



개인정보 보호 및 활용을 위한 기술(솔루션)



조달우수제품



혁신제품



GS인증 1등급



IR52 장영실 상



Ktl 마크인증



V&V성능평가완료



클라우드서비스
품질성능 확인

Contents

1. 개인정보 보호 조치의 필요성

2. 웹 개인정보 보호 조치 방법

3. 개인정보 관리 수준진단을 위한 개인정보접속기록 수집 방안

4. 개인정보보호 및 활용을 위한 가명 · 익명 처리방법

Chapter

01

개인정보 보호 조치의 필요성



1-01. 개인정보 보호 조치의 필요성(개인정보 필요성 및 보호법 강화)

2020년 8월 5일 시행된 개인정보보호법의 주요 개정 사항은 개인정보 보호체계를 일원화 하고, 가명정보 도입 등 데이터 이용을 활성화 하고, 개인정보처리자의 책임성을 강화하는 내용입니다.

데이터 이용 활성화

- 가명정보 도입 등 데이터 활용 근거 마련
- 양립성에 근거한 개인정보의 목적 외 이용·제공

- 개인정보의 이용·제공 범위 확대
- 가명정보의 이용·제공 범위 확대
- 익명정보를 개인정보보호법의 적용 대상에서 배제
- 개인정보의 추가적 이용·제공 근거 마련 (제15조3항, 제17조4항)
- 데이터 결합을 위한 법적 근거 마련 (제28조의3)

개인정보 보호체계 일원화

- 개인정보의 안전한 활용을 위해 감독기구 및 관련법령 정비
 - ✓ 분산된 개인정보보호 기능을 개인정보위원회 통합, 이관 (개인정보보호위원회, 행정안전부, 방송통신위원회, 금융위원회)

- 개인정보보호위원회를 국무총리 소속 중앙 행정기관으로 격상
- 정보통신망법과의 통합을 통한 법령 일원화

개인정보처리자 책임성 강화

- 가명정보의 안전한 활용을 위해 안전조치 의무 부과

- 추가정보 별도 분리·보관 관리 (법 제28조의4), (영 제29조의5제1항)
- 가명정보 처리시 금지의무 등 (법 제28조의5), (영 제29조의5제2항)

1-02. 개인정보 보호 조치의 필요성(개인정보 유출사고)

개인정보 유출 사건이 흉악범죄로 이어지는 사회현상이 증가함에 따라 개인정보 보호에 대한 중요성이 높아지고 있으며, 국민의 민감한 개인정보를 대량으로 보유하고 있는 공공기관은 개인정보 보호 관리 강화 및 신뢰도 향상을 위한 관리체계 수립이 의무화되고 있습니다.

❖ 개인정보 유출 사건 사례

• 웹 사이트 운영자 또는 사용자의 실수로 인한 개인 정보 유출

- 웹사이트 관리자가 공지사항이나 정보공개 등의 게시물을 등록하는 과정에서 부주의하게 개인정보를 유출한 사건
- 사용자가 민원이나 서비스 문의 과정에서 부주의하게 개인정보 유출한 사건

• 외부로부터 해킹에 의한 개인 정보 유출

- 악의적 목적으로 홈페이지의 데이터베이스를 해킹하여 개인정보가 유출된 사건

• 내부자에 의한 고의 개인 정보 유출

- 협력업체 직원이 USB를 통해 임직원 개인정보 수천만 건을 유출해 대출업자에게 판매한 사건
- 퇴사한 직원이 악의를 품고 고객 데이터를 몰래 가져가 경쟁사로 이직한 사건
- 불법적인 통신소에서 받은 주민번호와 이름을 고객정보시스템에 입력하여 더 많은 개인정보를 불법으로 수집하여 유출한 사건

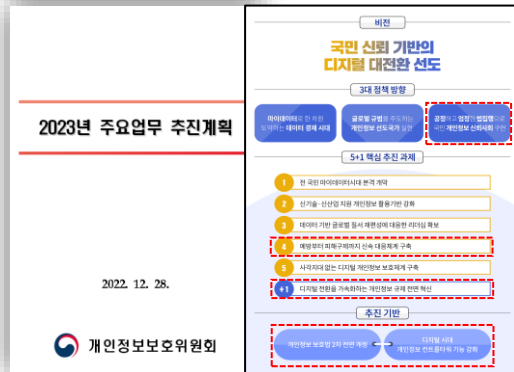


e-나라지표 (국정모니터링시스템)	2022 05월		2022 06월		2022 07월		2022 08월		2022 09월		2022 10월		2022 11월		2022 12월		2023 01월		2023 02월	
	상당	신고	상당	신고	상당	신고	상당	신고	상당	신고	상당	신고	상당	신고	상당	신고	상당	신고	상당	신고
적법하지 않은 개인정보 수집	586	20	508	13	496	11	434	26	493	30	420	6	479	15	406	16	424	7	522	6
적법하지 않은 개인정보 이용 또는 제공	553	6	557	5	652	7	611	5	524	35	506	9	542	8	495	11	473	1	571	1
적법하지 않은 개인정보 보유 및 파기	76	9	91	6	86	6	177	8	85	9	78	6	82	4	100	9	74	7	90	5
고유식별번호 처리제한 등	66	1	63	2	53	0	67	4	73	3	54	2	68	4	58	4	71	3	59	1
영상정보처리기기 설치 운영 제한	502	41	504	34	551	43	430	39	436	48	435	33	566	47	815	31	819	14	781	43
기밀정보 처리 제한	17	0	5	1	5	0	7	0	7	0	3	0	9	0	2	0	4	-	12	0
개인정보의 안전성 확보 조치 미비	279	7	264	16	349	10	373	13	287	14	292	3	348	22	327	30	497	26	394	23
열람·정정 등 정보주체의 권리 보호 미비	177	18	166	11	219	14	173	12	118	9	897	7	140	10	202	23	210	11	192	15
보이스 피싱 등 금융사기 피해 예방	7,322	0	5,238	0	6,556	0	6,853	0	7,356	0	7,149	0	7,867	0	5,868	0	4,100	-	6,163	0
타인 정보의 도용 등 침해	1,293	0	1,200	0	1,257	0	1,334	0	1,394	0	1,402	107	1,476	156	1,388	153	1,432	-	1,568	0
개인정보보호 관련 법령 결여 등 기타	6,775	120	974	20	695	6	732	4	814	73	815	24	1,008	0	949	0	853	-	922	0
합계	17,646	222	9,590	108	10,919	97	11,191	111	11,647	221	12,111	197	12,585	266	10,610	277	8,957	69	11,264	94

