안

BACK TO BASIC

2024. 6. 4.

변호사 김진환
kim.jh@whaleandsun.com

WHALE & SUN
SPIRIT OF CONSULTATION

김 진 환 변호사

법률사무소 웨일앤썬 대표
㈜지키다 대표

주요 경력

- 서울지방법원 및 남부지원 판사(1998-2001)
- 김앤장 법률사무소 변호사(2001-2021) : Privacy & Data Security 그룹 리더
- 대법원 산하 사법연수원 외래교수(2000-2013)
- 미국 뉴욕주 변호사(2006-현재)
- 개인정보 보호법 해설서 자문위원(2016) 및 집필위원(2020)
- 개인정보보호위원회 고문변호사(2012-2020, 2022-2023)
- 개인정보분쟁조정위원회 위원(2022-2023)
- 개인정보보호위원회 비상임 위원 (2023-현재)
- 개인정보국외이전전문위원회 위원장(2024-현재)

주요 담당 업무

- 옥션, 네이트·싸이월드, 현대카드, 넥슨, KT 1·2차, 카드3사, 빗썸 등 해킹 및 정보유출 사건 등 조사 및 형사 대응, 민형사 행정소송 수행
- 국내외 약 200여개 기업에 대한 자문 및 개인정보 컨설팅·프로젝트 수행

주요 저술

- 전자거래법 (공저, 사법연수원, 2000-2013)
- 상법주석 (공저, 사법행정학회, 2001)
- The Privacy, Data Protection and Cybersecurity Law Review (Edition1): Korea Chapter (공저, Law Business Research, 2014)
- 온주(온라인 주석서) 정보통신망법, 전자문서법, 전자서명법 (공저, 로앤비, 2017, 2019, 2023)
- 개인정보보호법 (공저, 박영사, 2024)

주요 수상

- 개인정보보호 대상 : 국회 행정안전위원회 위원장상(2012), 개인정보 : 안전행정부 장관 표창(2013)
- Leading Lawyer : IT, Telecommunication & Media(Asia Law & Practce, 2014, 2016, 2018)
- Leading Individual, Asialaw Profiles(Euromoney, 2017)
- 개인정보 : 국민포장(2022)

목차

- 개정 개인정보 보호법의 주요 개정사항
- 개정 개인정보 보호법 적용 사례 분석
- 기업·기관의 Back-to-Basic 대응방안

개정 개인정보 보호법의 주요 개정사항

개정 개인정보 보호법의 주요 개정사항 1

- **이동형 영상정보처리기기 운영 기준 마련**

  ① 고정형 vs. 이동형 구별; ② 불빛, 소리, 안내판 등으로 명확히 표시 후 거부의사 부재시

- **동의를 포함한 개인정보의 수집·이용 방법 개선**

  ① 목적 내 제공에 정당한 이익 추가; ② 필수 동의(제) 폐지; ③ 마케팅 “구분” 동의

- **개인정보의 국외 이전 다양화 및 국외 이전 중지명령 신설**

  ① 인증 획득 경우와 인정제 추가; ② 국외 이전 중지명령과 재이전 규제

- **개인정보 처리방침의 평가 및 개선권고**

  ① 기재 사항 누락 여부; ② 이해하기 쉽게 작성; ③ 쉽게 확인할 수 있도록 공개

- **개인정보의 전송 요구권 신설**

  ① 일반적 마이데이터제도; ② 시행 시기 미정; ③ 수범자의 범위 등 주요 사항 시행령 위임

- **자동화된 결정에 대한 정보주체의 권리 신설**

  ① AI 포함 완전히 자동화된 시스템; ② 권리/의무에 중대한 영향; ③ 거부권, 설명요구권

개정 개인정보 보호법의 주요 개정사항 2

- **개인정보 보호책임자의 업무·자격요건 보완 및 독립성 보장 신설**

  ① 미지정시 사업주/대표자; ② 독립적 업무수행 보장; ③ 자격요건 강화

- **징벌적 손해배상액 및 보장 보험 등 가입 의무 확대**

  ① 5배 손해까지 배상; ② OSP 외 일반 개인정보처리자에 보험 및 적립금제 확대

- **개인정보 분쟁조정제도 개선**

  ① 의무적 조정제도 대폭 확대; ② 조정위의 사실조사권 인정; ③ 이의 부제기시 조정 수락 의제 신설

- **과징금 규정 정비**

  ① 과징금 부과 대상 대폭 확대; ② 과징금 부과 기준 확대(전체 매출액 vs. 관련 매출액)

