

# Chap 7

## 개인정보 보호와 비식별 조치

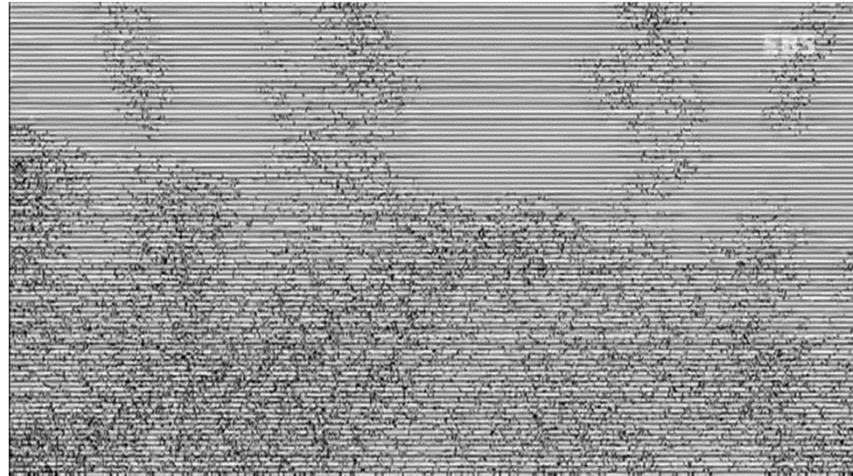
컴퓨터윤리 20191 봄학기

최현석

# 학습목표

1. 개인정보의 개념과 종류 이해
2. 개인정보 침해 유형과 실태
3. 개인정보 침해 사전 대응방안과 사후 대응방안
4. 개인정보 비식별화 조치 개념과 세부기법

지식채널e - 그들은 모두 알고 있었다  
(<https://youtu.be/HkQNXO88hcM>)



# 개인정보 개요

## ❖ 개인정보

- 식별 또는 식별 가능한 생존하는 개인에 관한 정보

## ❖ 개인정보의 성립요건

### 생존하는 개인 정보

- 사망하였거나 사망으로 추정되는 자에 대한 정보는 보호 대상이 아님
- 사망자와 유족간의 관계를 나타내는 정보는 유족에 대한 식별이 가능하여 개인정보임

### 개인 식별 가능한 정보

- 다른 정보와 결합하여 특정 개인을 식별할 수 있는 정보도 개인정보임
- 신체적, 정신적, 사회적 상태를 판단하거나 확인이 가능한 정보도 개인정보임

# 개인정보 개요

## ❖ 프라이버시 (privacy)

### ■ 소극적 해석

- 혼자 남아있을 권리(the right to be left alone)
- 원하지 않는 공표로부터의 자유(freedom from unwanted publicity)

### ■ 적극적 해석

- 정보주체의 자신에 관한 정보의 통제권
- 자신의 정보에 관한 생성, 이용, 유통까지 통제

# 개인정보 개요

## ❖ 개인정보 개념

- 사회변화에 따라 개인정보 개념 확대

### 산업사회

성명, 주소,  
주민등록번호 등

공간 프라이버시  
의사소통 프라이버시



### 정보사회

성명, 주소,  
주민등록번호 등  
+  
위치정보, 생체정보,  
전화통화내역, IP주소,  
웹사이트 접속내역 등

정보 프라이버시

# 개인정보 개요

## ❖ 대한민국 법률에서의 개인정보 정의

법률	개인정보의 정의
개인정보보호법 (제2조)	살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함)
정보통신망 이용 촉진 및 정보보호 등에 관한 법률 (제2조)	생존하는 개인에 관한 정보로서 성명, 주민등록번호 등에 의하여 특정 개인을 알아볼 수 있는 부호, 문자, 음성, 음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함)

# 개인정보 개요

## ❖ 개인정보 유형

유형	개인정보의 예
인적사항	성명, 주민등록번호, 주소, 본적지, 전화번호 등 연락처, 생년월일, 출생지, 이메일 주소, 가족 관계 및 가족구성원 정보 등
신체적 정보	(신체정보) 얼굴, 지문, 홍채, 음성, 유전자정보, 키, 몸무게 등 (의료·건강정보) 건강상태, 진료기록, 신체장애, 장애등급, 병력 등
정신적 정보	(성향정보) 도서, 비디오 등 대여기록, 잡지구독정보, 물품구매내역, 웹사이트 검색내역 등 (내면의 비밀 등) 사상, 신조, 종교, 가치관, 정당, 노조 가입 및 활동내역 등
재산적 정보	(개인금융정보) 소득, 신용카드번호, 통장계좌번호, 동산, 부동산 보유내역, 저축내역 등 (신용정보) 개인신용평가정보, 대출 또는 담보설정 내역, 신용카드 사용내역 등
사회적 정보	(교육정보) 학력, 성적, 출석상황, 자격증 보유내역, 상벌기록, 생활기록부 등 (법적정보) 전과, 범죄기록, 재판 기록, 과태료 납부내역 등 (근로정보) 직장, 고용주, 근무처, 근로경력, 상벌기록, 직무평가기록 등 (병역정보) 병역여부, 군번, 계급, 근무부대 등)
기타	전화통화내역, IP주소, 웹사이트 접속내역, 이메일 또는 전화메시지, 기타 GPS등에 의한 개인위치정보 등

표 7-2

개인정보의 유형분류



# 개인정보 개요

## ❖ OECD(경제협력개발기구) 개인정보 보호원칙

- 개인 데이터의 국제 유통과 프라이버시 보호에 관한 가이드라인 권고

OECD 8원칙	주요내용
수집제한의 원칙 (Collection Limitation Principle)	<ul style="list-style-type: none"> <li>• 개인정보는 적법하고 공정한 방법으로 수집</li> <li>• 정보주체에게 알리거나 동의를 구해야 함</li> <li>• 민감한 개인정보의 수집 제한</li> </ul>
정보정확성의 원칙 (Data Quality Principle)	<ul style="list-style-type: none"> <li>• 개인정보는 사용목적에 부합</li> <li>• 이용목적상 필요한 범위내에서 개인정보의 정확성, 완전성, 최신성을 확보해야 함</li> </ul>
목적 명시 원칙 (Purpose Specification Principle)	<ul style="list-style-type: none"> <li>• 개인정보 수집시 목적이 명확히 제시</li> <li>• 정보 이용시 목적과 부합해야 하며, 이용목적이 변경될 경우 다시 명시해야 함</li> </ul>
이용제한의 원칙 (Use Limitation Principle)	<ul style="list-style-type: none"> <li>• 정보주체의 동의가 있거나, 법률 규정에 의하지 않고는 이용목적의 이용 및 공개 금지</li> </ul>
안전성 확보의 원칙 (Security Safeguard Principle)	<ul style="list-style-type: none"> <li>• 개인정보의 침해, 누설, 도용등을 방지하기 위한 물리적/조직적/기술적 안전조치 확보</li> </ul>
공개 원칙 (Openness Principle)	<ul style="list-style-type: none"> <li>• 개인정보 처리 및 보호를 위한 정책 공개</li> <li>• 개인정보관리자의 신원 및 연락처, 개인정보의 존재사실, 이용목적 등에 대한 접근 용이</li> </ul>
개인참여의 원칙 (Individual Participation Principle)	<ul style="list-style-type: none"> <li>• 정보주체의 개인정보 열람/정정/삭제청구권 보장</li> <li>• 정보주체가 합리적 시간과 방법에 의해 개인정보에 접근할 수 있도록 보장</li> </ul>
책임의 원칙 (Accountability Principle)	<ul style="list-style-type: none"> <li>• 개인정보관리자에게 원칙 준수 의무 및 책임 부과</li> </ul>

표 7-3 OECD개인정보보호 8개 원칙

# 개인정보 침해 유형과 실태

## ❖ 개인정보 침해

- 당사자가 동의하지 않는 정보를 무단으로 가져가는 행위
- 당해 정보주체와 관련된 정보가 오/남용(도용, 변경, 유출, 훼손 등) 됨으로써 정보 주체의 자기정보통제권이 침해 되는 것

# 개인정보 침해 유형과 실태

(정보통신망 이용 촉진 및 정보보호 등에 관한 법률)

