개인정보보호는 신뢰입니다.

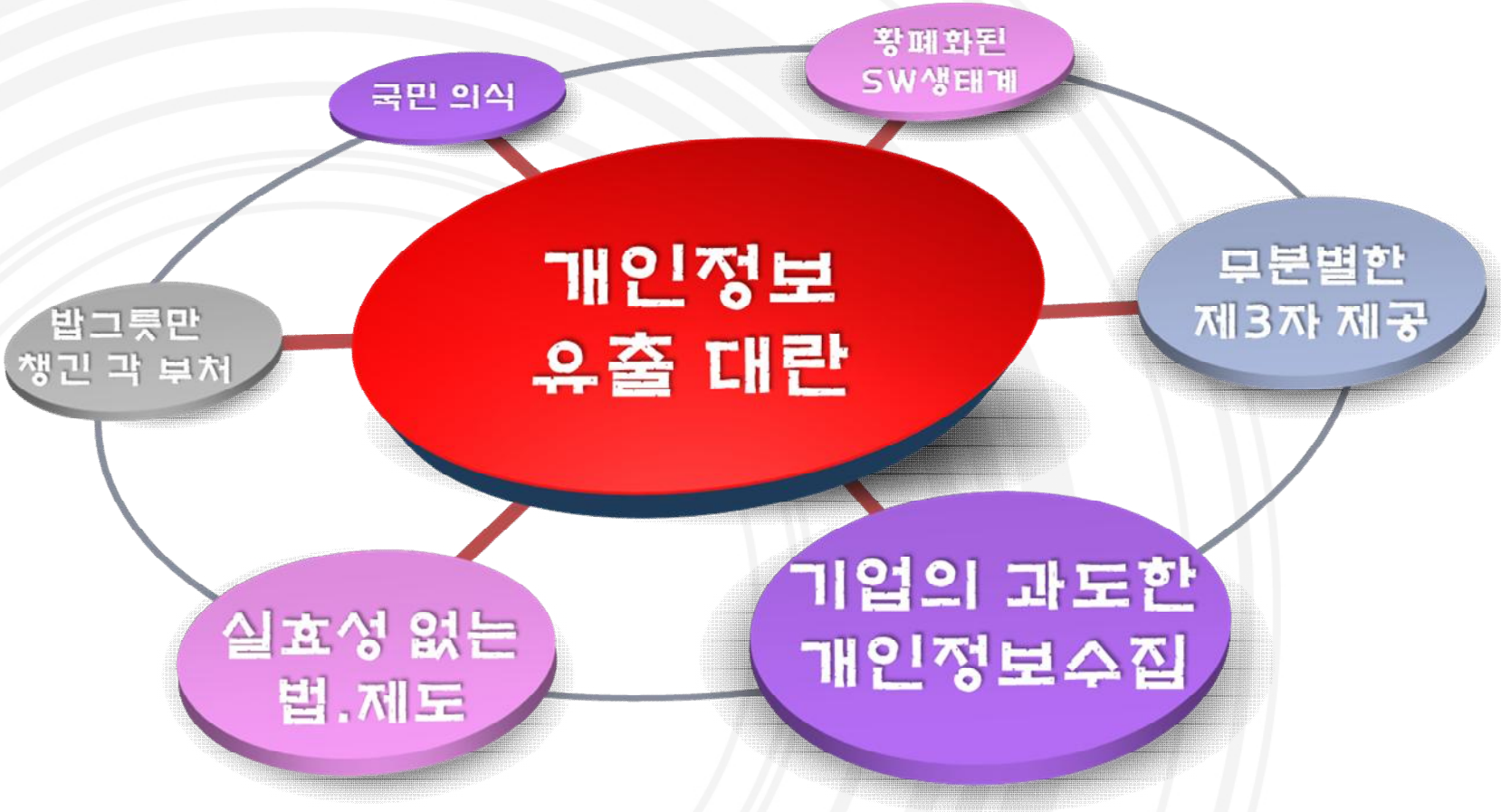
개인정보 유출사고로 본 효과적인 개인정보보호 방안

2014년 6월

정보화사회실천연합
Practice Coalition for Information Society

끈이지 않고 발생하는 개인정보 유출

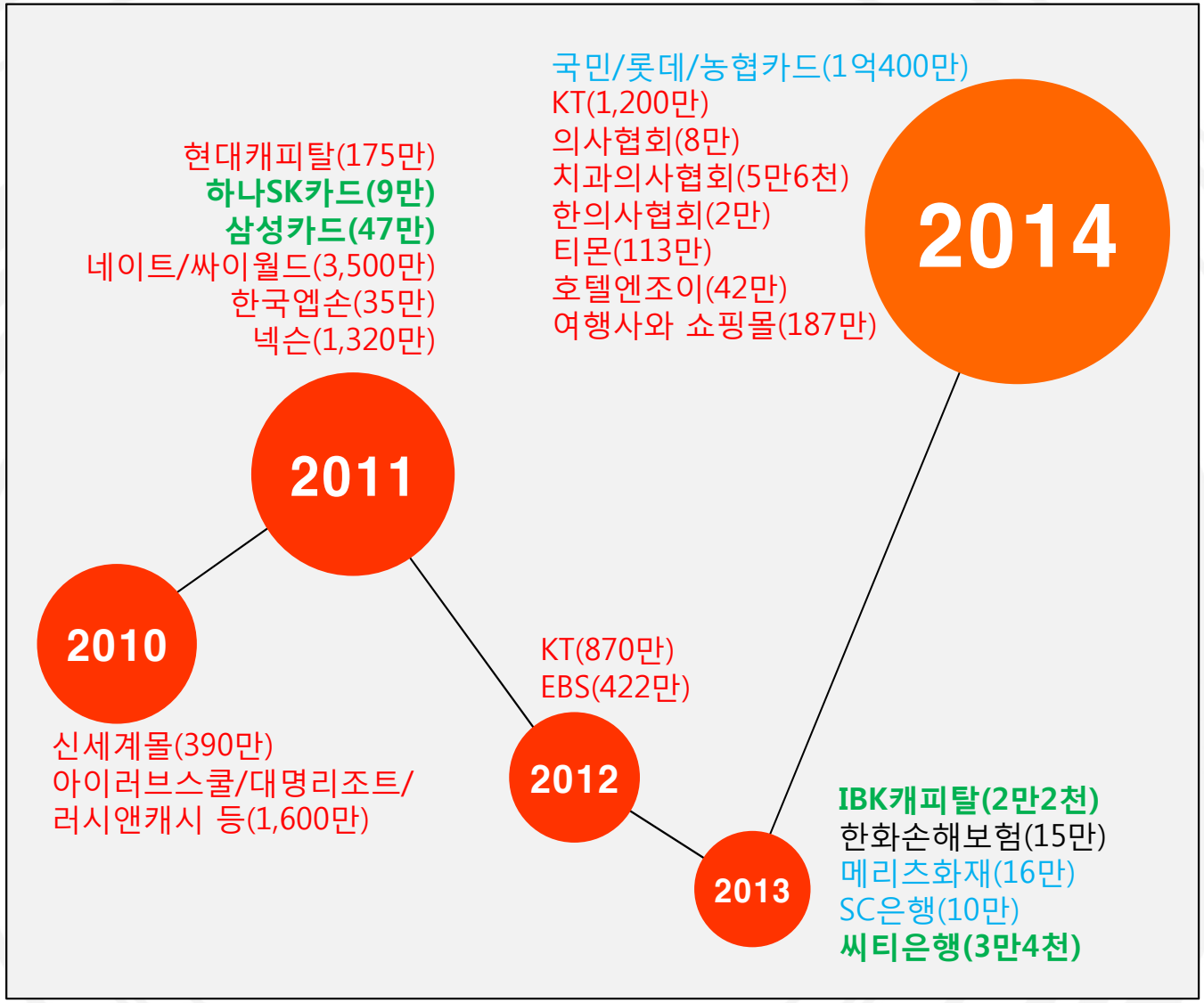
한번 유출되면 회수가 불가능한 꼬리표 없는 개인정보



정보화사회실천연합
Practice Coalition for Information Society

최근 5년간 주요 개인정보 유출 사고

최근 5년간 주요 개인정보 유출 사고



유출
- 유출사고(금융사·공공기관 등에서 **5년간 1억9283만** 건 유출)
- 사금융·온라인 도박사이트·웹하드 업체 등에서 돈 받고 판매
- 개인정보 거래업자들이 해킹으로 불법 취득

가공
- 주민번호 통해 다른 경로로 입수된 개인정보들 통합
- 이미 유출된 개인정보를 새 정보로 업데이트
- '블랙 빅데이터' 구축해 의료·대출·교육 등으로 재분류