- **개인정보 보호수준 평가제 실시**

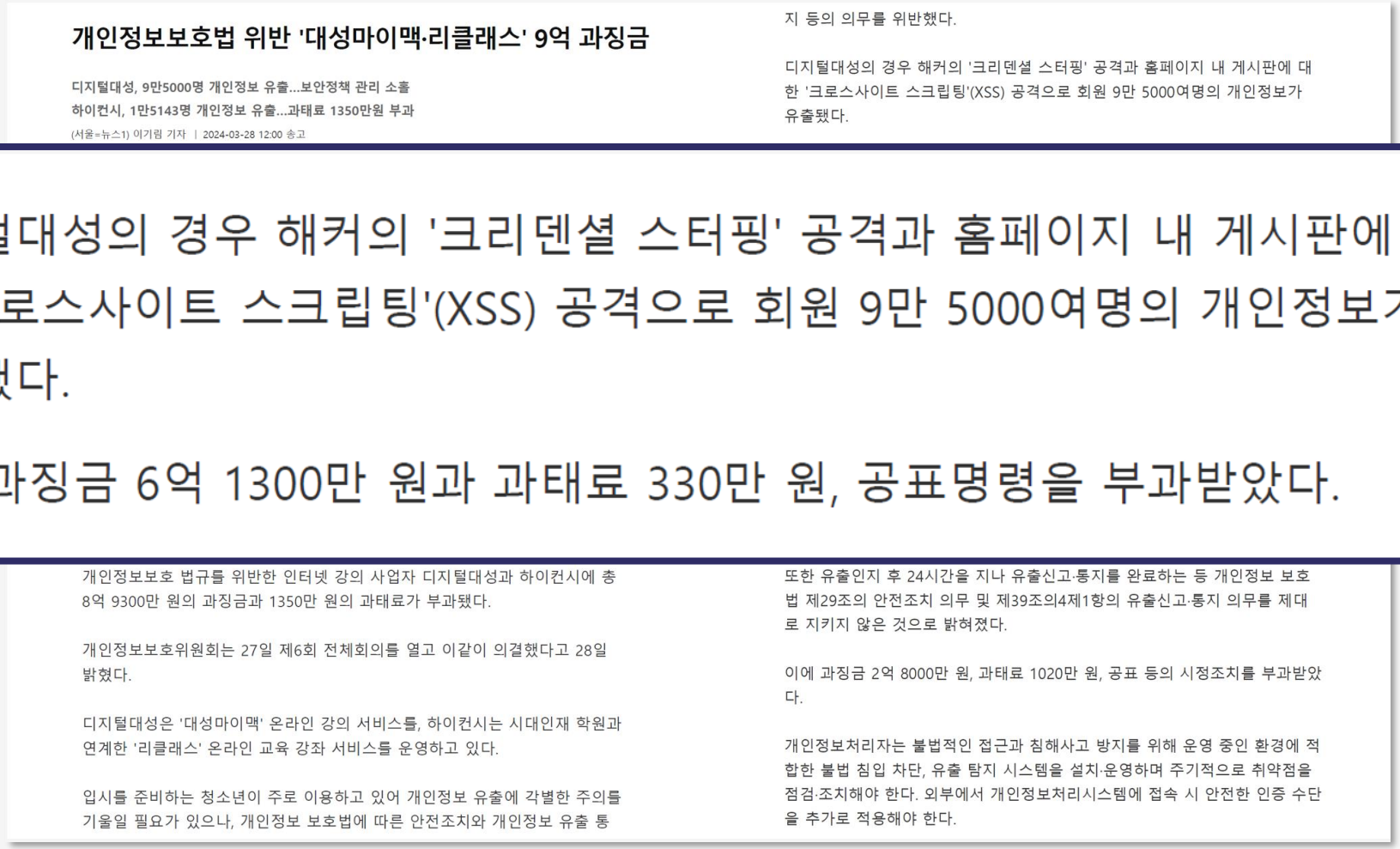
  ① 1,600여개 공공기관으로 확대; ②정량 : 정성 = 60 : 40

- **수탁자에 대한 제재 및 처벌 규정 추가**

  ① 과태료 및 과징금에 명문화; ② 형사처벌 규정에 명문화

개정 개인정보보호법 적용 사례 분석

개정법 적용 사례 1: 디지털 대성 사건



개인정보보호법 위반 '대성마이맥·리클래스' 9억 과징금

디지털대성, 9만5000명 개인정보 유출…보안정책 관리 소홀
하이컨시, 1만5143명 개인정보 유출…과태료 1350만원 부과

(서울=뉴스1) 이기림 기자 | 2024-03-28 12:00 송고

개인정보보호 법규를 위반한 인터넷 강의 사업자 디지털대성과 하이컨시에 총 8억 9300만 원의 과징금과 1350만 원의 과태료가 부과됐다.

개인정보보호위원회는 27일 제6회 전체회의를 열고 이같이 의결했다고 28일 밝혔다.

디지털대성은 '대성마이맥' 온라인 강의 서비스를, 하이컨시는 시대인재 학원과 연계한 '리클래스' 온라인 교육 강좌 서비스를 운영하고 있다.

입시를 준비하는 청소년이 주로 이용하고 있어 개인정보 유출에 각별한 주의를 기울일 필요가 있으나, 개인정보 보호법에 따른 안전조치와 개인정보 유출 통지 등의 의무를 위반했다.

디지털대성의 경우 해커의 '크리덴셜 스터핑' 공격과 홈페이지 내 게시판에 대한 '크로스사이트 스크립팅'(XSS) 공격으로 회원 9만 5000여명의 개인정보가 유출됐다.

또한 유출인지 후 24시간을 지나 유출신고·통지를 완료하는 등 개인정보 보호법 제29조의 안전조치 의무 및 제39조의4제1항의 유출신고·통지 의무를 제대로 지키지 않은 것으로 밝혀졌다.