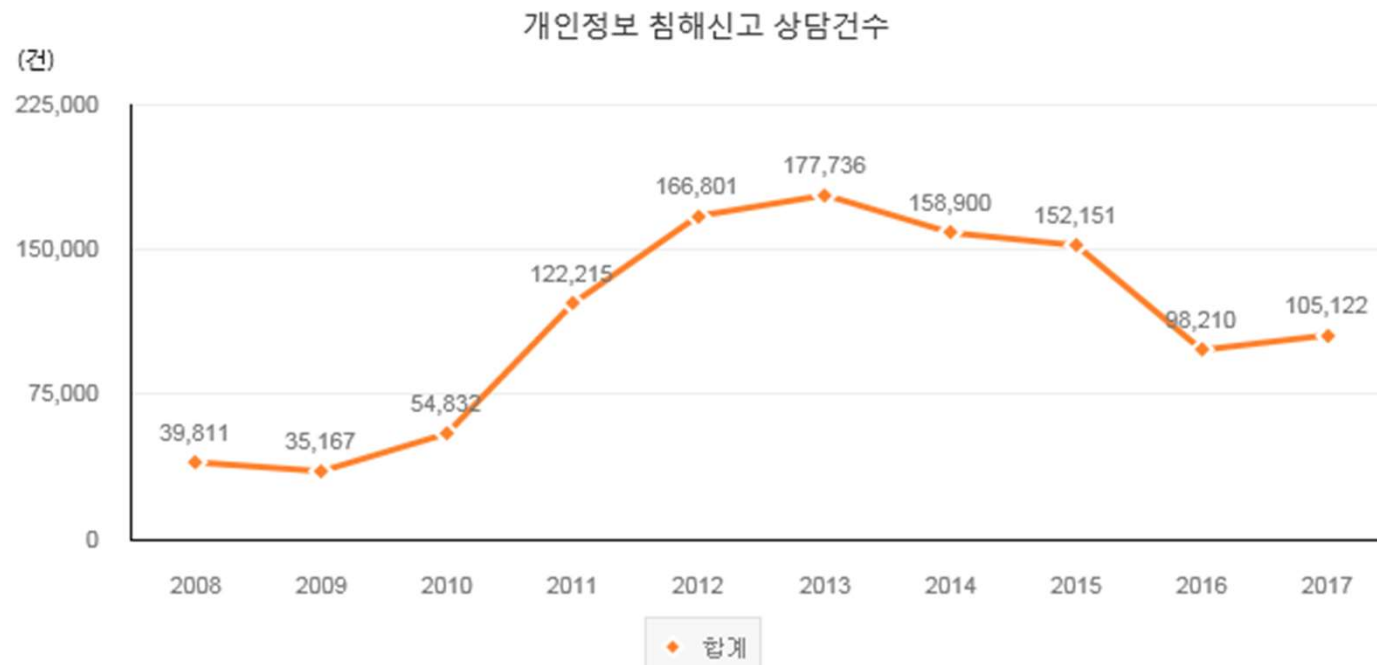
## ❖ 정보통신망법에 따른 개인정보 침해 유형

침해 유형	법률근거
이용자 동의 없는 개인정보 수집	제22조제1항
개인정보수집시 고지 또는 명시 의무 불이행	제22조제2항
과도한 개인정보 수집	제23조
고지·명시한 범위를 초과한 목적 외 이용 또는 제3자 제공	제24조, 제24조의2
개인정보취급자에 의한 훼손·침해 또는 누설	제28조의2
개인정보처리 위탁 시 고지 의무 불이행	제25조제1항
영업의 양수 등의 통지 의무 불이행	제26조제1항
개인정보관리책임자 미지정	제27조제1항
개인정보보호 기술적·관리적 조치 미비	제28조
수집 또는 제공받은 목적 달성 후 개인정보 미파기	제29조
동의철회·열람 또는 정정요구 등 불응	제30조제1항및2항
개인정보 오류정정요구 접수후 미정정 정보이용	제30조제5항
동의철회·열람 또는 정정을 수집방법보다 쉽게 해야 할 조치 미이행	제20조제6항
법정대리인의 동의없는 아동의 개인정보 수집	제31조제1항
영리목적의 광고성 정보전송	제50조내지 제50조의5
타인정보의 훼손·침해·도용	제49조

# 개인정보 침해 유형과 실태

## ❖ 개인정보 침해신고 상담건수

- 2013년 정점 후 감소 추세이나 2017년 다시 증가



[http://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx\\_cd=1366](http://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx_cd=1366)

# 개인정보 침해 유형과 실태

## ❖ 개인정보 생명주기(life-cycle)별 침해유형

수집	저장 및 관리	이용 및 제공	파기
동의 없는 개인정보 수집 및 수집 시 고지사항 불이행	조직내부 취급자에 의한 개인정보 유출, 훼손, 변경 등	당초 수집 시 고지한 이용목적을 넘어서는 개인정보 이용	수집 및 목적 달성후의 개인정보 미파기
해킹 등 불법수단에 의한 개인정보 수집	외부인의 불법접근에 의한 개인정보 유출 및 훼손, 변경	동의 없는 개인정보의 무단 제공 및 공유	개인정보 삭제 요구 불응
불법 수집된 개인정보 구매	기술적, 관리적 조치 미비로 인한 개인정보 유출	타인의 개인정보를 무단으로 이용하는 경우	
서비스 이용과 관련 없는 과도한 개인정보의 수집	사업자의 인식부족, 과실 등으로 인한 개인정보의 공개		

# 개인정보 침해 유형과 실태

## ❖ 개인정보 수집 유형

구분	내용
수집 경로	<ul style="list-style-type: none"> <li>● 서비스 이용계약 체결을 위해 정보주체로부터 직접 수집하는 경우 (웹사이트 회원가입, off-line에서의 회원가입 신청서 작성 등)</li> </ul>
	<ul style="list-style-type: none"> <li>● 정보주체 이외로부터 수집하는 경우 (게시판에 공개된 정보의 수집, 명함·졸업명부·전화번호부 등에서의 수집)</li> </ul>
수집 방법	<ul style="list-style-type: none"> <li>● 서비스 제공 및 이용 관계에 의한 수집 (회원가입)</li> <li>● 해킹 등 불법 수단에 의하여 수집하는 경우</li> <li>● cookie 정보의 수집</li> <li>● 스파이웨어 등 정보의 자동수집</li> <li>● 교통카드, RFID 등에 의한 수집</li> </ul>

# 개인정보 침해 유형과 실태

## ❖ 개인정보 침해 유형별 사례 - 수집단계

침해 유형	침해 사례	개선 방향
개인정보 수집시 미고지 (동의 없는 개인정보 수집 포함)	<ul style="list-style-type: none"> <li>인터넷 쇼핑몰 등에서 물품 구매를 위해 회원 가입을 하여 성명, 주민번호, 주소 등 개인정보를 제공하였으나, 제공하는 개인정보의 수집 및 이용목적, 보유기간, 회원탈퇴 방법 등 관련 사항이 전혀 고지되어 있지 않은 경우</li> </ul>	정보통신망법 제22조에 의하여 규제 가능
동의 및 고지 없는 개인정보 주체이외로부터의 수집	<ul style="list-style-type: none"> <li>웹사이트에서의 인물정보 서비스 제공 등을 통하여 개인정보를 수집, TM 등에 활용 또는 DB화하여 매매하는 경우</li> </ul>	법제화 필요(수집 및 이용 시 고지하는 방안 등)
법정 대리인의 동의없는 개인정보의 수집	<ul style="list-style-type: none"> <li>게임웹사이트가 법정대리인(부모)의 동의 없이 아동을 회원가입시켜 당해 아동이 게임, 아이템 등을 결재하여 부모의 인지 없이 많은 요금이 청구되는 사례</li> </ul>	정보통신망법 제31조에 의하여 규제 가능

# 개인정보 침해 유형과 실태

## ❖ 개인정보 침해 유형별 사례 - 수집단계 (계속)

침해 유형	침해 사례	개선 방향
서비스 이용과 관련없는 과도한 개인정보의 수집	<ul style="list-style-type: none"> <li>인터넷 서비스 회원가입을 시 직업, 종교, 군복무 경력 등 당해 서비스 이용과 전혀 관계없는 정보를 제공하여야 회원가입이 가능한 사례</li> </ul>	정보통신망법 제23조에 의하여 규제 가능
해킹등 불법수단에 의한 개인정보의 수집	<ul style="list-style-type: none"> <li>트로이 목마 등 해킹 프로그램을 이용하여 타인의 ID 및 비밀번호를 수집하여 이를 활용하여 타인 명의로 인터넷 회원가입을 하거나, 금융 서비스를 제공받는 등 경제적 이익을 취하는 경우</li> </ul>	정보통신망법 제48조, 제49조 및 제50조의 2에 의하여 규제 가능
기만에 의한 개인정보수집	<ul style="list-style-type: none"> <li>경품당첨을 가장하여 주민번호 등 개인정보를 입력하도록 한 후 경품 제공은 전혀 이루어지지 않는 사기성 개인정보의 수집 사례</li> </ul>	