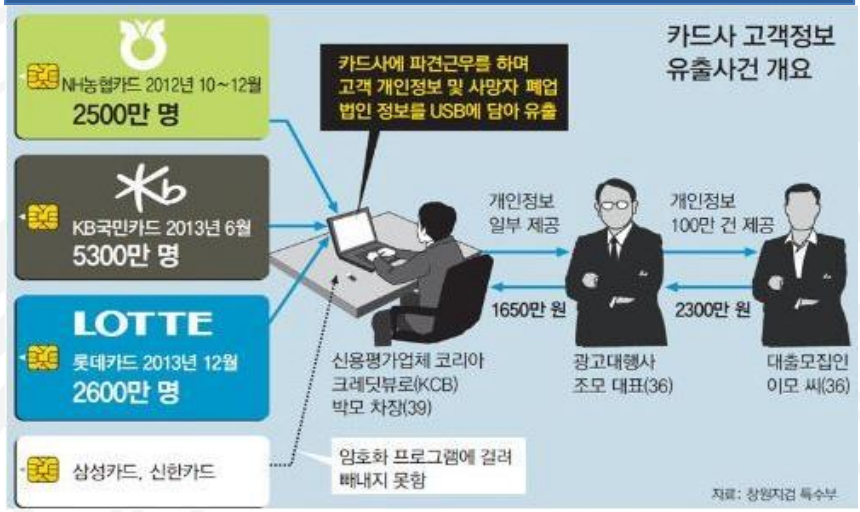
배포
- 인터넷 슬럼(방치된 사이트)에서 판매자·구매자 접촉
- 인터넷 메신저 통해 거래
- 대포통장 이용해 입금

악용
- 홍보·마케팅 이용(쇼핑몰 홍보 e메일 발송·대출 스팸 문자 등)
- 보이스피싱 등 범죄 악용
- 사금융·온라인도박 사이트에서 이용된 개인정보에 대출·도박내역 추가해 재수집

정보화사회실천연합
Practice Coalition for Information Society

카드사 및 KT의 유출사고로 본 문제점

카드사 고객정보 유출 개요



KT 개인정보유출 해킹사고 개요

문제점

USB에 담긴 1억400만 건
- 보조기억매체(USB) 접근통제 방치
- 4D로 전락한 열악한 SW 종사자

문서뿐인 내부통제규정, 정보보안절차
- 보안서약서는 받았으니
- 매일 보는데 괜찮겠지
- 작업 PC에 보안프로그램 미 설치
- 운영 DB에 직접 접속 작업

초보적인 해킹기술로 유출
- 법이 정한 대상만 암호화 처리(로그인, 회원가입 등)
- 트래픽 증가 명분으로 암호화 대상 축소

유명무실한 탐지 시스템
- 특정 IP로 하루 34만 번 접속
- 3개월 동안 홈페이지에 1,266만 번 접속

성과주의에 매몰된 정보시스템 구축 사업
- 짧은 정보화 사업 기간
- 디자인이 우선 정보보호는 뒷전

개인정보 유출의 2차 피해 현황

보이스 피싱 (Voice phishing)

전화를 통해 불법적으로 개인 정보를 빼내서 범죄에 사용하는 범법 행위

스미싱(Smishing)

문자 메시지(SMS)를 이용해 개인정보/금융정보를 낚는다(fishing)는 의미의 합성어

피싱사기 피해건수 및 금액 ('06.6 ~ '13.12)
피해건수 : 44,816건 피해금액 : 4,758억원

스미싱사기 피해건수 및 금액 ('13.1 ~ '13.5)
신고건수 : 17,936건 추정피해금액 : 12.39억원

〈표 3-3〉 스미싱 피해 신고 현황 및 금액(추정)

단위 : 건, 만원

구분 / 월별	신고 건수	신고 금액
1월	8,197	57,379
2월	4,723	33,061
3월	1,095	7,665
4월	2,595	16,594
5월	1,326	9,207
총 계	17,936	123,906