이에 과징금 2억 8000만 원, 과태료 1020만 원, 공표 등의 시정조치를 부과받았다.

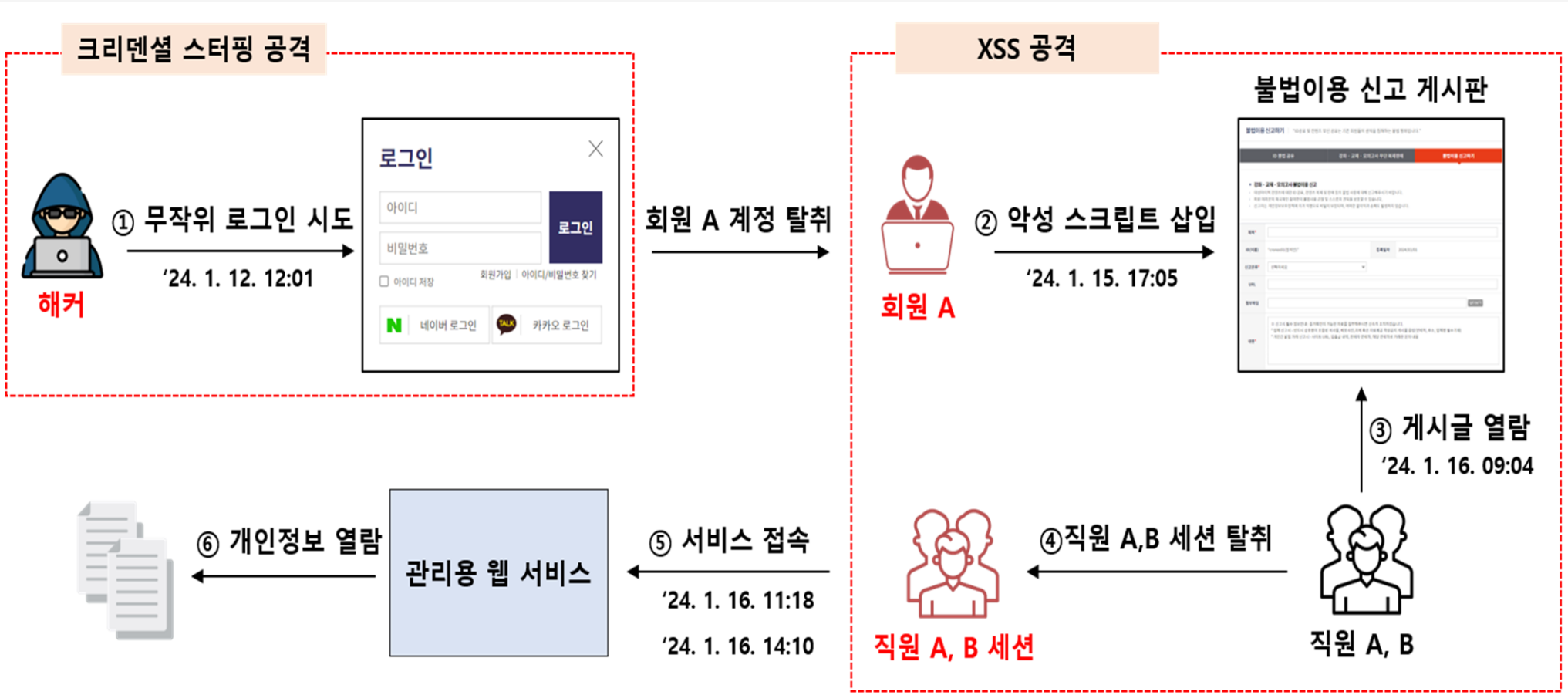
개인정보처리자는 불법적인 접근과 침해사고 방지를 위해 운영 중인 환경에 적합한 불법 침입 차단, 유출 탐지 시스템을 설치·운영하며 주기적으로 취약점을 점검·조치해야 한다. 외부에서 개인정보처리시스템에 접속 시 안전한 인증 수단을 추가로 적용해야 한다.

디지털대성의 경우 해커의 '크리덴셜 스터핑' 공격과 홈페이지 내 게시판에 대한 '크로스사이트 스크립팅'(XSS) 공격으로 회원 9만 5000여명의 개인정보가 유출됐다.

이에 과징금 6억 1300만 원과 과태료 330만 원, 공표명령을 부과받았다.

