

개인정보 침해 및 위반 사례

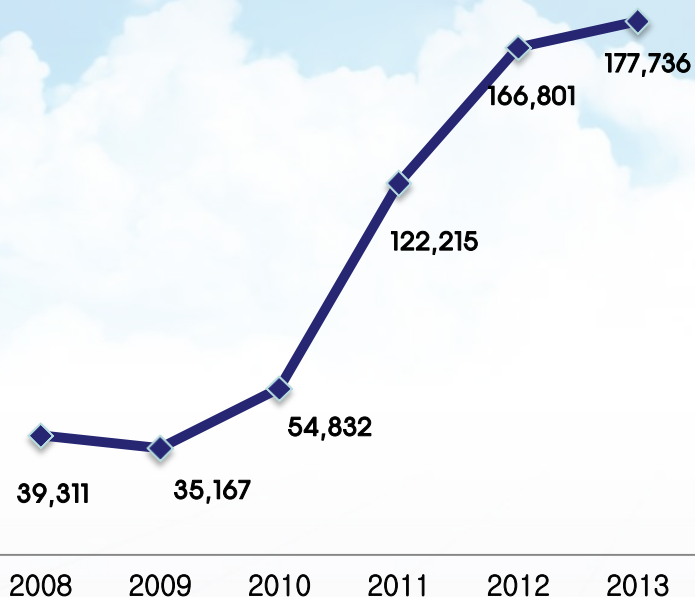
2014



1. 개인정보 침해 현황

개인정보 침해 규모

〈개인정보 침해민원 추이〉



출처 : 개인정보침해신고센터

대규모 개인정보 유출 사례

발생일	발생기업	피해규모	사고원인
08. 2	옥션	1,800만 명	해킹
08. 4	하나로 텔레콤	600만 명	텔레마케팅업체에 제공
08. 9	GS 칼텍스	1,150만 명	자회사 직원이 유출
10. 3	신세계몰 등 25개	2,000만 건	해킹
11. 4	현대캐피탈	175만 건	해킹 및 내부 관리 소홀
11. 5	세티즌	140만 명	홈페이지 해킹
11. 7	SK컴즈(네이트동)	3,560만 명	해킹(관리자 ID/PW 탈취)
11. 8	삼성카드	47만 건	자사 직원이 유출
11.11	넥슨	1,320만 건	해킹
12. 5	EBS	422만 건	해킹
12. 7	KT	873만 건	해킹
12.11	연예기획사 등	413만 건	구글링
13. 2	코웨이	198만 건	자사 직원이 유출
13. 6	청와대	10만 건	해킹
14. 1	신용카드사	10,400만건	시스템개발업체직원이유출
14. 2	의사협회 등 22개	1,700만 건	해킹
14. 3	KT	982만 건	해킹
14. 3	통신 3사 등	1,230만 건	해킹(주정)



2. 개인정보 처리 단계별 위반 유형

개인정보의 생명주기와 침해/유출 위험



2. 개인정보 처리 단계별 위반 유형

개인정보의 수집 경로와 불법 사용 유형





2. 개인정보 처리 단계별 위반 유형

개인정보의 처리에 따른 동의

- 개인정보 처리 동의 및 동의 절차 누락, 최소 수집 원칙 위반, 구분 동의 및 별도 동의 위반, 홍보 마케팅 목적의 처리 미동의시 서비스 제한, 동의를 받는 방법 위반

1. 개인정보 수집 목적 : 상담의 접수와 처리 및 **기관 홍보자료의 발송**

2. 수집하는 개인정보의 항목

- 필수정보 : 성명, **주민등록번호**, 전화번호, 이메일주소
- 선택정보 : 학력, 가족관계, **가입정당**

3. 귀하는 개인정보의 수집에 대한 동의를 거부할 수 있으며 동의를 거부할 경우 민원의 접수 및 처리가 불가합니다.

참고 : 입력하신 개인정보는 지역행사 운영을 목적으로 **유관기관에 제공 될 수 있습니다.**

동의하시겠습니까? 동의 ☐ 미동의 ☐



2. 개인정보 처리 단계별 위반 유형

개인정보의 전송, 저장

- 고유식별정보 / 비밀번호 / 바이오 정보의 암호화 미적용, 접근권한 관리 미흡, 접속기록 누락, 외부망의 시스템 접근시 전용선 또는 VPN 미적용, 안전한 비밀번호 미적용

성명	주민등록번호	아이디	비밀번호
홍일동	751111-1111000	Hong1	abcd
홍이동	751111-1111001	Hong2	1111
홍삼동	751111-1111002	Hong3	Abcd11
홍사동	751111-1111003	Hong4	love2u!!
홍오동	751111-1111004	Hong5	qaWS5@11



