KISA 한국인터넷진흥원

개인정보보호 위반사례 및 대응

개인정보

유출 / 노출 / 법규위반

출처 : 보안뉴스

1-1. 개인정보 유출이란?

- 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보 처리자가 통제를 상실하거나 또는 권한 없는 자의 접근을 허용한 경우

01
- 개인정보가 포함된 서면, 이동식 저장장치, 휴대용컴퓨터 등을 분실 또는 도난당한 경우

02
- 개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우

03
- 개인정보처리자의 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이문서, 기타 저장매체가 권한이 없는 자에게 잘못 전달된 경우

04
- 기타 권한이 없는 자에게 개인정보가 전달되거나 개인정보처리시스템 등에 접근 가능하게 된 경우

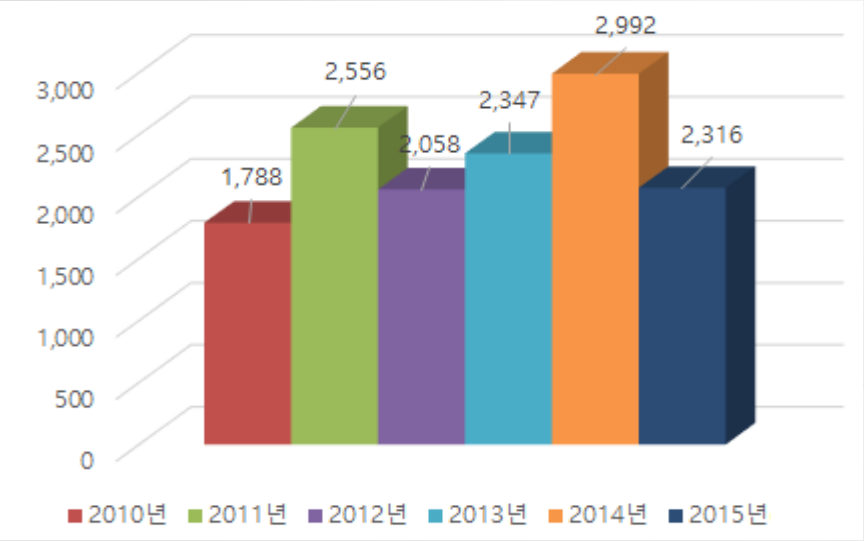
1-2. 개인정보 유출 신고 현황

○ **총 유출건수 : 67건, 1억 3,035만명**

- 구분 : 공공 10건(187만명), 민간 57건(1억 2,848만명)

