스마트 시대의 개인정보보호 현실 및 대응방안

2014. 4. 24.

개인정보안전단장 권현준

제9회, [NES2014]
차세대 기업보안 세미나/전시회

KISA 한국인터넷진흥원
Korea Internet & Security Agency

목 차

1장 스마트 시대의 빛과 그림자

스마트 혁명의 시대

- 스마트폰 및 모바일 활성화로 정치, 경제, 사회, 문화 등 전 분야에서 혁신과 변화

정치

소통 방식의 변화

SNS를 통해 수많은 팔로워들과 교류(리트윗 등)하면서 실시간 의사소통

경제

상거래 방식의 변화

모바일 쇼핑 및 결제 활성화로 소비자 구매 행태 변화

사회 · 문화

문화생활 방식의 변화

모바일 티켓, 위치정보확인, SNS 등 다양한 서비스를 통한 문화 생활 변화

스마트 혁명의 빛 : SNS와 정치

- **SNS를 활용한 다방향 소통으로 새로운 정치 문화의 창출**

  ※ 국가의 선거 및 정치과정에서 트위터 등 SNS의 영향력 증가(국내 총선 및 대선 등)

SNS 기반 新 정치

트위터 투표 독려

오바마 Facebook 대선 출정식

LinkedIn

twitter

facebook

me2day

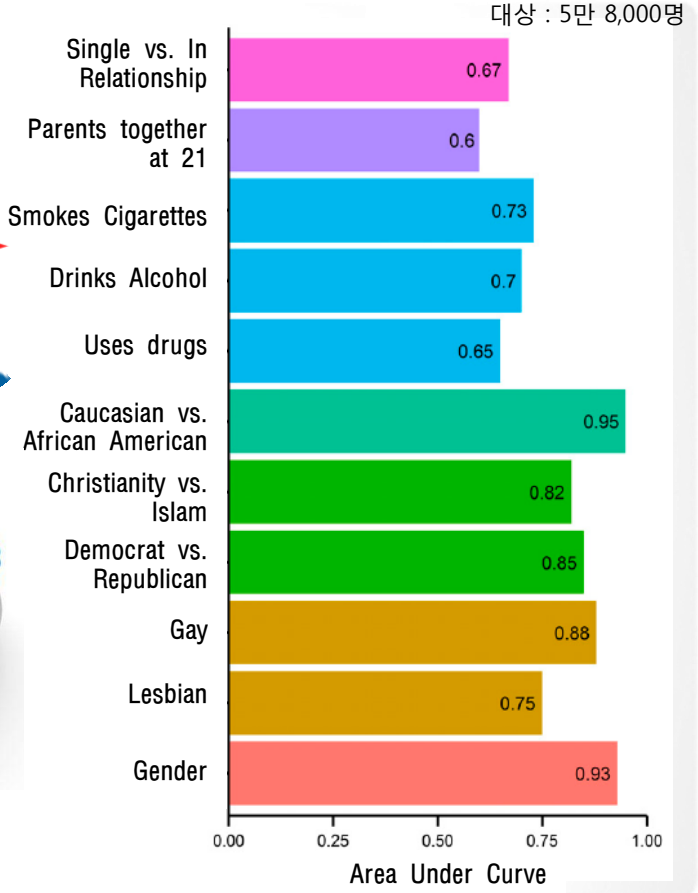
와이즈넛사의 2012 대선 SNS 분석

스마트 혁명의 빛 : 모바일과 생활방식

- 모바일상거래(종이티켓→전자티켓), 위치찾기(종이지도→실시간 LBS) , 실시간 소통(PC기반 블로그→실시간SNS), 맛집 검색(입소문→실시간 댓글) 등 다양한 분야에서 모바일을 통한 생활 방식의 변화

스마트 혁명의 그림자: 사생활의 공개 ①

- 페이스북 게시물에 대한 **의사표현만 분석해도** 사용자의 민감한 개인정보 예측
  - 인종(95%), 성별(93%), 지지정당(85%), 종교(82%) 등에 대한 정보 파악



[출처 : Michal Kosinski 외, PNAS, 2013]

스마트 혁명의 그림자: 사생활 공개 ②

- 자신도 모르는 사이에 얼굴과 이름 노출될 수 있어 **프라이버시 침해**

페이스북 얼굴인식 기능

- 여러 장의 사진 업로드시, 사진속 비슷한 인물 그룹화 및 태그 기능
  - 기존 태그된 얼굴정보를 분석하여 신규 인물에 대해 자동으로 이름 제안
- 사진의 태그 추천기능이 디폴트로 사용됨

침해사례

길거리 시위 키스 사진이 페이스북에 업로드됨

⬇

얼굴인식 기능으로 커플의 이름 노출

⬇

노출 이름으로 신상털이

⬇

性的 취향 등 원하지 않은 사생활 공개

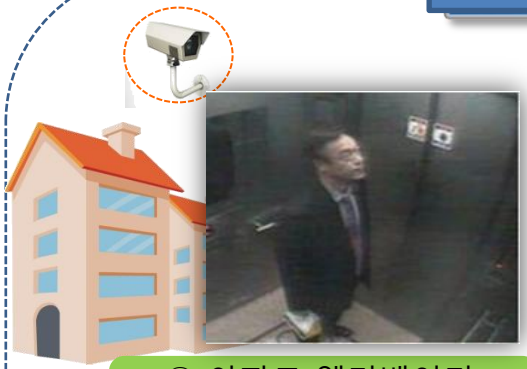
스마트 혁명의 그림자 : 사생활 공개 ③

개인당 하루 평균 최소 59회에서 최대 110회 CCTV에 노출 (2010.12 국가인권위 조사)

- 수도권 시민 하루 평균 83회 노출 (지하철 환승 시 50회, 백화점 3시간 동안 45회)

※ 방범용 3만5천대, 대중교통 20만대, 상점 · 기업 등 250만대, 주요고속도로 1천5백대 설치(2009.11. KBS)

<김팀장의 하루(2009.3, 조선닷컴)>



① 아파트 엘리베이터, 2회 (출근, 퇴근)

② 지하철2호선 삼성역, 14회

③ 삼성동 코엑스 에스컬레이터, 53회

④ 삼성동 코엑스 편의점, 4회

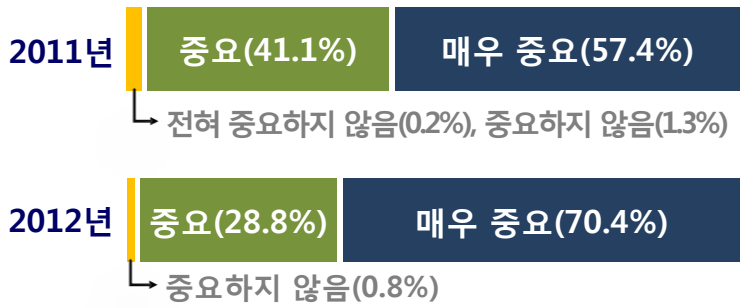
⑤ 6900번 버스, 1회

(사실) 빛이 강렬하면 그림자도 짙음

- 정보기술의 스마트화에 따라 현대인의 **프라이버시 침해에 대한 우려**가 증대

개인정보보호의 중요성

[개인정보보호의 중요성에 대한 인식률]

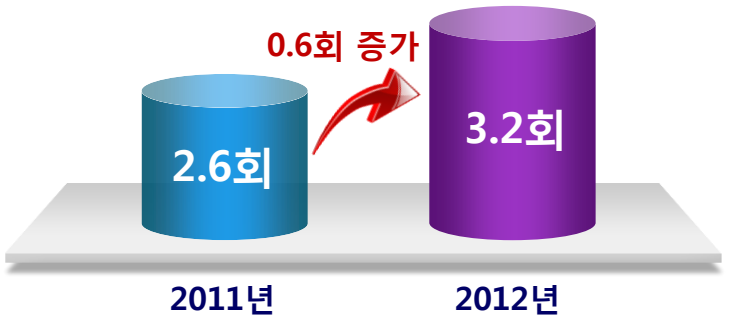


- 국내 인터넷 이용자의 99.2%는 개인정보보호가 중요하다고 인식하는 것으로 나타남

출처 : 2012 정보보호 실태조사(개인편), KISA

프라이버시 침해 피해 증가

[개인/프라이버시 침해로 인한 피해 경험 횟수]



- 만12~59세의 인터넷 이용자 중 프라이버시 침해로 인한 평균 피해 횟수는 3.2회로 조사됨

출처 : 2012 정보보호 실태조사(개인편), KISA

[화두] 과연 스마트 혁명은 개인정보보호와 충돌한 운명인가?

2장 스마트 시대의 주요 개인정보 이슈

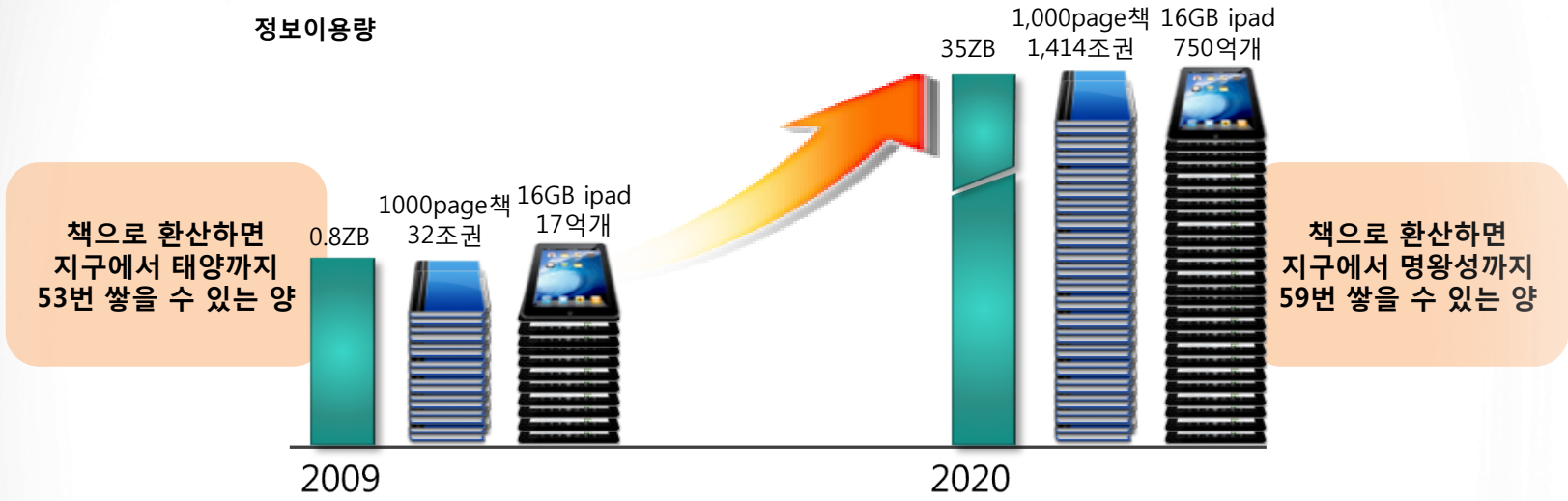
1. Big Data
2. 잊혀질 권리
3. 디지털 유산
4. 웨어러블 컴퓨터

1. Big Data : 디지털 데이터 폭증

Big Data란?