2. 개인정보 처리 단계별 위반 유형

개인정보의 전송, 저장

- 고유식별정보 / 비밀번호 / 바이오 정보의 암호화 미적용, 접근권한 관리 미흡, 접속기록 누락, 외부망의 시스템 접근시 전용선 또는 VPN 미적용, 안전한 비밀번호 미적용

안전한 암호화 알고리즘

1. 대칭키 : SEED, ARIA / AES -128/192/256 등
2. 공개키 : RSA, KDSA, RASES-OAEP 등
3. 해 쉬 : SHA-224/256/384/512 등

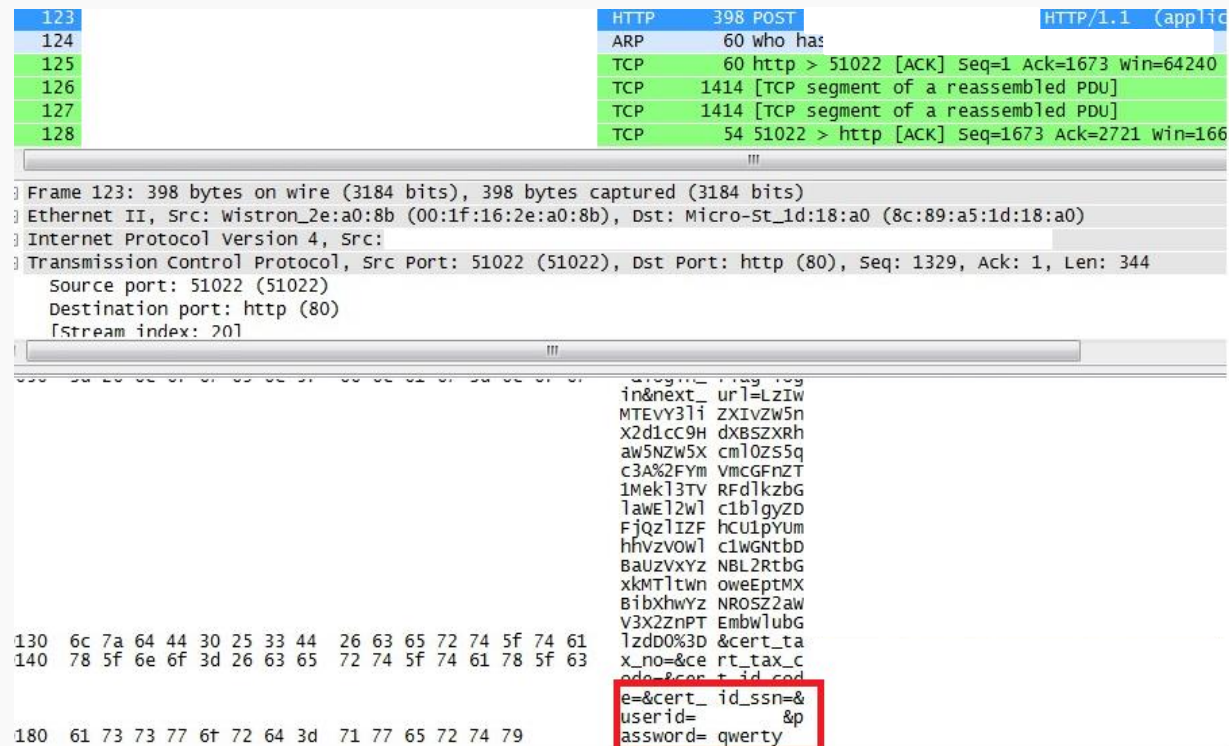
안전한 암호 기준

- 구성 및 길이 : 대문자, 소문자, 숫자, 특수문자 중
 1. 2가지 조합 10자리 이상
 2. 3가지 조합 8자리 이상
- 내용과 패턴
 1. 사전적 단어의 제외
 2. 사용자의 ID 연관성 배제
 3. 개인정보의 포함 배제

2. 개인정보 처리 단계별 위반 유형

개인정보의 전송, 저장

- 고유식별정보 / 비밀번호 / 바이오 정보의 암호화 미적용, 접근권한 관리 미흡, 접속기록 누락, 외부망의 시스템 접근시 전용선 또는 VPN 미적용, 안전한 비밀번호 미적용