WHALE & SUN
SPIRIT OF CONSULTATION

개정법 적용 사례 1: 디지털 대성 사건



개인정보 보호위원회 보도자료

개정법 적용 사례 1: 디지털 대성 사건

- **사건 개요**
  - 2024년 1월 발생
  - 직원 25명, 회원 95,171명의 개인정보 유출
  - IPS·웹방화벽 등 도입하였으나, 실제 정책을 적용하지 않은 채 운영하여 공격 미탐지 및 미차단
  - 72시간 경과 후 유출 통지 실시

- **개인정보 보호위원회의 판단 및 제재**
  - 법률, 시행령 및 안전성 확보조치 기준 고시 위반
  - 강사 교재, EBS 교재 판매 및 갤럭시 버즈 이벤트 매출도 관련 매출액에 포함
  - 과징금 6억 1,300만원, 과태료 330만원, 시정명령 및 공표명령

개정법 적용 사례 2: 골프존 사건

개인정보 유출된 골프존, 과징금 75억원·과태료 540만원 부과 받아

골프존, 개인정보 유출사고로 과징금 75억원 · 과태료 540만원 · 시정·공표명령

골프존, 개인정보 유출사고로 과징금 75억원 · 과태료 540만원 · 시정·공표명령

기업의 책임성 강화 위해 개정 개인정보보호법 규정 적용 첫 사례

안전조치의무 · 주민등록번호 처리제한 및 개인정보 파기 위반

[이미지=개인정보보호위원회]

공표명령은 개인정보 보호법 개정(2023년 9월 15일)으로 신설된 처분 규정으로, 사업자 홈페이지 등에 과징금 · 과태료 등의 처분받은 사실을 공표하는 제도다.

골프존은 지난해 11월 해커로부터 랜섬웨어 공격을 받았다. 이 과정에서 해커는 골프존 직원들의 가상 사설망 계정정보를 탈취해 업무망 내 파일서버에 원격접속(2023년 11월 22일)하고, 파일서버에 저장된 파일을 외부로 유출(2023년 11월 22일~23일)한 후 다크웹에 공개했다.

탈취된 계정정보 중에는 서버 관리자 계정도 포함됐으며, 윈도우의 공유폴더 기능을 이용, 임직원들의 PC에 파일서버의 폴더가 생성·공유됐다. 이로 인해 업무망 내 파일서버에 보관되어 있던 약 221만명 이상의 서비스 이용자 및 임직원의 개인정보(이름, 전화번호, 이메일, 생년월일, 아이디 등)가 유출됐고, 일부의 경우 주민등록번호(5,831명)와 계좌번호(1,647명)도 유출됐다.

일서버에서 외부로 파일을 유출할 수 있었다.

