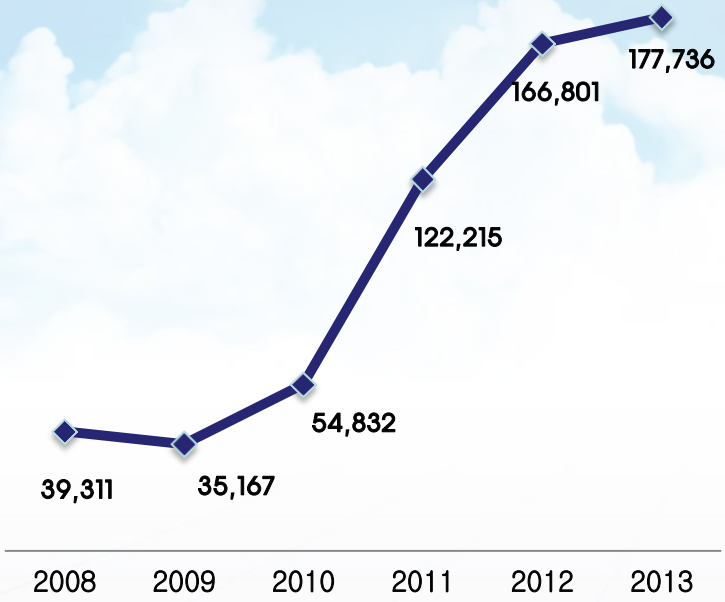
개인정보 침해 및 위반 사례

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(네이트등)	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	의사협회등22개	1,700만 건	해킹
14. 3	KT	982만 건	해킹
14. 3	통신 3사 등	1,230만 건	해킹(추정)