The image shows a Wireshark packet capture of an HTTP POST request. The packet list on the left shows packets 123 through 128. Packet 123 is selected, showing details for Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The payload is an HTTP POST request to http://10.10.10.10:80. The request body contains a URL-encoded string: `in&next_url=LZIW MTEVY31i ZXIvZW5n X2d1cC9H dXBSZXRh aw5NZW5X cm10ZS5q c3A%2FYm VmcGFnZT lMek13TV Rfdlkzbg lawE12w1 c1blgyZD FjQz1IZF hCU1pYUm hhvzvow1 c1wGntbd BaUzVxYZ NBL2Rtbg xkMTltwn oweEptMX BibXhwYZ NROSZ2aw V3X2ZnPT EmbwLubG lzdd0%3D &cert_ta x_no=&ce rt_tax_c ode=&ce rt_id_cod e=&cert_id_ssn=&userid=&password= qwerty`. The password field is highlighted with a red box.

No.	Time	Source	Destination	Protocol	Length	Info
123	0.000000	10.10.10.10	10.10.10.10	HTTP	398	POST / HTTP/1.1 (application/javascript)
124	0.000000	10.10.10.10	10.10.10.10	ARP	60	who has 10.10.10.10
125	0.000000	10.10.10.10	10.10.10.10	TCP	60	http > 51022 [ACK] Seq=1 Ack=1673 win=64240
126	0.000000	10.10.10.10	10.10.10.10	TCP	1414	[TCP segment of a reassembled PDU]
127	0.000000	10.10.10.10	10.10.10.10	TCP	1414	[TCP segment of a reassembled PDU]
128	0.000000	10.10.10.10	10.10.10.10	TCP	54	51022 > http [ACK] Seq=1673 Ack=2721 win=166

Frame 123: 398 bytes on wire (3184 bits), 398 bytes captured (3184 bits) on interface 0

Ethernet II, Src: Wistron_2e:a0:8b (00:1f:16:2e:a0:8b), Dst: Micro-St_1d:18:a0 (8c:89:a5:1d:18:a0)

Internet Protocol Version 4, Src: 10.10.10.10, Dst: 10.10.10.10

Transmission Control Protocol, Src Port: 51022 (51022), Dst Port: http (80), Seq: 1329, Ack: 1, Len: 344

Source port: 51022 (51022)

Destination port: http (80)

[Stream index: 20]

130 6c 7a 64 44 30 25 33 44 26 63 65 72 74 5f 74 61
140 78 5f 6e 6f 3d 26 63 65 72 74 5f 74 61 78 5f 63
180 61 73 73 77 6f 72 64 3d 71 77 65 72 74 79

in&next_url=LZIW MTEVY31i ZXIvZW5n X2d1cC9H dXBSZXRh aw5NZW5X cm10ZS5q c3A%2FYm VmcGFnZT lMek13TV Rfdlkzbg lawE12w1 c1blgyZD FjQz1IZF hCU1pYUm hhvzvow1 c1wGntbd BaUzVxYZ NBL2Rtbg xkMTltwn oweEptMX BibXhwYZ NROSZ2aw V3X2ZnPT EmbwLubG lzdd0%3D &cert_ta x_no=&ce rt_tax_c ode=&ce rt_id_cod e=&cert_id_ssn=&userid=&password= qwerty

2. 개인정보 처리 단계별 위반 유형

개인정보의 전송, 저장

- 고유식별정보 / 비밀번호 / 바이오 정보의 암호화 미적용, 접근권한 관리 미흡, 접속기록 누락, 외부망의 시스템 접근시 전용선 또는 VPN 미적용, 안전한 비밀번호 미적용

사번	로그인시간		로그아웃시간		업무시작시간		업무종료시간		접근권한
1	20	7	20	4	20	0	20	0	
1	20	1	20	1	20	0	20	0	
1	20	6			20	0	20	0	
1	20	6	20	3	20	0	20	0	
1	20	7			20	0	20	0	
1	20	3			20	0	20	0	
1	20	5	20	3	20	0	20	0	
1	20	7			20	0	20	0	
1	20	9			20	0	20	0	
1	20	4			20	0	20	0	
1	20	0	20	8	20	0	20	0	
1	20	5	20	5	20	0	20	0	
1	20	5	20	1	20	0	20	0	
1	20	0	20	3	20	0	20	0	
1	20	4	20	3	20	0	20	0	
1	20	3			20	0	20	0	

2. 개인정보 처리 단계별 위반 유형

개인정보의 이용

- 개인정보의 목적 외 이용 및 제3자 제공, 개인정보 취급자에 대한 교육 및 관리감독 미흡, 개인정보 파일의 관리 누락, 개인정보처리방침의 수립 및 공개 미흡