출처: 개인정보보호위원회(한국인터넷진흥원 개인정보침해신고센터 접수자료)

1-03. 개인정보 보호 조치의 필요성(개인정보보호 강화)

개인정보보호위원회 '23년 주요업무 추진계획에 따르면 디지털 시대에 맞는 신뢰 기반의 개인정보 보호·**활용** 체계를 구축하기 위하여 접속기록 관리시스템 도입을 의무화하고, 공공기관 관리수준 진단 전면 혁신을 예정하고 있습니다.



개보위 '23년 업무 추진 목표: “국민 신뢰 기반의 디지털 대전환 선도”

○공공부문의 반복적인 개인정보 유출*에 따른 안전조치 강화 필요

*수원시 사건(공무원의 흥신소 정보유출), 신당역 사건(공기업 직원의 내부 인터넷 정보열람) 등

○급속한 디지털 전환으로 대량의 데이터 처리가 증가하면서, 공공·민간의 개인정보 유출 위험 및 2차 피해 발생 지속

*유출신고 개인정보(해킹) : '19년 1,404만(1,308만) → '20년 1,200만(1,143만) → '21년 991만(814만)

⇒ **디지털 시대에 맞는 신뢰 기반의 개인정보 보호·활용 체계 구축 필요**

○개인정보보호위원회 '2023년 주요업무 추진계획'

[4] 예방부터 피해구제까지 신속 대응체계 구축

□투명하고 안전한 공공부문 개인정보 관리 정착

1. 민감한 국민 개인정보를 대량 처리하는 1,515개 시스템을 집중관리 대상으로 선정

접속관리시스템 도입 의무화 및 접근 통제 강화

*('23년) 주민등록 연계시스템 등 60개 → ('24년) 지자체 표준시스템 등 50개 순차점검

- 개인정보 고의 유출 시 원-스트라이크 아웃(파면·해임) 등 처벌 강화(1월~)

2. 행정·사법분야 법령* 전면 정비로 개인정보 과다수집 원천 차단 (~12월)

*선거·정당 200개, 법원, 법무, 민사법, 형사법 577개 등 14개 분야 1,670개 법령

3. 공공기관 관리수준 진단을 전면 혁신하고 '보호수준 평가제' 도입('24년)

*기관별 자체진단 및 정성평가 도입, 현장검증 확대('22년 60건 → '23년 90건) 등 평가내실화

*조달 실적 기반 공공기관 56.3%, 지자체 26.3% 시스템 미도입

1-04. 개인정보 보호 조치의 필요성(개인정보보호 강화)

한국인터넷진흥원(KISA)은 데이터 경제로의 패러다임 전환으로 중요성이 더욱 높아지고 있는 개인정보의 보호와 활용을 주제로 '2023 개인정보 7대 이슈'를 선정하였으며, **가명정보 활용 도전 과제** 및 **공공분야 개인정보보호 조치 대폭 강화**를 예고 하였습니다.

한국인터넷진흥원-KISA 「공공기관 개인정보 보호 조치 강화 방안」

- **(처벌·단속강화) 원스트라이크아웃제도***를 도입하고 부정이용 처벌 규정을 신설하는 등 공공분야에서 개인정보의 유출에 대한 징계 및 형사 처벌 강화
*한 번이라도 고의 유출, 부정이용 시 공직에서 퇴출하는 제도로 중대한 사생활 침해, 각종 범죄 악용 등 비위 정도가 심각한 경우 1회 개인정보 유출, 부정이용에도 파면·해임
- **(보호·관리강화) 공공분야 집중관리 시스템을 지정**하여 접근 권한 관리, 접속 기록 점검, **승인·소명·통지 절차를 마련**하는 등 **안전조치 기준을 강화**, 영향 평가의 실효성 확보 및 시스템 감리 시 개인정보 보호 점검을 강화하는 등 **개인정보 처리 시스템 개발 내실화**
- **(사각지대 소멸)** 공공 시스템별 통합 관리 체계를 구축하고 시스템 이용 기관, **개인정보 관리 취약 지자체의 책임을 강화**하여 개인정보 처리의 책임 및 역할 명확화, 공공기관 개인정보 관리 수준 진단을 내실화 하고 정부 평가에 수준 진단 결과를 반영해 수준 진단의 실효성 확보
- **(보호 기반 구축)** 적정 인력 배치 및 시스템 확충을 통해 **개인정보 보호 체계를 강화**하고 조사·평가·진단 등 개인정보 위의 공공 부문 대응 기능을 확대 해 개인정보 보호 기반을 구축, **SI 개인정보 침해 예방 시스템 도입**으로 공공 부문 개인정보 과다 수집 원천 차단
- **(법제도 강화)** 상기 공공 부문 개인정보 유출 방지 대책 시행을 위해 **「주요 공공기관에 대한 안전조치 특례 규정」을 신설**하는 등 **「개인정보 보호법 시행령」 개정** 검토 등



Chapter

02

웹 개인정보 보호 조치 방법



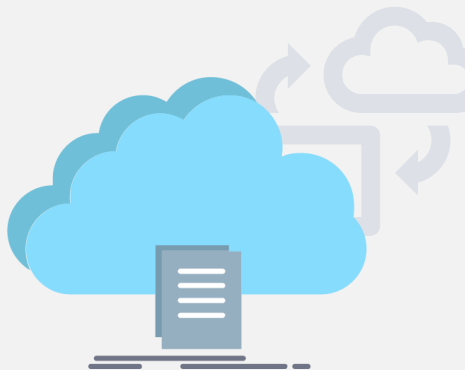
2-01. 웹 개인정보 보호 조치 필요성

컴플라이언스 준수

개인정보법	신용정보법
개인정보의 안전성 확보 조치 마련	기술적/물리적/관리적 보안대책 마련
개인정보 보호책임자 지정	개인신용정보 관리 및 보호인 지정

