

개인정보보호 실태 진단 및 정책 소개

2013년 3월



안전행정부

Contents

I. 현황

II. 법 시행개요 및 성과

III. '12년 수준진단 및 개선사항

IV. 향후 계획



MINISTRY OF
SECURITY AND
PUBLIC ADMINISTRATION

I. 현황



“불편한 진실”, 4가지 !

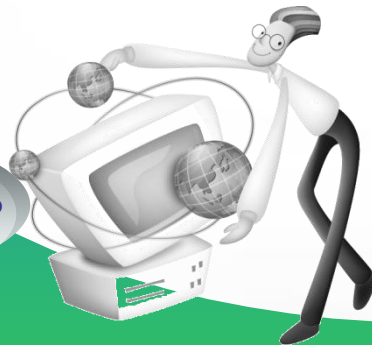


1. 기본적 인식



2. 돌다리, 두드리기만

3. 외양간.언제 고치나?



4. 치명적 손실



“불편한 진실”, 4가지 !

1. 활용 vs. 보호

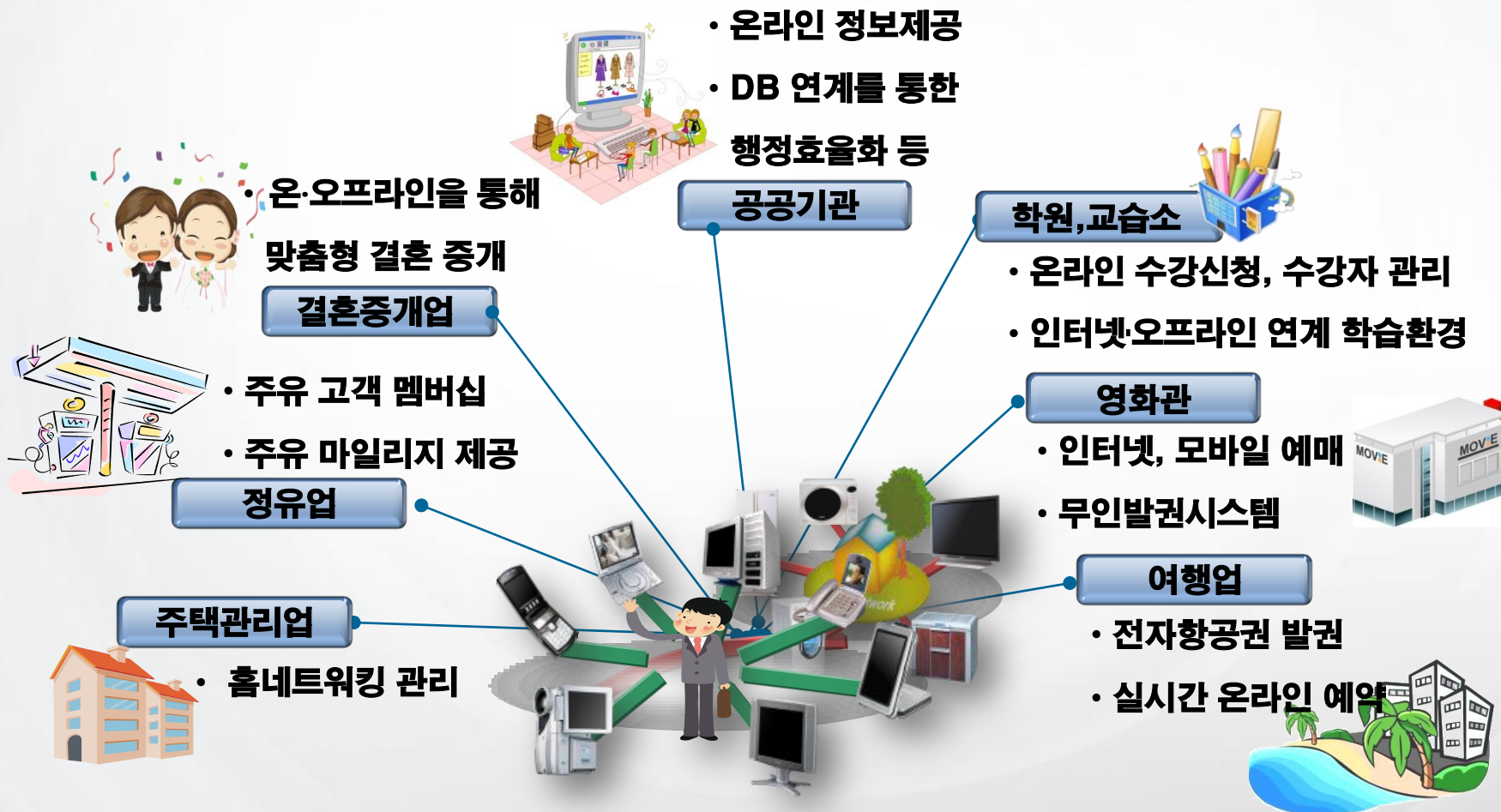
- 개인정보 : 개인을 식별할 수 있는 일체의 정보 (성명, 주민번호, 전화번호, 영상 등)
- 개인정보보호(Privacy) : 혼자 있을 권리 (소극적) → 자기정보결정권 (적극적)



“불편한 진실”, 4가지 !

1. 활용 vs. 보호

● 개인정보 활용 증대 : 정보기술과 결합하여 공공, 민간 서비스 확대



“불편한 진실”, 4가지 !

▶ “개인정보보호”, 기본적인 책무 (Going Concern, Trust Issue)

- 기관 운영의 기반인 동시에 안전한 관리/보호 대상 -

기관/기업
(개인정보처리자)
(약 350만개)



지금, 우리는 ?

국민/이용자
(정보주체)
(약 5,000만명)



“불편한 진실”, 4가지 !

2. 돌다리, 두드리기만 한다.

기관/기업 실태조사 결과 ('12. 12월 기준)

- 법 인지도 : 75.5%, 동의절차, 법적 필수조치사항 인지도 : 71.4%

→ 전담 인력/조직 : 10.9%, 보안 투자 : 26.1% (투자 전무 : 73.3%)



“불편한 진실”, 4가지 !

2. 돌다리, 두드리기만 한다.

☞ 규제 / 처벌 강화, 그 악순환

감지된 편익

넓게 분산

Majoritarian Politics

좁게 집중

Client Politics

- 경제적 규제 (죄수의 딜레마)
- 규제 지속 강화 → 부담 증가

넓게 분산

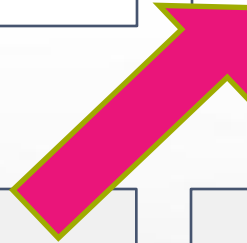
감지된 비용

Entrepreneurial Politics

- 사회적 규제 (엄격, 절차규정)
- 위기, 재난, 사회적 책임

좁게 집중

Interest-group Politics



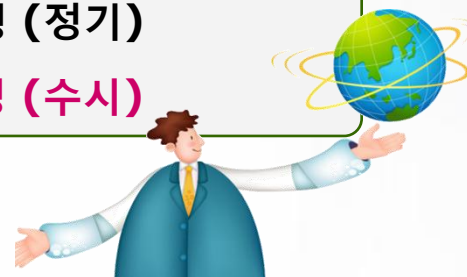
"불편한 진실", 4가지 !

3. 소 잃고도 외양간 안 고친다.

☞ '12년 실태점검/처벌사례 : 총 47회 756개소 점검, 과태료 57건, 시정조치 360건 등

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, 러서치 등



모니터링

- 개인정보 유/노출현황
- 온라인 점검
(원격 진단/취약점 분석)

▶ 관계부처/기관 연계



침해사고, 민원

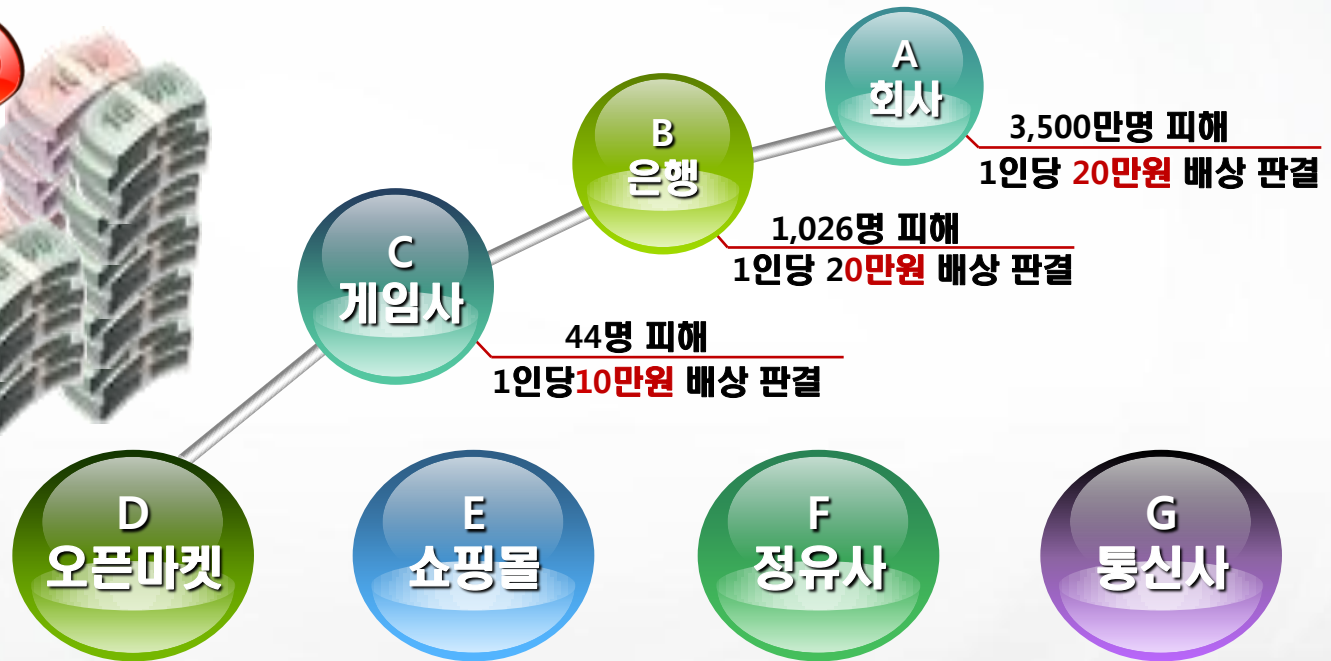
- 개인정보 침해신고, 민원
- 분쟁조정 신청
- 사고 발생, 언론 보도 등