# 개인정보 침해 유형과 실태

## ❖ 개인정보 저장 및 관리 유형

구분	내용
저장 유형	<ul style="list-style-type: none"><li>● 정보를 DB화하여 정보시스템의 서버 및 컴퓨터 하드디스크에 저장 (디지털)</li><li>● 회원가입신청서 등 문서를 캐비넷, 금고 등 특정 장소에 보관 (아날로그)</li></ul>
관리 유형	<ul style="list-style-type: none"><li>● 정보보호 시스템(방화벽, 암호화 S/W의 활용 등)을 통한 기술적 조치</li><li>● 개인정보 취급 및 관리에 대한 내부 지침 마련, 취급자에 대한 교육 등을 통한 관리적 조치</li></ul>

# 개인정보 침해 유형과 실태

## ❖ 개인정보 침해 유형별 사례 - 저장 및 관리 단계

침해 유형	침해 사례	개선방향
사업자의 인식부족, 과실 등으로 개인정보가 공개된 경우	<ul style="list-style-type: none"> <li>● 인터넷 쇼핑몰 운영자가 상품의 품질에 대해 이의를 제기한 소비자의 신상정보 및 거래 정보 등을 그대로 게시판에 공개한 사례</li> <li>● 성형외과 병원이 고객의 성형수술 전후사진을 웹사이트에 무단 게재한 사례 ※병원은 현행 정보통신망법의 적용 대상자가 아니어서 규제 불가</li> </ul>	정보통신망법 제24조에 의하여 규제 가능 법적용대상자확대 필요
기술적·관리적 조치 미비로 인한 개인정보 유출	<ul style="list-style-type: none"> <li>● 사업자의 업무실수(요금내역 발송 이메일 리스트를 한명씩 밀려 입력함으로써 다른 사람에게 요금내역서가 송부됨)로 고객 3천명의 신용카드번호 및 신상정보 등이 유출된 사건</li> </ul>	정보통신망법 제28조에 의하여 규제 가능
개인정보와 관련 된 고객 항의( 정정, 열람청구 등)에 대한 불응 또는 미조치	<ul style="list-style-type: none"> <li>● 인터넷 웹사이트 가입자가 서비스 이용 종단을 위해 회원탈퇴를 하고자 하였으나, 탈퇴 방법이 없거나, 탈퇴 방법이 마련되어 있어도 사업자가 이행하지 않음으로써 계속적으로 이용요금이 부가되거나, 광고성 전자우편이 수신되는 경우</li> </ul>	정보통신망법 제30조에 의하여 규제 가능

# 개인정보 침해 유형과 실태

## ❖ 개인정보 침해 유형별 사례 -이용 및 제공 단계

침해 유형	침해 사례	개선방향
타인 개인정보의 도용 등을 통한 무단 이용	<ul style="list-style-type: none"> <li>타인의 사진 및 전화번호 등을 무단 게재함으로써 개인의 명예훼손 및 정신적 피해를 발생시키는 경우</li> </ul>	정보통신망법 제61조에 의하여 규제 가능
정보주체의 동의 없는 개인정보의 무단 제공 및 공유	<ul style="list-style-type: none"> <li>인터넷 웹사이트 사업자가 제휴 업체 (보험, 카드사 등)에 정보 주체의 동의 없이 개인정보를 제공하고 제휴 업체들은 제공 받은 개인정보를 활용하여 TM 등 마케팅을 실시한 사례</li> </ul>	정보통신망법 제24조에 의하여 규제 가능
수집 시에 고지한 이용목적을 넘는 개인정보 이용	<ul style="list-style-type: none"> <li>이동통신사가 고객의 정보를 활용하여 요청하지도 않은 유료 부가서비스를 무단으로 가입시킨 사례</li> </ul>	정보통신망법 제24조에 의하여 규제 가능

# 개인정보 침해 유형과 실태

## ❖ 개인정보 침해 유형별 사례 -파기 단계

침해 유형	침해 사례	개선 방향
수집 및 목적 달성 후에도 개인정보를 파기하지 않는 경우	<ul style="list-style-type: none"> <li>● 웹사이트 회원탈퇴 후에도 지속적으로 광고성 전자우편이 전송되는 경우</li> </ul>	정보통신망법 제 29조에 의해 규제 가능
	<ul style="list-style-type: none"> <li>● 이동통신사가 자사의 서비스 이용 해지고객의 개인정보를 파기하지 아니하고 보관하는 경우 ※다른 법령 규정 등에 의하여 보관할 필요성이 있는 경우 미파기 및 지연 가능</li> </ul>	민간분야 개인정보보호법 시안에 미파기 경우를 반영

홈플러스, '고객 개인 정보' 장사...231억 챙겼다  
(SBS8뉴스|2015.02.01)  
(<https://youtu.be/x4MkkpFhEF8>)

당첨자 바꾸고 개인정보만...마트 경품행사  
고객 우롱  
(<https://youtu.be/4HId7SSfYic>)

# 개인정보 침해 유형과 실태

## ❖ 개인정보 침해에 대한 벌칙 규정

### ■ 내용에 따라 (교재 pp.270~272 참조)

- 10년 이하의 징역 또는 1억원 이하의 벌금
  - ✓ 공공기관의 개인정보 처리업무를 방해할 목적으로 공공기관에서 처리하고 있는 개인정보를 변경하거나 말소하여 공공기관의 업무 수행의 중단,마비 등 심각한 지장을 초래한 자
- 5년 이하의 징역 또는 5천만원 이하의 벌금
- 3년 이하의 징역 또는 3천만원 이하의 벌금
- 2년 이하의 징역 또는 2천만원 이하의 벌금

# 개인정보 침해 대응방안

## ❖ 개인정보 침해 대응방안

### ▪ 사전 대응방안

- 개인정보 유출을 방지하기 위한 개인정보 관리
  - ✓ 아이핀(I-PIN)과 마이핀(My-PIN)
  - ✓ 쿠키(cookie)
  - ✓ e프라이버시 클린서비스
  - ✓ SNS와 개인정보 보호
  - ✓ 개인정보 오남용 피해예방 10계명
  - ✓ 메신저 피싱 방지 5계명

### ▪ 사후 대응방안

- 개인정보 유출에 따른 피해구제
  - ✓ 개인정보침해신고센터 (<https://privacy.kisa.or.kr/kor/main.jsp>)
  - ✓ 개인정보분쟁조정위원회 (<https://www.kopico.go.kr/main/main.do>)

# 사전 대응방안

## ❖ 아이핀(I-PIN)과 마이핀(My-PIN)

### ■ 아이핀

- 인터넷상 개인식별번호  
(Internet Personal Identification Number)
- 인터넷 상에서 주민등록번호를 사용하지 않고 본인임을 확인할 수 있는 개인정보보호서비스