*「개인정보 보호법」 제34조에 따라 개인정보 유출사고 신고 접수된 현황임

1-3. 개인정보 침해 신고 현황

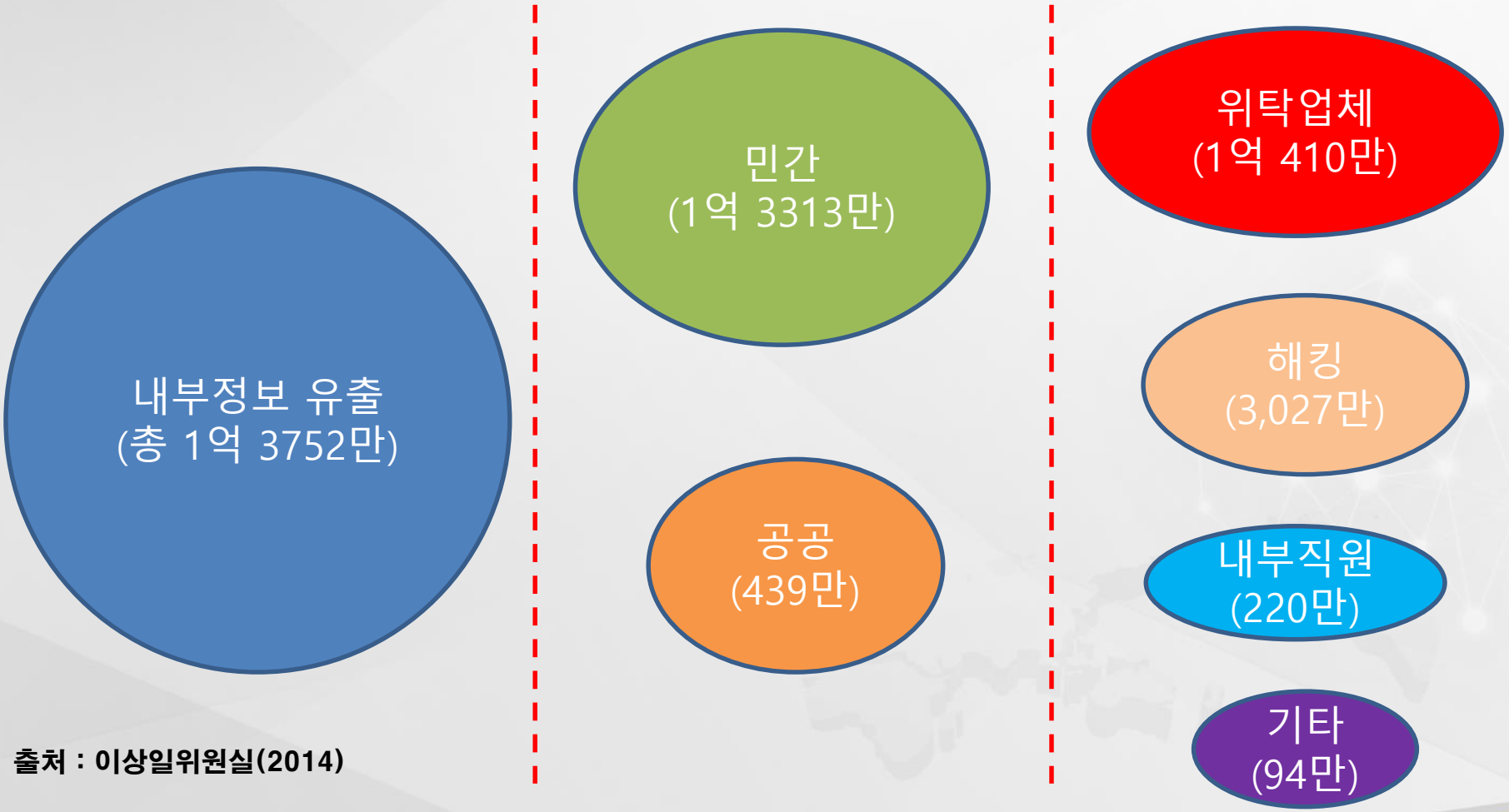


< 연도별 개인정보침해 신고 현황 >

접 수 유 형
이용자의 동의 없는 개인정보 수집 관련
개인정보 수집시 고지 또는 명시 의무 관련
과도한 개인정보 수집
목적 외 이용 또는 제3자 제공 관련
개인정보 취급자에 의한 훼손.침해 등
개인정보 처리 위탁시 고지의무
영업의 양수 등의 통지의무
개인정보관리책임자 관련
기술적.관리적 조치 미비 관련
수집 또는 제공받은 목적 달성 후 개인정보 미파기
동의철회.열람 또는 정정 요구 관련
동의철회, 열람.정정을 수집보다 쉽게 해야할 조치
아동의 개인정보 수집
주민등록번호 등 타인 정보의 훼손.침해.도용

1-4. 왜 개인정보 유출이 발생하는가?

관리소홀 탓 개인정보 유출, 해킹보다 3배 높다!!!



출처 : 이상일위원실(2014)

1-4. 왜 개인정보 유출이 발생하는가?