▶ 경찰, KISA 등

"불편한 진실", 4가지 !

4. 치명적인 손해

☞ 개인정보 유출 피해자 : 집단 분쟁, 집단 소송 제기



유출 피해자

1,800만 명

2,000만 명

1,125만 명

600백만 명

배상금액

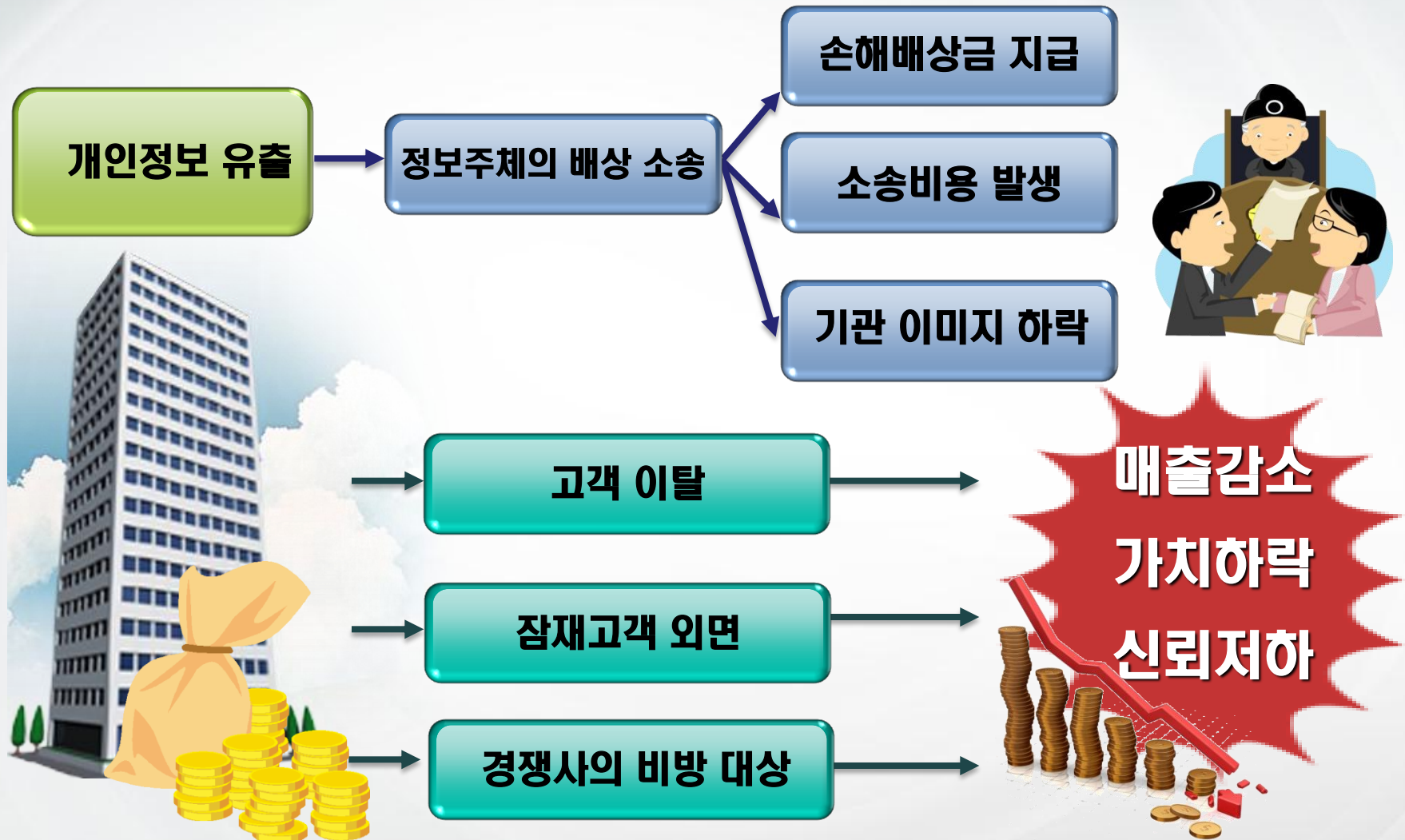
1차 판결 항소

소송 진행중

소송 진행중

소송 진행중

개인정보 침해로 인한 피해

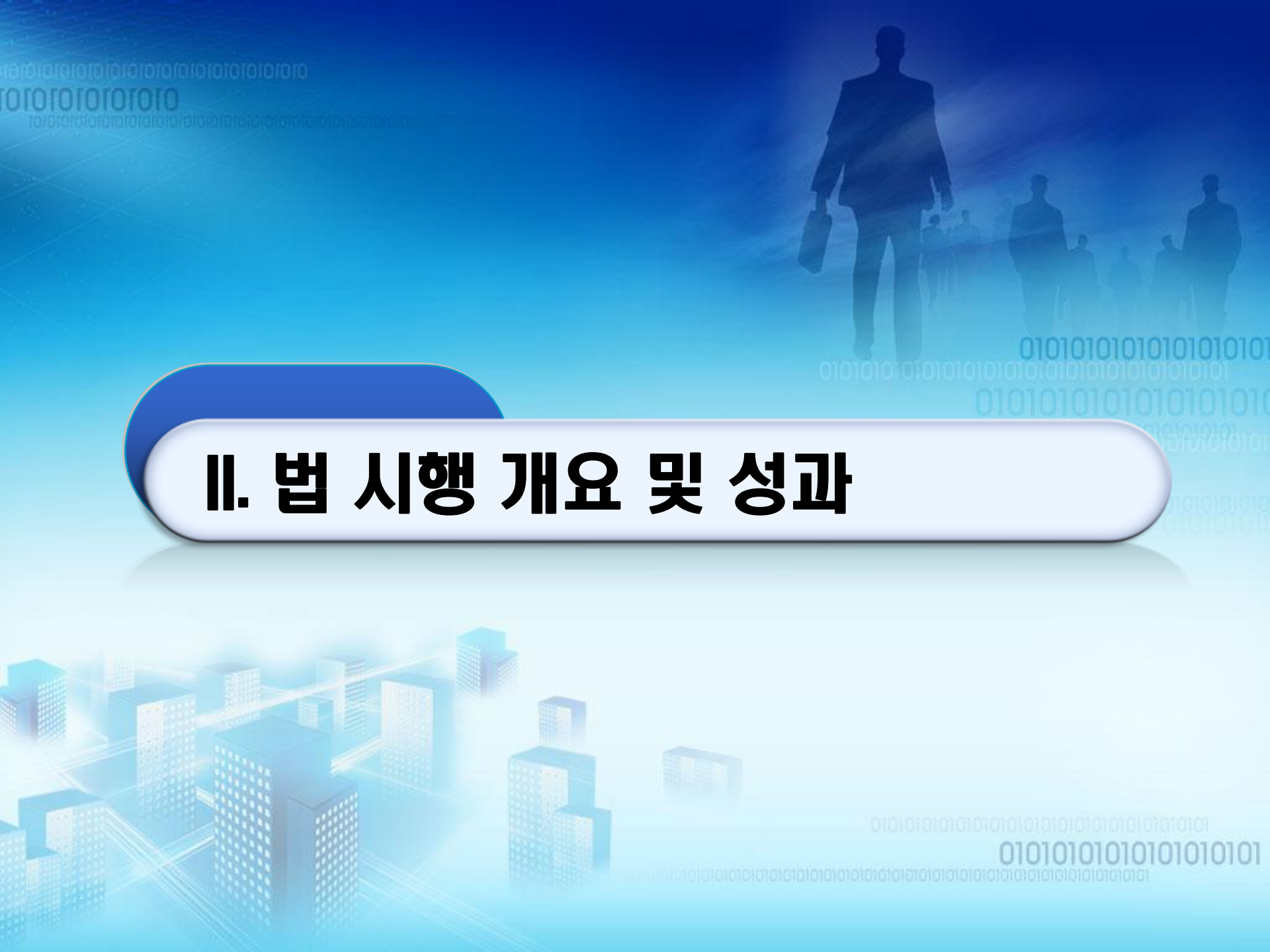


"불편한 진실", 4가지 !