- 일반적인 DB SW가 저장, 관리, 분석할 수 있는 범위를 초과하는 규모의 데이터 (Mckinsey, '11.)
- high-volume, high-velocity, high-variety의 특징을 보임

2020년 전 세계 보유 데이터량(IDC)



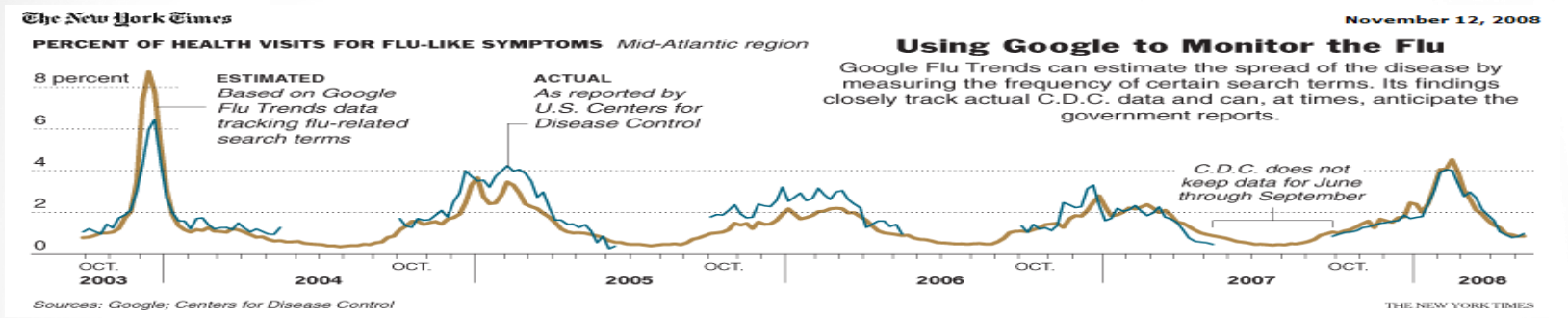
2020년 세계의 데이터양은 '09년 대비 44배 증가로 Big Data분석의 중요성 부각

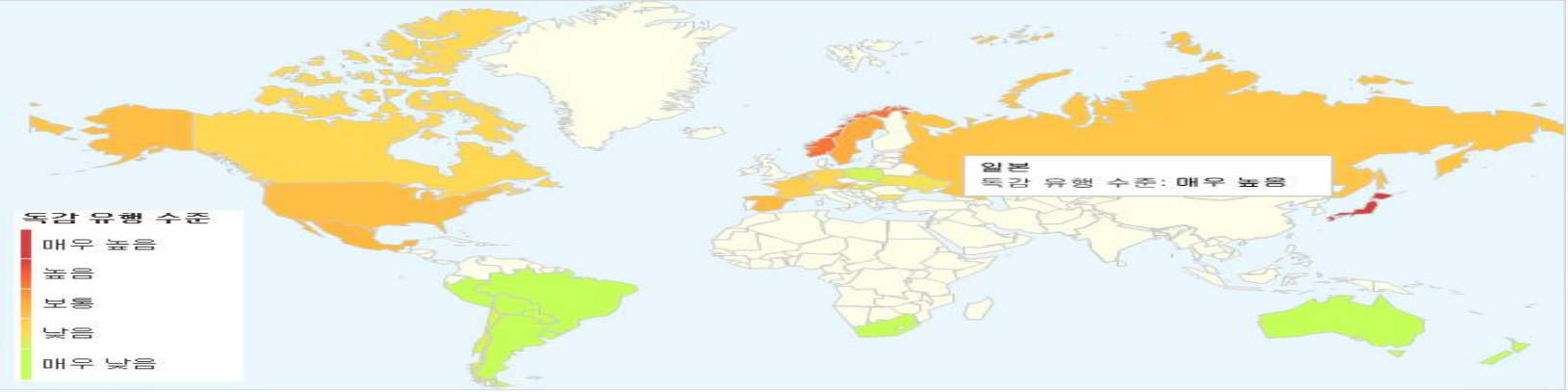
- 1인당 보유 데이터량은 117GB에서 4.6TB로 증가(1천 페이지 책 28만권 분량)

※ GB(gigabyte 10^9), TB(terabyte 10^{12}), PB(petabyte 10^{15}), EB(exabyte 10^{18}), ZB(zettabyte 10^{21})

1. Big Data : 활용 사례 ①

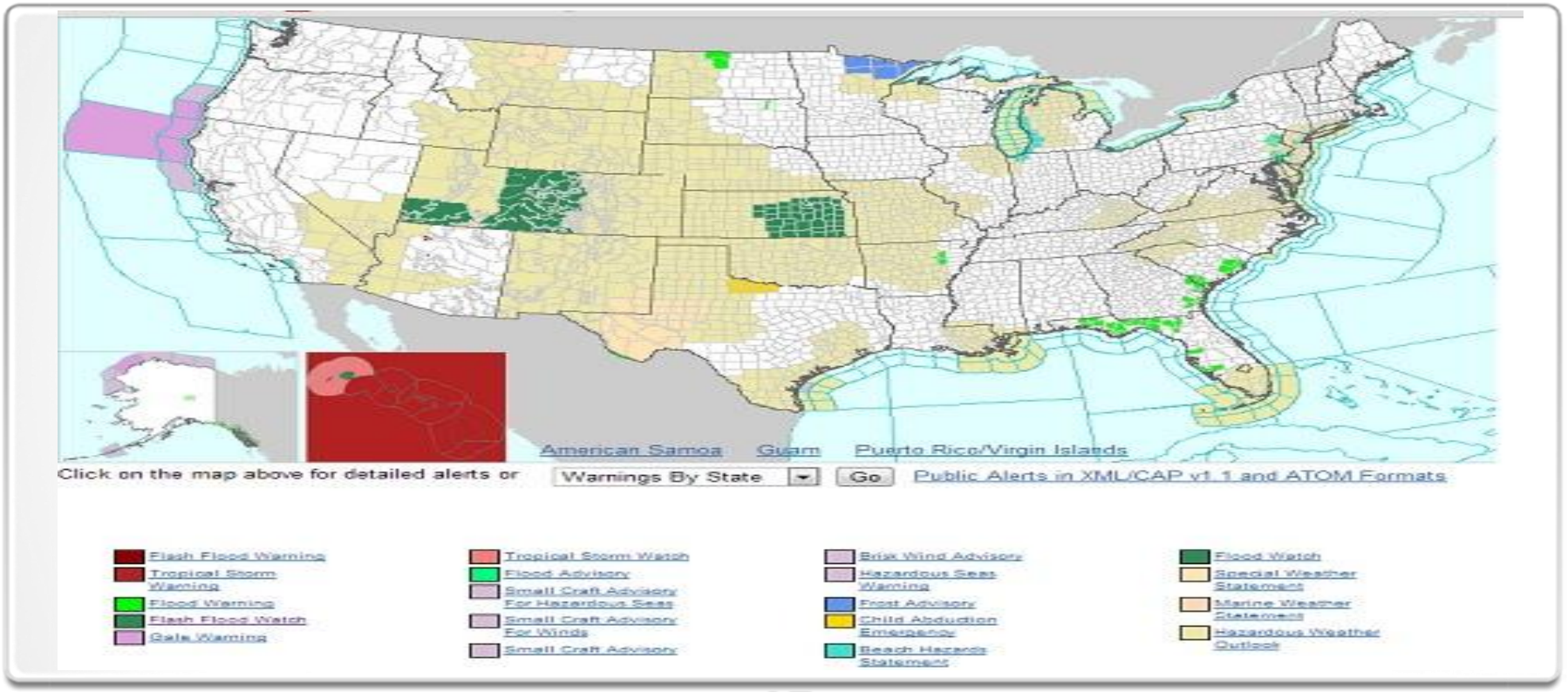
- **Google 독감 트렌드 서비스**
  - 2008년 11월 부터 선보인 '독감 트렌드' **서비스는 전 세계 각지에서 독감과 관련된 검색어의 입력 빈도를 지역별로 파악**해 독감 유행 수준을 '매우 낮음'부터 '매우 높음'까지 5개 등급으로 구분해 표시(美질병통제예방센터보다 1~2주 빠름)





1. Big Data : 활용 사례 ②

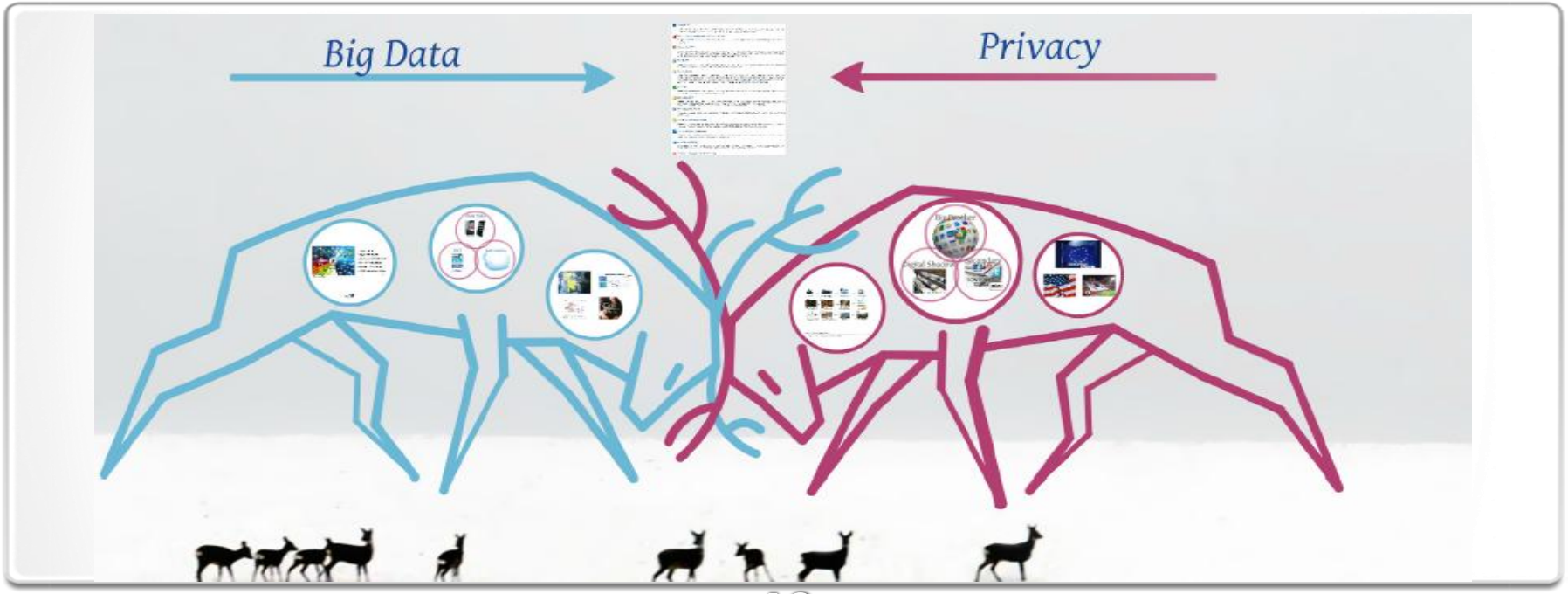
- 美, 국립해양대기청(NOAA)의 '전국기상서비스(National Weather Service)'
  - 지역센서, 배, 비행기 등을 통해 35억개 이상의 정보 수집
  - 6시간 간격으로 미국 전역의 홍수, 가뭄, 허리케인, 뇌우 등 24가지의 경보를 제공



1. Big Data : 프라이버시 (공공)

- 정부는 양방향 · 개인 맞춤형 정보 제공이라는 '정부 3.0' 새로운 패러다임 제시
  - 공공정보를 적극적으로 개방하고 공유하며 부처간 칸막이를 없애 소통하고 협력함으로써, 국민 맞춤형 서비스를 제공
  - 한국도로공사는 '재정-민자 통합요금정산시스템' 구축 및 '전국호환교통카드시스템' 확대를 통해 고객의 불편 해소 기여