✓ **무단제공** 및 **사적 열람**이 **전체의 약 80%**

◉ 기관 유형별 (단위 : 명)

구분	중앙행정기관	교육기관	지방자치단체	기타공공기관	계
'12년	28	20	32	8	88
'13년	83	17	42	12	154
'14년	98	9	48	13	**168**

약 2배 증가

◉ 징계 유형별 (단위 : 명)

구분	파면	해임	강등	정직	감봉	견책	경고등	계
'12년	2	4	0	7	15	8	52	88
'13년	4	6	0	12	21	36	75	154
'14년	1	3	1	20	27	65	51	168

◉ 위반 내용별 (단위 : 명)

구분	무단 제공	외부 유출	사적 열람	단순 노출	기타	계
'12년	39	4	21	15	9	88
'13년	33	5	68	4	44	154
'14년	58	2	71	11	26	168

출처 : '**공공기관의 개인정보 오·남용 징계 현황**', 행정자치부

공무원이 주민 1500명 개인정보 유출

평창 미탄면 9급, 이장에 명부 줘
군 "감사 끝나면 중징계할 방침"

공무원이 지역 주민 1500여명의 개인정보를 유출해 물의를 빚고 있다.

1-5. 유출된 개인정보가 어떻게 악용되는가?

Cybercrime-as-a-Service

✓ 소프트웨어를 통해 무작위로 추출 가능한 기본정보의 경우,
- 미국은 5~8달러, 영국, 캐나다, 호주의 경우 20~25달러

✓ 우리나라의 경우 주민번호나 아이핀 번호의 경우 건당 2,000원 수준

내용 구성별 유출된 카드정보 암거래 가격 (단위:달러)

패키지	미국	영국	캐나다	호주	유럽(EU)
임의 추출 가능한 기본 정보	5~8	20~25	20~25	21~25	25~30
계좌번호 추가	15	25	25	25	30
생년월일 추가	15	30	30	30	35
종합적인 개인정보	30	35	40	40	45