개인정보취급방침

CHECK PRIVACY POLICY

제2조(정의)
 이 약관에서 사용하는 용어의 정의는 다음 각 호와 같습니다.
 1. 이용자: 본 약관에 따라 회사가 제공하는 서비스를 받는 자
 2. 이용약관: 서비스 이용과 관련하여 회사와 이용자간에 체결하는 계약
 3. 가입: 회사가 제공하는 신청서 양식에 해당 정보를 기입하고, 본 약관에 동의하여 서비스 이용계약을 완료시키는 행위
 4. 회원: 당 사이트에 회원가입에 필요한 개인정보를 제공하여 회원 등록을 한 자
 5. 이용자번호(ID): 회원 식별과 회원의 서비스 이용을 위하여 이용자가 선정하고 회사가 승인하는 영문자와 숫자의 조합
 6. 패스워드(PASSWORD): 회원의 정보 보호를 위해 이용자가 자신이 설정한 영문자와 숫자, 특수문자의 조합
 7. 이용해지: 회사 또는 회원이 서비스 이용이후 그 이용계약을 종료시키는 의사표시

제3조(약관의 효력과 변경)
 회원은 변경된 약관에 동의하지 않을 경우 회원 탈퇴(해지)를 요청할 수 있으며, 변경된 약관의 효력 발생일로부터 7일 이후에도 거부사유를 표시하지 아니하고 서비스를 계속 사용할 경우 약관의 변경 사항에 동의한 것으로 간주됩니다.
 ① 이 약관의 서비스 화면에 게시하거나 공지사항 게시판 또는 기타의 방법으로 공지함으로써 효력이 발생합니다.
 ② 회사는 필요하다고 인정되는 경우 이 약관의 내용을 변경할 수 있으며, 변경된 약관은 서비스 화면에 공지하며, 공지 후 7일 이후에도 거부사유를 표시하지 아니하고 서비스를 계속 사용할 경우 약관의 변경 사항에 동의한 것으로 간주됩니다.
 ③ 이용자가 변경된 약관에 동의하지 않는 경우 서비스 이용을 중단하고 본인의 회원등록을 취소할 수 있으며, 계속 사용하는 경우에는 약관 변경에 동의한 것으로 간주되며 변경된 약관은 전항과 같은 방법으로 효력이 발생합니다.

제4조(준용규정)
 이 약관에 명시되지 않은 사항은 전기통신기본법, 전기통신사업법 및 기타 관련법령의 규정에 따릅니다.

제2장 서비스 이용계약

제5조(이용계약의 성립)
 이용계약은 이용자의 이용신청에 대한 회사의 승낙과 이용자의 약관 내용에 대한 동의로 성립됩니다.

네이버 이용시 수집되는 정보는?



네이버 접속

IP 주소, 방문일시, 서비스 이용기록 등과 같은 생성정보 수집

생성정보란?

인터넷 서비스 이용과정에서 자동적으로 만들어지는 '기밀 인터넷 정보'입니다.
 이러한 정보가 없다면, 서비스를 정상적으로 제공할 수 없습니다.



쿠키의 이용

서비스 이용의 편의를 위해 꼭 필요한 경우에 한해 제한적으로 쿠키 활용

쿠키란?

쿠키란 인터넷 접속 시 자동 생성되는 방문 기록 정보로 이용자는 웹 브라우저의 기능 설정을 통해 쿠키를 허용하거나 거부할 수 있습니다.



부가 서비스 및 맞춤 서비스 이용

특정 서비스 이용 과정에서 이용자 선택에 의해 추가정보 수집이 발생하는 경우 별도의 이용자 동의를 받습니다.



회원가입

이름, 생년월일, 성별, 아이디, 비밀번호, 별명, 연락처 (이메일주소 또는 휴대전화번호), 가입인증 정보

네이버는 회원가입 시 본인확인을 하지 않는 간편가입(비밀번호)을 제공합니다.
 또, 주민등록번호도 수집하지 않습니다.