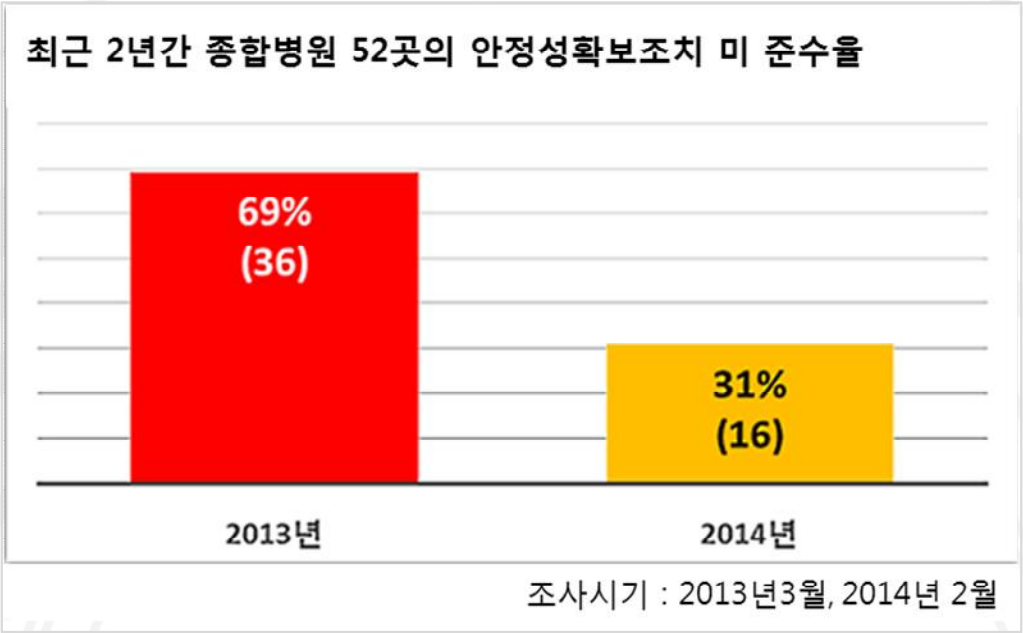
자료 : 한국전화결제산업협회

파밍(Pharming)

피싱(Phishing)과 농사(Farming)의 합성어, PC에 가짜 은행사이트로 유도하는 악성코드 설치, 금융정보 빼낸 후 예금을 무단 인출하는 수법