➡ 개인에 관한 자료들이 광범위하게 취합 · 이용되어 사생활 침해 가능성 증가



1. Big Data : 프라이버시(민간)

- 기업은 빅데이터의 분석을 최대한 활용하여 기업 수익과 연계하려고 노력
  - 스포츠, 금융, 통신, 의료, 카드, 부동산, 스포츠 등 다양한 분야에서는 빅데이터를 이용하여 타켓마케팅으로 수익 극대화를 추구
  - 미국에서는 유통업체가 이용자의 구매이력을 분석하여 임산부용 쿠폰을 발송 여고생의 임신 사실을 부모보다 먼저 알아내어 마케팅에 이용하는 상황 발생
  - 얼굴 인식 기술이 '구글 글래스' 와 같은 기기와 연결될 경우, 심각한 사생활 침해 가능

- 빅데이터 기술의 발전으로 사적 공간의 경계가 점차 모호해지며 분쟁 증가 예상
  - 영화 '마이너리리포트' 에서는 범죄예측시스템을 이용하여 발생하지 않은 사건임에도 범죄자가 됨

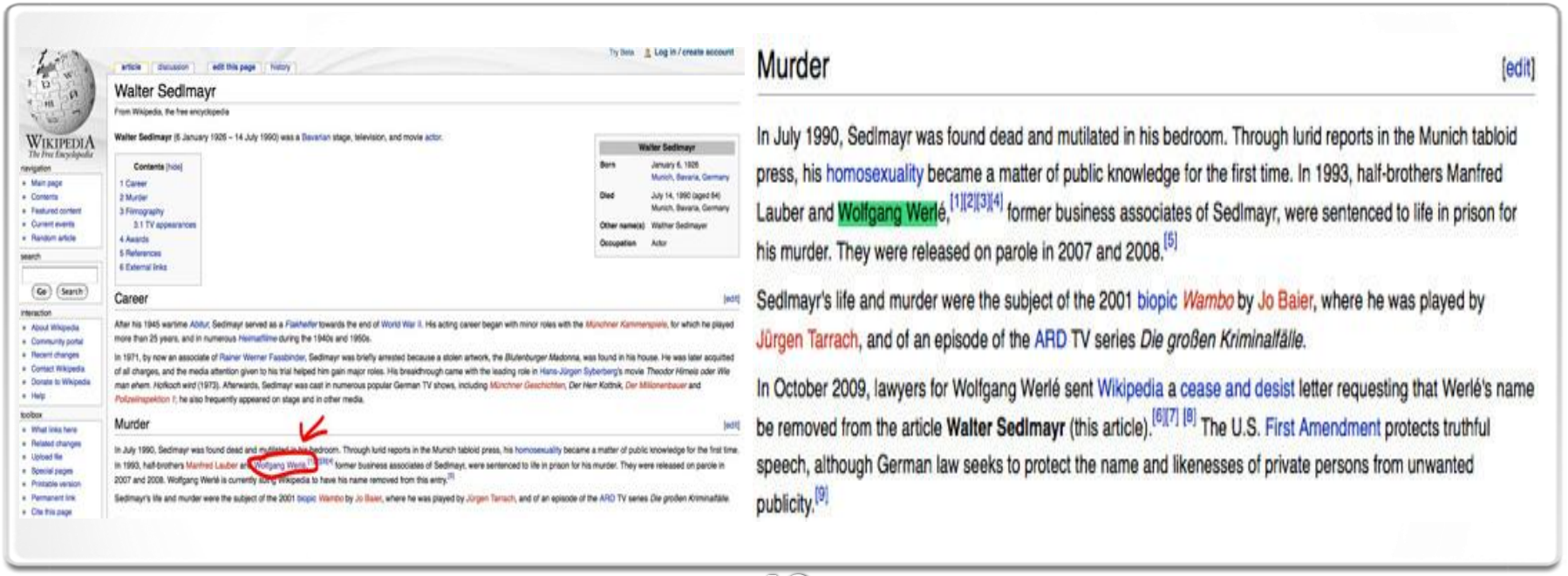
2. 잊혀질 권리 : 개념

- 자신과 관계있는 정보가 더 이상 보존.이용하는 것이 필요하지 않은 경우 삭제조치를 하여 타인이 이용(검색)할 수 없도록 함으로써 해당 정보로부터 자유로울 권리

2. 잊혀질 권리 : 해외 소송 사례 (독일)

- **범죄자 신상정보 삭제 인정 : Walter Sedlmayr 사건('07)**
  - **Walter Sedlmayr의 살인자는 '위키피디아'에 공개된 자신들의 이름에 대한 삭제를 요청하였으나 거부**
  - **독일 법원은 위키피디아 독일어판에서 이들의 이름을 삭제하도록 판결('08.1월)**

※ **독일**은 1973년의 '형기를 마친 범죄자의 신상은 삭제해 주어야 한다'는 연방헌법 재판소의 판례와 관련 성문법에 따라 전과사실 삭제를 인정하였으나, **미국**의 경우, 위키피디아 영어판 삭제에 대해 법원은 헌법상의 표현의 자유와 언론의 자유를 중시하여 인정하지 않음



2. 잊혀질 권리 : 해외 소송 사례 (미국)

- **보도기사 삭제 불인정 : Chris Purtz 사건('11)**
  - 미국 언론기관 Daily Californian은 미식축구 선수인 Chris Purtz가 스트립 클럽에서의 폭행으로 소속팀에서 방출되었다는 기사를 웹에 게시('06.10월)
  - Chris Purtz의 아버지는 해당 기사로 인해 Chris Purtz가 자살하여, 해당 기사를 삭제해 달라고 요청하였으나 거부당함 ('11.1월)

※ 미국 법원에서는 표현의 자유를 중시하여 불인정

THE DAILY CALIFORNIAN
DAILYCAL.ORG
Tuesday, January 18, 2011 | 5:57 am

ADD WWW.DAILYCAL.ORG TO BOOKMARKS
SIGN UP FOR: MOBILE | RSS FEED
General Search
Advanced Search

ABOUT | NEWS | SPORTS | ARTS & ENTERTAINMENT | OPINION | BL

Football Player Suspended After Incident At Adult Club

Bryan Thomas is the city news editor. Contact him at bthomas@dailycal.org.

By BRYAN THOMAS
DAILY CAL STAFF WRITER
Thursday, October 12, 2006
Category: News

Printer Friendly
Comments (1)
Email/Share

A Cal football player is suspended indefinitely from the team pending an investigation of reports that he was involved in a physical confrontation and verbal abuse at a San Francisco adult club early Sunday, Cal Athletics said yesterday.

UC Berkeley senior and linebacker Chris Purtz, 21, went early Sunday morning with a friend to the Lusty Lady adult club, where employees said he shoved a worker and used racist and homophobic slurs.

Club employees described Purtz as intoxicated and said he identified himself as a Cal football player.

At the club, Purtz entered a video pornography booth while his friend, who identified himself as Purtz's agent, demanded prostitutes for the two men, according to Dee Timmons, an employee at Lusty Lady who said he let the men into the club.

Purtz does not have an agent, said Cal Athletics spokesperson John Sudsbury.

2. 잊혀질 권리 : 주요 이슈

삭제대상

- **어느 정보까지 삭제를 인정할 것인가?**
  - 사업자가 서비스 제공을 위해 보유하고 있는 개인정보에 국한해 삭제할지 여부
  - 게시글, 검색결과 , 기사글 등 자신과 관련된 다양한 모든 정보의 삭제 인정 여부

사업자의 부담

- **정보 삭제를 위해 얼마나 많은 시간과 비용이 소요될 것인가?**
  - 사업자에게 경제적 · 기술적 부담을 초래하여 기업 활동 위축 우려

삭제가능성

- **인터넷이라는 오픈된 환경에서 자신의 정보를 모두 지울 수 있나?**
  - 제3자가 링크. 복사하여 옮긴 많은 사이트를 어떻게 파악하고 실제 삭제할 수 있는지 여부
  - 실제 삭제 가능한 기술적 범위 내에서 잊혀질 권리를 규정하는 것이 필요하다는 의견 제시

※ ENISA(European Network & Security Agency) "The Right to Be Forgotten – Between Expectations and Practice" ('12.11월)

타인의 권리침해

- **인터넷상에서 타인에 대한 표현 금지?**
  - 정보 자기결정권적인 측면에서는 바람직하나, 타인의 표현의 자유나 알권리 침해 우려

2. 잊혀질 권리 : 국외 입법 동향

- **유럽의 경우, 잊혀질 권리 법제화(EU 개인정보호규정안) 관련한 찬반의견이 대립**
  - **자기정보결정권 강화라는 측면에서 환영한다는 입장(EU집행부 · 의회 등)**
  - **EU 각 산업계는 잊혀질 권리 도입에 대한 반대 의견 제시**

    ※ 기술적 실현가능성, 표현의 자유 제한, 서비스 형태를 고려하지 않은 권리 인정 등을 이유로 법제화 반대 또는 개정안 내용 수정 요구
  - **영국 정부는 잊혀질 권리는 비현실적일 뿐 만 아니라 인터넷 경제의 위축을 초래할 수 있으므로 도입이 시기상조라고 반대 의견('13.4월)**

- **미국의 경우, 표현의 자유(수정헌법 제1조)를 중시하여 잊혀질 권리에 대한 활발한 논의는 없으나, 개별법으로 제한적 삭제권 도입**

  ※ 미국 캘리포니아 온라인 프라이버시법(California Online Privacy Act, CalOPPA)에 미성년자에 관한 게시 정보 삭제권 신설('15.1.1 시행)

2. 잊혀질 권리 : EU 개인정보보호규정안 제17조 잊혀질 권리 주요내용

- **(개념)** 정보주체가 자신과 관련된 정보에 대해 삭제 및 확산 방지를 개인정보 처리자에게 요청할 수 있는 권리

  ※ EU 개인정보보호규정안 제17조 (Right to be forgotten and to erasure)에 규정

- **(삭제요청)** 삭제사유를 구체적으로 제시하여 삭제 요청 시 지체 없이 삭제할 의무를 부과하며, 다른 권리 등의 침해 방지를 위해 예외사유 규정

  ※ 삭제요청사유 : 개인정보의 수집 및 처리 목적이 달성된 경우, 정보 수집.이용 동의를 철회하거나 보유기간이 경과한 경우, 다른 이유로 본 규정안을 위반하는 정보 처리의 경우 등

  ※ 삭제예외사유 : 표현의 자유에 반하는 경우, 공중 보건 분야에서 공익을 위한 경우, 역사.통계.과학 연구 목적으로 필요한 경우, 타 법률에 의해 보관해야 하는 경우

- **(제3자에 대한 삭제통보)** 개인정보처리자는 해당 정보를 링크.복제한 제3자에게 정보주체의 삭제요청 사실을 통보하는 의무를 부과하여 제3자가 삭제할 수 있도록 규정

  ※ 사실상 개인정보처리자에게 복제된 정보주체의 정보를 삭제하는 책임 부여

- **(벌칙)** 잊혀질 권리 및 삭제권 위반 시 개인에게 최고 50만 유로의 벌금을, 기업은 연간 전세계 매출액의 1%까지 과징금 부과를 할 수 있도록 규정

3. 디지털 유산 : 개념

- (개념) 사망시 보유하고 있던 모든 디지털 형태의 재산에 관한 권리와 의무
- (특성) 디지털 형태, 다양성 및 혼합성, 온라인서비스제공자의 역할 증대
  - 디지털 유산은 다양한 성질을 가진 정보가 결합·융합된 형태로 존재하므로 각 정보의 내용에 따라 법적 성질을 고려하여야 함

온라인상 개인정보

이용자 제작 컨텐츠

디지털 형태의 음악이나 동영상, 디지털 디자인, 홈페이지, 블로그, 미니홈피, 카페, 소셜서비스, 온라인 게시물 및 댓글, 도메인 이름, 계정, 게임 아이템, 아바타, 게임머니, 가상화폐 등

3. 디지털 유산 : 주요 이슈

상속대상

- 사망시 보유하고 있던 디지털 형태로 존재하는 재산의 어느 범위까지 상속의 대상으로 볼 것인가?