자료:인텔시큐리티 맥아피연구소

자료가 선별, 가공되어 고가로 활용

1-6. 유출되고 나서는? - 개인

사회활동 지장 초래

범죄에까지 악용

금전적 피해 발생

정신적 피해 심각

신상털기

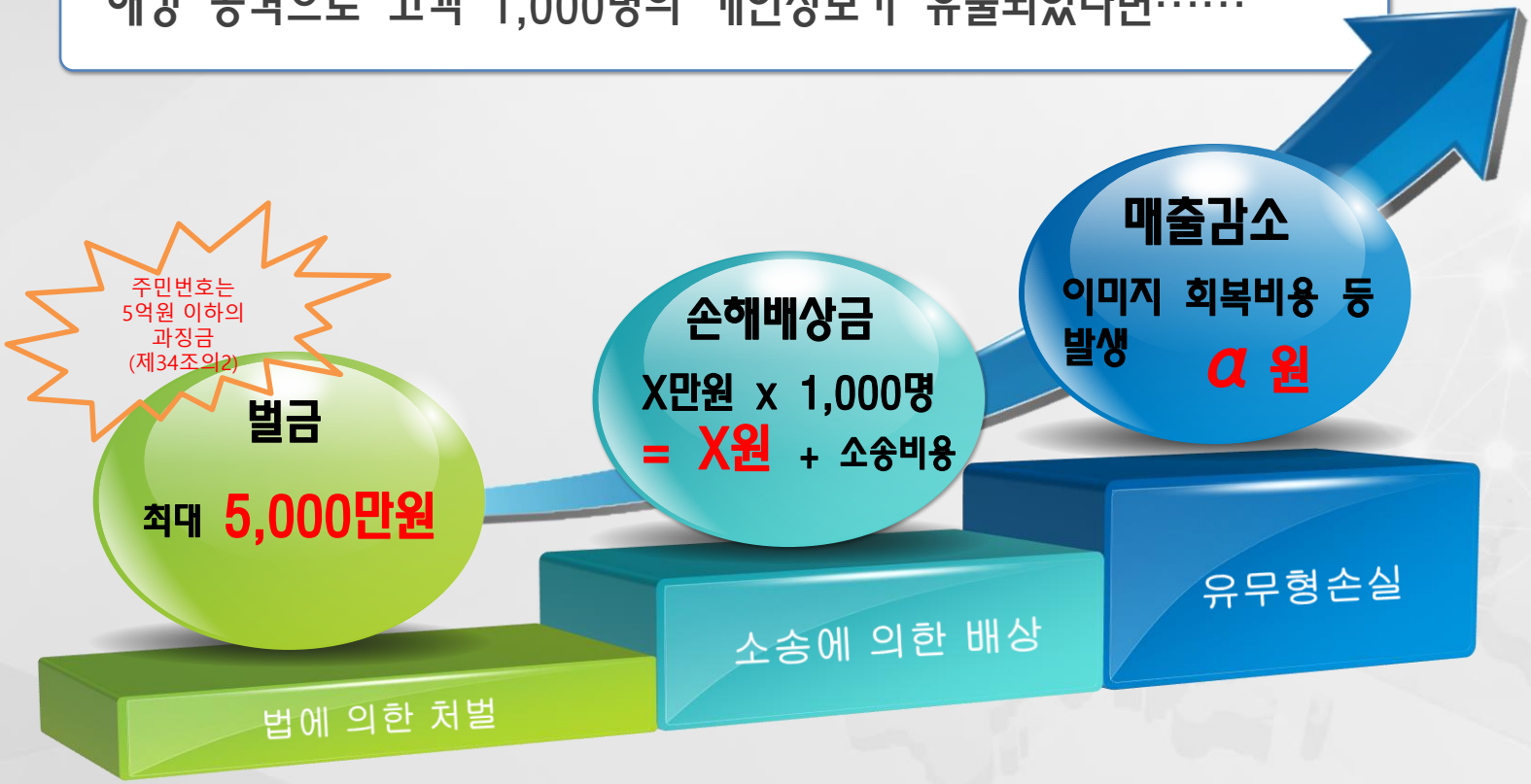
명의 도용

보이스 피싱

1-6. 유출되고 나서는? - 기업

우리 회사 고객의 개인정보가 유출된다면?

고객의 개인정보를 암호화하지 않고 저장하여 사용하고 있었는데,
해킹 공격으로 고객 1,000명의 개인정보가 유출되었다면……



1-7. 유출된 후에는 어떻게 해야 하는가?

유출된 정보주체 개개인에게 지체 없이 통지

⇨ **개인정보보호법 제34조 제1항**

- 시한 : 유출되었음을 알게 되었을 경우 지체 없이(5일 이내)
- 통지 항목 : ①유출된 개인정보의 항목, ②유출 시점과 및 그 경위, ③피해 최소화를 위한 정보주체의 조치방법, ④기관의 대응조치 및 피해구제 절차, ⑤피해 신고 접수 담당부서 및 연락처

※ 대상 : 유출 규모와 상관없이 모든 유출 개인정보처리자
※ 개인정보보호법 제75조 제2항 제8호(**3천만원이하의과태료**)
정보주체에게 같은 항 각 호의 사항을 알리지 아니한 자

피해 최소화를 위한 대책 마련 및 필요한 조치 실시

⇨ **개인정보보호법 제34조 제2항**

- 접속경로 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등 피해를 최소화하기 위해 필요한 긴급조치 이행
- 긴급조치 이행 등에 어려움이 있는 경우 전문기관에 기술지원 요청

※ 대상 : 유출 규모와 상관없이 모든 유출 개인정보처리자
※ 피해 최소화 대책을 마련하지 않거나 필요한 긴급 조치를 하지 않은 경우 : **시정명령**

1만 명 이상 유출된 경우 유출 통지 결과를 신고

⇨ **개인정보보호법 제34조 제3항**

- 1만 명 이상 개인정보가 유출된 경우 유출 통지 및 조치 결과를 지체 없이 행정자치부 또는 전문기관(한국인터넷진흥원, www.privacy.go.kr)에 신고

※ 대상 : 1만 명 이상 유출 된 개인정보처리자
※ 개인정보보호법 제75조 제2항 제9호(**3천만원이하의과태료**)
조치결과를 신고하지 아니한 자 (행정자치부 또는 전문기관에 통지 결과 등을 신고하지 않은 경우)