4. 치명적인 손해

SK 컴즈 사례 분석 : "Multiple Principle"

구분	서울중앙지법	서울서부지법
접근통제 (법 제28조제2호, 고시 제3조)	<u>o 접근통제 보호조치 준수</u> -개인정보 대량유출 실시간 모니터링 조치는 접근통제 보호조치에 불포함 -SK컴즈는 F/W, IDS를 운영하고 있고, 해킹방지기술 한계 등을 고려할 때 유출징후 감지실패는 법 위반 아님	<u>o 접근통제 보호조치 위반</u> -침입탐지시스템(DLP솔루션 포함)의 경고발생 기준이 지나치게 완화되어 설정 ※ 10G 용량의 개인정보 text 파일이 새벽에 FTP 원격접속으로 외부 전송되는 것을 미탐지 - DB 원격접속시 자동로그아웃시간 및 접속가능최대시간 미설정
암호화 (법 제28조제4호, 고시 제6조)	<u>o 암호화 보호조치 준수</u> -비밀번호 일방향 암호화 등 이행	<u>o 암호화 보호조치 위반</u> -비밀번호 일방향 암호화시 보안 강도가 낮아 권고되지 않는 알고리즘(MD5) 사용
공개용 알집 프로그램 사용	<u>o 개인정보 유출과 인과관계 없음</u> -해커가 공개용 알집 파일과 동일한 명칭의 악성코드 (ALAD.dll)를 생성하고 알집 업데이트서버를 이용해 SK 컴즈 직원 PC에 악성코드를 심었으나, 공개용 알집 자체에 악성코드가 포함된 것은 아님	<u>o 개인정보 유출과 인과관계 있음</u> -악성코드(ALAD.dll)는 기업용 알집에서 발견된 바 없고, 공개용 알집은 알집서버와 상호통신이 이루어 지는 등 보안상 취약점 큼
기타	o (FTP 관련 쟁점 없음) o 최소수집, 주민번호 수집금지, 망분리 위반 등은 불인정	o FTP를 gateway 및 PC에서 미제거

The background features a blue gradient with silhouettes of people walking in the upper right and a cityscape with glowing lines in the lower left. Binary code (0s and 1s) is scattered throughout the background.

II. 법 시행 개요 및 성과

1. 개인정보보호법 제정 및 시행 ('11. 9~)

모든 개인정보처리자를 규율하는 **일반법**

- 그동안 공공기관의 개인정보보호법, 정보통신망법 등 개별법 체계
→ 법 제정 이후 공공기관, 사업자, 비영리단체 등 모든 개인정보처리자 규율

개인정보 처리에 대한 **기본원칙 정립**

- 세계 각국과의 FTA체결로 상호간 개인정보 교류 증대가 예상되며,
전 세계적 국제통상 관련 프라이버시 라운드(Privacy Round) 대두
→ 수집단계, 이용·제공 단계, 폐기단계 등 처리단계별 준수사항 명시

정보주체의 **권리 및 피해구제** 강화

- 정보주체의 개인정보의 열람·정정·삭제·처리정지 요청권 보장
- 개인정보유출통지, 집단분쟁조정, 단체소송 등 피해구제 강화

<참고 1> 국가별 개인정보보호법제

미국

- 프라이버시법(Federal Privacy Act, 1974)
 - 공공부문 규율, 민간부문 자율 통제
- [오바마 정부] 프라이버시와 국가보안의 IT 보안정책
 - CTO(국가최고기술책임관) 신설 및 개인정보보호정책 강화

EU

- 각국은 EU 개인정보보호지침에 따라 일반법 제정·시행 중
 - '전자통신프라이버시 지침에 유출통지 의무화('02) 및 SNS, 온라인 광고 규제에 따라 EU지침 개정 공식화('10.2월)

→13. 1, 개인정보보호 패키지 개혁안 추진 (Regulation 신설 / 엄격화)

일본

- 개인정보보호법 제정·시행 (2005)
 - 고객 개인정보보호 관심 증대에 따른 보호조치 강화
 - 개인정보보호 관련 법제, 인적·기술적 기반의 정비 및 대응강화
 - 개인정보보호 예산의 확충 및 대응체계 강화

네덜란드

- 개인정보보호법 제정 및 시행(2001)
 - 정보등록법(1998)의 정보처리행위에 대한 신고·등록범위 확장
 - 민간·공공, 온·오프라인의 개인정보처리 규율
 - 정보처리의 적절성 확보 및 실질적인 조사·감독 수행

2. 개인정보보호법 주요 내용

수집이용 및 제공 제한

- 정보주체 동의 원칙 (예외 : 법령, 급박 등)
 - 민감/고유식별번호, 별도 동의방식
- 명확한 고지 (항목/방식 구체적 명시)
 - 선택정보 미동의 가능, 별도 고지
- 필요 최소성, 목적 명확성 원칙

저장 관리시 의무사항

- 관리/기술/물리적 안전성 확보조치
 - 개인정보처리방침, 책임자 지정 등
- 처리 위탁 및 양도시 제한사항
 - 별도 문서조치, 관리감독 및 공개 등
- 개인정보 파기조치 (영향평가 등)

**개인정보보호
이제는 실천 !!**

- CCTV 설치목적 제한
 - 안내판 설치, 임의조작 및 녹음 금지
- 개인영상물 안전관리 및 제공 제한
 - 보호조치, 목적외 이용/제공 금지 (예외)

CCTV 설치운영 제한

- 개인정보 열람, 정정삭제, 처리정지 요구
- 유출 통지 (5일 이내) 및 신고제 (1만명 이상)
- 집단분쟁조정 및 단체소송

권리구제 및 보장

3. '12년 주요정책 성과

법 시행 후속조치

☞ 관계법령 일괄 정비

- 개별법령에 주민번호 및 민감정보 수집근거 마련

※ 27개 부처 229개 대통령령 개정

☞ 개인정보보호 가이드라인 마련·배포

※ CCTV(3월), 인사·노무(7월), 쇼핑 및 배송(8월), 소상공인 보호조치(8월), 학원·교습소(9월), 의료(9월), 암호화 조치(10월)

범 정부 대책 마련·추진

☞ 「주민번호 수집·이용 최소화 종합대책」 마련

- 행안부·방통위·금융위 합동, 국가 정책 조정회의 보고

☞ 주민번호 수집 서식 개정

- 주민번호 삭제 또는 주민번호를 생년월일로 대체

※ 민원행정서식 848건 개선, 민간서식 163종 발굴

침해 예방 및 실태검사

☞ 홈페이지 개인정보노출 사전 모니터링(10만개 사이트)

☞ 취약분야 집중점검 및 행정처분 실시

- 은행·보험·택배·CCTV등

☞ 개인정보보호 합동점검단 구성 및 운영

- 경찰·금융위·방통위·교과부·복지부등 14명
- 합동점검·예방관제·기술지원

3. '12년 주요정책 성과

체계적 교육·홍보

☞ 순회교육 및 대국민 계도

- 공공민간 교육(21회), 컨퍼런스
- TV 공익광고, 극장광고 등 홍보활동

☞ 「개인정보보호 범국민운동본부」출범·운영

※ 민간단체, 전문기관, 학회 등으로 이루어진
민간자율규제기구

- 「대학생 개인정보보호지원단」운영
- 추석맞이 소비자 개인정보보호 캠페인

취약분야 현장 지원

☞ 지역현장방문단 운영

- 전국(230개 시군구) 1만 3천개 사업자
대상 CCTV 안내판 설치 등 지원
- 전국 50개 주요지역 10,238개 사업자
방문, 개인정보 필수조치사항 안내

☞ 소상공인·중소사업자 지원

- 보안프로그램 지원
※ 백신 무상보급(4,487개), 보안솔루션 지원(617개)
- 진단 및 컨설팅
※ 웹 취약점 진단(518건), 컨설팅(425건)

<참고1> 대상별 정책대응

공공기관 (2만 5천개)

- 법적 의무 이행
- 기관자체 개선

- ① 권역별 순회 및 기관 자체 교육
- ② 기관별 자율 수준진단 실시(중앙 자자체, 지방공기업 등)
- ③ 교육, 의료 등 분야별 T/F 운영(지침 마련)

대·중견기업 (3만 5천개)

- 인식전환 및 교육
- 자율규제 및 개선

- ① 순회 교육 및 간담회
- ② 컨퍼런스 및 전문교육 지원
- ③ 법 위반사항에 대한 행정처분 및 시정개선

중소업체 · 소상공인 (317만개)

- 준 계도활동

- ① 유형별 맞춤형 지원 (ASP, 본점, 프랜차이즈 등)
- ② 현장 방문지원단 운영 및 컨설팅(시·군·구)
- ③ 대학생 개인정보 보호지원단 운영 및 지원

단체 · 협회 (27만개)

- 자율규제 및 개선

- ① 사업자 단체·협회 순회 교육 및 지원
- ② 범국민운동본부 운영 및 자율 규약(MOU)
- ③ 업종별 사례집 배포·자문

※ 일반 국민 : 파급력이 큰 매체 활용한 홍보·교육 (TV 공익광고, 극장광고, 포털 등)