상속범위

- 누구에게 상속을 인정할 것인가?

처리기준

- 디지털 유산과 관련한 문제를 단지 온라인서비스제공자의 약관(개인정보 취급방침 포함)에만 맡겨 둘 것인가 아니면 입법적으로 해결할 것인가 ?

3. 디지털 유산 : 국내외 처리현황 ①

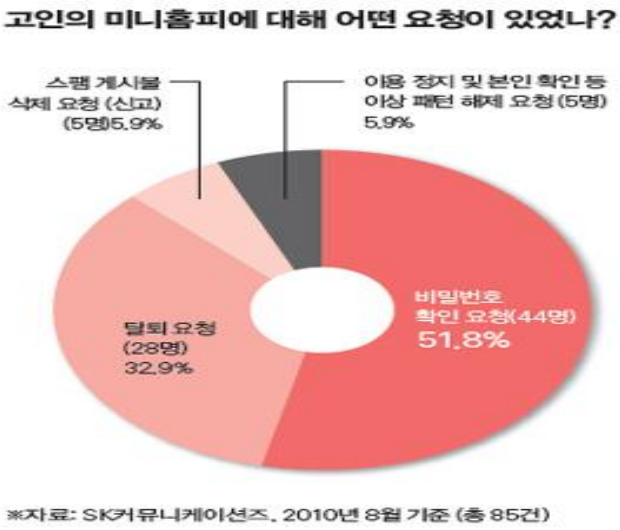
- **(해외) 야후, MSN 등의 글로벌 사업자들은 대부분 사망 후 가족의 청구로 백업 또는 영구삭제(폐쇄)**

  ※ 페이스북이나 트위터의 경우 사망증명시 직계가족의 요청으로 기념계정으로 설정 가능

  ※ 미국의 경우 디지털 유산위탁관리회사 (ex. Deathswitch)가 존재하여 서비스 제공

- **(국내) Daum, SK컴즈 등의 국내 사업자는 사망사실증명 및 가족의 청구로 이용해지, 도용 및 스팸관리 등 실시(이용약관에 근거)**

  ※ 사망자의 ID이용・비밀번호 제공・명의변경은 인정하지 않으며, 사업자에 따라 공개 게시물에 한하여 백업을 인정하는 경우도 있음



3. 디지털 유산 : 국내외 처리현황 ②

- **구글 휴면 계정 관리자(Inactive Account Manager)('13.4월~)**

  - **사후에도 자기정보 결정권을 행사할 수 있다는 기능을 사업자가 제공**

① **휴면기간 및 공유자 지정 :** 이용자는 휴면 계정이 되는 기간을 설정하고, 또한 자신의 데이터를 공유할 가족 또는 친구를 10명까지 미리 지정

② **휴면사실 고지 :** 이용자가 설정한 휴면기간 동안 구글계정에 접속하지 않으면 구글은 이용자에게 그 사실을 알리고, 알림 서비스 이후에도 구글 계정에 접속하지 않으면 구글은 미리 지정된 사람들에게 그 사실을 알림

③ **데이터 공유 및 계정 폐쇄 :** 이후 구글은 지정된 사람들에게 이용자의 데이터를 공유하도록 하고, 이용자는 데이터 공유 후 자신의 (휴면) 계정이 삭제되도록 미리 설정 가능

4. 웨어러블 컴퓨터의 개념

- 웨어러블 디바이스는 신체에 부착하여 컴퓨팅 행위를 할 수 있는 모든 것을 지칭하며, 일부 컴퓨팅 기능을 수행할 수 있는 애플리케이션 까지 포함(MIT)

초기 부착형 타입('60-'70)
- 전자기기의 단순 부착 형태
- 시계나 신발에 계산기나 카메라를 부착하는 형태

프로토 타입 등장('80-'90)
- 입출력 장치와 컴퓨팅 기능의 도입
- 컴퓨터를 착용하고 손이나 발에 달린 입력장치를 이용하여 결과가 출력되는 형태로 다양한 프로토 타입이 등장함

Before PC

유비쿼터스 컴퓨팅 등장('90-'00)
- 경량화의 성공과 산업에서의 본격 적용
- 컴퓨팅 기능이 빨라지고 실제 착용이 가능할뱜큼 부품들이 가벼워 군사 및 산업분야에서 사용되기 시작함

PC Era

통신 네트워크와의 접촉 시도 ('00-'09)
- 본격적인 Connected Device로의 확장 시도
- 네트워크 불안정성, 기기적 성능 부족으로 저변확대 실패

Internet Era

스마트 디바이스와의 결합 ('09- Now)
- 본격적인 상용화를 시작함
- 스마트폰의 액세서리 개념인 앱세서리 형태로 보급 시작

Wearable Device의 본격적 도래 ('14~)
- 자체적으로 네트워크와 접속 가능
- 스마트폰 이외 디바이스와의 확장성이 강화 (IoT로의 진입)

Smart Revolution

IoT Era

출처 : Eco-System 관점에서 바라본 Wearable Device 시장 전망, 심수민(KT), 2013. 7.

4. 웨어러블 컴퓨터의 유형

출처 : ICT 기획시리즈, "차세대 웨어러블의 현재와 미래 그리고 이슈", 2014. 3.

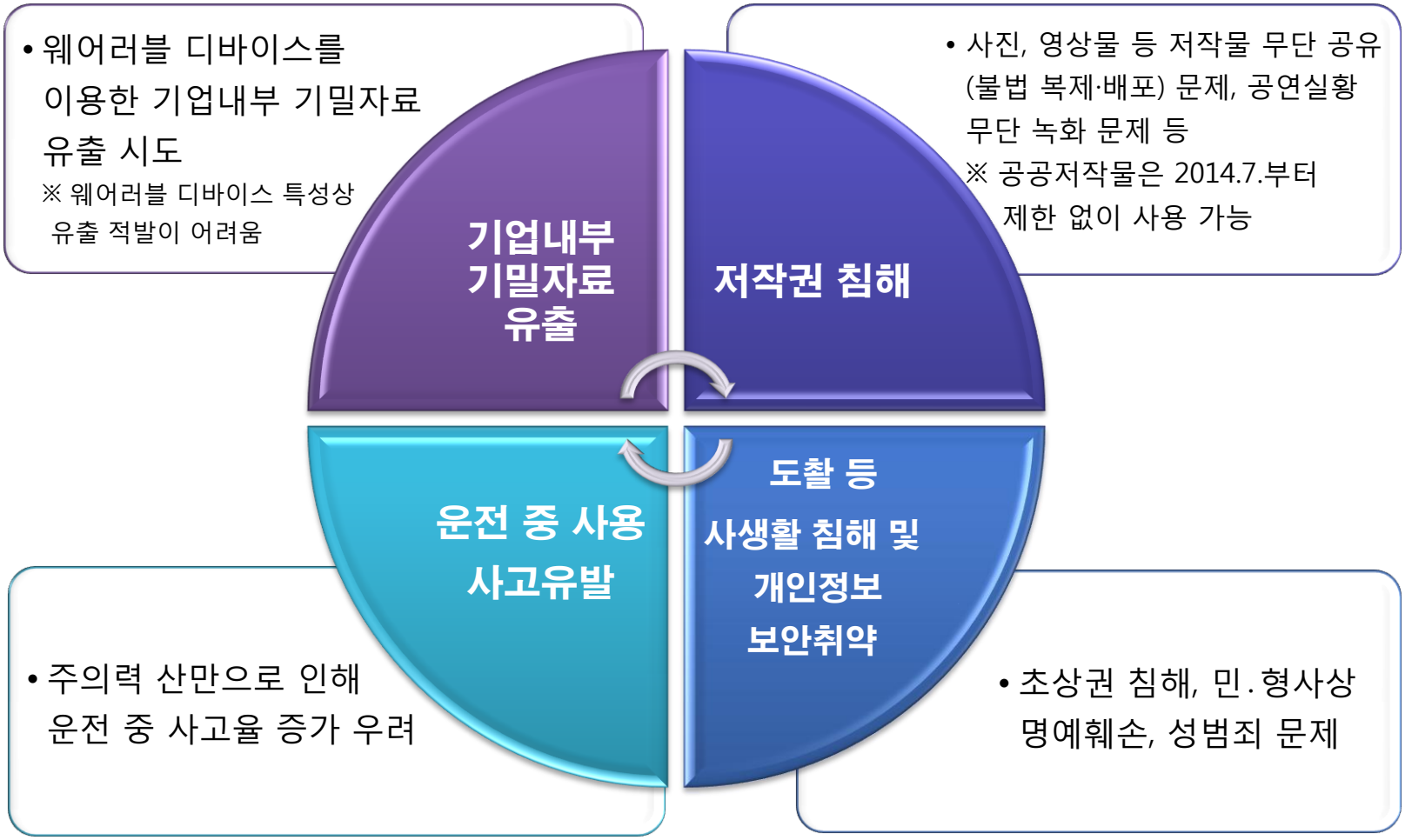
4. 웨어러블 컴퓨터의 사례

- No Place Like Home(Dominic Wilcox) : GPS가 내장된 신발로, 신발 LED표시를 이용하여, 사전에 USB를 통해 입력한 장소로 안내(오즈의 마법사에서 영감)

출처 : http://dominicwilcox.com/portfolio/gpsshoe

4. 웨어러블 컴퓨터의 이슈 분야

- 웨어러블 컴퓨팅 이용에 따라 예상되는 법적 이슈



4. 웨어러블 컴퓨팅이 발생시킬 수 있는 법 이슈(개인정보보호법 기준)

① 수집동의받아야 하는가? (법15조)
- 받는다면 어떻게?

② 열람을 요청한다면? (법35조)
- 내 사생활을 찍은 것인데 행인이 요청하면?

③ 삭제를 요구한다면? (법36조)

④ 난 2살인데 구글 글라스쓰면 개인정보처리자인가요?
- 동의는 옹알이로 받나요?

⑤ 보험설계사는 우리 보험자 직원은 아닌데… 그 사람이 개인적으로 구글 글라스 사서 영업에 이용한 것까지 우리회사가 신경써야 하나요?

위치정보

다른정보와 결합

정보주체

개인정보의 수집

웨어러블 디바이스

개인정보의 전달

ICT서비스 제공자

⑥ 처음에는 개인정보가 아니였는데 다른 정보와 결합해서 개인정보가 될 수 있다면? (법2조)

- 무엇을 어찌해야 하는 것인가?