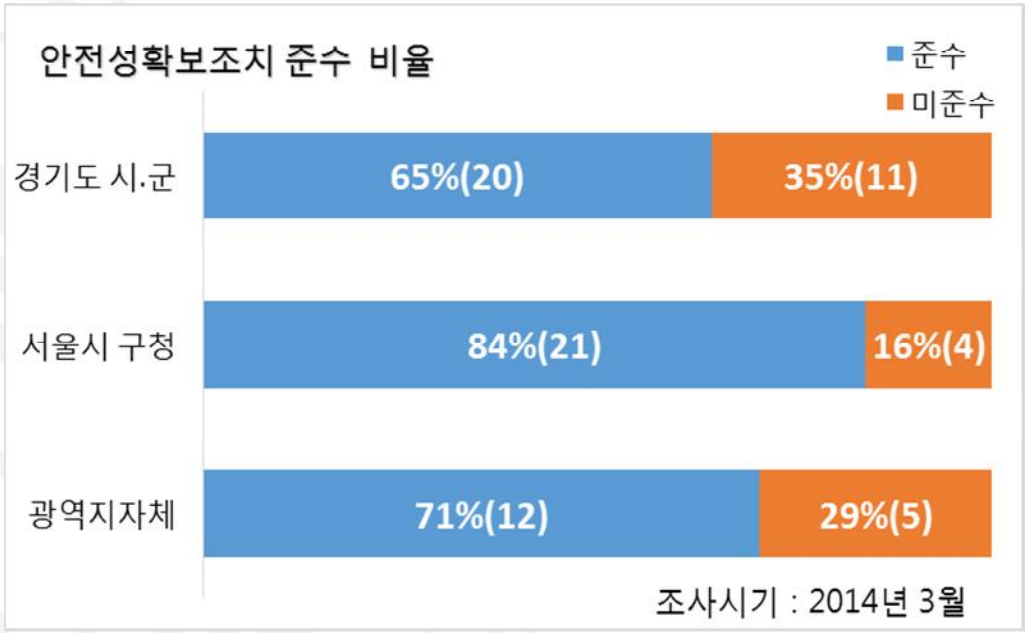
안전성확보 조치 준수 실태조사

대형 종합병원의 개인정보 보호 실태조사 현황



조사시기 : 2013년3월, 2014년 2월

공공기관의 개인정보 보호 실태 조사 현황



조사시기 : 2014년 3월

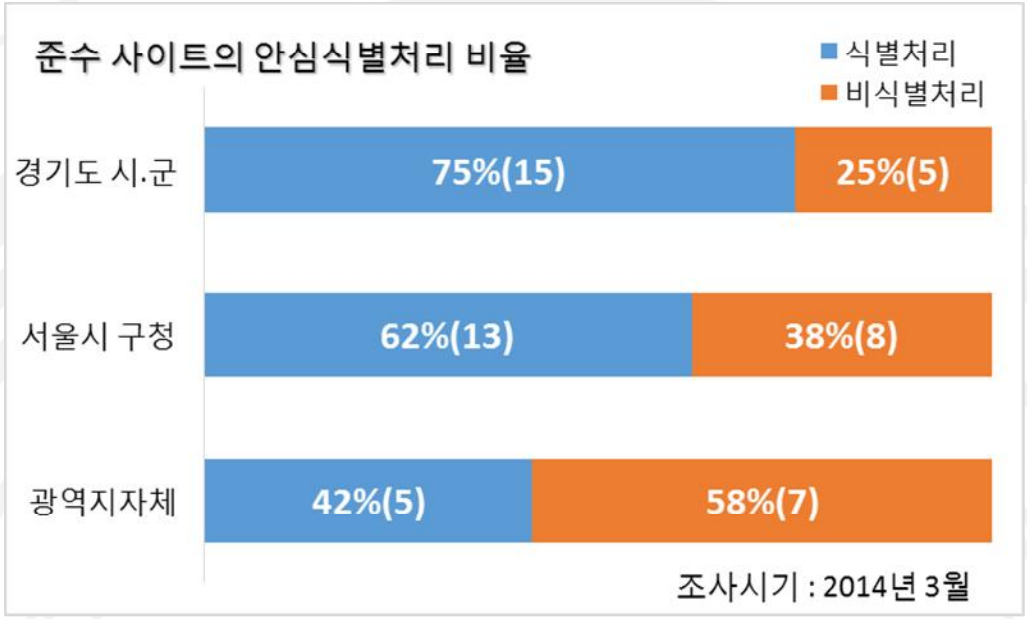
개인정보보호법(2011.9.30) 시행 2년6개월, 민간 및 공공기관 약 30%가 미 준수

기본조차 안 지키는 개인정보 보호

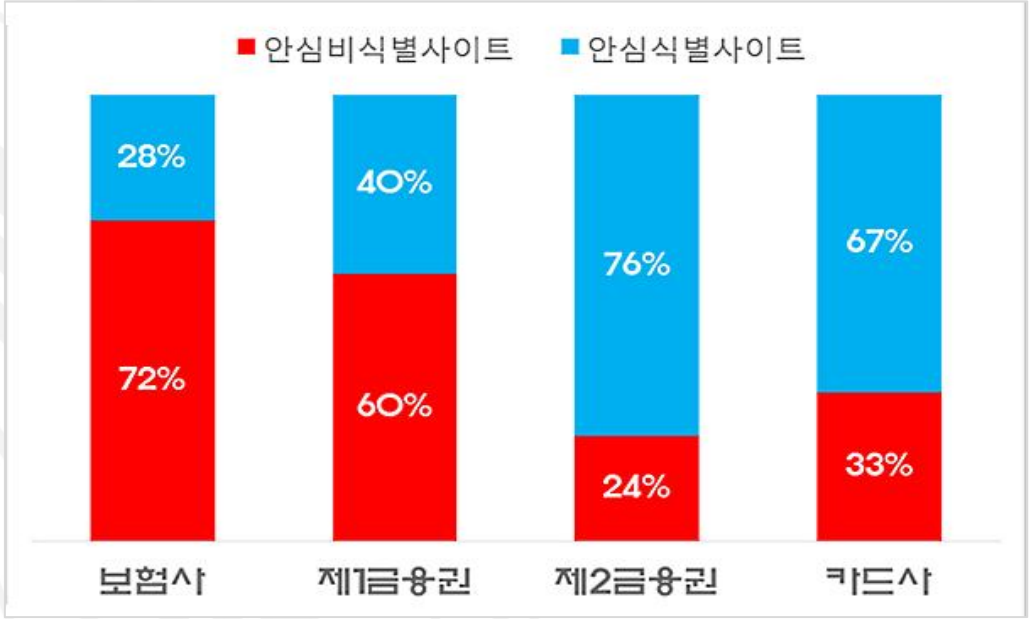
정보화사회실천연합
Practice Coalition for Information Society