1만 명 이상 유출된 경우에는 추가적으로 홈페이지에 공지

⇨ **개인정보보호법 시행령 40조 제3항**

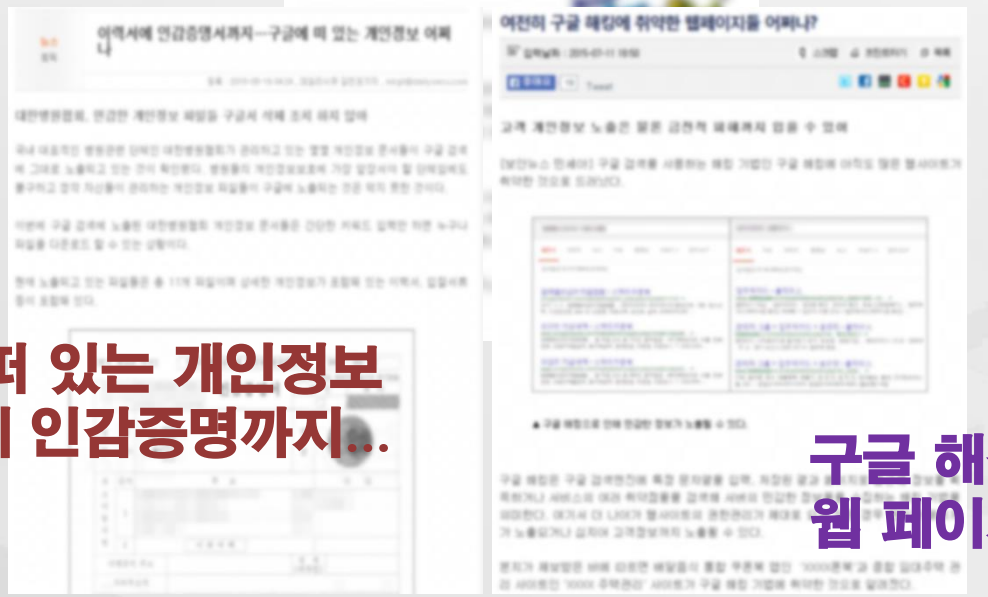
- 1만명 이상 개인정보가 유출된 경우 개별 통지와 함께 유출된 사실을 인터넷 홈페이지에 7일 이상 게재

※ 대상 : 1만 명 이상 유출 된 개인정보처리자
※ 홈페이지 등에 공지하지 않거나 7일 미만 게재하는 경우 : **시정명령**

2-1. 개인정보 노출이란?

일반적으로 홈페이지를 이용하는 자(이하 홈페이지 이용자)가 **해킹 등 특별한 방법을 이용하지 않고**, 정상적으로 인터넷을 이용하면서 타인의 개인정보를 취득할 수 있도록 **인터넷에 방치되어 있는 것**

XX보험사 고객정보 70만건 인터넷에 노출



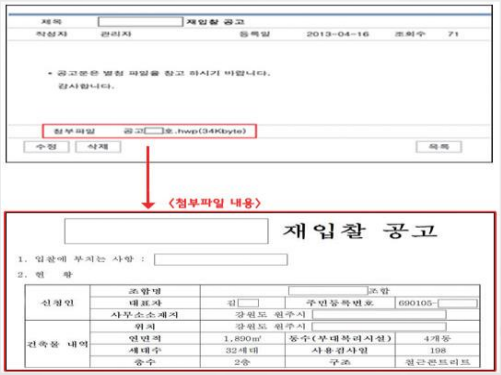
구글에 떠 있는 개인정보 이력서에 인감증명까지...

구글 해킹에 취약한 웹 페이지들...