- 개인정보보호법(2017.10.19) 제31조
- 안정성확보조치기준고시제5조4항 “개인정보처리자는취급중인 개인정보가**인터넷홈페이지, P2P, 공유설정, 공개된무선망이용**등을 통하여 열람권한이 없는 자에게 공개되거나**유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터 및 모바일 기기 등에 조치를 취하여야 한다**”
- 신용정보업감독규정의제20조

행정·공공기관 Cloud 전환 정책



- 2021년부터 진행된 “행정·공공기관 클라우드 전환” 정책으로 2025년도까지 행정·공공기관에서 운영 중인 모든 정보시스템을 클라우드로 전면 전환·통합 계획
- 대대적인 시스템 개편 사업으로 클라우드 이전 시 새로운 보안 S/W가 필요함에 따라, 클라우드에 적용이 가능하며 호환성이 입증된 개인정보 필터링 S/W 필요

이미지 파일 개인정보 보안 강화



- 개인정보보호위원회(홈페이지 개인정보 노출 방지 안내서)에서 이미지에 대한 개인정보 유출 사례 분석을 통해 이미지 속 개인정보를 차단해야 한다고 명시
- 2023년도 현재 개인정보 유·노출 사고 빈도가 많아져, 개인정보보호 인식 높아짐에 따라 취약 사각지대(이미지 파일 내의 개인정보) 보안 필요

2-02. 웹 개인정보 보호 기대효과

최근 웹 개인정보 보호 기술은 다양한 환경에 적용이 가능하며, 적용 후 개인정보 유·노출에 대한 보안이 보장 됩니다.
이렇게 웹 개인정보보호는(공공)기관 및 지자체 의 개인정보 보안을 강화 함으로, 다양한 긍정적 효과를 볼 수 있습니다.

개인정보 유·노출에 대한 안전한 Web환경 조성

웹시스템 개인정보 유·노출에 대한 기술적, 관리적 1차 보안 기반
확보 <컴플라이언스 준수>

개인정보의 보안성 강화로 기관 이미지 상승

개인정보 유·노출에 대한 사용자가 기관에 대한 이미지 신뢰도
상승 효과

개인정보담당자의 관리적 편의성 강화

홈페이지 및 대상 시스템 개인정보 유·노출에 대한 자동 탐지 및
차단으로 담당자의 업무 효율성 강화

개인정보의 **보안성을 강화** 하고

효율적으로 관리 가능



2-03. 웹 개인정보 보호 조치 방법(웹 시스템 개인정보 보호 솔루션)

개인정보 유출 차단 솔루션 (개인정보 필터링)

목적

- 주로대국민게시판(홈페이지)에업로드되는웹콘텐츠, 첨부파일내의개인정보 검출시차단을목적으로함
- 일반HTTP뿐만아닌HTTPS통신내에개인정보검출가능

기대효과

- 웹시스템개인정보유·노출에대한기술적관리적 1차보안이가능(차단)
- 웹시스템에업로드되는개인정보에대한자동탐지 및 차단으로해당담당자의업무 효율성강화

개인정보 노출 점검 솔루션 (WEB)

목적

- 주로대국민시스템(홈페이지) 게시판에이미올려져 있는콘텐츠 등에 인가되지않은개인정보가 기재되었는지 검색(SCAN)을목적으로함
- 개인정보필터링 솔루션에서오탐및 미탐시업로드되는개인정보에대한2차적보안기능

기대효과

- 웹시스템개인정보유·노출에대한기술적관리적 2차보안이가능

개인정보 노출 점검 솔루션 (파일 서버, DB)

목적

- 다양한서버(리눅스, 윈도우, 유닉스등)파일서버내에산재한개인정보패턴을 검색(SCAN)하여 개인정보현황을파악하기위한솔루션

기대효과

- 서버내에방치된개인정보를파악 후 불필요한개인정보를삭제하기위한현황파악에적합
- 시스템서비스후파일서버, DB서버내에 불필요하게 쌓여있던개인정보에대한관리가가능해지며, 해당담당자의업무 효율 및 성과향상

Chapter

03

개인정보 관리 수준진단을 위한 개인정보접속기록 수집 방안



3-01. 개인정보 접속기록 관련 수준진단 지표

개인정보 관리수준 진단 지표의 필수 요건을 충족하여 고득점을 획득하기 위해서는 자동화된 솔루션 구축을 통해 관리 효율성 극대화 방법이 최선입니다.

지표번호	지표 키워드	진단단위	대응 솔루션
공통-36	접속기록의 보관관리	시스템	개인정보접속기록 솔루션
공통-37	접속기록의 필수사항 기록	시스템	개인정보접속기록 솔루션
공통-38	접속기록의 필수사항 기록	시스템	개인정보접속기록 솔루션
공통-39	접속기록의 정기적 점검	시스템	개인정보접속기록 솔루션
공통-40	접속기록의 안전한 보관	시스템	개인정보접속기록 솔루션
공통-48	개인정보의 분리 저장 및 보관	시스템	개인정보접속기록 솔루션
공통-59	가명정보와 추가정보의 접근권한 관리	기관	개인정보 가명 익명 솔루션
공통-60	가명정보 처리 내용의 관리와 필수사항의 기록 보관	기관	개인정보 가명 익명 솔루션
혁신-1	기관장의 관심과 노력	4점	PC / 웹 / 접속기록 / 가명익명 등 전반적인 보호조치를 위한 관리적 / 기술적 / 물리적 보안

접속기록에 기록하여야 하는 항목

개인정보의 안전성 확보조치 기준_해설서

- 접속기록에는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 아래의 항목들을 기록하여야 한다.