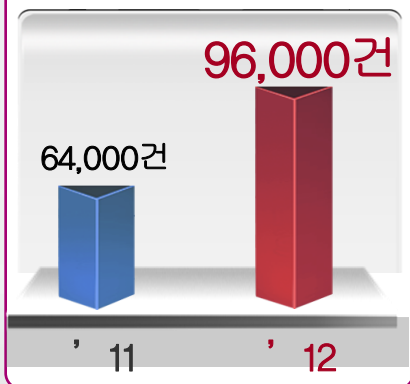
<참고2> 인식확산 및 개선 (2012년말 기준)

● 추진실적

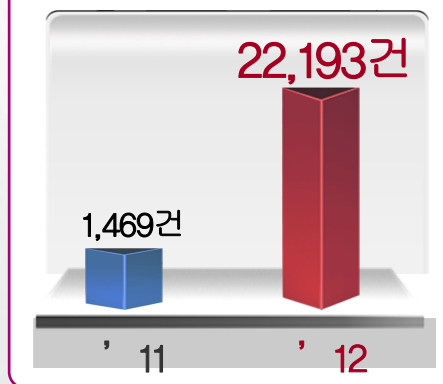
1. 교육이수 : 총 891,425명
 - (공공) 826,731명(전체 공무원의 91.9%)
 - (민간) 6,353명
 - (사이버) 58,341명
2. 간담회 및 컨퍼런스 개최
 - 간담회 : 61개 단체, 7회
 - 컨퍼런스 : 3회
3. 현장 컨설팅 및 사례집 발간
 - 27개 업종, 267개 사업자

● 주요성과

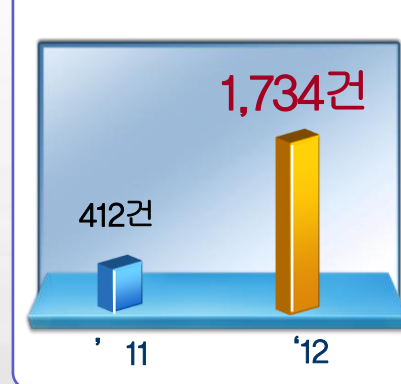
침해 상담신고



개인정보보호
자가진단



유권해석 질의



자율규제 MOU 체결



<참고3> 실태 개선 및 지원 (2012년말 기준)

추진실적

1. 기술지원센터 운영

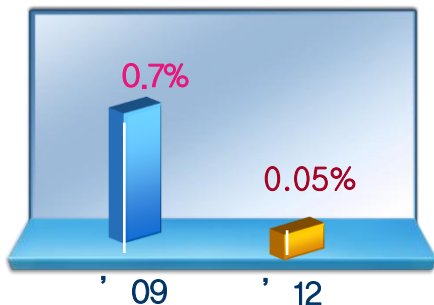
- PC백신 무상보급 : 4,478개
- 보안솔루션도입비용 지원 : 180개
- 기술상담 및 컨설팅 : 320건
- 취약점 점검 : 352건

2. 소상공인 현장방문 지원

- 229개 시군구
- 1만 3천개 사업자

주요성과

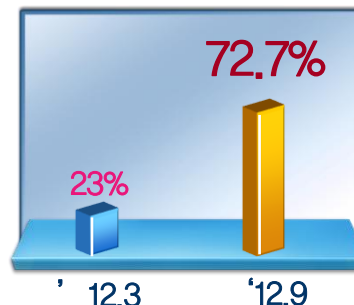
웹사이트 개인정보 노출건수



I-PIN 보급현황 (웹사이트)

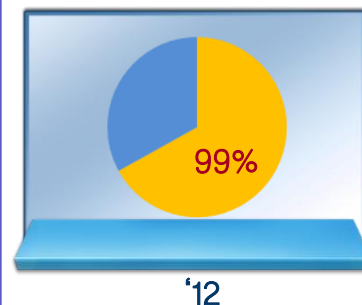


CCTV 안내판 설치

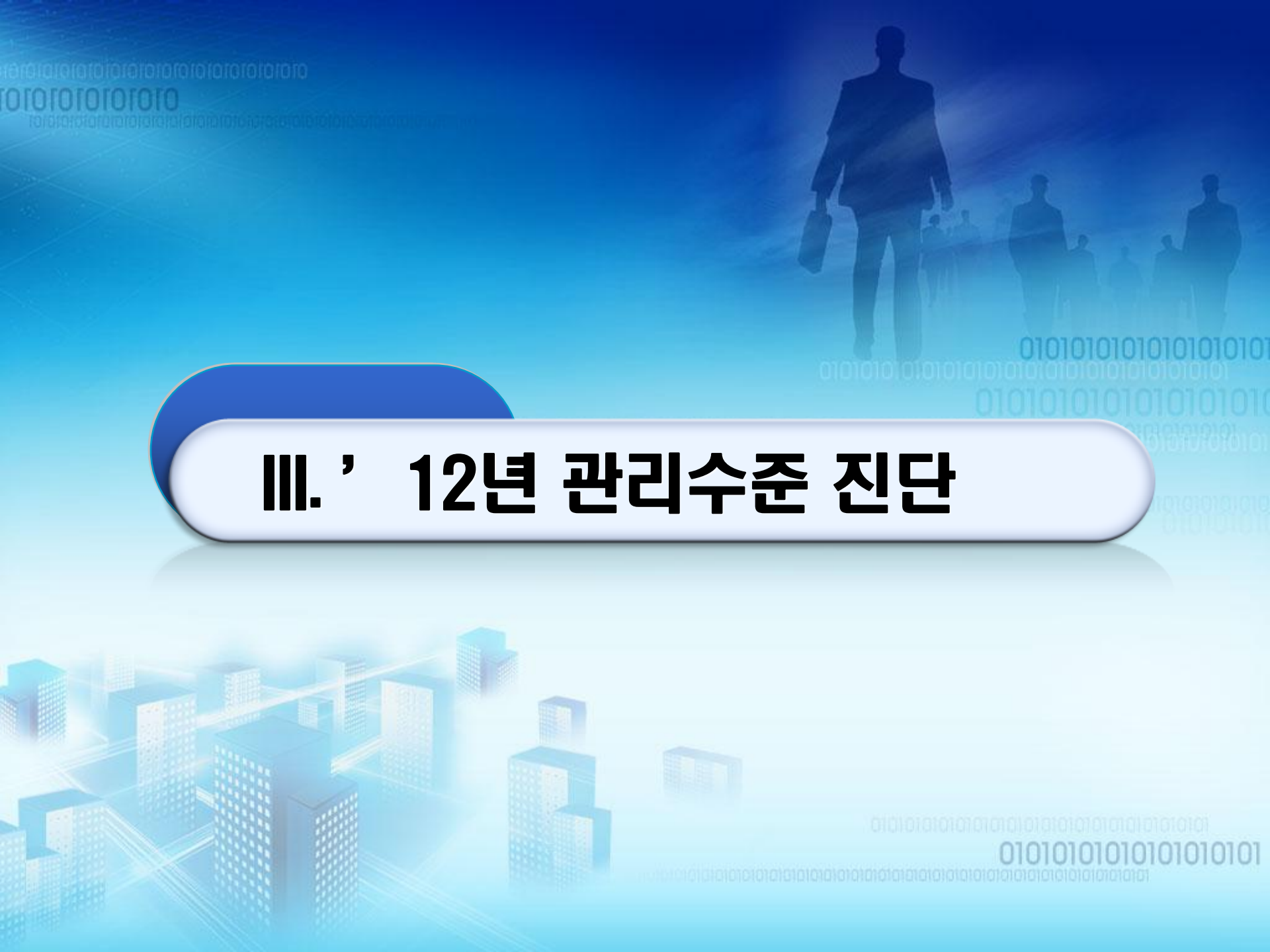


※ CCTV 설치대수 368만5천대

개인정보암호화 (중앙부처·지자체)



※ 7,630개

The background features a blue gradient with silhouettes of business professionals in the upper right and a stylized city skyline with glowing lines in the lower left. Binary code (0s and 1s) is scattered across the background.

Ⅲ. ' 12년 관리수준 진단

1. 수준 진단 개요

- 개인정보보호 관리체계, 보호대책, 침해대책 등 관리수준 진단 및 적극적인 개선 유도
 - '12년 진단대상 : 중앙부처(43), 지방자치단체(16), 지방공기업(129) 등 188개 기관
 - 조직·예산 등 관리체계 구축은 양호, 위탁 관리 및 시스템 접근기록 관리 등 침해예방·관리활동은 개선 필요

진단 절차 및 방법



2. 진단 결과 중점 개선필요사항

< 위탁 업무 관리 >

- 개인정보 처리업무를 위탁하는 경우, **처리에 관한 사항을 문서화 [계약서 등]**
- 수탁자(수탁업체) **교육 및 관리, 감독 강화**

위탁업무 문서화

위탁계약 목적

준 개인정보처리위탁 계약서(안)

OOO("갑"이라 한다)과 △△△("을"이라 한다)은 개인정보 처리업무를 "을"에 위탁함에 있어 다음과 같이 합의한다.