안전성확보 조치 식별처리 현황

공공기관 실태조사 현황



금융기관 실태조사 현황



비 식별처리(부분암호화)는 트래픽 증가를 명분 삼아 이용자를 고려하지 않음

법만 지키면 된다는 잘못된 개인정보 보호 의식

정보화사회실천연합
Practice Coalition for Information Society

개인정보 관련 행정조치 내역

개인정보보호법 위반행위별 행정처분 현황

위반 주체 / 위반 내역 / 조치 내용	공공기관				민간사업자			
	과태료	시정조치	개선권고	합계	과태료	시정조치	개선권고	합계
수집 동의 위반(§15, §17, §22, §23, §24)	4	1	15	20	31	141	88	260
과도한 개인정보 수집(§16, §18)	0	2	0	2	0	11	41	52
침해, 열람 등 위반(§34, §35, §36, §37, §59)	0	1	0	1	1	6	2	9
안전 조치 미흡(§29)	8	12	90	110	36	67	97	200
위·수탁 위반(§26)	7	6	10	23	28	26	2	56
CCTV 설치·운영 위반(§25)	0	9	14	23	23	124	102	249
기타(§21, §28, §30, §31, §32, §33)	0	13	31	44	13	70	63	146
합 계	19	44	160	223	132	445	395	972

출처 : 안전행정부

정보통신망법 위반행위별 행정처분 현황

위반행위	2012년		2013년	
	개선권고	과태료 처분	개선권고	과태료 처분
라. 법 제23조의2제1항을 위반하여 주민등록번호를 수집·이용하거나 같은 조 제2항에 따른 필요한 조치를 하지 않은 경우(법 제67조에 따라 준용되는 경우를 포함한다)	-	-	36	1
아. 법 제24조의2제3항(법 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 제공 또는 취급위탁에 대한 동의를 받을 때 개인정보의 수집·이용에 대한 동의와 구분	1	-	-	1
자. 법 제25조제2항(법 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자에게 개인정보 취급위탁에 관한 사항을 공개하지 않거나 알리지 않은 경우	1	11	-	4
타. 법 제27조의2제1항(법 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 취급방침을 공개하지 않은 경우	-	-	-	1
파. 법 제27조의3제1항(법 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자 및 방송통신위원회에 통지 또는 신고하지 않은 경우	-	-	-	13
하. 법 제28조제1항(법 제67조에 따라 준용되는 경우를 포함한다)에 따른 기술적·관리적 조치를 하지 않은 경우	-	10	-	18
거. 법 제29조제1항 본문을 위반하여 개인정보를 파기하지 않거나 같은 조 제2항에 따른 조치를 취하지 않은 경우(법 제67조에 따라 준용되는 경우를 포함한다)	-	1	-	8
너. 법 제30조제3항·제4항 및 제6항(법 제30조제7항, 제31조제3항 및 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 필요한 조치를 하지 않은 경우	-	1	-	1
허. 법 제50조제1항부터 제3항까지의 규정을 위반하여 영리 목적의 광고성 정보를 전송한 경우	-	625	-	258
고. 법 제50조제4항 또는 제5항을 위반하여 광고성 정보를 전송할 때 밝혀야 하는 사항을 밝히지 않거나 거짓으로 밝힌 경우	-	17	-	69
노. 법 제50조제7항을 위반하여 비용을 수신자에게 부담하도록 한 경우	-	20	-	471
로. 법 제50조의7제1항을 위반하여 인터넷 홈페이지에 영리목적의 광고성 정보를 게시한 경우	-	-	-	29
계	2	685	36	874