다른정보와 결합

결제정보

센서수집 정보

⑦ 웨어러블 디바이스가 수집한 정보가 누군가에 의해 처리된다면…

- 제3자 제공인가? (법17조)
- 위탁인가? (법26조)
- 안정성확보조치를 해야하는 것인가? (법29조)
- 파기는? (법21조)

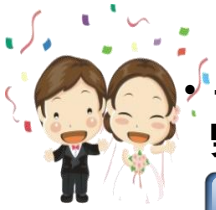
3장 개인정보 침해 현황 및 사례

개인정보의 활용 확대 (유출동기의 증가)

민간 및 공공의 거의 대부분의 업무는 개인정보에 기반

- 온라인 뱅킹
- 전자금융거래 등

금융기관



- 온·오프라인을 통해 맞춤형 결혼 중개

결혼중개업

- 주유 고객 멤버십
- 주유 마일리지 제공

정유업

주택관리업

- 홈네트워킹 관리

학원,교습소

- 온라인 수강신청, 수강자 관리
- 인터넷·오프라인 연계 학습환경

영화관

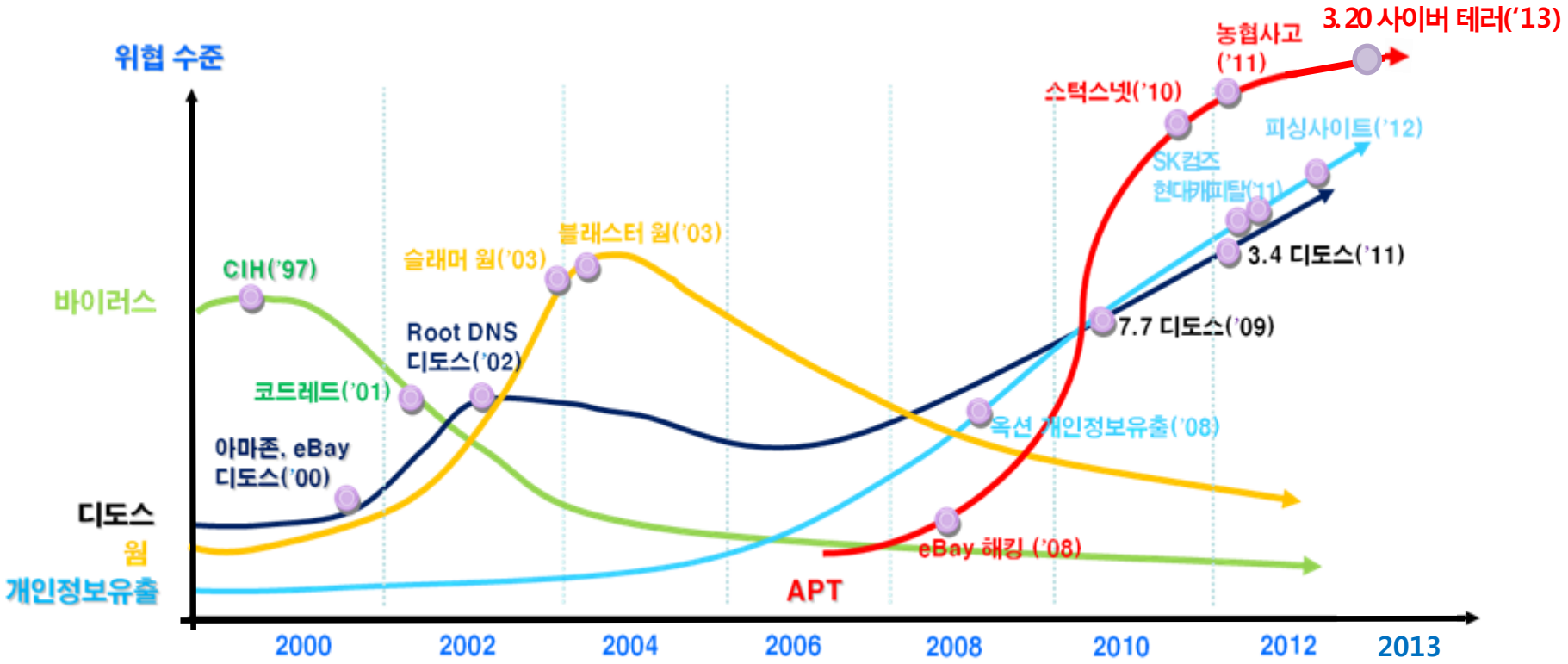
- 인터넷, 모바일 예매
- 무인발권시스템

여행업

- 전자항공권 발권
- 실시간 온라인 예약

보안 위협의 진화 (유출수단의 증가)

- 목적 : 자기과시 ➡ 금품갈취 ➡ 사이버테러(사회혼란)
- 기법 : 수동 ➡ 은닉, 자동화 ➡ 조직적, 지능화
- 대상 : 개별시스템 ➡ 대규모, 네트워크 ➡ 사회기반시설, 국가



※ APT(Advanced Persistent Threat) : 명확한 목표물에 대해 장시간 동안 치밀하고 정교하게 공격하는 것

개인정보 침해사고 증가 (결과)

東亞日報

2010년 03월 12일 금요일 A14면 사회

개인정보 2000여만건 中 해커에 구입 되팔아

일당 2명 불구속입건

국내 유명 백화점과 인터넷 포털 사이트 등에서 2000만 건에 달하는 개인정보를 빼내 시중에 유통시킨 일당이 경찰에 붙잡혔다. 인천지방경찰청은 중국 해커로부터 사들인 개인정보를 누리꾼들에게 판매한 혐의(정보통신망 이용 촉진 및 정보보호 등에 관한 법률 위반 등)로 최모 씨(25)를 구속하고 배모 씨(25) 등 2명을 불구속 입건했다고 11일 밝혔다.

경찰에 따르면 친구 사이인 최 씨 등은 2008년 11월부터 최근까지 중국 해커에게 2차례에 걸쳐 [illegible]을 주고 국내 인터넷 사이트 개인정보 2000여만 건을 인 메신저를 통해 누리꾼 5000만 원을 받고 판매하고 있다. 또 이들은 [illegible] 최근까지 온라인 포털 사이트 들에게 '수능시험 문제를 해킹해 주겠다'는 등의 쪽지를 보내 33명에게서 2168만 원을 받아 가로챈 것으로 드러났다.

인천=황금천 기자 kchwang@donga.com

19시간 금융마비 농협, 사고원인도 파악못해

중앙일보

2011년 07월 29일 금요일 001면 종합

3500만 명 개인정보 털렸다

〈비밀번호·주민번호〉

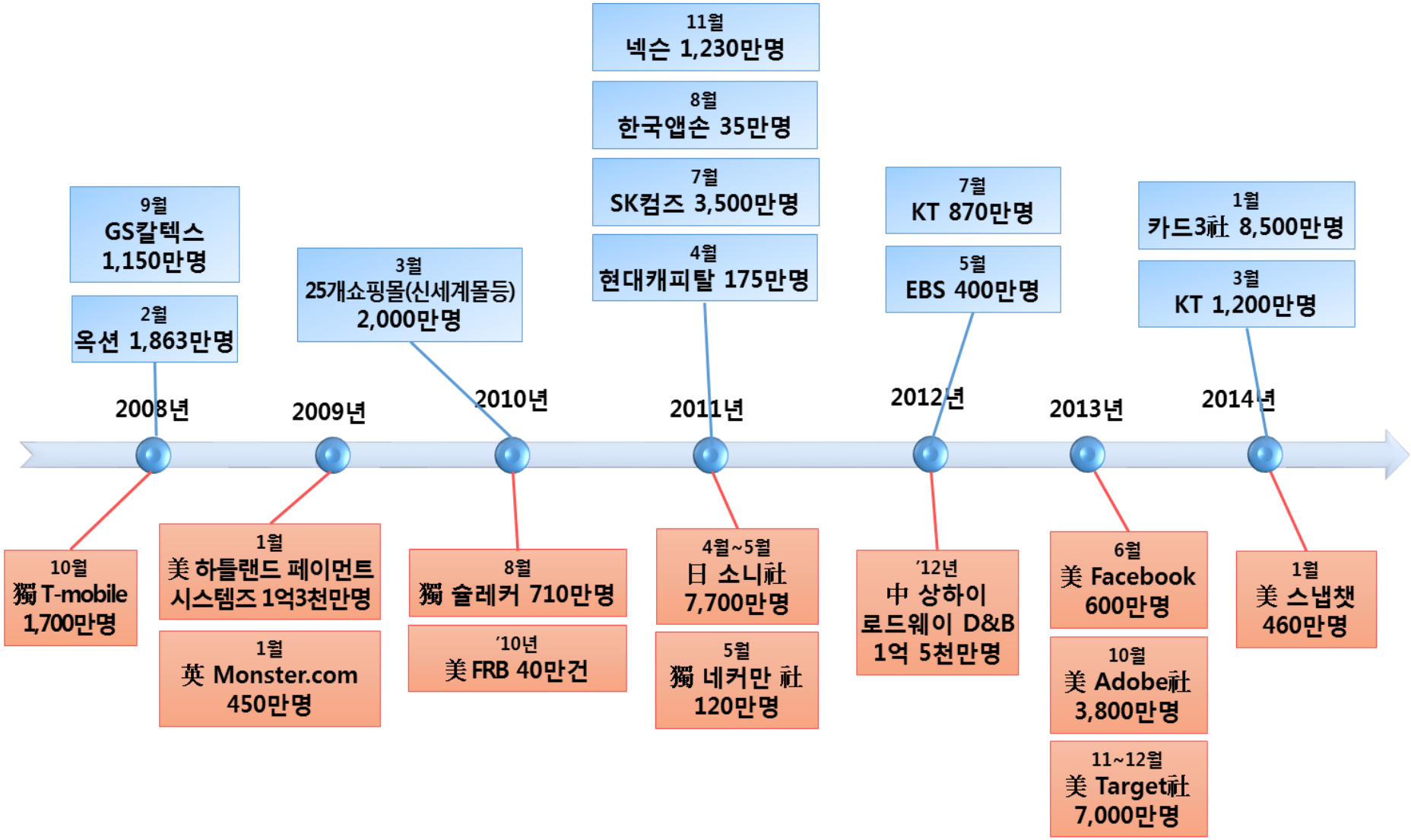
네이트·싸이월드 최악 해킹

국내 사상 최대 규모의 해킹사고가 발생했다. SK커뮤니케이션즈는 네이트와 싸이월드 회원 3500만 명의 개인 정보가 해킹으로 유출됐다고 28일 밝혔다. 네이트와 싸이월드 회원 수는 각각 2500만 명, 3300만 명이다. 중복 가입자가 많은 만큼 사실상 대부분의 가입자가 피해를 본 셈이다. 유출된 정보 중에는 이름·휴대전화번호·e-메일 주소가 포함돼 있어 보이스 피싱, 스팸 메일로 인한 2차 피해가 우려된다.

SK커뮤니케이션즈가 이상 징후를 발견한 건 26일, 시스템 정기 모니터링을 하는 과정에서였다. 이 회사의 권창현 실장은 "중국발 악성코드가 접근한 것을 감지했으며, 28일 새벽에 정보 유출이 일어났음을 최종 확인했다"고 말했다. 이나리 기자 windy@joongang.co.kr

➡ 2면 '해킹'으로 이어집니다

연도별 주요 개인정보 침해사고

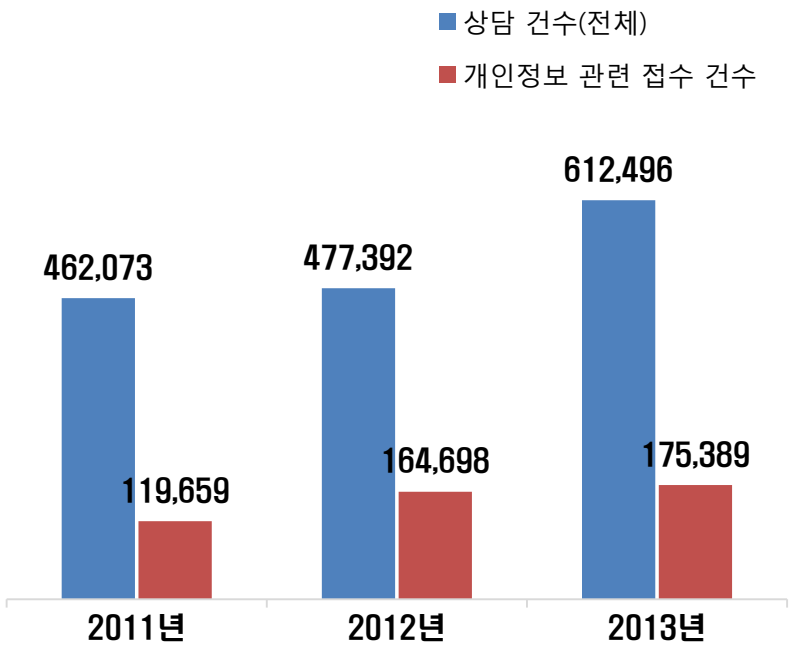


개인정보 유출 및 신고상담의 증가

- **대부분의 개인정보 침해사고는 온라인에서 발생**
  - 개인정보 유통의 대부분이 온라인에서 이루어지고 정보통신망을 통해 침해 발생
- **118 상담센터에서 접수하는 상담 중 29%가 개인정보 관련 상담**
  - 접수현황 ('13년) : 개인정보(29%), 해킹/바이러스(19%), 스팸(17%) 등