2-2. 개인정보 노출 현황

구 분	노출 사이트 수	노출건수	구분			
			중앙부처	지자체	기 타	사업자
13년	727	56,226	1,048	18,863	20,723	15,592
14년	687	130,264	1,629	26,045	15,394	87,196
15년	774	182,445	509	6,623	32,903	142,410

<게시글>



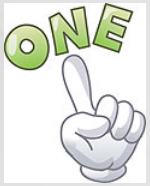
<첨부파일>

<홈페이지 설계 오류>

2-3. 왜 개인정보 노출이 발생하는가?

출처 : 인터넷

2-4. 노출사고를 예방하려면?



개인정보 최소 수집 및 파기

다시 한번 문서/홈페이지 확인

관리자페이지는 반드시 보안설정

주기적 점검은 필수

3-1. 홈페이지 법규 위반 사례

제15조(개인정보의 수집·이용)

제22조(동의를 받는 방법)

제29조(안전조치의무)

제30조(개인정보처리방침의 수립 및 공개)

< 홈페이지 온라인 점검 결과(16년 1월~3월)

3-1. 홈페이지 법규 위반 사례

제15조(개인정보의 수집·이용)제1항제1호

01 개인정보의 수집·이용 목적

02 수집하려는 개인정보의 항목

03 개인정보의 보유 및 이용 기간

04 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

※ 반드시 필요한 항목과 부가적인(선택) 항목을 구분하여 고지

3-1. 홈페이지 법규 위반 사례

제22조(동의를 받는 방법)제3항

- 개인정보의 처리 목적이 재화나 서비스를 홍보하거나 판매를 권유하기 위한 경우는 **별도로 동의**

■ [선택]홍보 및 마케팅 목적의 개인정보 수집·이용 동의

목적	항목	보유기간	동의여부
새로운 상품 안내 마케팅 (전화, 이메일)	휴대전화번호, 이메일	서비스 탈퇴 후 5일까지	□ SMS(문자) □ 전화 □ 이메일 □ 동의안함
맞춤형 광고	쿠키정보, 쿠키를 통해 수집되는 행태정보	서비스 탈퇴 후 5일까지	□ 동의함 □ 동의안함

동의를 거부 할 수 있으며, 동의를 거부하시는 서비스 이용에 불이익이 없습니다

3-1. 홈페이지 법규 위반 사례

제29조(안전조치의무)

개인정보의 암호화(고유식별정보, 비밀번호, 바이오정보)

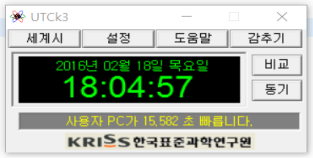
01 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송·수신 하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화 하여야 한다

02 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다 단, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다

03 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점 (DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다

※ 주민등록번호는 구간에 관계없이 2016.1.1.부터 암호화해야 한다


```
[HTTP request 1/3]
[Response in frame: 13]
[Next request in frame: 15]
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "mode" = "login"
    Key: mode
    Value: login
  Form item: "contentUid" = "9be517a74fa674f8014faad5c63302bd"
    Key: contentUid
    Value: 9be517a74fa674f8014faad5c63302bd
  Form item: "contentView" = "contentView"
    Key: contentView
    Value: contentView
  Form item: "returnUrl" = "/index.9is"
    Key: returnUrl
    Value: /index.9is
  Form item: "userId" = "testjy"
    Key: userId
    Value: testjy
  Form item: "userPassword" = "test1234!"
    Key: userPassword
    Value: test1234!
```



3-1. 홈페이지 법규 위반 사례

제30조(개인정보 처리방침의 수립 및 공개)

표준 개인정보 보호지침 제37조(필수적 기재사항) 법, 령, 고시

01 개인정보의 처리 목적

02 개인정보의 처리 및 보유 기간

03 개인정보의 제3자 제공에 관한 사항
(해당되는 경우에만 정한다)

04 개인정보처리의 위탁에 관한 사항
(해당되는 경우에만 정한다)

05 정보주체의 권리·의무 및 그 행사방법에 관한 사항

06 처리하는 개인정보의 항목

07 개인정보의 파기에 관한 사항

08 개인정보 보호책임자에 관한 사항

10. 개인정보관리책임자 및 담당자의 연락처

귀하께서는 회사의 서비스를 이용하시며 발생하는 모든 개인정보보호 관련 민원을 개인정보관리책임자 혹은 담당부서로 신고하실 수 있습니다.
회사는 이용자들의 신고사항에 대해 신속하게 충분한 답변을 드릴 것입니다.