위탁업무 목적 및 범위

제1조 (목적) 이 계약은 "갑"이 △△△에게 개인정보처리업무를 위탁하고, △△△가 "을"은 이를

제2조 (용어의 정의) 본 계약에서 별도로 정의하지 않은 용어는 개인정보 보호법, 동

재위탁 제한

제3조 (위탁업무의 목적 및 범위) "을"은 계약이 정하는 바에 따라 () 목적

제4조 (재위탁 제한) ① "을"은 "갑"의 사전 동의 없이 제3자에게 위탁할 수 없다.

안전성 확보조치

[기술적,관리적 보호조치]

제5조 (개인정보의 안전성 확보조치) "을"은 "갑"의 개인정보를 안전하게 처리하기 위하여

제6조 (개인정보의 처리제한) ① "을"은 "갑"의 개인정보를 계약 종료 후에도 위탁업무

처리금지

제7조 (수탁자에 대한 관리·감독 등) ① "갑"은 "을"에 대한 관리·감독을 위하여 다음 각 호의 사항을 관리

제8조 (손해배상) ① "을" 또는 "을"의 하위 계약자(수탁자)가 "갑"의 개인정보를 계약에 의하여

본 계약에 따라 제공받은 개인정보를 오·남용하거나 유출·변조·훼손 등 다른 법령 또는

날인

손해배상

갑 을

OO시 OO구 OO동 OO번지 OO시 OO구 OO동 OO번지

성 명 : (인) 성 명 : (인)

- 표준 개인정보처리위탁 계약서(안)은 개인정보보호 종합지원 포털(privacy.go.kr)의 자료실에서 확인

수탁자 교육 및 관리,감독



- 개인정보가 분실, 도난, 유출, 변조 또는 훼손되지 않도록 정기적으로 수탁자를 교육



- 수탁자가 개인정보를 안전하게 처리하는지를 정기적으로 감독
 - 개인정보처리 현황 및 실태, 목적외 이용 및 제공, 재위탁 여부, 안전성 확보조치 여부 등

2. 진단 결과 중점 개선필요사항

< 개인정보처리시스템 관리 >

☞ 안전성 확보조치 및 관리를 위한 **접근권한 관리, 접속기록 정기점검 등 수행**

접근권한 및 접속기록

접근권한 관리

- 책임자 : 전체권한 부여
예) 읽기, 쓰기, 변경
- 취급자 : 업무 목적에 따라
최소한의 범위로 부여 예) 읽기

차등부여

- 전보, 퇴직 등 인사이동 시
해당 계정을 변경 및 말소

권한삭제

- 접근권한 부여, 변경, 말소에
대한 내역 기록 및 보관(3년)

이력관리



접속기록 관리

- 사용자별 수행한 명령기록
- 사용자의 접속상태
- 사용자들의 정보[로그인, 로그아웃, 재부팅] 등 점검
- 불법적인 접근방지를 위한 대책마련 등 후속조치 이행

정기점검, 후속조치

- 접속 ID, 날짜 및 시간, IP주소, 수행업무 등을 저장(6개월이상)
- 정기적으로 백업을 수행

기록관리

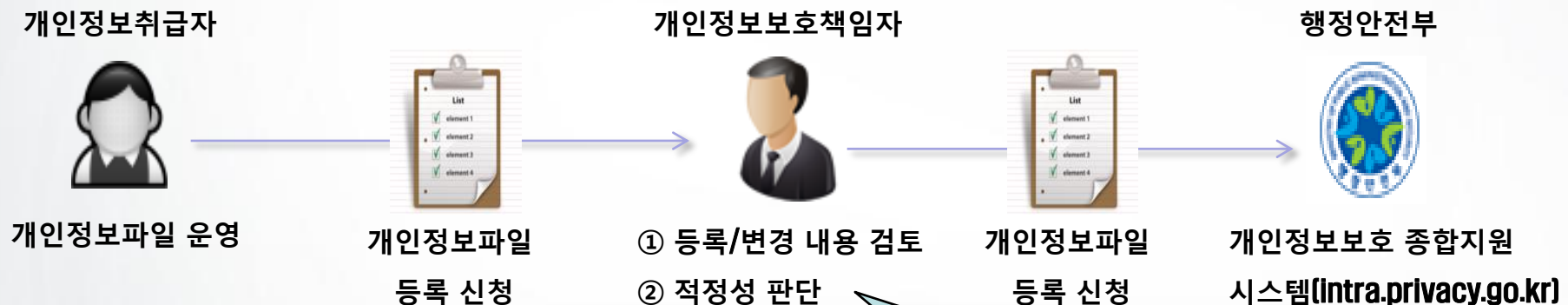
※ 개인정보 침해대응 절차(업무처리 및 대응, 피해구제, 비상연락망 등) 직원 전파 및 교육 강화

2. 진단 결과 중점 개선필요사항

< 개인정보파일 관리 >

- 개인정보파일을 운영하는 경우, **개인정보파일을 누락 없이 등록**
 - 기관별로 누락된 파일 추가 등록, 보유기간 등 등록항목 보완이 필요 **[즉시조치]**

개인정보파일 등록



[등록내용]

개인정보파일 명칭, 운영 근거 및 목적, 개인정보 항목, 처리방법, 보유기간, 정보주체의 수 등

* 주의사항 : 개인정보파일을 과다하게 운영하지 않으며, 누락되지 않도록 주의

보유기간은 보유목적에 부합된 최소기간으로 산정

- ① 개별 법령의 규정에 명시된 자료의 보존기간에 따라 산정
- ② 개인정보보호책임자의 협의를 거쳐 기관장의 결재를 통하여 산정

<참고> 12년 현장점검결과

● 총 47회 756개소 점검, 441개소 처분 (12.1 ~ 12)

처분완료	위반기관	과태료	시정조치	개선권고
441	364(100%)	36(9.9%)	144(39.6%)	215(59.1%)

- 기획점검 : 자료를 분석하여 침해 우려가 큰 업종으로 대상 선정, 취약점 위주 점검
- 특별점검 : 침해 신고 및 민원 접수, 언론 보도된 기관 등을 대상으로 점검

<업종별 위반기관 수 및 실태점검 시 위반비율>

구분	금융업	학원	협회/연맹	공공기관	운송업	의료업	기타	전체
점검기관	37	25	25	74	27	21	232	441
위반기관	33	20	17	49	17	11	217	364
위반비율	89.2%	80.0%	68.0%	66.2%	63.0%	52.4%	93.5%	82.5%

<참고> '12년 현장점검결과

▣ 법 조항별 위반사항

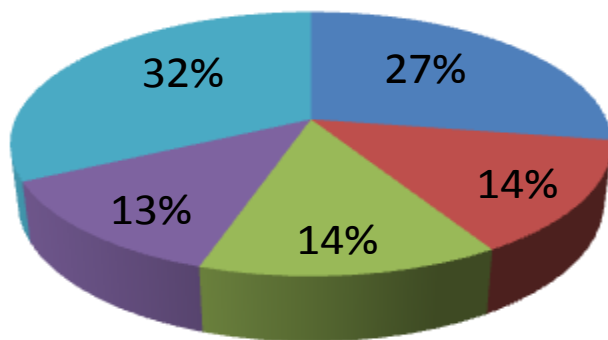
☞ 제25조 (영상정보처리기기) : 은행권 및 대중교통 시설의 CCTV 기획점검

제15조(개인정보 수집·이용제한) : 전 업종 공통 위반사항

제29조(안전조치의무) : 대부분 기술적 보호 조치 위반

제26조(업무위탁에 따른 제한) : 위탁행위, 관계에 대한 이해 부족

제30조(개인정보처리방침의 수립·공개) : 기초적, 경미한 사항 위반



- 제25조(영상정보처리기기의 설치·운영 제한)
- 제15조(개인정보의 수집·이용)
- 제29조(안전조치의무)
- 제30조(개인정보 처리방침의 수립 및 공개)
- 기타

3. 우수사례 - 위탁업무

- 위탁업무의 유형 및 특성에 따라 관리/감독 계획을 수립 [구미시설공단]
- 수탁자 대상 실태관리 점검표를 개발하여 매월 점검 [중소기업청]

관리/감독 계획 및 점검

문서번호		기획일시	
공제번호	2012. 12.	공제일자	공제
공제번호	2012. 12.	공제일자	공제

- 개인정보 관련 업무 효율화 및 안전한 보호를 위한 -
수탁업체 대상 관리·감독 계획

- 개인정보 관련 업무 효율화 및 안전한 보호를 위한 - 수탁업체 대상 관리·감독 계획

「개인정보보호법」 제26조에 의거하여, 업무 위탁 시 발생할 수 있는 개인정보의 유출 및 남용 등으로 인한 피해를 막고 정보주체의 개인정보를 안전하게 보호하기 위해 수탁업체를 대상으로 관리·감독 계획 수립

1. 추진방향

- 개인정보보호법에서 규정한 모든 계획에 충실함
- 사후적 소극적 관리·감독에 전 과정부터 개입하여 개인정보가 안전하게 관리·감독되는 방향 제시

2. 위탁 대상 업무

- 업무위탁 : 개인정보처리자가 제3자에게 위탁하는 경우 제3자에게 위탁하는 개인정보의 전부 또는 일부를 위탁하여 개인정보가 안전하게 관리·감독되는 방향 제시
- 위탁대상 : 업무위탁으로 생길 수 있는 개인정보 유출 및 남용 방지 대책 마련