[개인정보 유출 사고 피해]

[118 상담센터 운영]



개인정보 침해사고 및 피해 경로

개인정보 수집 · 이용

- 공공기관
- 오프라인 사업자
- 통신사업자
- 인터넷 사업자
- 비영리, 동호회

개인정보 유출 경로

- 내부자 고의
- 위탁 대리점
- 외부공격 (해커)
- 내부자 관리부주의

개인정보 축적·거래

온라인

음성시장을 통한 개인정보 거래

오프라인

CD 등 저장매체를 통한 직접 판매

2차 피해 발생

명의도용

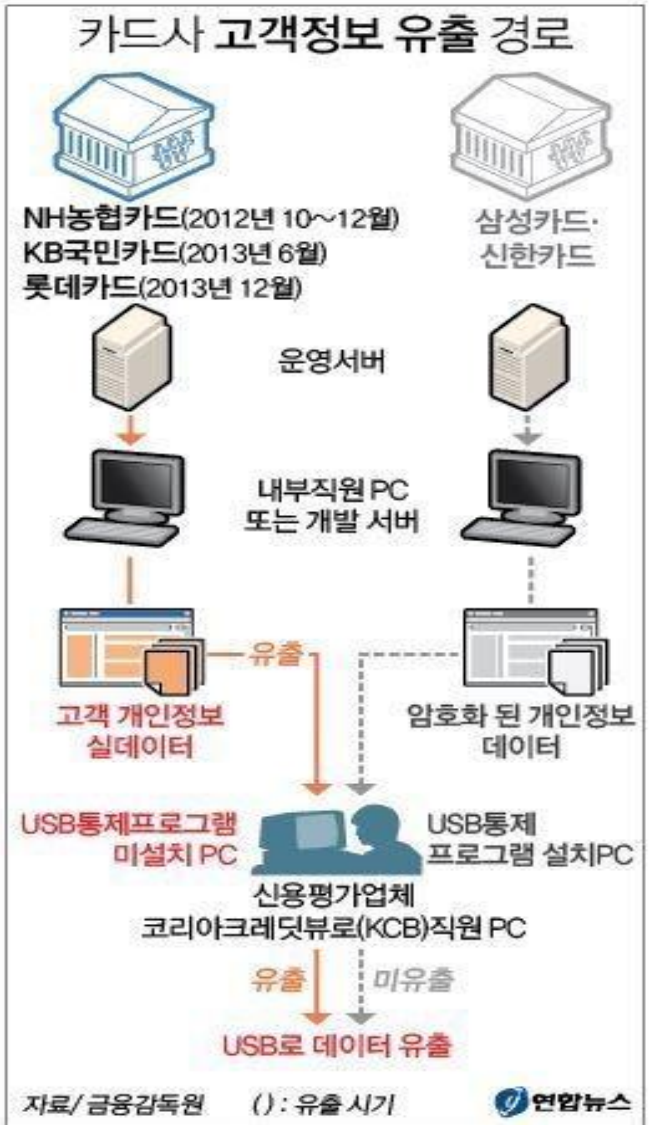
- 대포폰 개설
- 신용카드 발급
- 회원가입

스팸발송, 명예훼손, 해킹 등 악성행위에 이용

구매 등 금전적 피해 유발

대량 스팸, SMS(스미싱) 등 사이버사기에 악용 (Target Marketing)

개인정보 유출 사례– 카드3사



보안대책이 우수한 카드사가 적용중인 대책

A카드

(기술적 조치) USB 등 이동식 저장매체 및 IT 개발자 PC에 자료저장 차단, 외부로 메일 발송시 암호화로 열람 차단
※ DRM, DLP 솔루션 적용
(관리적 조치) 사용자 PC의 외부반출 통제, 외부 개발자가 프로젝트 종료시 데이터 삭제(전문 SW 이용 포맷)

B카드

(기술적 조치) 업무용 PC에 문서 저장시 자동 암호화로 내부 업무용 PC 이외에 문서 열람 차단, USB/외장하드 등 이동식 저장매체의 자료 업로드 차단
※ DRM, DLP 솔루션 적용(추정)
(관리적 조치) 해제권한을 관리자 이상에게만 허용, 외부에 전송 파일을 관리자가 한 번 더 검토, 이메일 전송시 부서장 승인 후 전송(통제 솔루션 이용), 외부업체가 IT 작업시 가상 데이터 사용

4장 개인정보 보호 법제의 이해

개인정보 관련 법률간 관계

- 개인정보 보호법은 개인정보 보호 분야의 **일반법**

➢ **타 법률에 특별한 규정 없는 경우**

→ 개인정보 보호법에 따름

사회전반의 개인정보 보호를 규율
개인정보를 다루는 모든 사업자, 개인 등

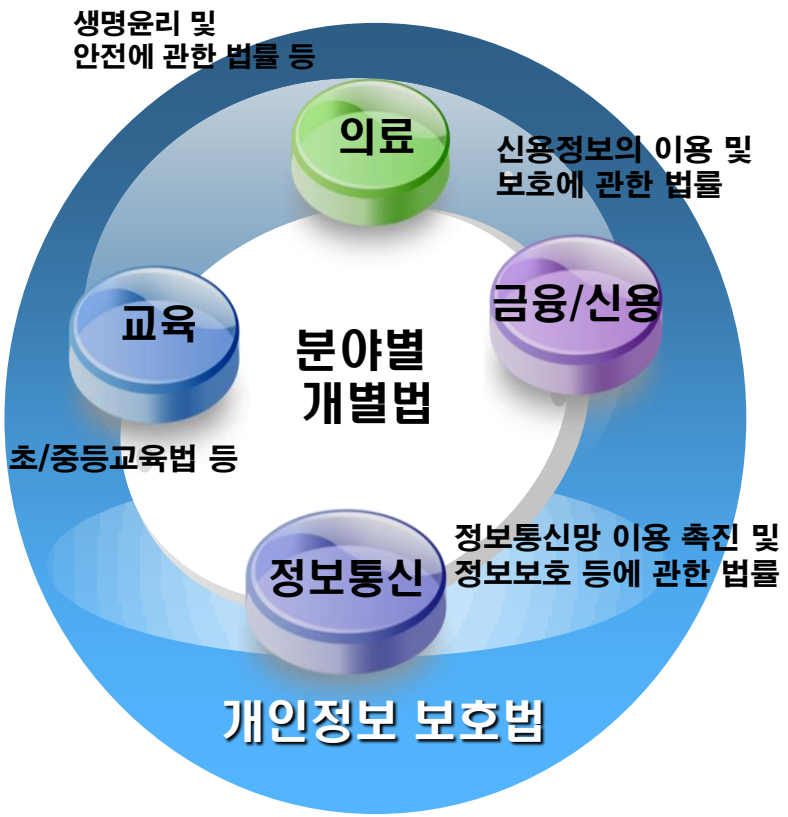
➢ **타 법률에 특별한 규정 있는 경우**

→ 해당 법률 규정에 따름

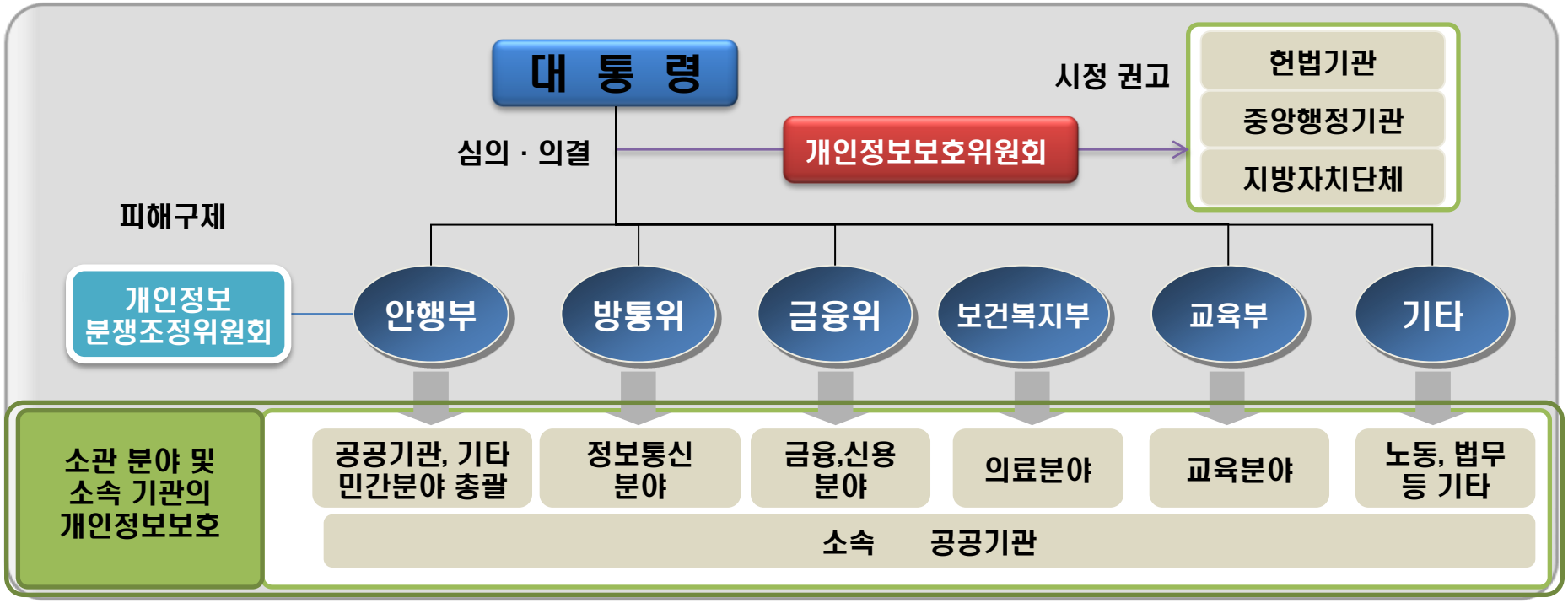
(정보통신망법, 전자금융거래법 등)

* 다른 법률의 규정이 개인정보보호법보다 보호수준이 강하거나 약한 특별한 경우

⇒ 해당 조문별로 개별법 적용



개인정보보호 행정체계



개인정보보호위원회

개인정보보호 정책 심의 · 의결

안전행정부

공공 및 기타 민간분야 개인정보보호 업무 수행

중앙행정기관

소관분야 및 개별법 개인정보보호 업무수행

개인정보 처리단계별 법적 의무사항 요약

<처리단계>

개인정보보호법령 규정
개인정보 수집 · 이용 개인정보 수집의 제한 (필요 최소한의 정보수집 등) 민감정보 및 고유식별정보 처리제한
인터넷상 주민번호 이외의 회원가입 방법 제공 영상정보처리기기 설치 · 운영, 개인정보처리방침 공개 개인정보보호책임자 지정 개인정보 안전성 확보조치
개인정보의 제3자 제공, 목적외 이용제공 금지 개인정보 처리위탁, 영업양도 등 개인정보 이전
개인정보 파기
개인정보 유출통지 · 신고 및 개인정보 침해신고 개인정보 열람, 정정 · 삭제, 처리정지권 분쟁조정위원회 및 집단분쟁조정 권리침해 중지 단체소송