- 계정 : 개인정보처리시스템에서 접속자를 식별할 수 있도록 부여된 ID 등 계정 정보
- 접속일시 : 접속한 시간 또는 업무를 수행한 시간(년-월-일, 시:분:초)
- 접속지 정보 : 개인정보처리시스템에 접속한 자의 컴퓨터 또는 서버의 IP 주소 등
- 처리한 정보주체 정보 : 개인정보취급자가 누구의 개인정보를 처리하였는지를 알 수 있는 식별정보
(ID, 고객번호, 학번, 사번 등)
- 수행업무 : 개인정보취급자가 개인정보처리시스템을 이용하여 개인정보를 처리한 내용을 알 수 있는 정보
※ 개인정보에 대한 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄) 등이 수행 업무에 해당될 수 있다.

※ 기록하는 정보주체 정보의 경우 민감하거나 과도한 개인정보가 저장되지 않도록 하여야 한다.



3-03. 접속기록 수집 항목(정보주체 정보)

접속기록에 기록하여야 하는 항목

처리한 정보주체 정보

-처리한정보주체정보:개인정보취급자가누구의개인정보를처리하였는지를알수있는식별정보
(ID,고객번호,학번,사번등)

※기록하는정보주체정보의경우민감하거나과도한개인정보가저장되지않도록하여야한다.

■ ■ ■ 접속기록 항목 예시 ■ ■ ■

- 계정 : A0001(개인정보취급자 계정)
 - 접속일시 : 2019-02-25, 17:00:00
 - 접속지 정보 : 192.168.100.1(접속한 자의 IP주소)
 - 처리한 정보주체 정보 : CLI060719(정보주체를 특정하여 처리한 경우 정보주체의 식별정보)
 - 수행업무 : 회원목록 조회, 수정, 삭제, 다운로드 등
- ※ 위 정보는 반드시 기록하여야 하며 개인정보처리자의 업무환경에 따라 책임추적성 확보에 필요한 항목은 추가로 기록해야 한다.

3-04. 접속기록 수집 예시

접속기록에 기록하여야 하는 항목

2019년 개인정보보호 8차 전문교육(9.23(월))

* 접속기록 필수 항목 남기기

[접속기록 필수항목]

- 계정 : 개인정보처리시스템에서 접속자를 식별할 수 있는 ID 등 계정 정보
- 접속일시 : 접속한 시점 또는 업무를 수행한 시점(년-월-일, 시:분:초)
- 접속지 정보 : 접속한 자의 PC, 모바일기기 정보, 서버의 IP주소 등 접속 주소
- 처리한 정보주체 정보 : 누구의 개인정보를 처리했는지 알 수 있는 (이름, ID 등)
- 수행업무 : 개인정보처리시스템에서 처리한 내용을 알 수 있는 정보

※ 접속기록 예시

번호	접속일	접속시간	계정(id)	접속지정보(IP)	수행업무(이벤트)	정보주체 정보
1	2019-07-06	10:15:10	gdhong01	192.168.4.123	고객정보 조회	882428-2222222
2	2019-07-06	10:16:05	glim02	192.168.4.17	고객정보 수정	971325-1111111
3	2019-07-06	11:10:47	jskim01	192.168.4.34	직원 조회	844505-1111111

3-05. 다운로드 접속기록 및 사유

▶ 개인정보 다운로드의 기록관리 및 사유 확인

개인정보의 안전성 확보조치 기준_해설서

- ② 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다.

특히 개인정보를 다운로드한 것이 발견되었을 경우에는 내부 관리계획으로 정하는 바에 따라 그 사유를 **반드시** 확인하여야 한다.

- 특히, 개인정보처리시스템에 접근하여 개인정보를 다운로드 한 경우에는 내부 관리계획으로 정하는 바에 따라 그 **사유를 확인**하고, 개인정보취급자가 개인정보의 **오·남용이나 유출을 목적으로 다운로드 한 것이 확인**되었다면 지체 없이 개인정보취급자가 다운로드 한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 한다.

3-06. 다운로드 접속기록 및 사유 조건

▶ 개인정보 다운로드의 기록관리 및 사유 확인

개인정보의 안전성 확보조치 기준_해설서

■■■ 다운로드 사유확인이 필요한 기준 책정 예시 ■■■

- (다운로드 정보주체의 수) 통상적으로 개인정보 처리 건수가 일평균 20건 미만인 소규모 기업에서 개인정보취급자가 100명 이상의 정보주체에 대한 개인정보를 다운로드 한 경우 사유 확인
- (일정기간 내 다운로드 횟수) 개인정보취급자가 1시간 내 다운로드한 횟수가 20건 이상일 경우 단시간에 수차례에 걸쳐 개인정보를 다운로드 한 행위에 대한 사유 확인
- (업무시간 외 다운로드 수행) 새벽시간, 휴무일 등 업무시간 외 개인정보를 다운로드 한 경우 사유 확인




- 다운로드란 개인정보처리시스템에 접속하여 개인정보취급자의 컴퓨터 등에 개인정보를 엑셀, 워드, 텍스트, 이미지 등의 파일형태로 저장하는 것을 말한다.

3-07. 개인정보 처리 시스템 다운로드 유형

다운로드 유형

개인정보다운로드/유형1

현황

 고객명단.xlsx

구성



DB에서 호출된 개인정보를 WEB/WAS에서
목록화하여 다운로드하는 경우

개인정보다운로드/유형2

현황

[illegible]

 고객명단.xlsx

구성



DB에서 호출된 개인정보를
ClientCS에서 다운로드하는 경우

개인정보다운로드/유형3

현황



The screenshot shows the ASPECTS HRMS system interface. The document title is "[이사회서] 사업자등록증 (종사업장 추가).pdf". The file size is 1.7MB and the format is pdf. A red box highlights the "다들용" button, which is used to upload the document.