- 기술적 보호조치
[6개분야 50개 점검항목]
- 관리적 보호조치
[10개분야 42개 점검항목]

- 위탁업무 형태, 수탁자 선정 시 고려사항, 위/수탁 계약 체결 시 주의사항, 수탁자에 대한 교육, 정기점검(목적 및 방법론) 등

기술적 보호조치		기관명	담당자 성명
구분명 (URL)			
측정지표	1. 개인정보보호 시스템	답변	
진단항목	(1) 키보드해킹방지솔루션, 백신프로그램 설치와 정기업데이트 여부		
세부사항	(1-1) 키보드해킹방지솔루션의 설치 여부		
	(1-2) 키 입력값 보호 외에 메모리 해킹 및 스크린 덤프 공격 등 타 악성 프로그램에 의한 정보유출 등을 차단하기 위한 기능(개인PC 방화벽, 해킹도구 진단 등)의 포함 여부		
	(1-3) 서버용 백신프로그램 설치와 정기업데이트 여부(서버용 백신 사용 시 윈도우 계열의 OS를 사용하는 경우만 기입)		
	(1-4) 개인PC의 백신프로그램 설치와 정기업데이트 여부		
측정지표	2. 개인정보보호 시스템	답변	
진단항목	(2) 침입차단시스템과 침입탐지시스템 설치 여부		
	(2-1) 침입차단시스템 설치 여부		

개인정보 처리에 관한 사항을 문서화 및 수탁자 교육 및 관리, 감독

3. 우수사례 – 개인정보보호책임자 역할 수행

- 개인정보보호책임자가 관리실태 자체점검 계획을 수립하여 점검을 실시하고 부서별 미흡사항에 대한 개선 조치를 점검 (울산광역시 도시공사)

자체점검 및 개선조치

문서번호	기획조정실-1511
등록일자	2012.06.13.
결재일자	2012.06.13.
공개구분	공개

★과장	기획조정실장	사장
■	■	06/13
업소	사업개발담당	■
	재무회계담당	■
	사업추진담당	■
	보상담당	■
	마케팅담당	■

2012년 상반기 개인정보관리실태 자체점검 계획

■ 점검반

구 분		직 위	성 명
점검확인자	정보보안책임관	사 장	■
점검감독자	개인정보보호책임자	기획조정실장	■
점검담당자	개인정보보호담당자	과 장	■

■ 부서별 점검결과

부서명	점검항목	점검결과(미흡사항)	개선조치사항
기획조정실	대장관리	·개인정보목적외제공대상 미기록 (2012년 고객만족도 조사 명부)	개인정보를 목적외로 타기관 등에 제공시 관련 법정서식에 기록관리 조치
	개인정보 수집	·자녀보육수당신청서에 불필요한 개인정보가 포함	·관련서식 변경조치 (예 : 주민등록번호를 생년월일로 대체)
	개인정보 제공	·개인정보를 타기관 등 제3자에 제공 시 안전성 확보조치가 부분적으로 미흡	·타기관 등 제공 시 반드시 공문으로 처리하여야 하며 제공받는자에게 안전성 확보조치를 위한 문구 추가 조치
	VOC 홈페이지 관리	·VOC홈페이지 공개 민원내용에 개인정보가 포함 될 수 있음	·VOC 관리자는 민원내용을 상시 모니터링 하여 개인정보가 노출되지 않도록 조치
사업개발단	개인정보 수집	·개발사업대상자 신청서 접수 시 개인정보 수집이용을 위한 동의서 미확립	·주민등록번호 등 고유식별번호 수집이용 시 정보주체의 동의를 받아야 하므로 개인정보 수집이용 동의서를 작성하여 확립 조치

개인정보보호책임자를 지정하고 책임, 권한, 역할 등 정의 및 이행

3. 우수사례 - 수집 및 이용 최소화

- 소관법령개정 수요조사를 통해 수집서식 개선 등 적극 수행 [지식경제부]
- 병적번호 사용 등 주민번호 사용 최소화 노력 이행 [병무청]
- 주민번호 보유근거가 없는 민원업무를 파악하여 시스템 개선 [광주광역시]

법률 개정

□ 주요 조치 내용

- 소관 법령 123개 중 2011. 7~9월까지 3차에 걸친 법령개정수요 조사를 통해 민원서식 변경 및 개인정보 수집 근거 마련(붙임1)
- 홈페이지 회원가입 시 주민번호 대체수단 제공 완료(붙임2)
- 소속·산하기관
- 유관기관 개
- 개인PC 내 개
- 부내 직원용
- 개인정보보호자
- 적법한 개인정보 수집·이용 방안 마련
- 부서별 개인정보 보유 목적, 근거, 범위(최소한의 정보수집) 등

• 시행령(3) - 고유식별정보 수집 등 근거 마련

• 시행규칙(15) - 서식변경 [생년월일]

관리체계 개선

○ 업무처리 시 주민번호를 중심으로 자료를 추출하는 불편성을 탈피,

■청 특유의 ■번호에 의한 자원관리 체계 정착

- ■번호 관리체계로 데이터베이스 변환 건수 : 총 1,778,362,000건
- 변환 테이블 수 : 880종
- 데이터베이스 구조 변경에 따른 관련 프로그램 수정 : 1,625종

※ ■번호 구성체계

편입청(2자리)	생년월(4자리)	세기(1자리)	일련번호 (6자리)
0 2	7 5 0 5	0	0 0 0 0 0 1

• 주민번호 대신 00번호 관리체계 구축(업무화면 및 명부에서 주민번호 사용금지)

시스템 개선

□ 보유현황 분석

- 전체 313종 민원 중에 263종에서 개인정보 보유 (붙임1_2 참고)
- 법령상 개인정보 보유근거 민원은 258종
 - 민원별 개별법(시행규칙 별지 서식)에 보유근거가 있는 민원 197종
 - 지방세기본법, 질서행위규제법에 보유근거가 있는 민원 61종
- 법령상 개인정보 보유근거가 없어 프로그램 개선대상 민원 5종

• 주민번호를 생년월일로 대체하도록 민원처리 시스템 개선

목적에 필요한 범위 내에서 최소한의 개인정보만을 수집 및 이용

3. 우수사례 - 개인정보파일 관리

- 파일별 보유기간 검토 · 산정 등 등록항목 적정성 유지 [대구도시철도공사]
- 본부 및 소속 · 산하기관의 파일까지 체계적으로 점검 · 관리 [행정안전부]
- * 외부전문가를 활용하여 개인정보파일, CCTV관리 현황을 점검하고 노출 모니터링 실시

등록내용 검토

제 목 : 개인정보파일 보유기간 산정 (안)

부대사업팀

문서번호	부대사업팀-1092	주 일	부대사업팀장	영 일 지 장	영 일 이 사	사 장
보유기간	문영구					07/08
결재일자	2011.07.08.					
승계여부	공개					

영 일 이 사
영 일 지 장

- 광고 · 임대 계약자 -
개인정보파일 보유기간 산정 (안)

□ 파일별 보유기간 산정

1. 계약자 신상정보 파일 보유기간

가. 계약완료 또는 해지시 채무관계 등이 완료된 후 10년 경과시 즉시 파기
⇒ **민법** 제162조(채권, 재산권의 소멸시효) ①채권은 10년간 행사하지 아니하면 소멸시효가 완성한다.

파일관리

개인정보파일을 운용하는 기관 명칭	부대사업팀
등록항목	
개인정보파일 명칭	- 역사기록관 방문자관리
개인정보파일 운영 근거	- 역사기록관출입및출입에관한규정 (역사기록관 훈령 제16호) - 정보주체자의 동의
개인정보파일 운영 목적	- 보안사고 및 테러
개인정보파일에 기록되는 개인정보 항목	- 필수항목 : 성명, 주소 - 선택항목 : 차광번호
개인정보 처리방법	- 전자적 방법을 이용 ※ 역사기록관 방문자관리 프로그램(CS)을 정문 PC에 설치하여 관리
개인정보 보유기간	- 보유기간 : 5년 - 보유근거 : 역사기록관출입및출입에관한규정(역사기록관 훈령 제16호)
개인정보를 통상적 또는 반복적으로 제공하는 경우	제공받는 자 해당 없음 근거 해당 없음 제공하는 경우 개인정보 범위 해당 없음
개인정보파일로 보유하고 있는 개인정보의 정보주체 수	- 13,110명 ('12. 8월 현재)

• 소속/산하기관의 개인정보파일을 직접 관리

• 파일 운영 및 보유기간 산정근거를 명확하게 기술

• 파일 보유현황 점검 및 최신현황 유지 [매월]