개인정보 보호법 개정('14.8.7 시행) 주요내용

주민번호 수집 법정주의

◉ 원칙적 처리금지, 예외적 처리 허용

모든 개인정보처리자 원칙적 주민번호 처리 금지, 다음 경우 예외적 처리 허용

현행법 제24조 제1항

- ~~① 정보주체로부터 **별도 동의**를 받은 경우~~
- ② **법령**에서 구체적으로 주민등록번호 처리를 요구·허용한 경우

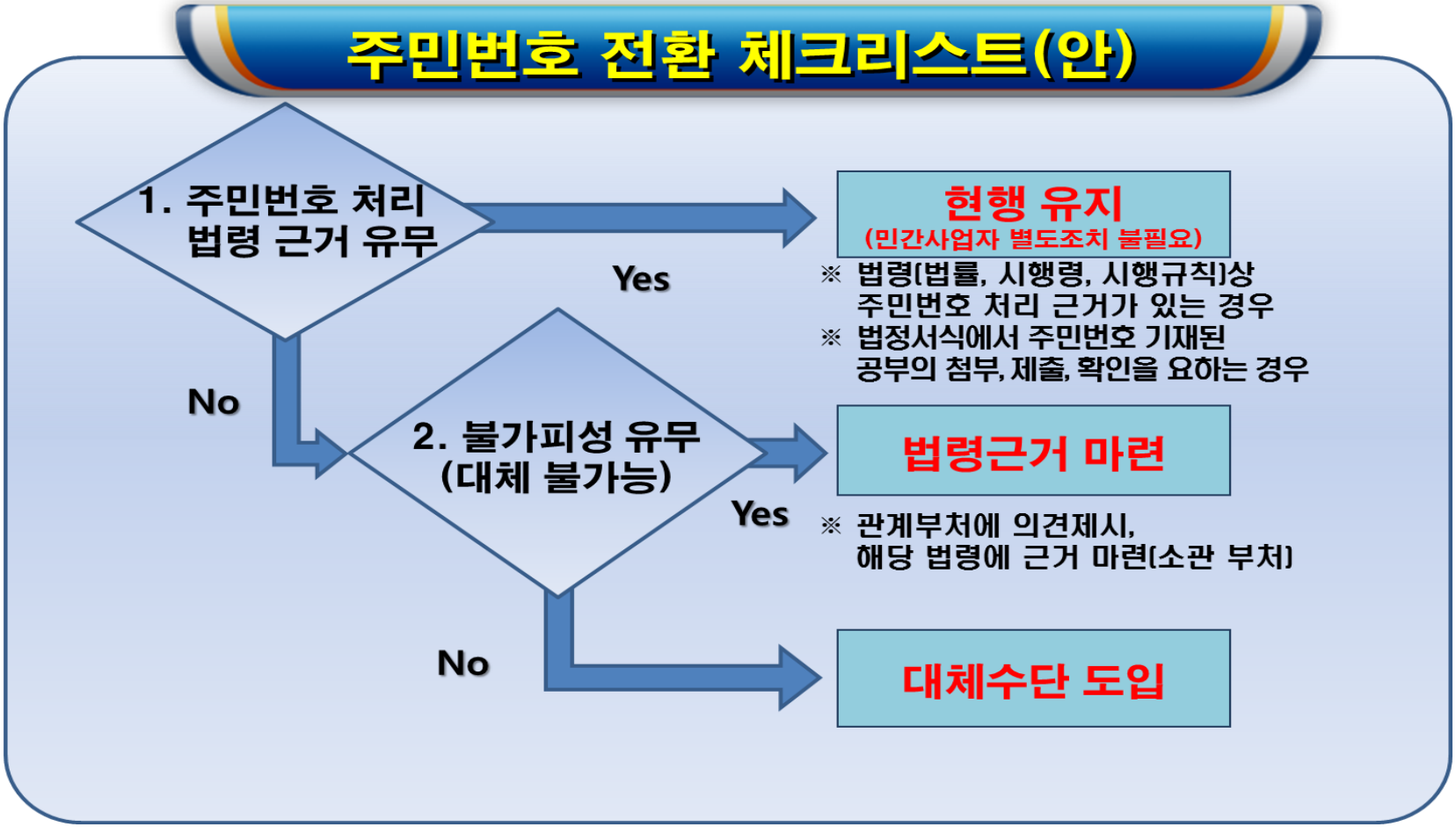
개정법 제24조의2 제1항

- ① **법령**에서 구체적으로 주민등록번호 처리를 요구·허용한 경우
- ② 정보주체 또는 제3자의 **급박한 생명, 신체, 재산 이익**을 위해 명백히 필요하다고 인정되는 경우
- ③ 기타 이에 준한 경우로서 **안전행정부령**으로 정하는 경우

◉ 기 보유 주민번호 중 법령 상 근거가 없는 경우 → 법 시행 후 2년 이내 파기

주민번호 처리금지 정책 대응방안

- 주민번호 수집이용 원칙적 금지 : 미수집 또는 대체수단 도입 등
- 불가피한 경우 법령근거 마련 및 필요 최소한 이용



주민번호 수집하는 법률 예시

신원 및 연령확인 근거 법령

법령		내용
금융실명거래법	법 제3조	금융거래시 실지명의 확인 (성명, 주민번호)
부가가치세법	법 제16조 등	세금계산서 등에 성명, 주민번호 기재
소득세법	법 제145조 등	원천징수영수증에 주민번호 등 기재
신용정보법	법 제34조	주민번호 등 개인정보 수집
전자서명법	법 제15조	공인인증서 발급시 성명, 주민번호 등 확인
의료법	법 제22조등	진료기록부에 주민번호 기재
청소년보호법	법 제29조등	청소년유해업소 출입시 주민등록증 확인
	법 제26조	16세 미만 청소년 심야시간 인터넷게임 제한

개인정보 보호법 개정('14.8.7 시행) 주요내용

과징금 및 징계권고 제도

◉ 과징금 제도 신설

주민번호 유출 등 경우 과징금(**5억원** 이하) 부과(제34조의2제1항),
다만 주민번호 안전성 확보조치 모두 이행시 과징금 면제

※ 과징금 및 과태료 부과시 기업 부담이 가중된다는 의견에 따라
'과징금 부과시 과태료 병과 금지' 규정(제76조) 추가

◉ CEO 등에 대한 징계권고 신설

안행부장관의 징계권고 대상에 개인정보처리자의 **대표자(CEO) 및 책임 있는 임원**이 포함됨을 명시(제65조제2항)

개인정보 보호법 개정('16.1.1 시행) 주요내용

주민번호 저장시 암호화

◉ 주민번호 보관시에도 암호화

주민번호가 분실, 도난, 유출, 변조 또는 훼손되지 않도록 암호화 조치를 통하여 안전하게 보관하여야 함

※ 위반시 3천만원 이하의 과태료 부과

[참고] 개인정보 보호법에 따른 제재조치

구분	주요내용	처벌 및 벌칙
수집·이용	정보주체의 동의 없는 개인정보 제3자 제공(17조)	5년 이하 징역 또는 5천 만원 이하 벌금
	개인정보의 목적 외 이용·제공(18조, 제19조, 제26조)	
	민감정보 처리기준 위반(제23조)	
	고유식별정보 처리기준 위반(제24조)	
	부정한 수단이나 방법에 의해 개인정보를 취득하거나 개인정보처리에 관한 동의를 얻는 행위를 한 자(제59조)	3년 이하 징역 또는 3천 만원 이하 벌금
	개인정보의 수집기준 위반(제15조)	5천 만원 이하 과태료
	만 14세 미만 아동의 개인정보 수집 시 법정대리인 동의획득의무 위반(제22조)	
	탈의실·목욕실 등 영상정보처리기기 설치 금지 위반(제25조)	
	직접마케팅 업무위탁으로 인한 개인정보 제공 시 정보주체에게 알려야 할 사항을 알리지 아니한 자(제15조, 제17조, 제18, 제26조)	3천 만원 이하 과태료
	최소한의 개인정보 외 정보의 미동의를 이유로 재화 또는 서비스 제공을 거부한 자(제16조, 제22조)	
	주민등록번호를 제공하지 아니할 수 있는 방법 미제공(제21조)	
	동의획득방법 위반하여 동의 받은 자(제22조)	1천 만원 이하 과태료

구분	주요내용	처벌 및 벌칙
제공·위탁	동의 없는 개인정보 제3자 제공(17조)	5년 이하 징역 또는 5천 만원 이하 벌금
	개인정보의 목적 외 이용·제공(18조, 제19조, 제26조)	
	직접마케팅 업무위탁으로 인한 개인정보 제공 시 정보주체에게 알려야 할 사항을 알리지 아니한 자(제15조, 제17조, 제18, 제26조)	3천 만원 이하 과태료
	업무위탁 시 공개의무 위반(제26조)	1천 만원 이하 과태료
개인정보 안전관리	개인정보의 누설 또는 타인 이용에 제공 (제59조)	5년 이하 징역 또는 5천 만원 이하 벌금
	개인정보의 훼손, 멸실, 변경, 위조, 유출(제59조)	
	영상정보처리기기 설치목적과 다른 목적으로 임의 조작하거나 다른 곳을 비추는 자 또는 녹음기능을 사용한 자(제25조)	3년 이하 징역 또는 3천 만원 이하 벌금
	직무상 알게 된 비밀을 누설하거나 직무상 목적 외 사용한 자(제60조)	
	안전성 확보에 필요한 보호조치를 취하지 않아 개인정보를 도난·유출·변조 또는 훼손당하거나 분실한 자(제24조, 제25조, 제29조 위반)	2년 이하 징역 또는 1천 만원 이하 벌금
	안전성 확보에 필요한 조치의무 불이행(제24조, 제25조, 제29조)	3천 만원 이하 과태료
	영상정보처리기기 설치·운영기준 위반(제25조)	
	개인정보를 분리해서 저장·관리하지 아니한 자(제21조)	1천 만원 이하 과태료
	개인정보처리방침 미공개(제30조)	
	개인정보관리책임자 미지정(제31조)	
	영상정보처리기기 안내판 설치 등 필요조치 불이행(제25조)	

구분	주요내용	처벌 및 벌칙
정보주체 권익보호	개인정보의 정정·삭제요청에 대한 필요한 조치를 취하지 않고, 개인정보를 계속 이용하거나 제3자에게 제공한 자(제36조)	2년 이하 징역 또는 1천 만원 이하 벌금
	개인정보의 처리정지 요구에 따라 처리를 중단하지 않고 계속 이용하거나 제3자에게 제공한 자(제37조)	
	개인정보 유출사실 미통지(제34조)	3천 만원 이하 과태료
	정보주체의 열람 요구의 부당한 제한·거절(제35조)	1천 만원 이하 과태료
	정보주체의 정정삭제요구에 따라 필요조치를 취하지 아니한 자(제36조)	
	처리정지된 개인정보에 대해 파기 등의 조치를 하지 않은 자(제37조)	
	시정명령 불이행(제64조)	
	정보주체의 열람, 정정·삭제, 처리정지 요구 거부 시 통지의무 불이행(제35조, 제36조, 제37조)	
	관계물품·서류 등의 미제출 또는 허위제출(제63조)	
	출입·검사를 거부·방해 또는 기피한 자(제63조)	
파기	개인정보 미파기(제21조)	3천 만원 이하 과태료