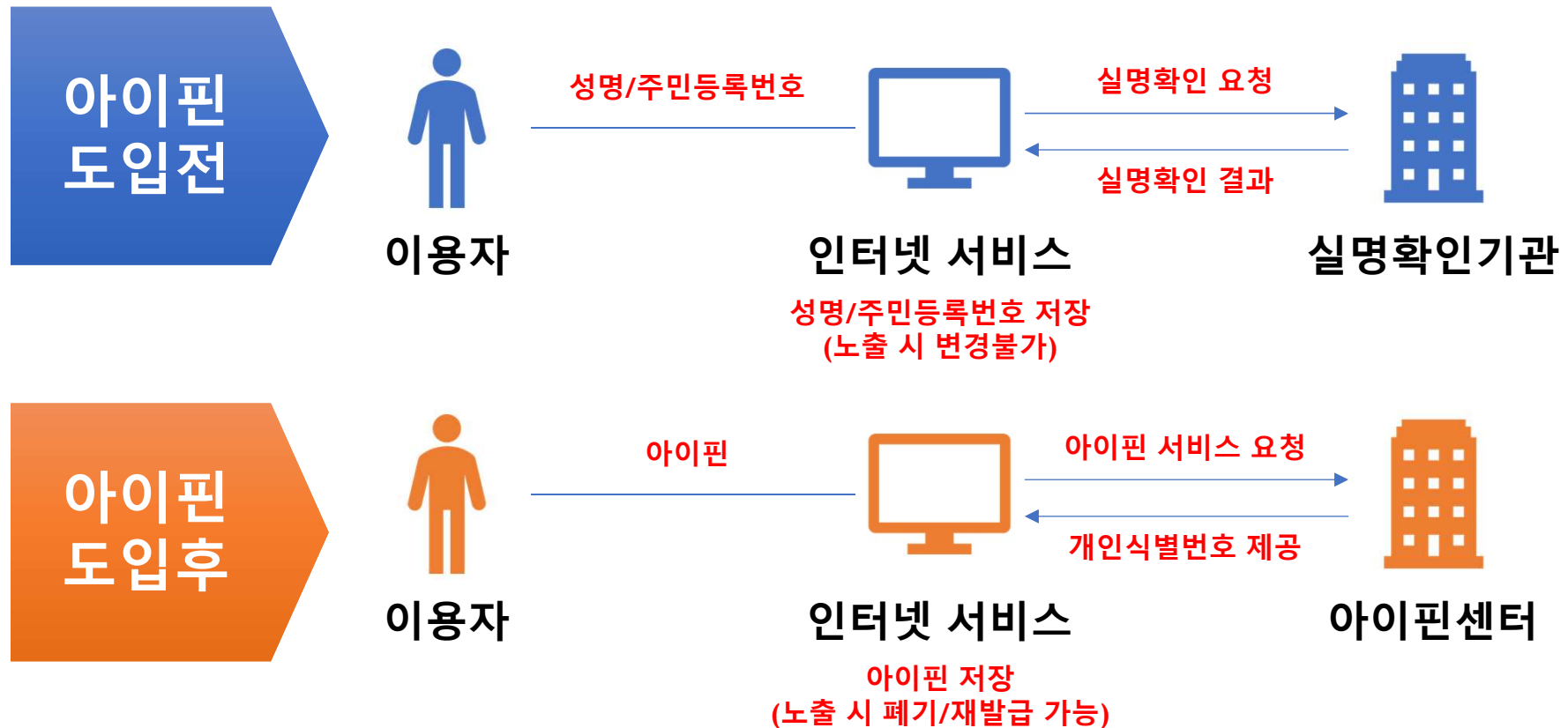
### ■ 마이핀

- 인터넷이 아닌 일상생활에서 사용할 수 있는 본인확인 수단
- 개인정보를 포함하고 있지 않은 13자리 무작위 번호
- 타인에게 유출될 경우 즉시 재발급 받아 개인정보를 보호 할 수 있는 서비스 (연 5회 변경가능)



# 사전 대응방안

## ❖ 아이핀/마이핀 서비스 개념



# 사전 대응방안

## ❖ 주민등록번호/아이핀/마이핀 비교

개별 웹사이트 저장		개별 웹사이트 저장 안함	
구분	주민등록번호	아이핀	마이핀
번호 체계	생년월일, 성별, 출신지, 접수번호, 검증코드	기관코드, 난수(문자포함)	발행연도, 기관코드, 난수, 검증코드
변경 여부	변경이 매우 곤란	폐기후 신규 가입	변경 가능
발급 방법	주민센터에서 출생신고시 발급	I-PIN 서비스 홈페이지, 동주민센터	I-PIN 서비스 홈페이지, 동주민센터
이용 영역	온라인 및 오프라인	인터넷상	인터넷이 아닌 일상생활
이용 방법	주민등록번호(필요에 따라 주민등록증 제시)	사용자 ID, 비밀번호	마이핀
의무 발급 여부	의무	선택	선택

표 7-7 주민등록번호, 아이핀, 마이핀의 비교

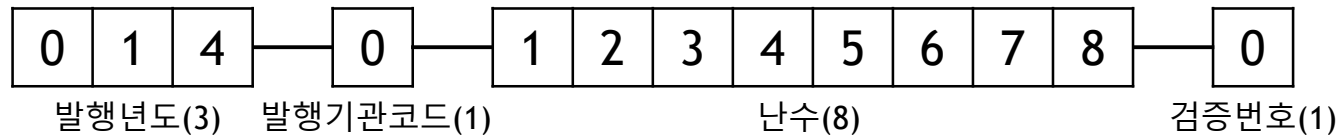
# 사전 대응방안

## ❖ 아이핀/마이핀 발급

### ▪ 온라인 발급 및 방문 발급 가능

- 공공 I-PIN 센터는 2018년 7월부터 신규/재발급 중단

### ▪ 마이핀 13자리 번호로 구성



인터넷 홈페이지와 가까운 동주민센터 방문을 통해 발급 가능합니다.

#### 1. 온라인 발급방법

공공I-PIN센터([www.gpin.go.kr](http://www.gpin.go.kr))  
나이스평가정보([www.niceipin.co.kr](http://www.niceipin.co.kr))  
서울신용평가정보([ipin.siren24.com](http://ipin.siren24.com))  
코리아크레딧뷰로([www.ok-name.co.kr](http://www.ok-name.co.kr)) 등  
인터넷 홈페이지에 접속하여 발급받습니다.

#### 2. 방문 발급방법

전국 읍/면사무소 및 동주민센터, 민간본인확인기관  
본사 및 지사에 방문하여 발급받습니다.

# 사전 대응방안

## 마이핀 홍보영상

### ❖ 마이핀 사용처

[http://www.mois.go.kr/video/bbs/type019/commonSelectBoardArticle.do;jsessionid=Dt2MQ9ICqdlu+GULgjrtXfH.node20?bbsId=BBSMSTR\\_000000000255&nttlId=54872&searchCode1=](http://www.mois.go.kr/video/bbs/type019/commonSelectBoardArticle.do;jsessionid=Dt2MQ9ICqdlu+GULgjrtXfH.node20?bbsId=BBSMSTR_000000000255&nttlId=54872&searchCode1=)

#### ■ 아직은 사용하는 곳이 많지 않음

##### 1. 멤버십카드 발급

회원카드 발급 시 굳이  
주민등록번호를 알려줄 필요가  
없어요!  
마이핀 번호만으로 OK!!

##### 2. ARS 상담

ARS 상담 시 본인확인을 할 때  
주민등록번호를 불러줄 필요가  
없어요^^  
마이핀을 불러주면 OK!!

##### 3. 도서대여 등

도서관에서 도서대여 시  
특정개인을 구분하기 위하여  
주민등록번호를 사용할 필요가  
없어요! 마이핀 번호로 OK!!



※ 차량출고 시 서류확인(현대/기아자동차), 고객센터의 ARS 응대(현대홈쇼핑, 넥슨, 현대오일뱅크, 네오플, 엔씨소프트, E1) 및 매장내 멤버십 가입(오케이아웃도어닷컴, 이마트, 대한항공, 신세계백화점) 등

# 사전 대응방안

## ❖ 쿠키 (cookie)

- 웹서버가 사용자의 하드디스크에 저장하는 사용자에게 관한 텍스트 파일
- 1994년 Netscape에 의해 사용된 기술
- HTTP Cookie(=web cookie, Internet cookie, browser cookie)

## ❖ 쿠키 목적

- 사이트 재접속시, 사용자 컴퓨터에 저장된 쿠키를 통해 사용자의 여러 개인 정보(id, email 등)를 수집

## ❖ 개인정보 유출

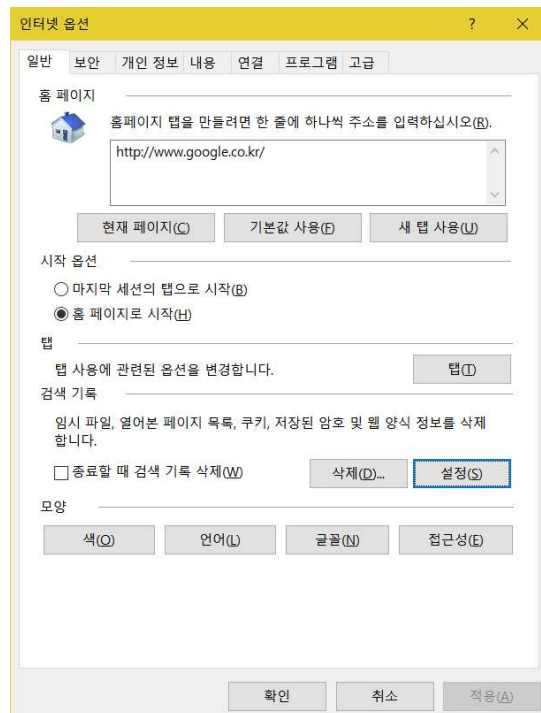
- 사용자가 어떤 사이트에 접속하여 어떤 정보에 접속했는지 파악 가능
- 어떤 상품을 구매했는지에 대한 정보 등