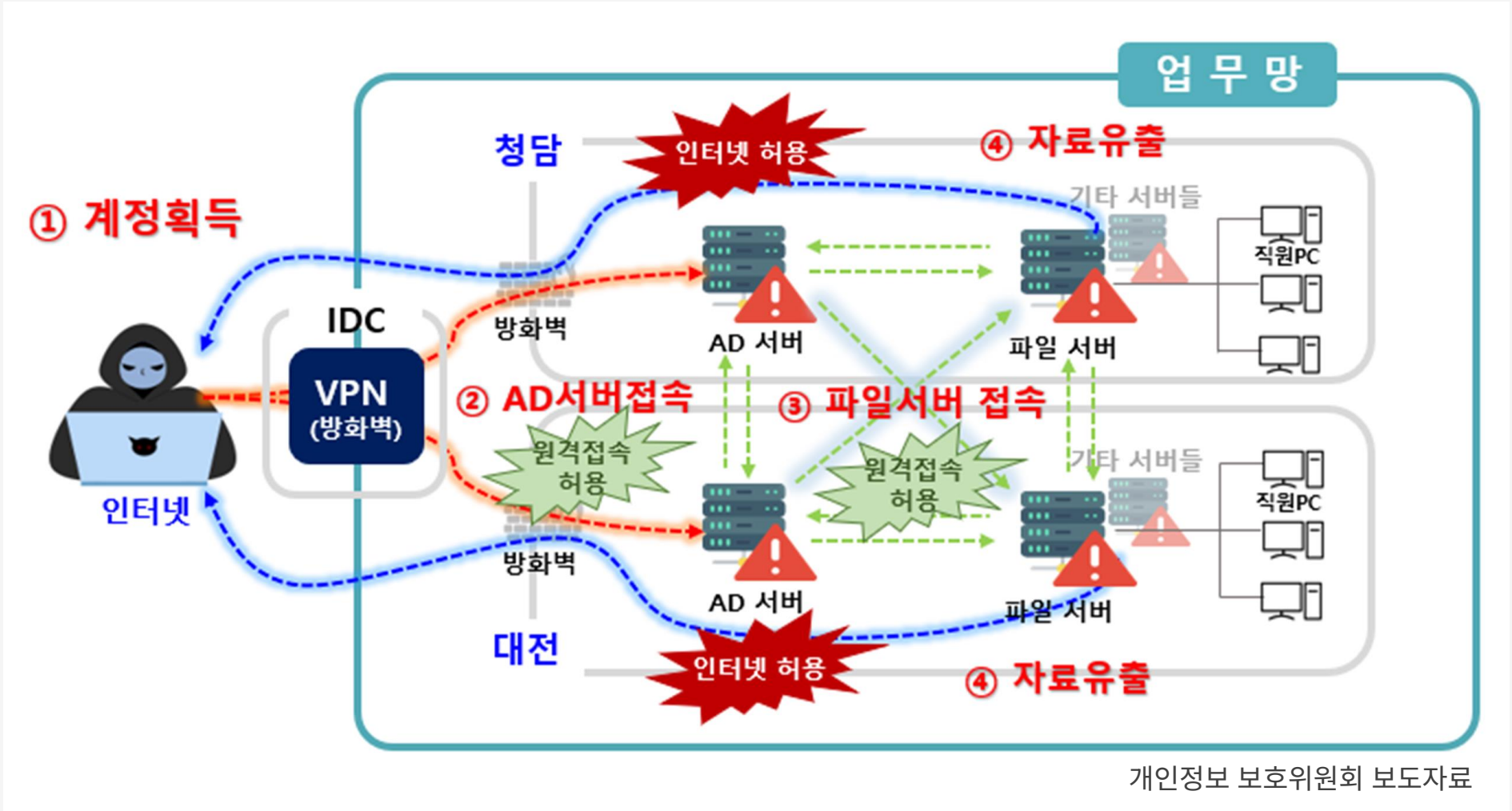
2. 주민등록번호 처리제한 및 개인정보 파기 위반

이어 주민등록번호 등을 암호화하지 않고 파일서버에 저장 · 보관하지 않은 점도 드러났다. 보유기간이 경과되거나, 처리목적 달성 등 불필요하게 된 최소 38만여명의 개인정보를 파기하지 않은 위반행위가 있었다.

개인정보는 △준회원 중 현재 회원으로 확인되지 않은 383,365명의 정보, △임직원 정보 중 퇴사하여 보유 근거가 없는 2,916명의 정보, △인턴사원 및 전문연구요원 1,159명의 채용관련 정보, △기타 고객응대(VOC) 관련 이용자 및 점주의 개인정보 등이다.

개인정보위는 골프존에 대해 보호법 제29조 안전조치의무 위반으로 과징금을 부과하고, 같은 법 제21조 개인정보 파기의무를 준수하지 않은 행위에 대해 과태료 부과를 결정했다.

개정법 적용 사례 2: 골프존 사건



개인정보 보호위원회 보도자료

개정법 적용 사례 2: 골프존 사건

- **사건 개요**
  - 2023년 11~12월 발생
  - 서비스 이용자 및 임직원 221만명의 개인정보 유출(준회원 196만명 포함)
  - 파일서버에 대한 주기적 점검 등 관리체계를 미흡하게 운영: 외부에서 ID/PW로만 접속 가능, 서버 간 원격접속 허용, 업무망 내 서버의 인터넷 통신 허용 등
  - 기간 경과 후 개인정보 미파기

- **개인정보 보호위원회의 판단 및 제재**
  - 법률, 시행령, 안전성 확보조치 기준 고시 위반
  - 시뮬레이터 판매 및 광고 매출도 관련 매출액에 포함
  - 과징금 75억원, 과태료 540만원, 시정명령 및 공표명령

개정법 적용 사례들의 함의

참고 사례: 카카오 사건

"6만5천명 정보 유출"…과징금 151억 '철퇴' 맞은 카카오, 행정소송 검토

개인정보위는 지난 22일 '제9회 전체회의'를 열고 개인정보보호 법규를 위반한 카카오에 대해 총 151억4천196만원의 과징금과 780만원의 과태료를 부과하고 시정명령과 처분결과를 공표하기로 의결했다고 23일 밝혔다.

카카오에 부과된 과징금은 이제까지 역대 최대 과징금이었던 골프존의 75억여원보다 두 배 이상 많은 금액이다.

상 많은 금액이다.

개인정보위는 지난해 3월 카카오톡 오픈채팅 이용자의 개인정보가 불법 거래되고 있다는 언론 보도에 따라 개인정보 보호법 위반 여부를 조사했다. 그 결과 해커는 오픈채팅방의 취약점을 이용해 오픈채팅방 참여자 정보를 알아내고, 카카오톡의 친구추가 기능 등을 이용해 일반채팅 이용자 정보를 알아냈다. 이 정보들을 '회원일련번호'를 기준으로 결합해 개인정보 파일을 생성, 판매한 것으로 확인됐다.

개인정보위가 확인한 카카오의 위반 사실은 ▲안전조치의무 위반 ▲유출 신고·통지 의무 위반 등 크게 두 가지다.

먼저 카카오는 익명채팅을 표방하며 오픈채팅을 운영하면서 일반채팅에서 사용하는 회원일련번호와 오픈채팅방 정보를 단순히 연결한 임시ID를 만들어 암호화 없이 그대로 사용했다.

치를 제대로 하지 않았다"며 "관련 사실은 확인됐다"고 말했다.

그러나 카카오는 개인정보위의 주장은 사실과 다소 다르다고 강조했다. 카카오는 "임시 ID는 숫자로 구성된 문자열이자 난수로서 여기에는 어떠한 개인정보도 포함돼 있지 않고 그 자체로는 개인 식별이 불가능해 개인정보라고 판단할 수 없다"며 "그럼에도 불구하고 자사 오픈채팅 서비스 개시 당시부터 해당 임시 ID를 난독화해 운영 및 관리했고, 이에 더해 2020년 8월 이후 생성된 오픈채팅방에는 더욱 보안을 강화한 암호화를 적용한 바 있다"고 피력했다.