개인정보 관리책임자

- 이 름 :
- 전 화 :
- 메 일 :

개인정보 관리담당자

- 이 름 :
- 전 화 :
- 메 일 :

기타 개인정보침해에 대한 신고나 상담이 필요하신 경우에는 아래 기관에 문의하시기 바랍니다.

- 개인분쟁조정위원회 (www.1336.or.kr / 1336)
- 정보보호마크인증위원회 (www.eprivacy.or.kr / 02-580-0533~4)
- 대검찰청 인터넷범죄수사센터 (http://icic.sppo.go.kr / 02-3480-3600)
- 경찰청 사이버테러대응센터 (www.ctrc.go.kr / 02-392-0330)

3-2. 현장점검/언론 법규 위반 사례

제26조(업무위탁에 따른 개인정보의 처리 제한)제4항

- 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 수탁자가 개인정보를 안전하게 처리 하는지를 감독하여야 한다

수탁자 선정

수탁자를 선정할 때에는 인력과 물적 시설, 재정 부담능력 등을 종합적으로 고려하여야 한다

수탁자 처리 업무 지연

개인정보처리자는 수탁자의 처리 업무의 지연, 처리 업무와 과련없는 불필요한 개인정보의 요구, 처리기준의 불공정 등의 문제점을 종합적으로 검토하여 이를 방지하기 위하여 필요한 조치를 마련해야 하여야 한다