# 사전 대응방안

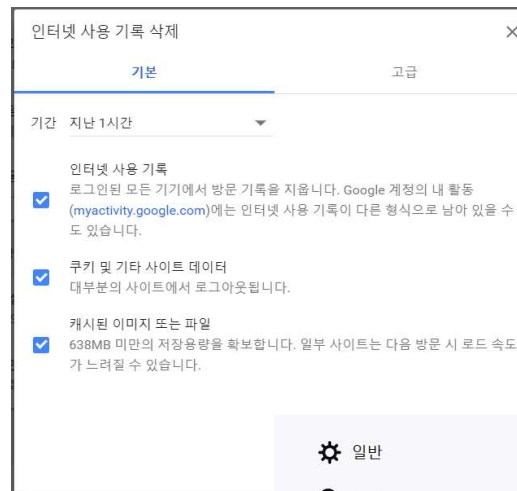
## ❖ 쿠키 주의사항

- 공용PC 사용시 PC 사용 후 최근 방문 기록 및 쿠키 삭제 필요

### Internet Explorer



### Google Chrome



### Mozilla Firefox



# 사전 대응방안

## ❖ e프라이버시 클린서비스

- [www.eprivacy.go.kr](http://www.eprivacy.go.kr)
- 인터넷에서 회원가입 등을 위해 실시된 본인확인 내역을 조회하고, 명의도용이 의심되거나 회원탈퇴에 어려움이 있는 웹사이트, 또는 더 이상 이용을 원치 않는 웹사이트에 대한 회원탈퇴를 지원



언제, 어디(어떤 웹사이트)서  
내 개인정보로 본인확인(인증)이  
이뤄졌는지 궁금하시나요?



주민등록번호 등 개인정보가  
도용되어 불법·유해사이트 가입 등에  
악용되지 않을까 걱정되시나요?

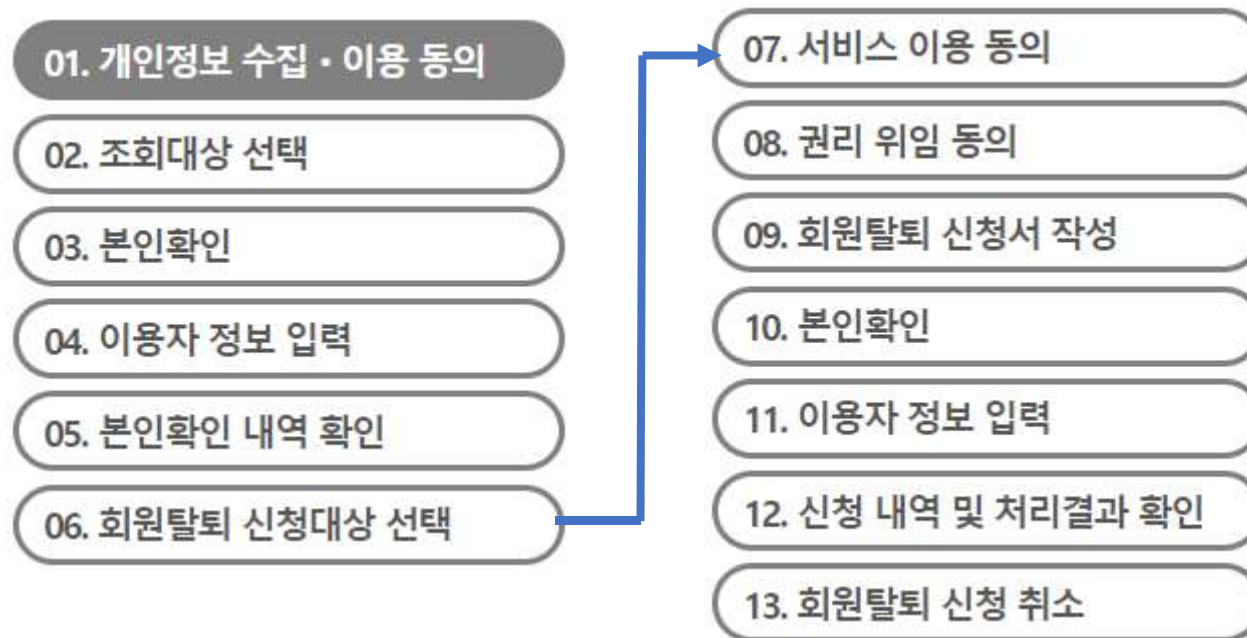


명의도용이 의심되거나  
불필요한 웹사이트에서 회원탈퇴 요구를  
거부하고 있나요?

# 사전 대응방안

## ❖ e프라이버시 클린서비스 이용절차

- <https://www.eprivacy.go.kr/useProc.do>



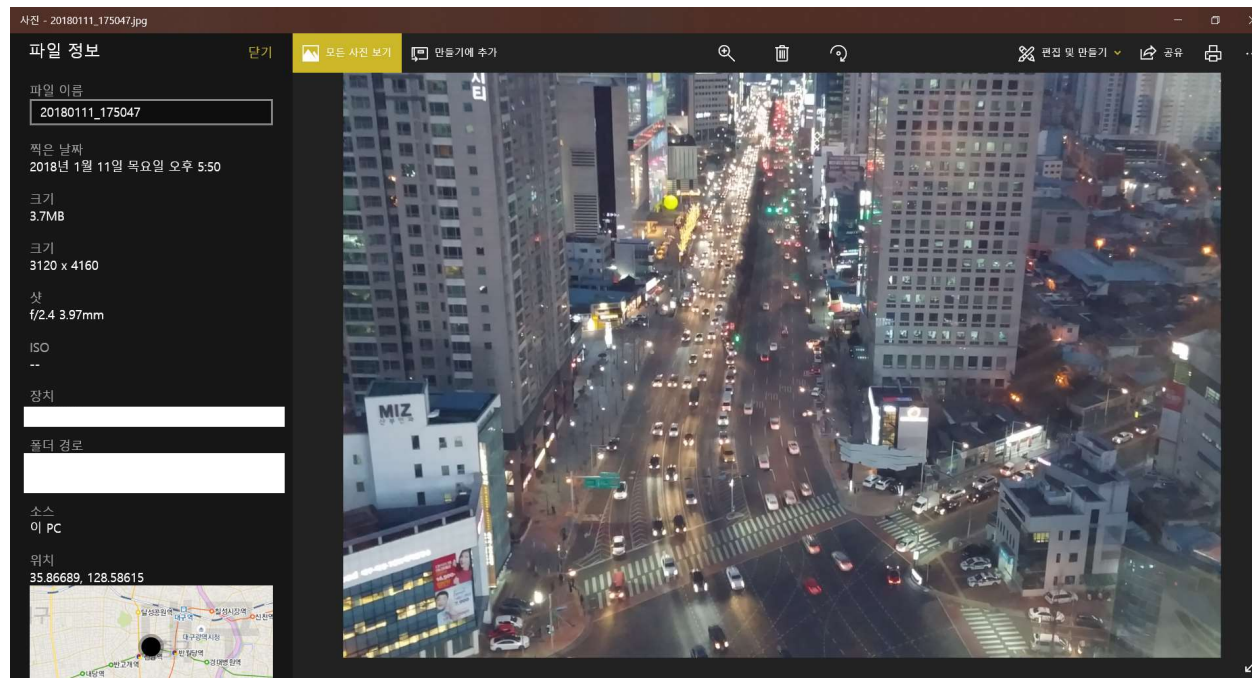


# 사전 대응방안

## ❖ SNS와 개인정보

- SNS에서의 개인정보 보호는 일차적으로 이용자의 책임이기 때문에 이용자들이 개인 정보보호에 보다 많은 관심 기울여야 한다

## ❖ 사례 - 사진 공유



# 사전 대응방안

## ❖ SNS 사용시 개인정보 보호 방안

- SNS 이용시 자신의 정보 노출을 최소화
- 관계 설정 등을 보다 신중히 접근하는 자세 필요
- 친구리스트를 주기적으로 체크
- 친구관계는 가능한 지인과만 맺도록 하자
- 자신이 어디에 정기적으로 다니는지 알 수 있는 사진이나 정보를 올리지 말자
- 정기적인 PC 보안 업데이트하기
- 민감한 자료의 공유를 자제하기
- 애플리케이션 보안 수준 설정 및 애플리케이션 사용전에 보안 규정 확인
- 확인되지 않은 링크는 클릭하지 말자

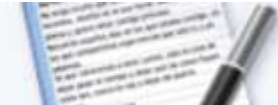
# 사전 대응방안

## ❖ 개인정보 오남용 피해예방 10계명

### ■ 개인정보 침해신고센터

([https://privacy.kisa.or.kr/kor/privacy/privacy03\\_new.jsp](https://privacy.kisa.or.kr/kor/privacy/privacy03_new.jsp))

01 회원가입을 하거나 개인정보를 제공할 때에는 개인정보처리방침 및 약관을 꼼꼼히 살핍니다.



