보건복지
개인정보보호센터
역할 및 운영현황

2022. 6.

보건복지부 SSiS 한국사회보장정보원

목차

CONTENTS

1 개 요

1 설립배경

▶ 공공, 민간구분 없이 해킹, 개인정보 취급자의 고의 또는 과실 등으로 인한 개인정보유출, 노출의 지속적 증가 (공공의 경우 사적열람 및 무단제공이 전체의 약 70%차지, 2014~2017)

민원처리 과정에서의 개인정보 유출

- 공무원이 민원을 낸 개인의 동의를 받지 않고 타인에게 휴대전화번호 안내(2020.4.18, 국민일보)
  - 불법주차 차주의 요청으로 신고자의 전화번호를 동의를 받지 않고 안내

사용자 ID공유로 인한 정보유출

- 국가 행정전산망 취급자가 특정인의 개인정보를 성착취 사건의 범죄자에게 제공 (2020.3.26, 중앙일보)
  - 공무원이 업무 편의를 목적으로 본인의 ID를 사회복무요원과 공유하고, 복무요원이 개인의 주요정보를 범죄자에게 제공(N번방)

개인 및 기업정보 유출

- 개인, 기업정보 800만건을 임의로 조회하고 12만건의 개인정보를 유출 (2014.2.5, 서울경제)
  - 유출된 개인정보 대상자를 찾아가 국가지원금 신청 업무를 도와 주고 수수료를 챙김

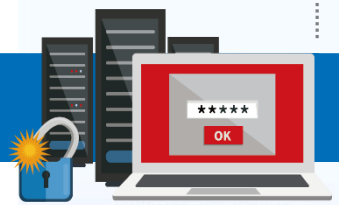
지자체 공무원의 개인정보 유출

- 지자체 공무원이 흥신소에 유출한 피해자 개인정보로 살인사건 발생 (2021.12.15, 조선일보)
  - 신변보호를 받고 있는 전 여자친구의 거주지 정보를 흥신소에서 알아내어 살해

② 개인정보보호센터 연혁

▶ **보건복지부는 정부부처 中 유일하게 보건복지 개인정보보호센터를 2010년부터 구축·운영 중**

- 보건복지부 소속 및 산하 공공기관의 개인정보 처리시스템 내 개인정보취급자의 개인정보 처리이력에 대한 상시모니터링을 통해 부정사용 방지와 오·남용 예방



2009.5~2009.9
보건복지
개인정보통합분석시스템 구축

2010.1~2011.12

2010. 개인정보 통합 모니터링센터 구축
(보건복지부 자체 운영)

보건복지
개인정보통합관제센터 운영
- 18개기관 112개 시스템
(보건사회연구원 위탁 운영)

2011.3
개인정보 보호법 제정
* 공공기관의 개인정보보호에 관한 법률 폐지

2012.1~2014.12

2015.1~현재

2015. 보건복지 개인정보관제센터(現 개인정보보호센터)
(사회보장정보원 위탁 운영)

2016.8. 보건복지분야 비식별조치 전문기관 지정

2016~2020. 개인정보 오·남용 예방 대상기관 확대사업
- 29개 기관 79개 개인정보처리시스템 접속기록 통합 연계·분석 중

2020.8
개인정보 보호법 개정
* 가명, 익명 정보의 활용

19.5.31 통합 연계·분석 방법 등 특허 취득
(제10-19865260호)

3 설립근거 및 관련 법규

▶ 보건복지부, 소속 및 산하기관의 방대한 개인정보 보호 목적으로 개인정보보호센터를 『보건복지부 개인정보 보호지침』에 근거하여 설치·운영

개인정보 보호법	개인정보 보호법 시행령	(개인정보보호위원회) 개인정보의 안전성 확보조치 기준 고시	표준 개인정보 보호지침
• 제18조(개인정보의 목적 외 이용·제공 제한) • 제29조(안전조치의무)	• 제15조(개인정보의 목적 외 이용 또는 제3자 제공의 관리) • 제30조(개인정보의 안전성 확보 조치)	• 제6조(접근통제) • 제8조(접속기록의 보관 및 점검)	• 제8조(개인정보의 목적 외 이용·제공)

보건복지부 및 소속·산하 공공기관 개인정보처리시스템의 개인정보 오·남용 예방 필요성

보건복지부 개인정보 보호지침(훈령 제195호) '제5장 개인정보 보호 지도·점검 및 개인정보보호센터 운영 등'