기업·기관의 대응방안

BACK TO BASIC

개인정보 관련 기업·기관의 대응방안 1: Mindset

개인정보 관련 기업·기관의 대응방안 1: Mindset

유의할 법원 판례들

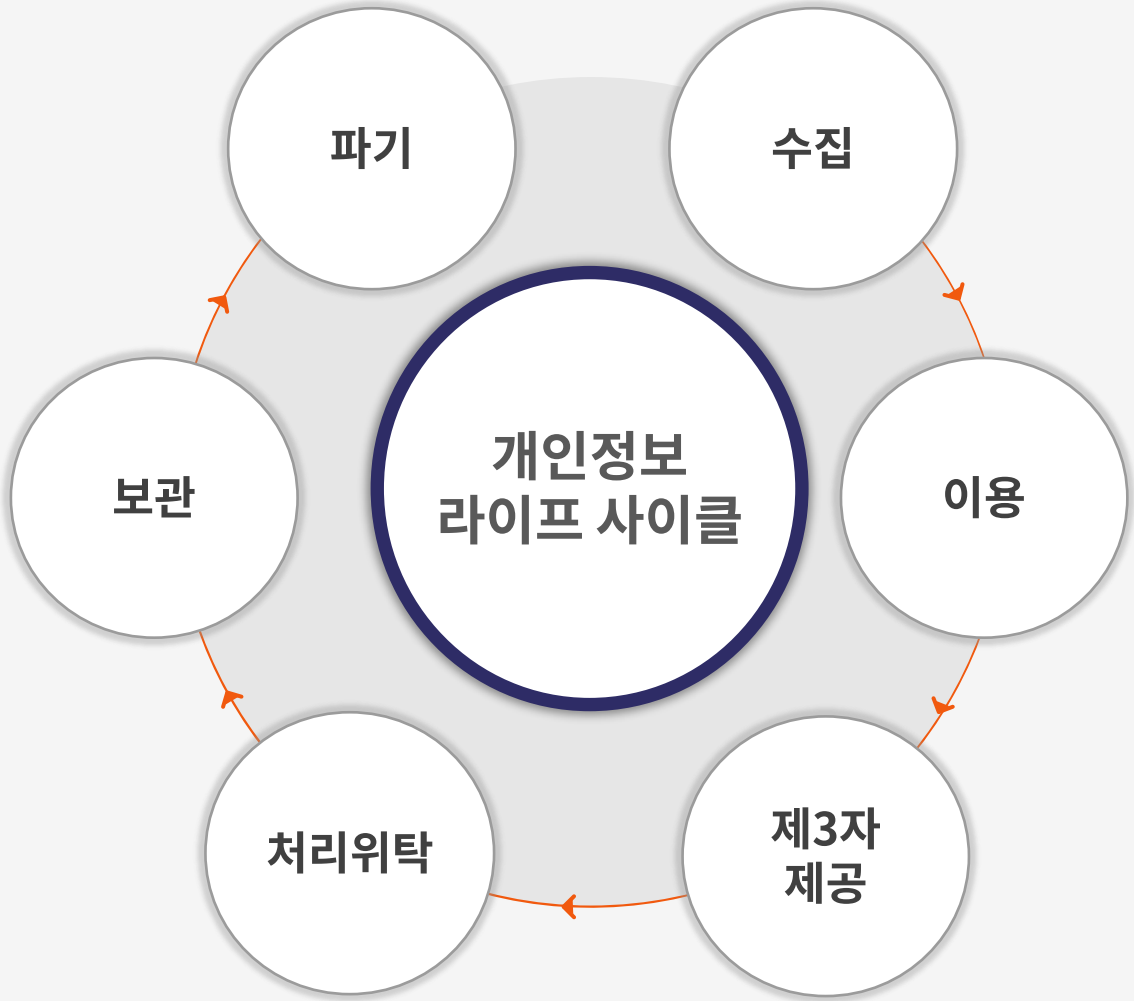
- 고소장에 피고소인의 주소와 전화번호를 기재한 것이 개인정보의 목적 외 이용에 해당한다고 판시한 사례(학과장이 학생회장을 명예훼손죄로 고소한 사건, 서울북부지방법원 2014노202판결, 대법원에서 확정)
- 개인정보의 분실·도난·유출·위조·변조 또는 훼손과 고시 위반행위 사이의 인과관계가 요구되지 않는다고 판시한 사례(인터파크 개인정보 유출 사건, 서울고등법원 2019. 11. 1. 선고 2018누56291 판결)

개인정보 관련 기업·기관의 대응방안 1: Mindset

개인정보 보호법은 不自然스러운 法이다!

정보 교류라는 인류 생활양식	VS.	사생활 보호
수 만 년	VS.	100년 미만
상식	VS.	비상식

개인정보 관련 기업·기관의 대응방안 2: 처리 현황 점검



개인정보 관련 기업·기관의 대응방안 2: 처리 현황 점검

비행기 조종사는 비행 전에 항상 비행기를 철저히 점검한다. 그들은 엔진에 시동을 걸기 전에 비행기의 모든 부분이 제대로 작동하는지 확인하기 위해 세부 사항이 전부 인쇄된 체크리스트를 활용한다. 수십 년 동안 일한 베테랑이라면 이런 점검 과정을 생략하거나 적어도 체크리스트를 쓰지는 않으리라고 생각하는 사람도 있을 것이다. 지금쯤이면 제2의 천성이나 다름없지 않겠는가?