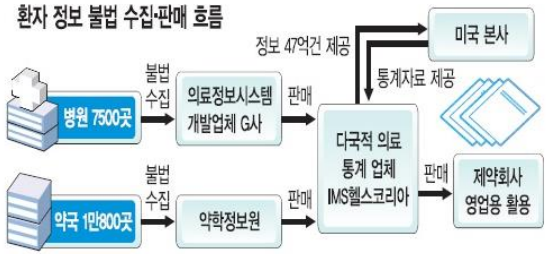
위탁 개인정보 보호

수탁자는 위탁받은 개인정보를 보호하기위하여 「개인정보의 안전성 확보조치 기준」에 따라 관리적·기술적·물리적 조치를 하여야 한다

환자 4400만명 정보 47억건 팔렸다… 다국적기업, 불법 수집

美 본사 거쳐 국내 되팔아… 70억대 수익, 24명 기소

입력 2015-07-24 02:35

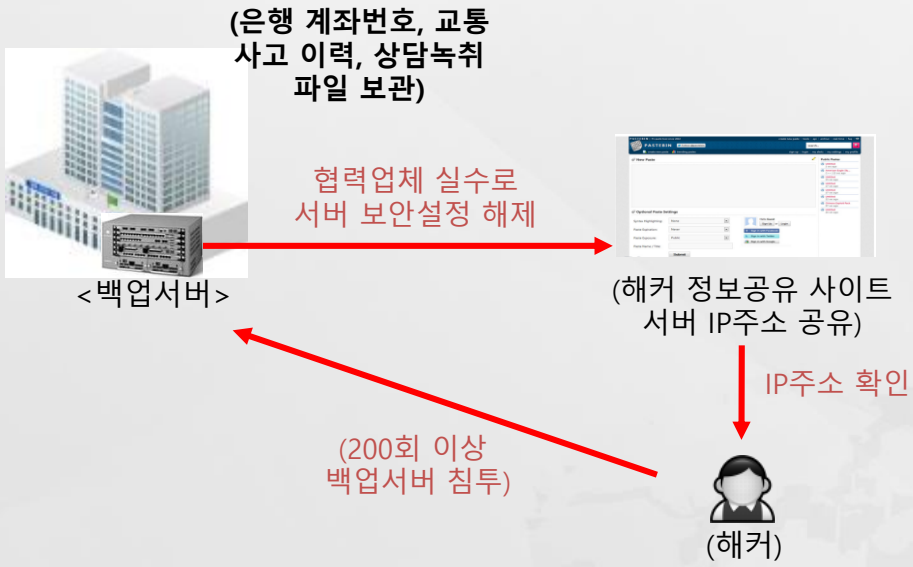


우리나라 전체 인구의 85%에 해당하는 4400만명의 진료·처방 정보 47억건이 불법 수집돼 다국적기업 측에 팔려나간 것으로 드러났다. 이 정보는 모두 해외의 다국적기업 본사에 넘겨져 영업용 자료로 쓰였다.

출처 : 국민일보

3-2. 현장점검/언론 법규 위반 사례

- ☞ 협력업체의 잘못으로 고객 상담 통화내용 파일 70만건이 보관된 백업서버가 외부에서 접속이 가능한 상태로 노출됨
- ☞ 개인정보처리시스템 유지보수 용역을 체결하면서, 보호조치를 하지 않아 용역업체 직원의 PC에 XX건의 개인정보가 보관됨



3-2. 현장점검/언론 법규 위반 사례

제29조(안전조치의무)

- 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다

01 내부관리계획의 수립·시행

02 접근권한의 관리

03 접근통제

04 개인정보의 암호화

05 접속기록의 보관 및 점검

06 악성프로그램 등 방지

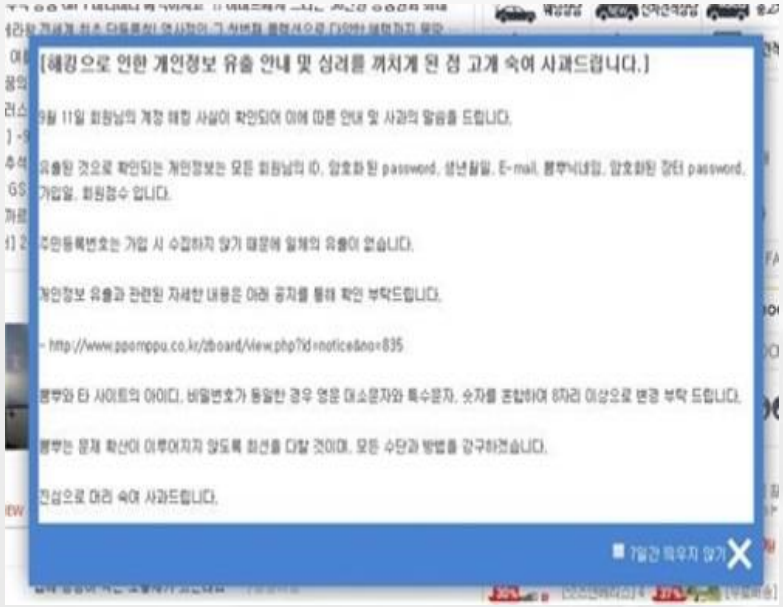
07 물리적 접근 방지

08 개인정보의 파기

※ 출처 : 개인정보의 안전성 확보조치 기준 [시행 2014.12.30.] [행정자치부고시 제2014-7호, 2014.12.30., 일부개정]

3-2. 현장점검/언론 법규 위반 사례

- ✓ 홈페이지 구조 및 취약점을 파악
- ✓ SQL 인젝션에 취약한 웹 페이지 확인
- ✓ SQL 인젝션을 통한 개인정보를 탈취



출처 : **MBN**

3-2. 현장점검/언론 법규 위반 사례

개인정보 보호법 시행이전에 수집한 개인정보의 파기??

[단독] 버려진 처방전 수만장 야산서 발견, 개인정보 유출

이준석 | 기사입력 2016-01-28 20:28 | 최종수정 2016-01-28 20:50

개인정보 처방전

KISA 한국인터넷진흥원

Internet On, Security In!

감사합니다