업무상비밀누설죄 3년이하 징역

5장 개인정보 안전성 확보조치

개인정보의 안전성 확보조치 기준【안행부고시 제2011-43호, 2011.9.30., 제정】

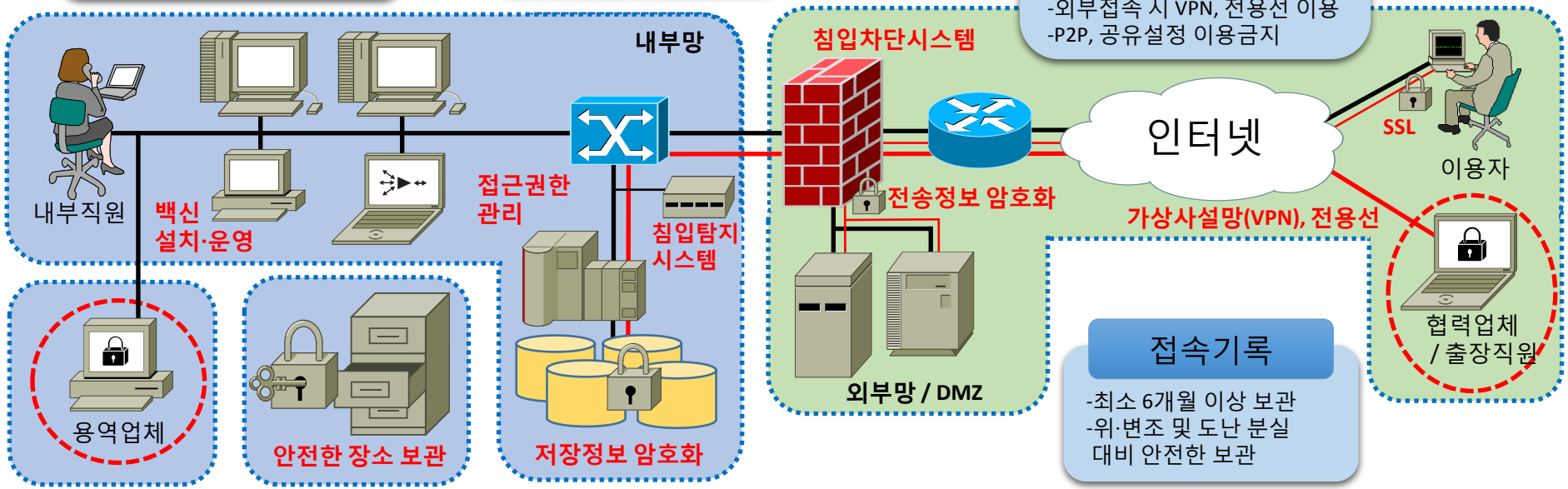
구분	주요내용
내부관리계획(제3조)	• 보호책임자 지정 및 역할과 책임, 취급자 교육 등 ※ 소상공인은 내부관리계획 수립의무 면제
접근권한 관리(제4조)	• 업무수행에 필요한 최소한의 범위로 차등 부여 • 접근권한 부여기록은 최소 3년간 보관
비밀번호 관리(제5조)	• 비밀번호 작성규칙 수립 의무화
접근통제시스템(제6조)	• 방화벽 등 접근통제시스템 설치·운영 • 업무용 컴퓨터만을 이용해 개인정보 처리시, O/S, 보안프로그램 등에서 제공하는 접근통제기능 이용
암호화(제7조)	• 암호화 대상 : 고유식별정보, 비밀번호, 바이오정보 • 암호화 기준 -(전송시) 정보통신망을 통한 송수신 및 전달시 암호화 -(저장시) ① 비밀번호 및 바이오정보 암호화 (비밀번호는 일방향 암호화) ② 고유식별정보는 인터넷구간, DMZ구간 저장시 암호화하고 내부망 저장시 위험도 분석에 따라 암호화 적용여부, 적용범위 결정
접속기록 보관(제8조)	• 최소 6개월 이상 보관
보안프로그램(제9조)	• 백신소프트웨어 등 보안프로그램 설치, 자동 또는 일1회 이상 업데이트
물리적 조치(제10조)	• 개인정보 물리적 보관장소에 대한 출입통제절차 등 (서면 보관장소, 개인정보처리시스템 설치장소 등)

개인정보의 안전성 확보조치 기준【안행부고시 제2011-43호, 2011.9.30., 제정】

보안프로그램 설치
-백신 소프트웨어
-자동 업데이트
-일 1회 이상 업데이트

접근권한
-권한 최소/차등 부여
-부여 기록 최소 3년 보관
-사용자 계정 공유 금지

접근통제
-웹 취약점 점검
-침입차단시스템(Firewall)
-침입탐지시스템(IDS)
-침입방지시스템(IPS)
-웹방화벽, SecureOS, ACL
-외부접속 시 VPN, 전용선 이용
-P2P, 공유설정 이용금지



접속기록
-최소 6개월 이상 보관
-위·변조 및 도난 분실 대비 안전한 보관

비밀번호
-영문, 숫자, 특수 문자 중
 > 2종류 이상(최소 10자리)
 > 3종류 이상(최소 8자리)
-주기적인(6개월) 변경

물리적 방지
-출입통제 절차 수립
-개인정보 포함 서류, 보조저장매체 등 안전한 장소 보관

암호화
-고유식별정보 암호화
-비밀번호, 바이오정보 일방향 암호화(Hash)
-정보통신망 송·수신(SSL) 및 저장매체 전달 시 암호화

내부관리계획
-개인정보 보호책임자 지정
-개인정보 보호책임자 및 취급자 역할 및 책임
-개인정보 안전성 확보조치 사항
-개인정보 보호 교육

처벌규정
-미이행시 3천만원 이하의 과태료
-미이행으로 인한 유출시 2년 이하 징역 또는 1천만원 이하 벌금

6장 개인정보보호 십계명

도둑?? 경비?? 누가 나쁠까?

개인정보 유출 주요 원인

내부자 고의

- 금전적 이익을 위한 고의 유출
- 지인의 부탁

개발자, 해커 등 외부인

- 악의적 해킹
- 시스템 개발 오류

관리자, 내부자 부주의

- 실수?!
- 개인정보보호 인식 미비

개인정보 보호를 위한 십계명(1/2)

1. 최소한의 개인정보만 수집하며 불필요한 개인정보 수집을 자제
2. 개인정보 수집 시 서비스 제공에 꼭 필요한 필수정보와 선택 정보 구분
3. 고유식별정보와 민감정보는 원칙적 처리금지
4. 홍보·판매 목적으로 개인정보 위탁시 고객에게 고지하고 철저히 관리
5. 개인정보파일은 DB보안 프로그램, 암호화 소프트웨어 등 안전한 방법을 사용하여 보관

개인정보 보호를 위한 십계명(2/2)

6. 보관이 필요한 증빙서류는 법령에서 정한 보유기간을 숙지하여 준수

7. 개인정보의 보유이용기간이 끝난 경우, 이용목적을 달성한 경우 알아볼 수 없도록 파기

8. CCTV에는 반드시 안내판 설치

9. 열람청구 등에 대한 정보주체의 요구가 있을 경우 지체없이 처리

10. 개인정보 유출통지, 집단분쟁조정, 단체소송에 대비

[부록] 개인정보 보호 관련 웹사이트

개인정보보호 종합지원 포털 (www.privacy.go.kr)

[부록] 한국인터넷진흥원 개인정보 관련업무

118 상담 센터

상담센터 업무 개요

- KISA 사업과 관련된 개인정보침해 및 불법스팸, 해킹/바이러스, 인터넷 이용 등에 대한 질의 · 상담을 24시간 연중무휴로 운영

※ 상담내용 : 개인정보, 불법스팸, 인터넷침해사고 등에 대한 예방/대응방법 및 근거 법률, 도메인, IP 등 인터넷주소, 아이핀 발급, 공인인증서 문제점 해결방안 등

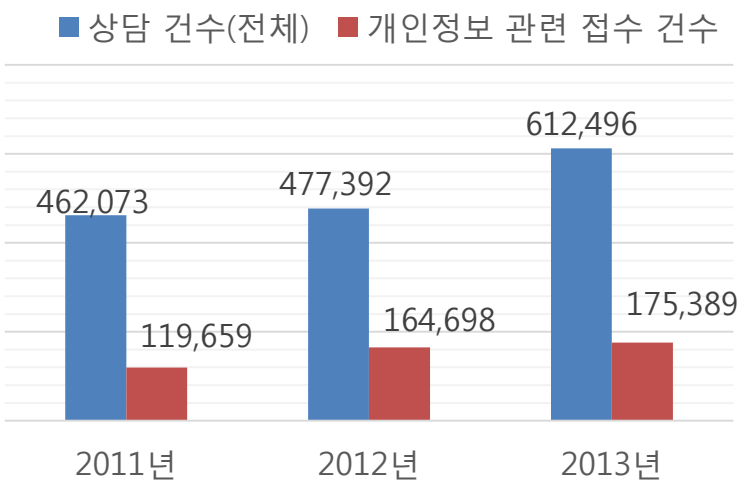
상담센터 이용방법(민원인 입장)

① 전화 : (국번없이) 118
※ ARS : (1)불법스팸, (2)개인정보, (3)해킹/바이러스, (4)공인인증서 분실, (5)기타

② 이메일 : 118@kisa.or.kr

③ 홈페이지 : http://privacy.kisa.or.kr
※ 개인정보민원실 → 개인정보민원신청 메뉴를 통해 신청

④ 방문 : IT벤처타워(가락동 소재) 9층



< 118상담센터 상담실적 >

[부록] 한국인터넷진흥원 개인정보 관련업무

주민등록번호 클린센터

클린센터 업무 개요

- “주민등록번호 이용내역” 검색 서비스
  - 민원인의 주민번호가 언제, 어느 웹사이트에서 이용되었는지 확인
- “회원탈퇴 지원” 서비스
  - 회원탈퇴를 직접하기 어려운 인터넷 이용자가 민원을 접수하면, 회원탈퇴를 지원

클린센터 이용절차 (민원인 입장)

① 클린센터(clean.kisa.or.kr) 홈페이지 접속

② 이름 및 주민번호 수집이용 동의

③ 본인 확인 및 ④ 본인 인증(인증방법 : 휴대폰 인증, 신용카드, 공인인증서)

⑤ 신평사의 주민번호 이용내역을 무료확인

※ KISA가 주민번호 이용내역 확인비용을 민원인 대신 지급

⑥ 주민번호 도용 등이 의심되는 경우 탈퇴민원 신청

[부록] 한국인터넷진흥원 개인정보 관련업무

개인정보 노출 조기경보, 대응시스템 운영

조기경보시스템 / 개인정보 노출대응 시스템

- 인터넷에 노출된 우리 국민의 개인정보를 검색하고 삭제 요청하여 노출된 개인정보의 인터넷 확산을 방지
  - 공개된 인터넷 홈페이지에 방취된 개인정보를 사전에 탐지하여 삭제 조치

안행부(공공기관 및 비영리 · 협회)

점검대상 : 12만 홈페이지

검색방법 : 자체 개발 S/W, 구글, 바이두등

점검유형 : 4종(주민번호, 운전면허번호, 여권번호, 외국인등록번호)

방통위(정보통신서비스제공자)

점검대상 : 230만 홈페이지

검색방법 : 자체 개발 S/W, 구글, 바이두 등

점검유형 : 9종(주민번호, 운전면허번호, 여권번호, 신용카드, 계좌번호, 건강보험, 휴대전화번호)

[부록] 한국인터넷진흥원 개인정보 관련업무

개인정보침해신고센터 (privacy.kisa.or.kr)

개인정보침해신고센터 업무 개요

- “개인정보침해신고” 민원 처리 서비스 (privacy.kisa.or.kr)
  - 정보주체(민원인 등)가 개인정보처리자의 처리행위로 인하여 권리 · 이익의 침해를 받은 경우, 고충 · 민원을 접수 · 처리하고 침해신고를 접수받아 위반행위자에 대한 계도 · 시정조치 명령 등 행정제재를 하는 등 법규준수 환경을 구축하기 위한 서비스

업무 처리 절차

① 개인정보침해신고 민원 접수
② 신고/상담 법령질의 구분
③ 신고접수
④ 사실조사
⑤ 사실조사 결과보고서 작성
⑥ 주무부처 이관(형사고발, 행정처분, 제도개선)
⑦ 종결(결과통보)

아름다운 인터넷, 안전한 인터넷 세상

한국인터넷진흥원이 만들어 나가겠습니다.

제9회, [NES2014]
차세대 기업보안 세미나/전시회

KISA 한국인터넷진흥원
Korea Internet & Security Agency