틀렸다. 지금도 모두가 체크리스트를 사용한다. 이들은 근거 없이 낙관하지 않으며, 정밀한 사전 준비를 통해 자신 있게 이륙한다. 승객 또한 조종사의 세심한 준비를 보고 안심할 수 있다.

마이크 벡틀, 내향인만의 무기 중에서

개인정보 관련 기업·기관의 대응방안 2: 처리 현황 점검

- **개인정보 보호법 위반 사례 중 수탁자 책임형이 64% 이상**
- **개인정보 유출 사건 중 수탁자 책임형이 77% 이상**
- **사업자의 85%가 시스템 개발 및 운영업무 위탁 중**

IT수탁사 개인정보 처리실태 현장점검 결과 (2014)

- 개인정보 처리 위수탁이란?
- 위탁자의 법적 책임? ① 민사상 손해배상책임(사용자책임), ② 형사상 양벌규정 적용, ③ 행정상 행정제재

개인정보 관련 기업·기관의 대응방안 2: 처리 현황 점검

나의 처리현황은 물론, 수탁자들도 철저히 점검하고 감독해야!

수탁자에 대한 과징금·과태료 처분 및 형사처벌 규정 신설 (§ 64의2, 71~73, 75)

위탁자의 사용자책임 면책 가능성을 종전과 같이 엄격히 해석하는 것에 대한 비판

- 권영준, "해킹사고에 대한 개인정보처리자의 과실 판단 기준", 저스티스 제132호, 한국법학원, 2012, 65면 등
- 최경진 외 12인, 개인정보보호법, 박영사, 2024, 381면

▼

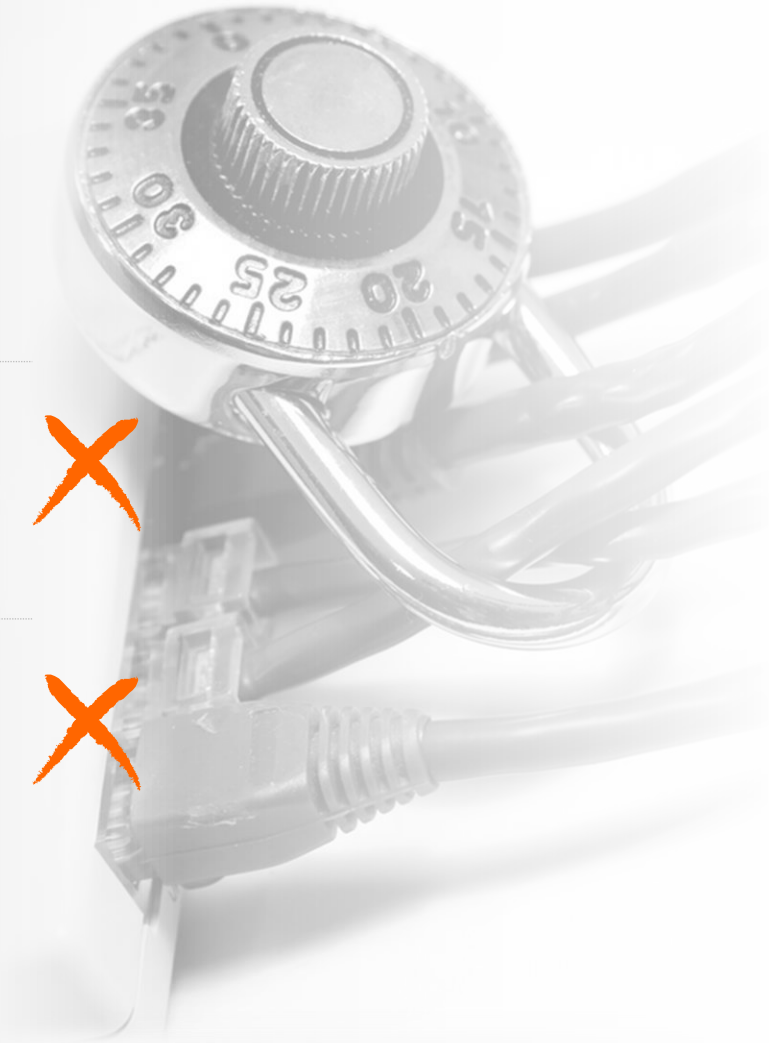
수탁자의 법 위반 시 위탁자의 민형사 및 행정상 책임이 면책될 가능성 증대

개인정보 관련 기업·기관의 대응방안 3: 법령 준수

“도대체 해킹을 어떻게 막으란 말이냐고!”

“개인정보 보호법은 보안전문가 처벌 전문 법률” ✗

“CISO/CPO를 맡겠다는 사람이 없어서 큰 일 …” ✗



개인정보 관련 기업·기관의 대응방안 3: 법령 준수

일단 법령이 정한 조치만은 100% 이행한다!