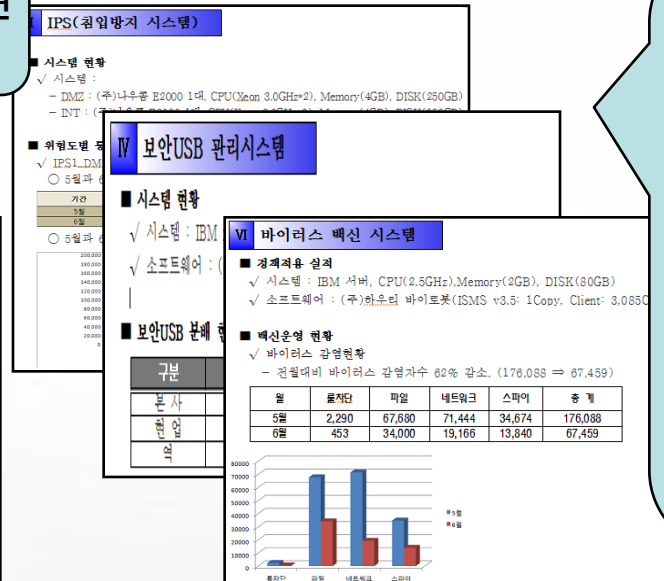
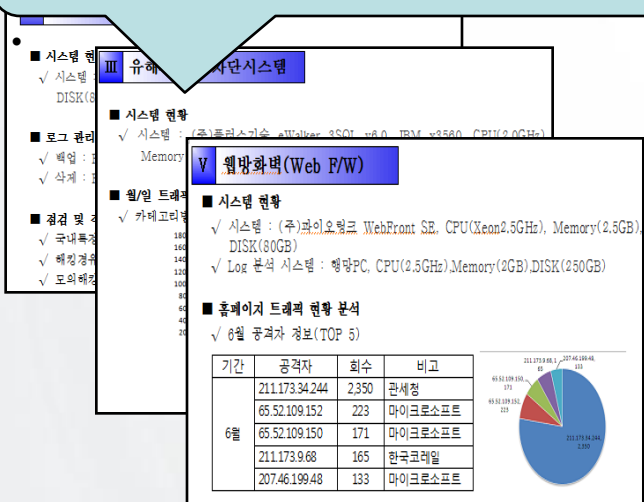
개인정보파일의 등록/변경 내용을 검토하고 적정성을 판단하여 누락없이 등록

3. 우수사례 - 노출방지 및 자율개선

- 개인정보보호 시스템을 구축하고 피싱사이트 차단, 침입차단, 노출 모니터링 등을 적극 수행 [서울시 도시철도공사]

시스템 운영 및 모니터링

- 피싱 사이트 차단
- 모의해킹 실시 후, 원인 분석 및 대응책 마련
- 패킷 분석 후 공격자의 IP강제 종료 처리 등



- PC 보안 : 바이러스백신
- 네트워크 보안 : 침입방지 시스템(IPS), 방화벽(F/W), 웹방화벽, 스팸메일 차단시스템
- 유출방지 : 보안 USB관리 시스템, 디지털콘텐츠권한관리(DRM), 개인정보필터링 시스템
- 서버보안 : SSL보안인증서, 서버접근제어툴, 서버취약점 진단툴 등

정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 **보안시스템 운영 및 모니터링 실시**

3. 우수사례 - 침해사고 대응절차

- 신속하고 체계적인 침해사고 대응을 위해 ‘개인정보 침해사고 대응지침서’ 마련 및 소속/산하기관, 전 직원에 배포 [보건복지부]

침해사고 대응지침

개인정보 침해사고 대응지침	
목 차	
1. 목적	1
2. 적용범위(대상)	2
3. 개인정보 침해유형	3
2012. 4. 개인정보 침해 업무처리 기본절차	4
5. 개인정보 침해신고	4
6. 사고대응 담당자별 업무	5
7. 부내 업무처리 프로세스	7
① 업무과실로 인한 개인정보 침해	7
② 과실로 인한 개인정보 유출	10
③ 개인정보 오·남용으로 인한 유출	13
④ 외부 침투에 의한 유출	17
8. 소속기관 및 산하 공공기관 업무처리 프로세스	20
① 업무과실로 인한 개인정보 침해	20
② 과실로 인한 개인정보 유출	23
③ 개인정보 오·남용으로 인한 유출	27
④ 외부 침투에 의한 유출	31
9. 피해구제 방법	34
10. 부서별 처리사항	36

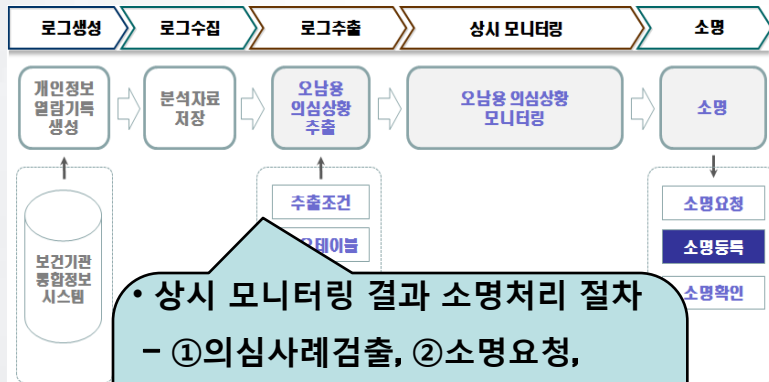
- 적용 범위 및 대상
- 개인정보 침해 업무처리 절차
- 침해 유형 및 신고
- 담당자별 업무
- 부내 업무처리 프로세스
- 소속/산하기관 업무처리 절차
- 피해구제 방법
- 부서별 처리사항 등

개인정보 유/노출 등 침해사고 발생에 대비하여 대응절차를 마련하고 교육 및 배포 등으로 신속하고 효율적으로 대응할 수 있는 체계 구축

3. 우수사례 - 접근기록 감사

- 개인정보 접근기록을 상시 모니터링하고 의심사항을 즉시 확인 [보건복지부]
- 접속기록 분석을 통해 불필요한 퇴사자 계정(13), 원격접속 계정(6) 등 삭제 [중소기업청]

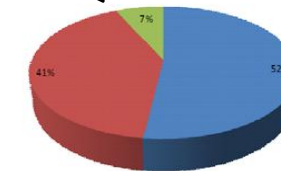
상시 모니터링



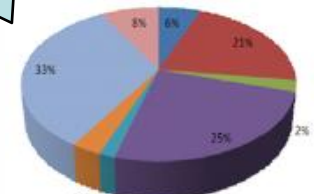
- 상시 모니터링 결과 소명처리 절차
 - ①의심사례검출, ②소명요청, ③소명등록, ④소명내용 심층분석, ⑤소명판정, ⑥문서시행, ⑦위반 의심자 조치, ⑧조치결과 확인