유료 서비스 이용

유료 서비스 이용자에 한하여 결제를 위한 최소한의 정보수집

- 신용카드 결제 시: 카드사 카드번호 등
- 휴대폰 결제 시: 통신사, 휴대폰번호, 결제승인번호 등
- 계좌이체 시: 은행명, 계좌번호
- 상품권 이용 시: 상품권 번호



본인인증

계정, 생년월일, 아이디 등 법률에 의해 본인인증이 필요한 경우

이름, 생년월일, 중개가입정보, 암호화된 동일한 식별정보, 인증수단에 따라 휴대폰 번호 또는 아이디, 내/외국인 구분



2. 개인정보 처리 단계별 위반 유형

개인정보의 처리 위탁

- 개인정보 처리 위탁에 따른 문서체결 누락, 개인정보 처리 수탁자에 대한 공개 누락, 수탁사에 대한 관리감독과 수탁사 직원 교육 미 실시

구분	업무위탁	제3자 제공
법 조항	제26조	제17조
예시	배송업무, TM, 콜센터	사업제휴, 공무수행
개인정보 이전 목적	위탁자의 업무 처리	이전 받는 자의 업무 처리
개인정보 이전 방법	개인정보처리업무 위탁 문서의 체결 및 수탁자의 공개	정보주체의 동의, 법령상 근거 등
관리 감독 책임	위탁자 책임	제공받는 자 책임
손해배상 책임	위탁자 부담	제공받는 자 부담

3. 개인정보보호법 위반 사례

2012년 부터 2013년 까지 700여개 공공 및 민간 대상 실태 검사 실시

위반사항 : CCTV 관련, 개인정보처리시스템의 안전성 확보 미흡, 위탁관리 절차 미준수

실태검사 결과 행정처분 약 600여건 : 과태료(20%), 시정조치(50%), 개선권고(30%)

조사 및 점검

-기획 점검 : 취약 분야, 위험 업종 대상 중심 실시, 제도개선 병행 (정기)

-특별 점검 : 침해사고, 유출 신고 등 사고 원인조사 및 책임 규명 (수시)

<개인정보보호 합동점검단>



현황 조사분석

- 업종별 개인정보처리현황
- 개인정보관리실태
- 개인정보 제공/활용현황

▶ KISA, NIA, 리서치 등



모니터링

- 개인정보 유/노출현황
- 온라인 점검 (취약점 분석)

▶ 관계부처/기관 연계



침해사고, 민원

- 개인정보 침해신고, 민원
- 분쟁조정 신청
- 사고 발생 언론 보도 등

▶ 경찰, KISA 등





3. 개인정보보호법 위반 사례

A의회

- 지방자치법 제73조와 청원법 제6조에서 청원을 위해 수집하는 개인정보를 성명, 주소로 정하고 있으나 청원인의 주민번호, 이메일 주소를 수집

B구청

- 업무용PC에 주민등록번호가 포함된 구청장 지시사항 처리내역 문서를 보관 하면서 저장된 파일에 대한 암호화 조치를 적용하지 않음

C부처

- 홈페이지 회원가입시 전송되는 주민번호와 비밀번호의 암호화 미조치
- 개인정보처리시스템에 대한 권한부여 이력 및 접속기록 미관리

D시청

- CCTV운영 안내판 중 관리자의 연락처 미기재
- CCTV운영에 관한 관리방침을 홈페이지에 미고지

E재단

- 기관 행사운영 업무에 대한 개인정보처리 수탁사와 문서 미체결
- 약 50여개 개인정보 처리 수탁사 중 10개 업체를 홈페이지에 미공개

F협회

- 개인정보 취급자에 대한 정기적인 교육 및 실태조사 미실시
- 타기관에 이전된 사업과 관련된 개인정보를 업무용 PC에 보관



3. 개인정보보호법 위반 사례

A의회

- 법령 또는 불가피한 경우를 제외한 개인정보 수집은 정보주체의 동의를 받아야 하며, 14년 8월 7일 부터는 법령에 근거 없는 주민번호 수집은 금지

B구청

- 업무용 PC에 고유식별정보를 저장할 때에는 암호화 조치를 적용해서 저장해야 하며, 수집 목적을 달성했거나 보유기간이 종료한 개인정보는 파기

C부처

- 고유식별정보, 비밀번호, 바이오정보를 전송할 때에는 암호화 조치 필요
- 개인정보처리시스템에 대한 권한관리는 3년, 시스템 접속기록은 6개월 보관

D시청

- CCTV 안내판에 설치목적과 장소, 촬영범위와 시간, 책임자와 연락처를 기재
- CCTV운영에 관한 관리방침을 수립하고 홈페이지에 게시

E재단

- 개인정보 처리 업무 위탁시 법 제26조에 따른 필수 문서 체결
- 업무별 개인정보 처리 위탁자를 정기적으로 조사하여 홈페이지에 공개

F협회

- 개인정보 취급자에 대한 정기적인 교육과 자체점검 등 관리감독 실시
- 수집목적과 보유기간이 달성된 개인정보의 파기 및 기관 양도양수 절차 준용

감사합니다.