구성



공개된게시판또는업무용게시판에서
개인정보가포함된파일을다운로드하는경우

3-08. 다운로드 접속기록 및 사유 수집 방법

▶ 다운로드 사유 수집

다운로드 개인정보 접속기록 수집 및 사유 수집 방법	
개인정보 처리시스템 자체 개발	<ol style="list-style-type: none"> 1. 개인정보처리 시스템 내에서 자체 개발로 다운로드 이력 로그 및 사유 수집 가능 (수집된 로그는 접속기록 솔루션과 연계 후 솔루션에서 통합 관리) 2. 다운로드가 발생하는 모든 페이지에 다운로드에 대한 사유 받을 수 있음
개인정보 접속기록 솔루션에서 수집	<ol style="list-style-type: none"> 1. 모든 다운로드에 대한 사유 페이지(팝업창)출력으로 다운로드 사유 수집 가능 2. 비정상위험 시나리오를 통한 오남용 분석 가능 3. 대상시스템 간단한 소스 수정으로 다운로드 이력 수집 및 사유 수집 가능 4. 접속기록 솔루션에서 통합 적인 관리 가능(비정상위험 분석 편의성 UP)

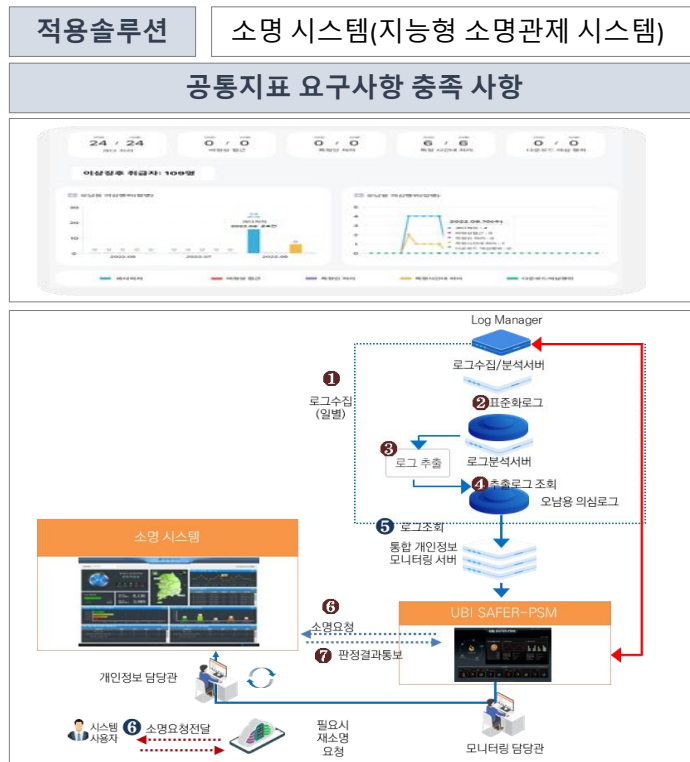
❖ 사유페이지예시



3-09. 비정상위험 분석 및 소명

개인정보 접속기록 수집 외에 기관 내부관리 규정에 정의된 비정상위험 분석 필요하며, 비정상행위 의심 로그는 해당 개인정보 취급자에게 소명을 받아야 합니다

지표번호	공통-38	단위	시스템
지표	개인정보취급자의 개인정보처리시스템 접속기록 등을 월1회 이상 점검하고 있는가?		
근거법령	「개인정보의 안전성 확보조치 기준」 제8조제2항		
평가기준 (착안 사항)	<ul style="list-style-type: none"> 개인정보취급자의 개인정보처리시스템 접속기록 등을 월1회 이상 정기적으로 점검해야 함 또한, 접속기록 점검 시 다음과 같은 ‘비정상 행위’를 발견한 경우에는 추가 조사, 소명요청 등 적절한 대응조치를 해야 함 		
비정상 행위	<ul style="list-style-type: none"> (계정) 접근권한이 부여되지 않은 계정으로 접속한 행위 등 (접속일시) 출근시간 전, 퇴근시간 후, 새벽시간, 휴무일 등 업무시간 외 접속한 행위 (접속지 정보) 인가되지 않은 단말기 또는 지역(IP)에서 접속한 행위 등 (처리한 정보주체 정보) 특정 정보주체에 대해 과도하게 조회, 다운로드 등의 행위 (수행업무) 대량의 개인정보에 대한 조회, 정정, 다운로드, 삭제 등의 행위 등 (기타) 짧은 시간에 하나의 계정으로 여러 지역(IP)에서 접속한 행위 등 		



Chapter

04

개인정보보호 및 활용을 위한 가명 · 익명 처리방법



4-01. 데이터 활용을 위한 개인정보 관련 법률 개정

데이터 3법

개정전->개인정보이용시사전에동의필요

개정 후

개인정보보호법

모든사항에서
개인정보이용

- 가명정보상업적 목적활용가능
- 개인정보관리감독가능
- 개인정보보호위원회
일원화

정보통신망법

온라인상의개인정보
·융합산업활성화위해개인
정보수집이용
·온라인상개인정보
규제·감독개인정보
보호위원회로변경

신용정보법

신용거래에서의
개인정보
·가명정보금융분야비
데이터분석·이용
·가명정보정보주체등
의없이이용및
제공가능

정보공개법

공공기관의정보공개에관한법률

제 3조

공공기관이 보유·관리하는 정보는 국민의 알 권리 보장 등을 위하여 이 법에서 정하는 바에 따라 적극적으로 공개하여야 한다.

제 9조

공공기관이 보유·관리하는 정보는 공개 대상이 된다.

데이터 산업법

데이터 산업진흥 및 이용촉진에 관한 기본법

제 10조

과학기술정보통신부장관과 행정안전부장관은 데이터간의 결합을 통해 새로운 데이터의 생산을 촉진하기 위하여 산업간의 교류 및 다른 분야와의 융합 기반 구축 등에 필요한 시책을 마련하여 추진하여야 한다.

제 14조

과학기술정보통신부장관은 데이터에 대한 객관적인 가치 평가를 촉진하기 위하여 데이터 가치의 평가 방법 및 평가 체계를 수립하여 이를 공표할 수 있다.