02 회원가입 시 비밀번호를 타인이 유추하기 어렵도록 영문/숫자 등을 조합하여 8자리 이상으로 설정합니다.



03 자신이 가입한 사이트에 타인이 자신인 것처럼 로그인하기 어렵도록 비밀번호를 주기적으로 변경합니다.



04 가급적 안전성이 높은 주민번호 대체수단(아이핀 i-PIN)으로 회원가입을 하고, 꼭 필요하지 않은 개인정보는 입력하지 않습니다.

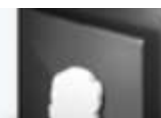


# 사전 대응방안

05 타인이 자신의 명의로 신규 회원가입 시 즉각 차단하고, 이를 통지받을 수 있도록 명의도용 확인서비스를 이용합니다.



06 자신의 아이디와 비밀번호, 주민번호 등 개인정보가 공개되지 않도록 주의하여 관리하며 친구나 다른 사람에게 알려주지 않습니다.



07 인터넷에 올리는 데이터에 개인정보가 포함되지 않도록 하며, P2P로 제공하는 자신의 공유폴더에 개인정보 파일이 저장되지 않도록 합니다.



08 금융거래 시 신용카드 번호와 같은 금융 정보 등을 저장할 경우 암호화 하여 저장하고, 되도록 PC방 등 개방 환경을 이용하지 않습니다.



09 인터넷에서 아무 자료나 함부로 다운로드 하지 않습니다.



10 개인정보가 유출된 경우 해당 사이트 관리자에게 삭제를 요청하고, 처리되지 않는 경우 즉시 개인정보 침해신고를 합니다.



# 사전 대응방안

## ❖ 메신저 피싱 방지 5계명

### ■ 개인정보 침해신고센터

([https://privacy.kisa.or.kr/kor/privacy/privacy04\\_new.jsp](https://privacy.kisa.or.kr/kor/privacy/privacy04_new.jsp))

01 메신저로 금전을 요구하는 경우 반드시 전화를 통해 확인하기



02 메신저를 통해 개인정보를 알려주지 않기



03 정기적으로 메신저 비밀번호를 변경, 관리하기



04 공공장소에서는 메신저 사용을 자제하기



05 메신저 자체 보안 설정 및 보안 프로그램을 최신 버전으로 업데이트 하기



# 사전 대응방안

## ❖ 개인정보보호수칙

개인정보 생명주기	서비스 제공자	서비스 이용자
수집	<ul style="list-style-type: none"><li>• 방침수립</li><li>• 책임자 지정</li><li>• 수집 원칙</li></ul>	<ul style="list-style-type: none"><li>• 정보제공 최소화</li><li>• 보호조치 확인</li></ul>
저장 및 관리	<ul style="list-style-type: none"><li>• 목적내 이용 및 제공</li><li>• 개인정보 공개 설정</li><li>• 보호조치</li></ul>	<ul style="list-style-type: none"><li>• 공개범위 최소화</li><li>• 정기적 업데이트</li><li>• 중요 정보의 안전한 관리</li><li>• 미사용 기능 비활성화</li></ul>
이용 및 제공	<ul style="list-style-type: none"><li>• 개인정보 위탁</li><li>• 국외 이전</li><li>• 양도시 고지 의무</li></ul>	<ul style="list-style-type: none"><li>• 신중한 정보 공유</li></ul>
파기	<ul style="list-style-type: none"><li>• 개인정보 파기</li></ul>	<ul style="list-style-type: none"><li>• 탈퇴시 자동 파기 요청</li></ul>

# 사후 대응방안

## ❖ 분야별 개인정보 침해신고

- 공공분야 개인정보 침해 → 행정자치부
- 금융분야 신용정보 침해 → 금융감독원
- 정보통신분야 개인정보 침해 → 방송통신위원회  
→ 개인정보침해신고센터 및 개인정보분쟁조정위원회

## ❖ 개인정보침해신고센터

- <https://privacy.kisa.or.kr>
- 한국인터넷진흥원 개인정보침해 신고센터

## ❖ 개인정보분쟁조정위원회

- <https://www.kopico.go.kr>




# 사후 대응방안

## ❖ 개인정보침해신고센터

- <https://privacy.kisa.or.kr>
- 개인정보침해 신고센터는 「개인정보 보호법」 제62조, 동법시행령 제59조 또는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 정보통신망법) 제52조, 동법시행령 제66조에 따라 개인정보에 관한 권리, 이익 침해 사실 신고의 접수·처리 등에 관한 업무를 담당

## 개인정보침해 신고센터 이용방법

- 전화 : 118(ARS 내선 2번)
- 팩스 : 061-820-2619
- 전자우편 : 
- 우편 : (58324) 전남 나주시 진흥길 9(빛가람동 301-2) 3층 개인정보침해 신고센터
- 인터넷 : 개인정보침해 신고센터(<http://privacy.kisa.or.kr>)
- 방문 : 평일 (09:00 - 18:00)  
(찾아오시는 길) 전남 나주시 진흥길 9(빛가람동 301-2) 3층 (지도보기)