2. 개인정보 처리 단계별 위반 유형

개인정보의 생명주기와 침해/유출 위험

2. 개인정보 처리 단계별 위반 유형

개인정보의 수집 경로와 불법 사용 유형

홍보, 마케팅 활용

개인 신상조회, 감시

금전의 갈취

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

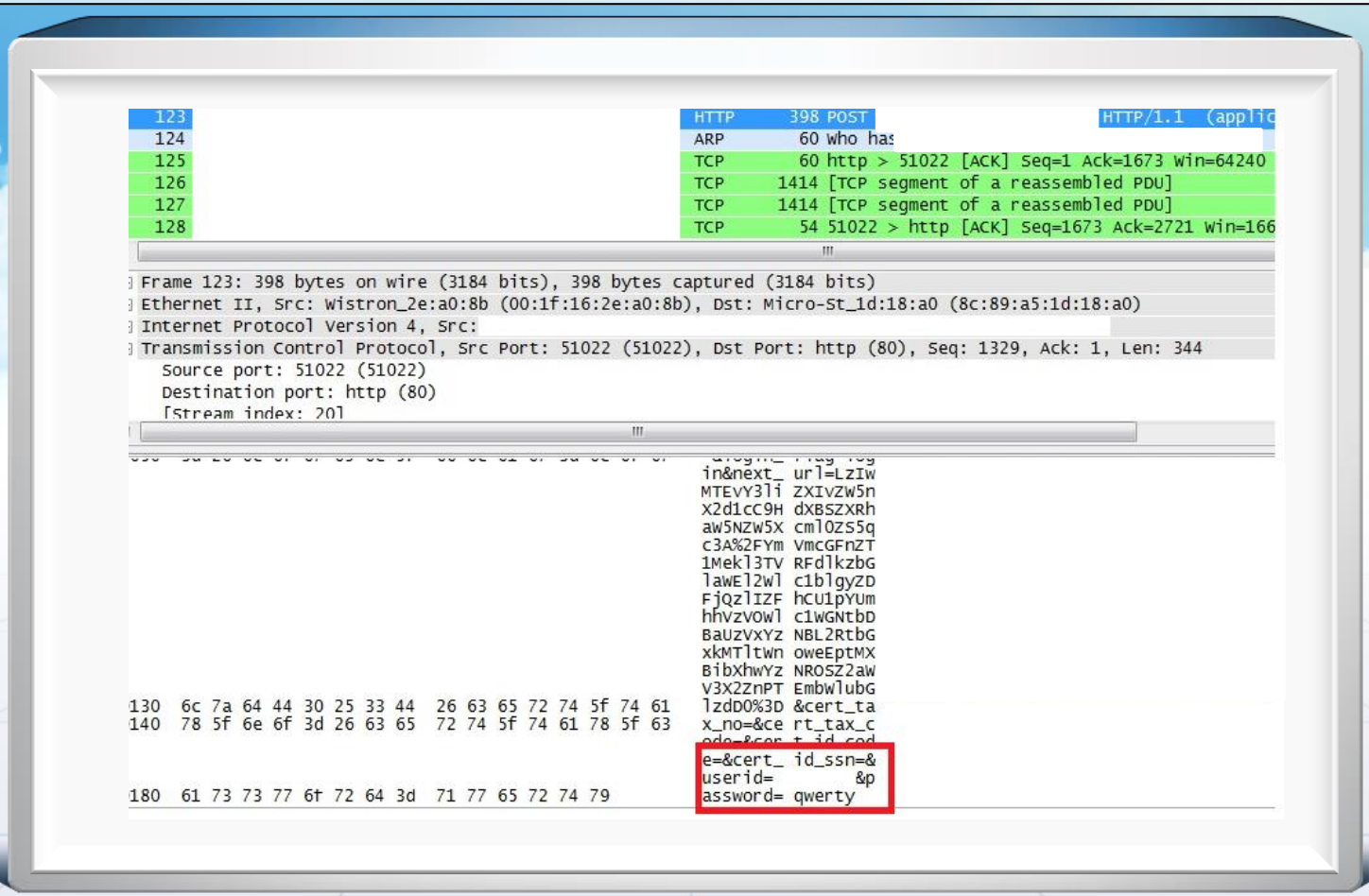
안전한 암호 기준

- 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



2. 개인정보 처리 단계별 위반 유형

개인정보의 전송, 저장

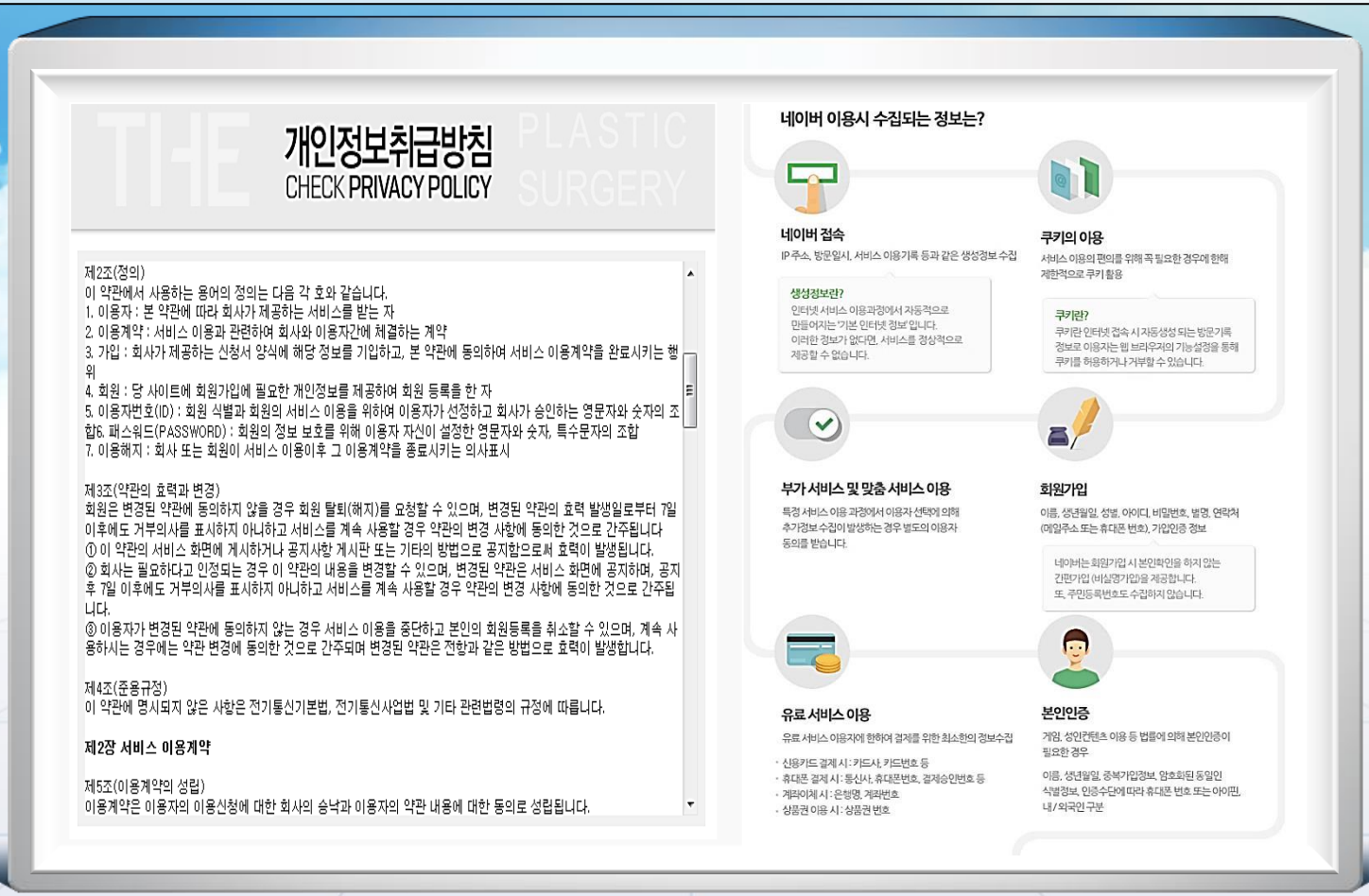
- 고유식별정보 / 비밀번호 / 바이오 정보의 암호화 미적용, 접근권한 관리 미흡, 접속기록 누락, 외부망의 시스템 접근시 전용선 또는 VPN 미적용, 안전한 비밀번호 미적용

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



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 미실시

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%)

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 보관하면서 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 수탁자를 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.