1

개인정보보호법, 신용정보법, 정보통신망법 등 데이터 3법의 개정을 통해 데이터 경제의 활성화를 위한 법적 기반 마련

2

데이터 활용을 위한 개인정보 등의 보안에 대한 중요성이 커짐

데이터 활용을 위해 개인정보보안 솔루션의 중요성이 증대

4-02. 데이터 활용을 위한 개인정보 가명처리 필요성

안전한데이터처리환경 조성

사용 목적에 맞도록 데이터의 효용성을 유지하면서
개인의 재식별 위험을 제거하여 최적의 가명 처리
방안을 확립 <컴플라이언스 준수>

결합데이터 활용

내부결합 / 외부결합 등 데이터 결합을 통하여 기존
정보를 벗어난 새로운 정보창출로 인사이트 창출

개인정보관리 수준진단

개인정보관리 수준진단의 평가요소로서 정보관리
가점추가로 수준상향평가 가능성을 높임

정보공개요구대응

연구, 유통, 정보공개 등 다양한 정보공개 요구에
적법한 대응방안 (가명화, 익명화, 각종 이력관리)

내부데이터 활용 및 결합

정책수립, 사업전략수립 등 안전하게 처리된
가명데이터로 각종 정책, 기획 등에 활용 가능

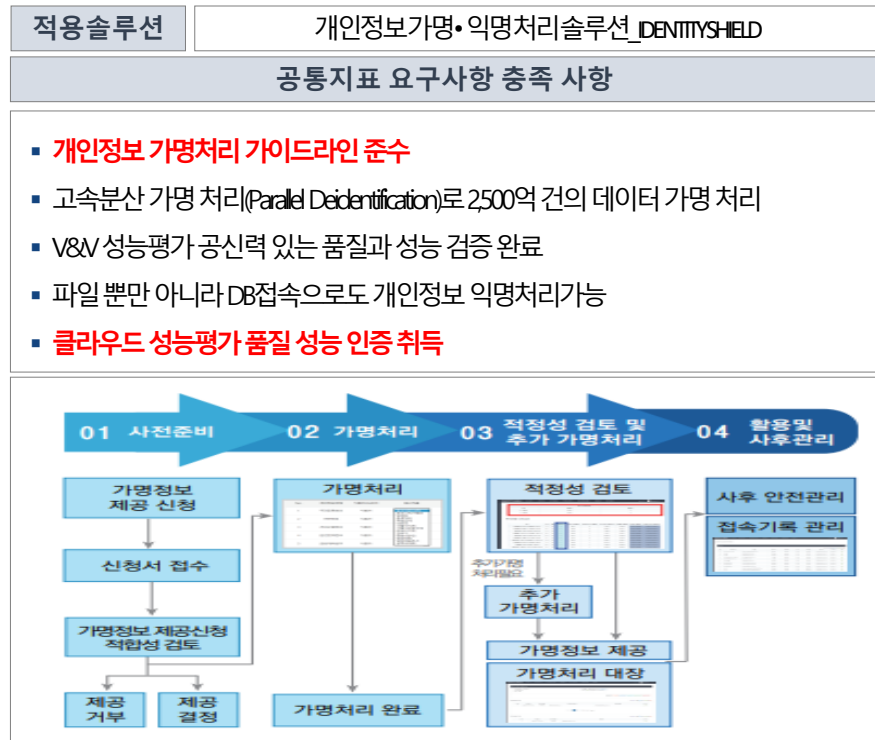
데이터산업활성화

가명정보 형태의 빅데이터 활용·제공도 가능하며,
다른 산업과 가명정보 빅데이터 결합 활용 가능

4-03. 개인정보 관리 수준진단 평가 지표 준수

개인정보가명·익명처리솔루션은가명정보와추가정보를분리보관하고있으며,추가정보에대한개인정보취급자의접근권한을분리하고있습니다.

지표번호	공통-59	단위	시스템
지표	가명정보와추가정보를분리보관(추가정보가불필요한경우에는즉시파기)하고,가명정보와추가정보에대한개인정보취급자의접근권한을분리하고있는가?		
근거법령	<ul style="list-style-type: none"> 「개인정보 보호법」 제28조의4제1항 「개인정보 보호법 시행령」 제29의5조제1항 		
평가기준 (착안사항)	<ul style="list-style-type: none"> 가명정보와추가정보를분리보관하거나,추가정보가불필요한경우에는그추가정보를즉시파기해야함 또한,추가정보를분리보관하는경우추가정보에대한개인정보취급자의접근권한을업무에필요한최소한의인원으로엄격히통제해야함 		
참고사항	<ul style="list-style-type: none"> 가명정보란? 개인정보를가명처리*함으로써원래의상태로복원하기위한추가정보의사용·결합없이특정개인을알아볼수없는정보를말한다. *개인정보의일부를삭제하거나일부또는전부를대체하는등의방법으로추가정보가없이특정개인을알아볼수없도록처리하는것 추가정보란? 개인정보의전부또는일부를대체하는데이용된수단이나방식(알고리즘등),가명정보와의비교·대조등을통해삭제또는대체된개인정보를복원할수있는정보(매핑테이블정보,가명처리에서용된개인정보등)를말한다. 가명정보와추가정보의물리적분리가어려운경우에는DB테이블분리등논리적분리도가능하나,이경우보다엄격한접근통제가필요하다. 		



4-03. 개인정보 관리 수준진단 평가 지표 준수

개인정보가명 · 익명처리 솔루션은 가명정보 처리에 대한 내용관리를 위해 필수사항을 기록 보관합니다.