면책을 위한 법령 준수 vs 사건·사고 방지를 위한 법령 준수

법령을 넘어선 기술 발전상에 따른 추가적인 기술적 조치는 선택 사항

보호위도 고시 §6③과 같은 포괄적 규정 해석에 있어서 엄격함과 합리성 갖추어야

개인정보 관련 기업·기관의 대응방안 4: 유출 등 사건·사고 대처

"고객 센터·홍보부서부터 총동원하라!"

"Facts Finding! Fact Finding! Fact Finding!"

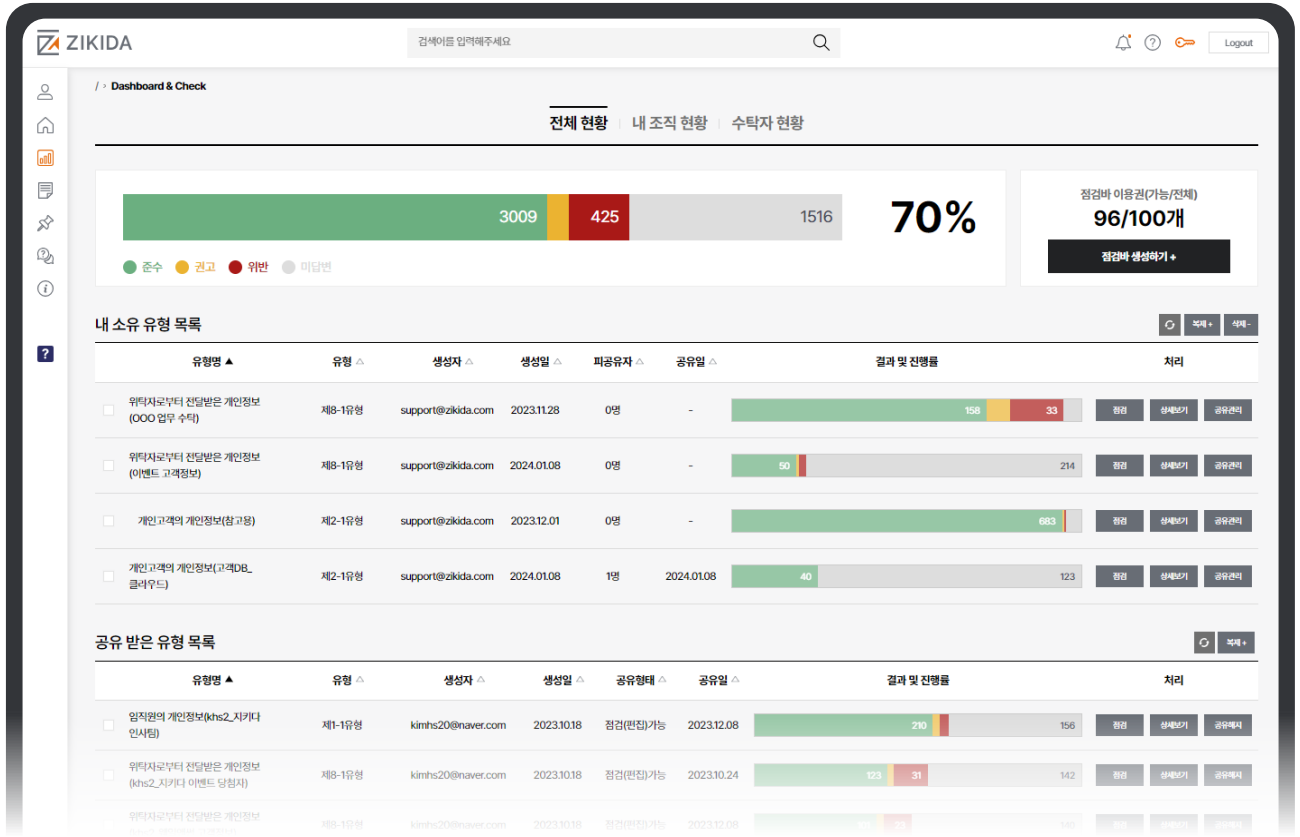
"하늘이 무너져도 솟아날 구멍은 있다... 그것도 항상!"

Useful Information

ZIKIDA

개인정보 관련 '점검'과 '관리·감독' 기능의 완벽한 통합

www.zikida.com



개인정보 실태점검 과정과 결과 등의 시각화

점검바(bar)를 통해 기업이나 기관 내·외부를 막론하고,
점검의 전 과정과 결과를 한 눈에 알아볼 수 있도록 지원하며,
그 상태를 실시간으로 모니터링

업데이트를 통한 스마트한 관리

법령, 고시, 가이드라인, 해설서, 행정해석, 판례 등을 반영하고
그 변동에 따라 지속적 업데이트를 진행하여 편의성 뿐만 아니라
기업이나 기관의 리소스(resources)를 크게 절약

기업 내부 및 수탁자에 대한 지속적 관리·감독 수행

법 위반 또는 best practice에 따른 권고 사항 등을 정확히 타겟팅
하여 기업 내부 및 수탁자들에 대한 실질적인 관리·감독 달성

Any Question?

변호사 김진환

kim.jh@whaleandsun.com / kim.jh@zikida.com

02-592-0153 / 010-9337-0741