출처 : 방송통신위원회

- 안행부 행정조치 : 310건 중 44건만 과태료처분
- 방통위 행정조치 : 28건 과태료처분

솜방망이 행정처분

정보화사회실천연합
Practice Coalition for Information Society

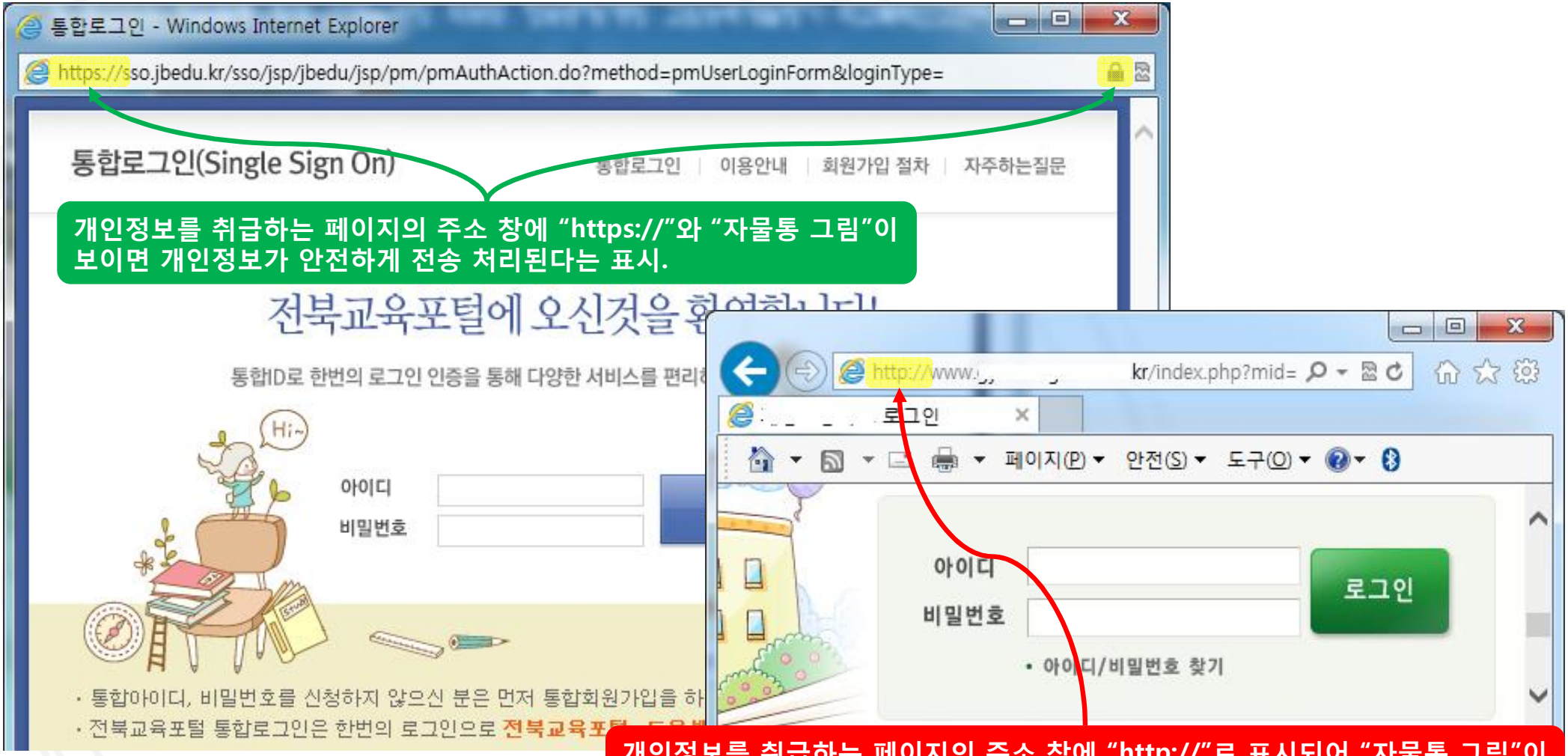
개인정보의 안전성 확보조치

보안서버 운영 웹사이트의 차이점

제29조(안전조치의무) 개인정보처리자는 개인정보가 분실・도난・유출・변조 또는 훼손되지 아니하도록 내부관리계획수립, 접속기록보관 등 대통령령으로 정하는 바에 따라 안전성확보에 필요한 기술적・관리적 및 물리적 조치를 하여야 한다.

개인정보의 안전성 확보조치

보안서버 구축을 통한 전송 시 개인정보의 암호화 비교 사례



개인정보 보호법의 한계

01 **보호의무 적용대상의 확대**
분야별 개별법에 따라 시행되던 개인정보 보호의무 적용대상을 공공/민간 부문의 모든 개인정보처리자로 확대 적용

02 **보호 범위의 확대**
컴퓨터 등에 의해 처리되는 정보 외 동사무소 민원신청서류 등 종이문서에 기록된 개인정보도 보호대상에 포함

03 **고유식별정보 처리 제한**
- 주민번호 등 고유식별정보는 원칙적 처리 금지, 사전 규제제도 신설
  - 위반 시 5년 이하 징역 또는 5천만원 이하 벌금
- 주민번호외 회원가입방법 제공 의무화 및 암호화 등의 안전조치 의무화
  - 위반 시 3천만원 이하 과태료