지표번호	공통-60	단위	시스템
지표	가명정보 처리 내용을 관리하기 위해 가명정보 처리 목적 등 필수사항을 기록·보관하고 있는가?		
근거법령	「개인정보 보호법」 제28조의4제2항 「개인정보 보호법 시행령」 제29의5조제1항		
평가기준 (착안사항)	<ul style="list-style-type: none"> 가명정보 처리에 대한 상세내역 관리를 위해 다음의 필수사항을 기록·보관 해야 함 가명정보 처리의 목적 가명처리한 개인정보의 항목 가명정보의 이용내역 제3자 제공 시 제공받는 자 		

참고사항	<table border="1"> <thead> <tr> <th>구분</th><th colspan="6">내용</th></tr> </thead> <tbody> <tr> <td>이용 신청 필수사항</td><td colspan="6"></td></tr> <tr> <td>가명정보의 처리 목적</td><td colspan="6">가명정보의 처리 목적을 구체 (통계작성, 과학적 연구, 공익적 기록보존 등)</td></tr> <tr> <td>가명처리한 개인정보의 항목</td><td colspan="6">가명처리된 대상이 될 이름 항목을 알람 (연, 성명, 나이, 주소 등)</td></tr> <tr> <td>가명정보의 이용내역</td><td colspan="6"> ① 책임자 : 가명정보 처리 관련 책임자 ② 가명정보 및 추가정보를 처리하는 자 : 가명정보를 처리하는 자 또는 추가정보를 처리하는 자(원호사 처리자 명단) ③ 가명처리 및 추가가명처리한 일시 ④ 이용방법 : 목적의 이용, 내부제공, 외부 제공, 영한 정보기관을 통한 영한 등 </td></tr> <tr> <td>제공받는 자 (제3자 제공사)</td><td colspan="6">(제3자에게 제공되는 경우) 가명정보를 제공받는 자의 명단</td></tr> <tr> <td>관련 파일명</td><td colspan="6"></td></tr> <tr> <td>가명정보 이용기간</td><td>년</td><td>월</td><td>일</td><td>~</td><td>년</td><td>월</td><td>일</td></tr> <tr> <td>가명정보 추가일자</td><td>년</td><td>월</td><td>일</td><td colspan="3" rowspan="3"></td><td></td></tr> <tr> <td>제공 책임자</td><td colspan="6">(인)</td><td></td></tr> <tr> <td>가명 책임자</td><td colspan="6">(인)</td><td></td></tr> </tbody> </table>			구분	내용						이용 신청 필수사항							가명정보의 처리 목적	가명정보의 처리 목적을 구체 (통계작성, 과학적 연구, 공익적 기록보존 등)						가명처리한 개인정보의 항목	가명처리된 대상이 될 이름 항목을 알람 (연, 성명, 나이, 주소 등)						가명정보의 이용내역	① 책임자 : 가명정보 처리 관련 책임자 ② 가명정보 및 추가정보를 처리하는 자 : 가명정보를 처리하는 자 또는 추가정보를 처리하는 자(원호사 처리자 명단) ③ 가명처리 및 추가가명처리한 일시 ④ 이용방법 : 목적의 이용, 내부제공, 외부 제공, 영한 정보기관을 통한 영한 등						제공받는 자 (제3자 제공사)	(제3자에게 제공되는 경우) 가명정보를 제공받는 자의 명단						관련 파일명							가명정보 이용기간	년	월	일	~	년	월	일	가명정보 추가일자	년	월	일					제공 책임자	(인)							가명 책임자	(인)						
구분	내용																																																																																			
이용 신청 필수사항																																																																																				
가명정보의 처리 목적	가명정보의 처리 목적을 구체 (통계작성, 과학적 연구, 공익적 기록보존 등)																																																																																			
가명처리한 개인정보의 항목	가명처리된 대상이 될 이름 항목을 알람 (연, 성명, 나이, 주소 등)																																																																																			
가명정보의 이용내역	① 책임자 : 가명정보 처리 관련 책임자 ② 가명정보 및 추가정보를 처리하는 자 : 가명정보를 처리하는 자 또는 추가정보를 처리하는 자(원호사 처리자 명단) ③ 가명처리 및 추가가명처리한 일시 ④ 이용방법 : 목적의 이용, 내부제공, 외부 제공, 영한 정보기관을 통한 영한 등																																																																																			
제공받는 자 (제3자 제공사)	(제3자에게 제공되는 경우) 가명정보를 제공받는 자의 명단																																																																																			
관련 파일명																																																																																				
가명정보 이용기간	년	월	일	~	년	월	일																																																																													
가명정보 추가일자	년	월	일																																																																																	
제공 책임자	(인)																																																																																			
가명 책임자	(인)																																																																																			



적용솔루션	개인정보 가명 · 익명 처리 솔루션_IDENTITY SHIELD
공통지표 요구사항 충족 사항	
<ul style="list-style-type: none"> 이저서티의 IDENTITY SHIELD 가명처리는 <ul style="list-style-type: none"> ①가명처리에 필요한 사전준비 ②위험성을 검토하여 가명처리 수행 ③사전준비와 가명처리 결과에 대한 적정성 평가 및 추가처리 ④가명정보를 안전하게 관리하는 사후관리단계로 이루어집니다. 	
<div> <div>1단계</div> <div>2단계</div> <div>3단계</div> <div>4단계</div> </div> <div> <div>사전준비</div> <div>가명처리</div> <div>적정성 평가</div> <div>사후관리</div> </div> <div> <div>적정</div> <div>부적정</div> </div> <div> <div>그 자체로 특정 개인을 식별할 수 있는 정보</div> <div>특정 개인을 식별할 수 없는 정보</div> </div> <div> <div>01 사전준비</div> <div>02 가명처리</div> <div>03 적정성평가</div> <div>04 사후관리</div> </div> <div> <div>▶ 빅데이터 분석 등을 위해 정보를 처리하려는 해당 정보가 개인정보인지 여부에 대해 판단</div> <div>▶ 목적달성을 위해 정확한 수준으로 가명 처리가 이루어졌는지 재식별 가능성은 없는지 판단</div> <div>▶ 비식별 대상 데이터에 대하여 가명처리, 총계처리, 데이터 삭제, 데이터 병주화, 데이터 마스킹 처리, K.L.T 프라이버시 모델 비식별화 처리</div> <div>▶ 검토결과 적정으로 판단된 가명정보에 대해 관련 법령 준수 등 관리적·기술적을 관리적 안전조치 이행</div> </div>	