# 사후 대응방안

## ❖ 개인정보침해신고센터

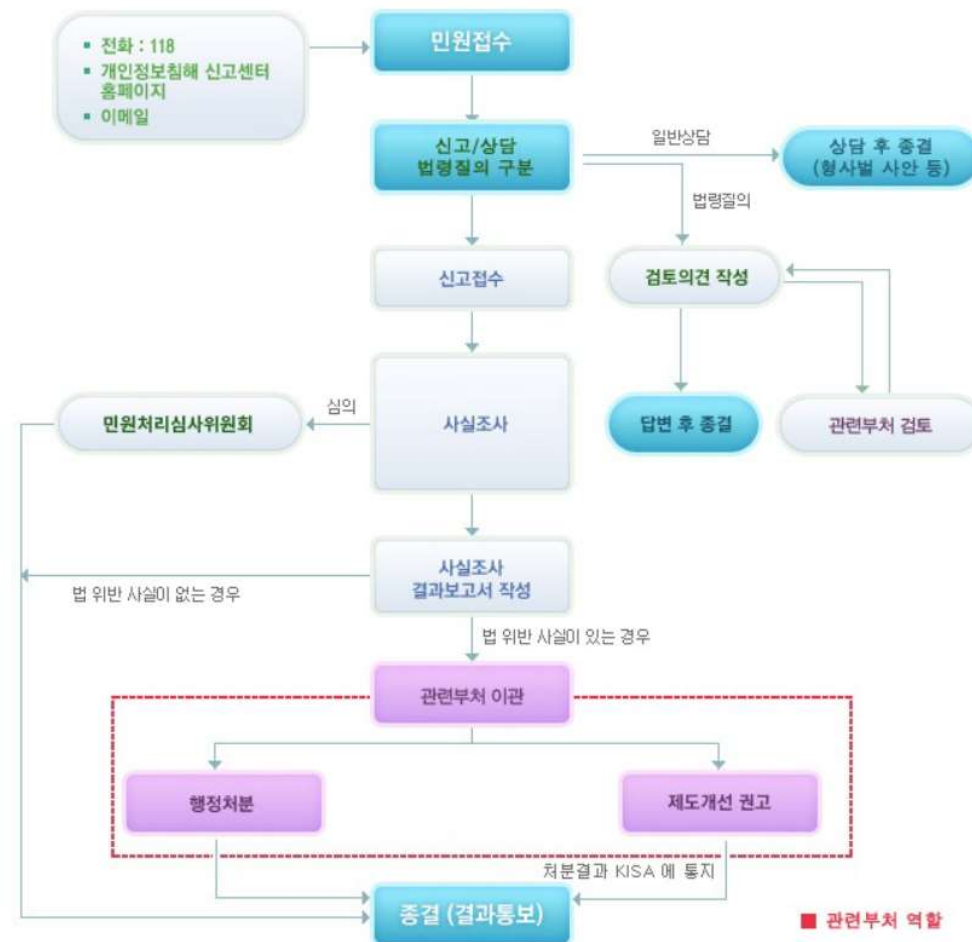
### ■ 개인정보 보호법 적용 대상이 아닌 사안별 신고기관 안내

④ 개인정보 보호법 적용 대상이 아닌 사안별 신고기관 안내

구분	기관명	연락처	홈페이지 주소
④ 해킹, 사기, 불법사이트 등 형사처벌 사안	경찰청 사이버테러대응센터	02)393-9112 182(민원상담)	www.ctrc.go.kr
④ 소비자피해, 불만사항, 분쟁조정	한국소비자원	02)3460-3000 1372(민원상담)	www.kca.go.kr
④ 공정거래법상의 불공정 거래행위	한국공정거래조정원	02)3445-9898 1588-1490(민원상담)	www.kofair.or.kr
④ 금융거래관련 피해 및 분쟁조정	금융감독원	02)3145-5114 1332(민원상담)	www.fss.or.kr
④ 민·형사 등 각종 소송관련 상담	대한법률구조공단	02)532-0132 132(법률상담)	www.klac.or.kr

# 사후 대응방안

## ❖ 개인정보침해 신고/상담 절차



개인정보침해신고센터  
[https://privacy.kisa.or.kr/kor/center/center02\\_new.jsp](https://privacy.kisa.or.kr/kor/center/center02_new.jsp)

# 사후 대응방안

## ❖ 개인정보분쟁조정위원회

- <https://www.kopico.go.kr>

- 제도의의

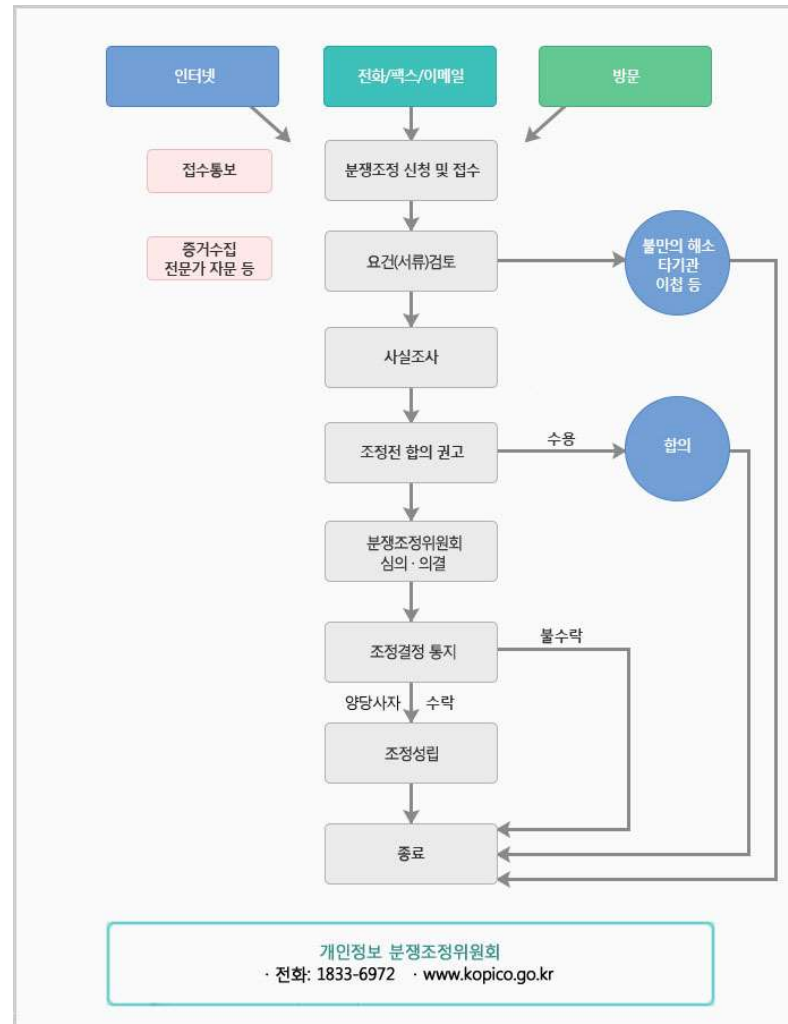
- 개인정보에 관한 분쟁이 발생하였을 때, 비용이 많이 들고 시간이 오래 걸리는 소송 제도의 대안으로
- 비용 없이 신속하게 분쟁을 해결함으로써 개인정보 침해를 당한 국민의 피해에 대하여 신속하고 원만하게 피해를 구제 (개인정보 분쟁조정, 집단분쟁조정)

- 효력

- 신청인과 상대방이 조정 결정을 수락하여 조정이 성립된 경우 “재판상 화해(민사소송법상 확정판결과 동일한 효력)”가 부여
- 조정성립 후 당사자가 결정내용을 이행하지 않을 경우에는 법원으로부터 집행문을 부여 받아 강제집행 가능

# 사후 대응방안

## ❖ 개인정보 분쟁조정 절차



# 개인정보 비식별 조치

## ❖ 비식별화 조치

- 정보집합물(데이터 셋)에서 개인을 식별할 수 있는 요소(식별자, 속성자)를 전부 또는 일부 삭제하거나 대체하는 등의 방법으로 개인을 알아볼 수 없도록 하는 조치
  - 식별자: 개인 또는 개인과 관련된 사물에 고유하게 부여된 값 또는 이름
  - 속성자: 개인과 관련된 정보로서 다른 정보와 쉽게 결합하는 경우 특정 개인을 알아볼 수도 있는 정보
- 개인정보 비식별 조치 가이드라인
  - 빅데이터, IoT 등 새로운 IT 기술과 융합산업의 활성화와 개인정보 보호 강화를 하기 위한 구체적인 가이드 라인