04 **영상정보 처리기기 규제**
- 공개된 장소에 설치·운영하는 영상정보처리기기 규제를 민간까지 확대
- 설치목적을 벗어난 카메라 임의조작, 다른 곳을 비추는 행위, 녹음 금지
  - 위반 시 3년 이하 징역 또는 3천만원 이하 벌금

05 **개인정보 수집·이용 제공기준**
공공민간 통일된 처리원칙과 기준 적용개인정보 수집·이용 가능 요건 확대
- 위반 시 5년 이하 징역 또는 5천만원 이하 벌금

06 **개인정보 유출 통지 및 신고제 도입**
- 정보주체에게 유출 사실을 통지
- 대규모 유출 시에는 안전행정부 또는 전문기관에 신고
  - 위반 시 3천만원 이하 과태료

법의 실효성의 한계

선언적인 고유식별정보 처리 제한으로 동의절차만 받으면 누구나 수집이 가능하여 실효성이 없음

암호화의 대상을 고유식별정보만 의무화하고 있어 이름, 전화번호, 주소 등은 무방비로 노출됨

개인정보 수집.이용의 모호성으로 과도한 개인정보 수집 및 무분별한 제3자 제공

개인정보 보호 책임자의 연락처는 책임자 연락처가 아니라 고객센터 대표번호를 기재하여도 무방함

부분 암호화 허용으로 정보주체가 개인정보의 안전한 처리를 식별 할 수 없음

정보화사회실천연합
Practice Coalition for Information Society

제 각각인 개인정보 관련법

정보의 중요도		법령	안전성확보조치에 관한 과태료 비교
일반법	보통	**개인정보 보호법** 제29조(안전조치의무)	**개인정보 보호법 시행령** [별표 2] <개정 2013.3.23> 과태료의 부과기준(제63조 관련) 차. 법 제24조제3항, 제25조제6항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우 / 법 제75조 제2항제6호 / 600 / 1200 / 2400
개별법	높음	**정보통신망 이용촉진 및 정보보호 등에 관한 법률** 제28조(개인정보의보호조치)	**정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령** [별표 9] <개정 2013.3.23> 과태료의 부과기준(제74조 관련) 하. 법 제28조제1항(법 제67조에 따라 준용되는 경우를 포함한다)에 따른 기술적·관리적 조치를 하지 않은 경우 / 법 제76조제1항제3호 / 1,000 / 2,000 / 3,000
개별법	매우높음	**신용정보의 이용 및 보호에 관한 법률** 제19조(신용정보전산시스템의안전보호)	**신용정보의 이용 및 보호에 관한 법률 시행령** [별표 4] <개정 2011.8.17>과태료의 부과기준(제38조 관련) 6. 법 제19조제1항을 위반한 경우 / 법 제52조 제3항제5호 / 600

정보화사회실천연합
Practice Coalition for Information Society

개선방안 : 법률

개인정보 보호 관련 조문의 통합 필요

개인정보 보호법 (2011)

정보통신 망법 (2001)

신용정보 보호법 (1995)

용도별 고유식별번호 도입 필요

만능, 공용 주민등록번호

개인정보 보호법 + 분야별 특수성 + 규모별 형평성

용도별 고유번호 + 엄격한 수집제한 + 수집된 주민번호 조기폐기

통합 개인정보 보호법

개선방안 : 고시

사전.예방 조치에 대한 제도 강화	실효적 효과
▪ "개인정보 수집 및 이용 동의"의 포괄적 동의 절차 행위 제한	▪ 무분별한 개인정보 수집의 제한 효과
▪ 법률의 근거 없이는 고유식별정보 수집의 엄격한 제한	▪ 파밍 피해 방지 효과
▪ 암호화의 대상을 범위의 확대 ▪ 부분 암호화 적용 제한	▪ 고객의 서비스제공자에 대한 가시적인 신분확인으로 기관의 신뢰도 증대
▪ 제3자 개인정보 제공의 엄격한 제한	▪ 홍보 및 스팸 문자, 메일 감소 효과
▪ 개인정보 보호 책임자의 연락처를 고객센터 등 연락처로 명시의 제한	▪ 문제점의 신속한 인지 및 조치

국민의 입장에서 개인정보는 보호되어야 한다.

감사합니다