4-04. 정보공개 예시



정보공개요청

적법한요청대응



기관

가명/익명처리
적정성검사

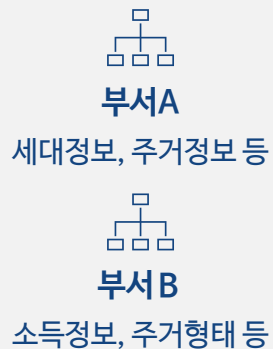
IDENTITY
SHEILD

데이터수집
가명처리
적정성검토
사후관리

데이터3법으로 나날이 늘어나는 연구, 유통, 정보공개 요구에 적법한 대응가능

수집, 가명처리, 적정성검토, 사후관리 등 관련업무 전반 자동화처리로 적법하고 원활한 업무가능

4-05. 내부데이터 결합 예시



IDENTITY
SHEILD
내부결합



적정성검사

새로운
결합정보

가구별,
소득별,
주거정보 등

1인가구, 소득별 주거지 분석 등 내부데이터를 활용한 자료 생성 가능

세대별, 소득별 거주지 위주의 타겟 정책설정 가능

4-06. 외부데이터 결합 예시


S사
차량등록정보, 주소지 등


T사
이동정보, 운행시간정보 등



결합전문기관
또는
데이터전문기관



적정성검사



**새로운
결합정보**

전기차운행정보,
차종별운행장소
정보 등...

정책활용 (데이터 기반 정책 수행으로 민원 최소화)

신규 전기차 충전소 설치 정책 반영

4-07. 이지서티 솔루션(개인정보 필터링)

개인정보필터링솔루션(U-PRIVACY SAFER)은 개인정보 실시간탐지및차단수행, 첨부파일 필터링, 개인정보 유출 차단 등을 통해 개인정보 보호에 따른 기술적·관리적 조치를 수행합니다.

제품명

U-PRIVACY SAFER

개인정보필터링



기술력



조달우수제품



혁신제품



CC인증 EAL3등급



GS인증
1등급



클라우드 서비스
품질성능 확인



국내외특허 24종



IR52
장영실상

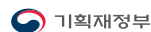
특장점

- **국내유일 CC인증 EAL3등급 보유**
- 개인정보 필터링 시스템은 웹 게시판과 첨부파일에 의해 개인정보가 유출되지 않도록 실시간 자동 탐지
- **국내유일 개인정보 필터링 분야 클라우드 품질성능 인증**
- 비정형데이터인 이미지파일에서도 개인정보 필터링 지원

구성도



주요실적



4-08. 이지서티 솔루션(개인정보 접속기록 관리 솔루션)

개인정보 접속기록관리솔루션(UBI SAFER-PSM)은 개인정보 생명주기(수집, 저장, 이용, 제공, 파기)에 따라 개인정보의 체계적 관리 기능을 제공하는 솔루션입니다.

제품명

UBI SAFER-PSM

개인정보 접속기록관리 솔루션



기술력



조달우수제품



GS인증 1등급



CC인증 EAL3등급
(2012년 획득이력 보유)



클라우드 서비스
품질성능 확인



V&V 시험평가



국내외 특허 24종

특장점

- GS인증 1등급 획득
- 모듈별 인증 (Agent, Manager, Master)
- 조달청 우수 조달 제품 지정
- 분야별 시장점유율 1위, AGENTLESS 방식의 시장 리더, 빅데이터 분석
- In-memory 기술을 통한 실시간 빅데이터 대용량 로그 처리 기술
- 국내 유일 클라우드 품질·성능 인증

구성도



주요실적



4-09. 이지서티 솔루션(지능형 개인정보 가명 익명처리 솔루션)

개인정보가명·익명처리솔루션(IDENTITY SHIELD)은 개인정보보호 및 컴플라이언스 준수를 위하여 개인정보데이터 활용에 대한 필수적인 가명처리기능을 제공합니다.

제품명

IDENTITY SHIELD

개인정보 가명·익명처리 솔루션



기술크



조달우수제품



GS인증 1등급



혁신제품



V&V 성능평가



클라우드 서비스 품질성능 확인

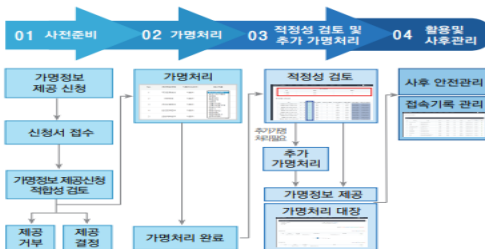


IR52 장영실상

특장점

- **개인정보가명처리 가이드라인 준수**
- 국내 최초, 최다 프라이버시 모델을 적용한 가명·익명 처리 레퍼런스 확보
- 고속분산가명처리(Parallel Deidentification)로 2,500억 건의 데이터 가명처리
- 정형데이터 뿐만 아니라, 다양한 비정형 데이터까지 개인정보 탐지, 가명처리가 가능 제공
- V&V 성능평가 공신력 있는 품질과 성능 검증 완료
- 파일 뿐만 아니라 DB접속으로도 개인정보 익명처리가 가능
- **클라우드 성능평가 품질 성능 인증 취득**

구성도



주요실적

빅데이터 플랫폼		가명 익명처리 솔루션		
 PUMPKIN	 와재보험협회	 NRF 한국연구재단	 금융강국재원	 최정호는 연봉 100만원도 안
 Amazing Food Solution, Inc.	 울산광역시농수산물 유통공사 ULSAN FOOD SUPPORT CENTER	 SCH 서울대학교 공명의료원	 보령시	
 새마을주방자식 소통만남	 한국과학기술사관 Korea National Science Museum	 삼성의료원	 KB국민은행	
 KFI 한국과학기술자 협회	 KITECH 한국과학기술자 협회	 부산시	 금융강국재원	
 EZHL	 한국문화예술위원회	 wmt 세계문화유산위원회	 EPIS	
 소방청	 K water	 해양경찰청 Korea Coast Guard	 가톨릭대학교 GACHON UNIVERSITY	
 KSPo 국민체육진흥공단	 yanolja	 광진테크노파크	 nipa 정보통신산업진흥원 National IT Industry Promotion Agency	
 doing lab	 KGU 경기대학교 산학협력단	 국민권익위원회 Korea Copyright Commission	 HF 한국주택금융공사	
 medien	 kt	 보건복지부	 I-ON COMMUNICATIONS	
 (주)에측컨테크놀로지	 KPCO	 관세청	 세종특별자치시교육청	

감사합니다.