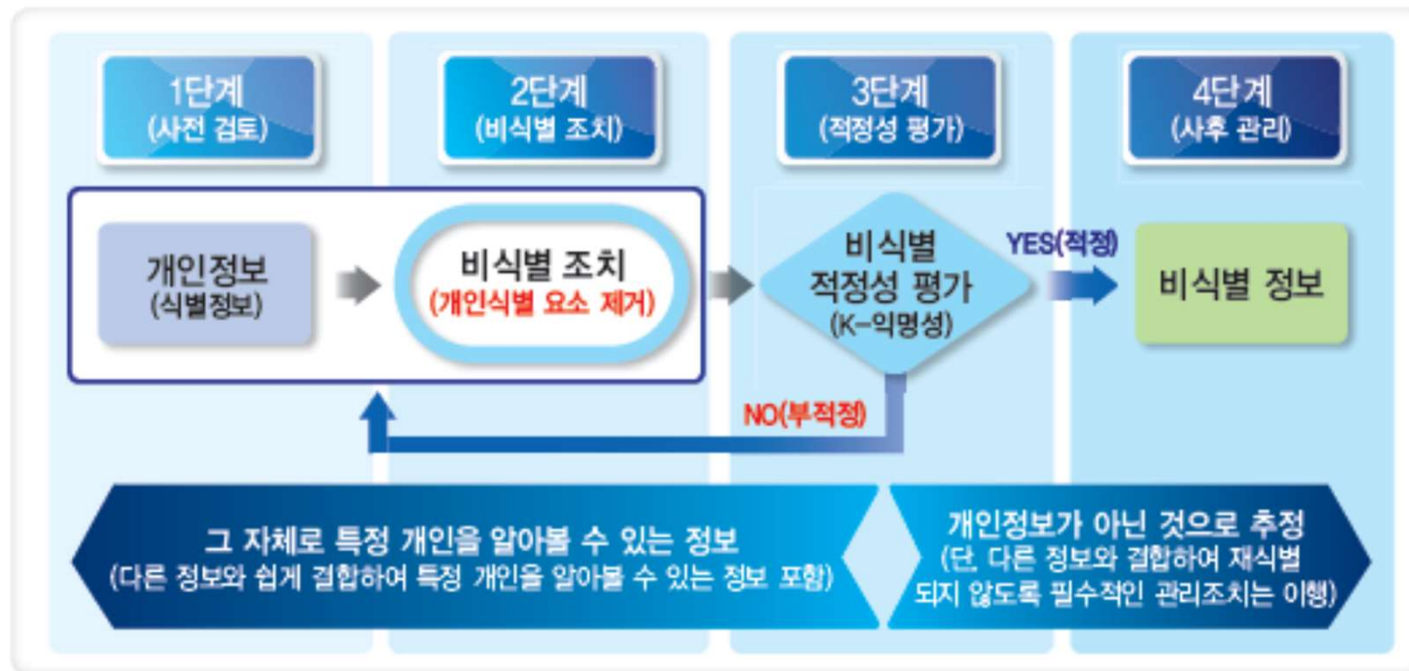
# 개인정보 비식별 조치

## ❖ 비식별 조치 및 사후관리 절차

### ● 단계별 조치사항

- ① (사전 검토) 개인정보에 해당하는지 여부를 검토 후, 개인정보가 아닌 것이 명백한 경우 법적 규제 없이 자유롭게 활용(4쪽 참조)
- ② (비식별 조치) 정보집합물(데이터 셋)에서 개인을 식별할 수 있는 요소를 전부 또는 일부 삭제하거나 대체하는 등의 방법을 활용, 개인을 알아볼 수 없도록 하는 조치(5~8쪽 참조)
- ③ (적정성 평가) 다른 정보와 쉽게 결합하여 개인을 식별할 수 있는지를 「비식별 조치 적정성 평가단」을 통해 평가(9~13쪽 참조)
- ④ (사후관리) 비식별 정보 안전조치, 재식별 가능성 모니터링 등 비식별 정보 활용 과정에서 재식별 방지를 위해 필요한 조치 수행(14~16쪽 참조)

### ● 비식별 조치 및 사후관리 절차 ●



[http://www.keris.or.kr/know/kn\\_support02.jsp?bbsid=board18&gbn=view&gp=1&ps=10&sp=&sw=&ob=sor1&ix=25823&orderkey=3](http://www.keris.or.kr/know/kn_support02.jsp?bbsid=board18&gbn=view&gp=1&ps=10&sp=&sw=&ob=sor1&ix=25823&orderkey=3)

# 개인정보 비식별 조치

## ❖ 비식별화 처리기법

### 일반적 기법 : 개인 식별요소 삭제 방법

처리기법	예시	세부기술
가명처리 (Pseudonymization)	<ul style="list-style-type: none"> <li>홍길동, 35세, 서울 거주, 한국대 재학 → 임꺽정, 30대, 서울 거주, 국제대 재학</li> </ul>	① 휴리스틱 가명화 ② 암호화 ③ 교환 방법
총계처리 (Aggregation)	<ul style="list-style-type: none"> <li>임꺽정 180cm, 홍길동 170cm, 이공쥬 160cm, 김팔쥬 150cm → 물리학과 학생 키 합 : 660cm, 평균키 165cm</li> </ul>	④ 총계처리 ⑤ 부분총계 ⑥ 라운딩 ⑦ 재배열
데이터 삭제 (Data Reduction)	<ul style="list-style-type: none"> <li>주민등록번호 901206-1234567 → 90년대 생, 남자</li> <li>개인과 관련된 날짜정보(합격일 등)는 연단위로 처리</li> </ul>	⑧ 식별자 삭제 ⑨ 식별자 부분삭제 ⑩ 레코드 삭제 ⑪ 식별요소 전부삭제
데이터 범주화 (Data Suppression)	<ul style="list-style-type: none"> <li>홍길동, 35세 → 홍씨, 30~40세</li> </ul>	⑫ 감추기 ⑬ 랜덤 라운딩 ⑭ 범위 방법 ⑮ 제어 라운딩
데이터 마스킹 (Data Masking)	<ul style="list-style-type: none"> <li>홍길동, 35세, 서울 거주, 한국대 재학 → 홍○○, 35세, 서울 거주, ○○대학 재학</li> </ul>	⑯ 임의 잡음 추가 ⑰ 공백과 대체

# 개인정보 비식별 조치

## ❖ 비식별화 처리기법

📌 프라이버시 보호 모델 : 재식별 가능성 검토 기법 \*  $k$ ,  $l$ ,  $t$  값은 전문가 등이 검토하여 마련

기법	의미	적용례
$k$ -익명성	<ul style="list-style-type: none"> <li>특정인임을 추론할 수 있는지 여부를 검토, 일정 확률수준 이상 비식별 되도록 함</li> </ul>	<ul style="list-style-type: none"> <li>동일한 값을 가진 레코드를 <math>k</math>개 이상으로 함. 이 경우 특정 개인을 식별할 확률은 <math>1/k</math>임</li> </ul>
$l$ -다양성	<ul style="list-style-type: none"> <li>특정인 추론이 안된다고 해도 민감한 정보의 다양성을 높여 추론 가능성을 낮추는 기법</li> </ul>	<ul style="list-style-type: none"> <li>각 레코드는 최소 <math>l</math>개 이상의 다양성을 가지도록 하여 동질성 또는 배경지식 등에 의한 추론 방지</li> </ul>
$t$ -근접성	<ul style="list-style-type: none"> <li><math>l</math>-다양성뿐만 아니라, 민감한 정보의 분포를 낮추어 추론 가능성을 더욱 낮추는 기법</li> </ul>	<ul style="list-style-type: none"> <li>전체 데이터 집합의 정보 분포와 특정 정보의 분포 차이를 <math>t</math>이하로 하여 추론 방지</li> </ul>



# 개인정보 비식별 조치

## ❖ 비식별화 처리기법

### 📌 가명처리(Pseudonymization)

- (개념) 개인 식별이 가능한 데이터를 직접적으로 식별할 수 없는 다른 값으로 대체하는 기법
- (대상) 성명, 기타 고유특징(출신학교, 근무처 등)
- (장점) 데이터의 변형 또는 변질 수준이 적음
- (단점) 대체 값 부여 시에도 식별 가능한 고유 속성이 계속 유지

### 📌 총계처리(Aggregation)

- (개념) 통계값(전체 혹은 부분)을 적용하여 특정 개인을 식별할 수 없도록 함
- (대상) 개인과 직접 관련된 날짜 정보(생일, 자격 취득일), 기타 고유 특징(신체정보, 진료기록, 병력정보, 특정소비기록 등 민감한 정보)
- (장점) 민감한 수치 정보에 대하여 비식별 조치가 가능하며, 통계분석용 데이터 셋 작성에 유리함
- (단점) 정밀 분석이 어려우며, 집계 수량이 적을 경우 추론에 의한 식별 가능성 있음

# 개인정보 비식별 조치

## 📌 데이터 삭제(Data Reduction)

- (개념) 개인 식별이 가능한 데이터 삭제 처리
- (대상) 개인을 식별 할 수 있는 정보(이름, 전화번호, 주소, 생년월일, 사진, 고유식별 정보(주민등록번호, 운전면허번호 등), 생체정보(지문, 홍채, DNA 정보 등), 기타 (등록번호, 계좌번호, 이메일주소 등))
- (장점) 개인 식별요소의 전부 및 일부 삭제 처리가 가능
- (단점) 분석의 다양성과 분석 결과의 유효성 · 신뢰성 저하

## 📌 데이터 범주화(Data Suppression)

- (개념) 특정 정보를 해당 그룹의 대푯값으로 변환(범주화)하거나 구간값으로 변환(범주화) 하여 개인 식별을 방지
- (대상) 개인을 식별할 수 있는 정보(주소, 생년월일, 고유식별정보(주민등록번호, 운전 면허번호 등), 기관 · 단체 등의 이용자 계정(등록번호, 계좌번호))
- (장점) 통계형 데이터 형식이므로 다양한 분석 및 가공 가능
- (단점) 정확한 분석결과 도출이 어려우며, 데이터 범위 구간이 좁혀질 경우 추론 가능성 있음

# 개인정보 비식별 조치

## ◆ 데이터 마스킹(Data Masking)

- (개념) 데이터의 전부 또는 일부분을 대체값(공백, 노이즈 등)으로 변환
- (대상) 쉽게 개인을 식별할 수 있는 정보(이름, 전화번호, 주소, 생년월일, 사진, 고유 식별정보(주민등록번호, 운전면허번호 등), 기관·단체 등의 이용자 계정(등록번호, 계좌번호, 이메일 주소 등) )
- (장점) 개인 식별 요소를 제거하는 것이 가능하며, 원 데이터 구조에 대한 변형이 적음
- (단점) 마스킹을 과도하게 적용할 경우 데이터 필요 목적에 활용하기 어려우며 마스킹 수준이 낮을 경우 특정한 값에 대한 추론 가능