접속기록 분석

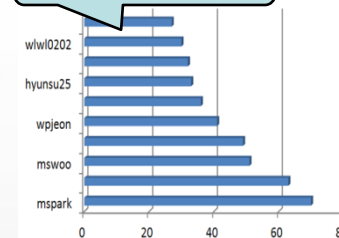
접근경로 분석



작업내용 분석



사용자별 접속 수



일평균 접속자 수

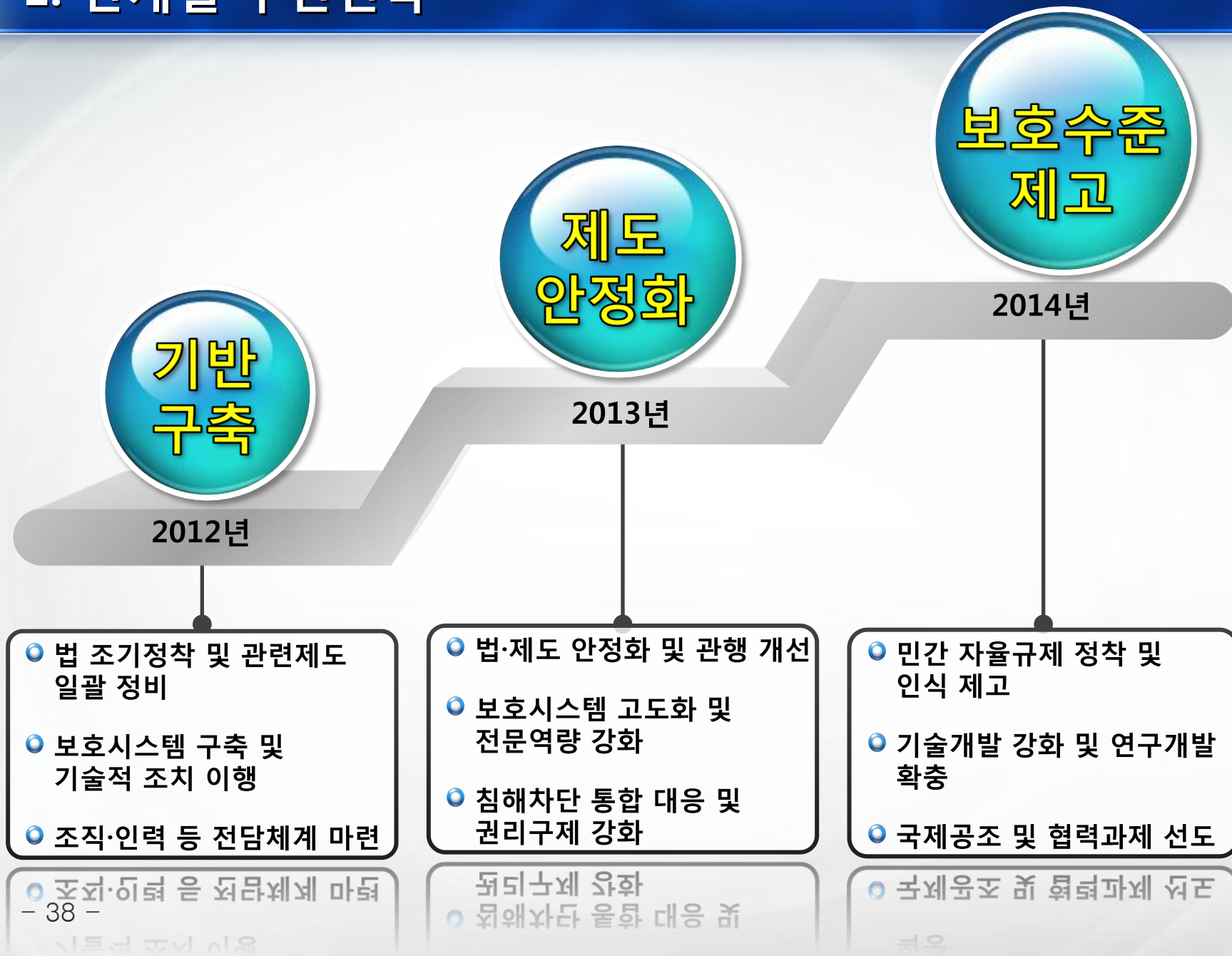


시스템에 대한 접속기록을 정기적으로 분석 및 기록하며 예상되는 취약점에 대한 개선과 후속 조치



IV. 향후 계획

1. 단계별 추진전략



2. '13년 주요 업무계획

민관 협업의 보호수준 향상

- **주요 업종 계약서/서식 일괄정비**
 - 과다, 불필요 수집 및 무단제공 관행 근절
- **인증 마크제 도입 추진**
 - 업종별 자율점검 및 개선 유도

법 제도 개선 및 보호 강화

- **개인정보보호법 개정**
 - 주민번호 수집 법정주의, 과징금 제도 신설
 - 유출기업 CEO 및 임원 징계 권고제 도입
- **빅데이터시대 개인정보보호대책 마련**
 - 데이터 공유/개방 및 보호조치 조화 등

**개인정보보호
이제는 실천 !!**

- **취약업종, 반복노출기관 점검 강화**
 - 민감정보 다량 보유 업종, 회원유치 과열업종
반복 다량 노출업종, 반복 민원/신고 발생업종
- **행정처분 확행 및 관계 기관 협력 강화**

합동 점검 및 실태개선

- **창업자 대상, 개인정보조치 지원 강화**
- **주민번호 대체수단 도입/전환 기술지원**
- **“지역거점 지원센터” 설치 및 운영**

기술지원 및 교육

<참고> 개인정보보호 합동점검단

□ 구성 및 주요 기능

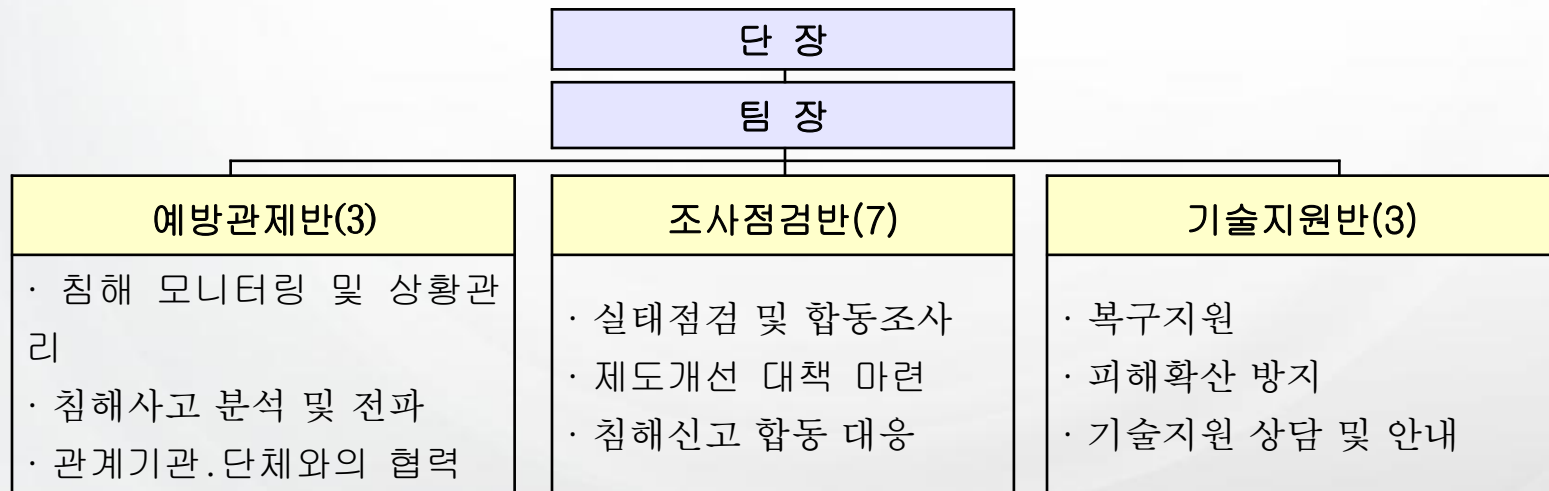
- 관계부처간 유기적인 협조를 통해 개인정보 침해사고에 효과적으로 대응하기 위한 「개인정보보호 합동점검단」을 구성·운영

근거 : 국무총리 훈령 제593호

구성 : 총 14명(행안부, 방통위, 경찰청, 금융위, 교과부, 복지부, 전문기관)

운영 : 행정안전부에 설치, 2012.11.8~2014.12.31까지 운영

기능 : 통신·금융·의료 등 주요분야 합동점검, 예방관제 및 기술지원



3. 역할과 자세 (개인정보보호, "1.0" → "3.0")

개인정보보호책임자

- 정책 수립 및 체계 정립
 - 보호계획/방침, 전담조직/투자
- 소양 및 관리역량 확보
 - 개인정보처리현황, 관리실태 이해
- 관리 감독 (Risk Mgt)
 - 내부통제시스템 및 정기감사

시스템운영관리자

- 기술적 보호조치 및 이행 관리
 - 접근권한/인적 보안, 접속기록 감사
- Communication 역량 강화
 - 보안투자, 개선조치사항
- 개인정보 생명주기별 관리/지원
 - 업무 + IT, 전사적 시계

Steering

Supporting

Compliance

개인정보취급자

- 인식 및 관행 변화
 - 업무처리절차/방식 개선, 교육
- 민원 처리 및 피해구제
 - Double/Cross Check, Reporting

4. 필수조치사항

〈 안전성 확보조치 〉

- 관리적 조치 : 내부관리 계획 수립, 접근 권한 관리 및 정기적인 관리감독 등 조치
- 기술적 조치 : 접근통제시스템 설치·운영, 고유식별정보/비밀번호 등 암호화, 접속기록 보관, 보안프로그램 설치·운영 등 조치
- 물리적 조치 : 안전한 보관시설 설치·운영, 잠금 장치 설치 등 조치

〈 수집시 고지사항 〉

- 개인정보수집·이용 목적, 수집항목, 보유·이용기간, 동의거부권, 불이익사항 등 필수사항 고지

〈 고유식별정보 수집 〉

- 고유식별정보(주민등록번호, 여권번호, 운전면허번호, 외국인등록번호) 수집/처리시 다른 개인정보 수집과는 별도 동의

〈 개인정보처리방침 수립 〉

- 개인정보처리방침 수립 시 처리 목적 및 보유기간, 제공 및 위탁, 권리·의무 및 그 행사방법, 처리하는 개인정보의 항목, 파기 등 법령상 내용을 누락 없이 모두 포함
- 개인정보 처리 위탁이 있을 경우 위탁 내용, 수탁업체명과 연락처 등을 포함

4. 필수조치사항

< 개인정보 처리 위탁 >

- 위탁하는 업무의 내용과 수탁자를 개인정보처리방침 등을 통해 공개
- 개인정보 위탁처리시 조치사항의 내용을 문서(계약서)에 포함
 - ※ 조치사항 : 목적 외 개인정보 처리 금지, 기술적·관리적 보호조치, 위탁업무의 목적 및 범위, 재위탁 제한, 안전성 확보조치, 관리감독, 손해배상 등 책임
- 수탁회사에 대한 정기적인 교육 및 실태점검 실시

< 파일 관리 및 파기 >

- 개인정보를 별도 보관 시, 개인정보처리시스템과 동일한 시스템이 아닌 별도의 하드디스크나 보조기억장치에 보관
- 수집목적 달성 및 보유기간의 경과 시 지체 없이(5일 이내) 파기

< CCTV 설치 및 운영 >

- 공개된 장소에 CCTV를 설치·운영할 경우에는 안내판 설치
- 안내판에는 설치 목적과 장소 등을 누락 없이 기재하고, 쉽게 알아볼 수 있는 곳에 부착
- CCTV를 위탁 관리하는 경우에는 안내판에 수탁업체명과 연락처를 추가적으로 기재



감사합니다

• 참고자료 : 개인정보보호 종합지원 포털 : www.privacy.go.kr(자료실)