제72조(개인정보 보호 지도 ·점검)
제73조(현황조사)
제74조(접속기록 통합 연계·분석 등)
제75조(접속기록 통합 연계·분석 대상)
제76조(개인정보보호센터의 운영)
제77조(접속기록 자체 분석)
제78조(추출기준)
제79조(추출기준의 표준화)
제80조(판정기준 표준화)
제81조(징계기준 표준화)

4 조직구성

▶ 개인정보 오·남용 예방, 개인정보 보호 등 2개의 팀으로 구성되어, 개인정보 보호를 수행

보건복지부

통합보호담당관

한국사회보장정보원

개인정보보호센터

개인정보 오·남용 예방

- 표준 접속기록 통합분석시스템 구축 및 운영
- 표준 접속기록 추출기준 개발 및 관리
- 표준 접속기록 연계· 품질관리
- 운영기관 개인정보 처리 적정성 소명 및 검토

개인정보 보호 및 기술지원

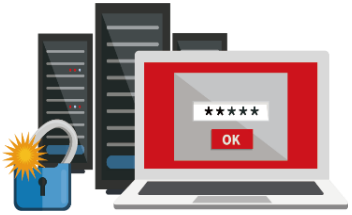
- 소속·산하 공공기관 개인정보보호 현황조사 지원
- 개인정보 보호 지원시스템 구축·운영
- 개인정보보호 전문 교육 및 컨설팅
- 소속·산하 공공기관 개인정보보호 업무 지원

2 주요 업무

① 개인정보 오·남용 예방

▶ 보건복지부 소속 및 산하 공공기관 개인정보처리시스템의 표준 접속기록 통합분석 시스템구축운영, 추출기준 표준화, 표준 접속기록 분석 및 품질 관리 등(29개 기관, 79개 시스템)

- 보건복지분야는 개인정보위 등록 공공기관 개인정보파일의 약 786억건 중 약 618억건(79%) 보유



표준 접속기록 통합분석시스템

운영기관(29개 기관)

보건복지부 및 소속 공공기관(12개)

- 보건복지부
- 국립병원(8개)
- 국립장기조직혈액관리원
- 질병관리청
- 국립재활원

산하 공공기관(17개)

- 국민건강보험공단
- 국민연금공단
- 한국사회보장정보원
- 국립중앙의료원
- 국립암센터
- 대한적십자사
- 한국보건의료인국가시험원
- 한국의료분쟁조정중재원
- 아동권리보장원
- 건강보험심사평가원
- 한국보건산업진흥원
- 한국사회복지협의회
- 한국노인인력개발원
- 한국장애인개발원
- 한국보육진흥원
- 한국건강증진개발원
- 한국장기조직기증원

(주요사업) 개인정보 오·남용 예방 대상기관 확대 사업

사업내용

보건복지부 및 소속·산하 공공기관의 개인정보처리시스템 중 중요도가 높은 시스템을 선정하여, 개인정보 오·남용 예방 업무를 수행하도록 지정

대상기관 선정기준

- 개인정보 보유량
- 개인정보의 유형 (위험도 등)
- 시스템 유형 (고유업무 수행)
- 취급자의 범위(사용자, 이용자)
- 취급자의 수

② 개인정보 보호 및 기술 지원

▶ 보건복지부 개인정보 관리수준 현황조사 지원, 소속·산하 공공기관의 개인정보 보호 관련 교육, 컨설팅 수행, 개인정보 보호 분야 담당 교육, 개인정보 보호 지원시스템 구축·운영 등

개인정보보호 전문인력 양성

- 개인정보보호 전문인력 양성 과정 운영 (연 2회)
- 개인정보보호 경연대회 등

개인정보보호 관리수준 현황조사

- 보건복지부 개인정보보호 관리수준 현황조사 점검계획 수립 및 PMO 지원
- 개인정보보호위원회 개인정보보호 관리수준 진단 대응

개인정보 보호 컨설팅

- 공공기관 개인정보 관리수준 진단
  미흡기관 및 신규기관 등 대상
  개인정보보호 컨설팅 지원

개인정보보호지원 시스템 운영

- 보건복지부 소속·산하공공기관별 개인정보 보호 관리수준 이력관리
  - 관리수준 진단 현황조사 등록, 관리, 평가수행 등
  - 관리체계 서면조사 등

3 접속기록 통합연계 · 분석 절차 및 흐름도

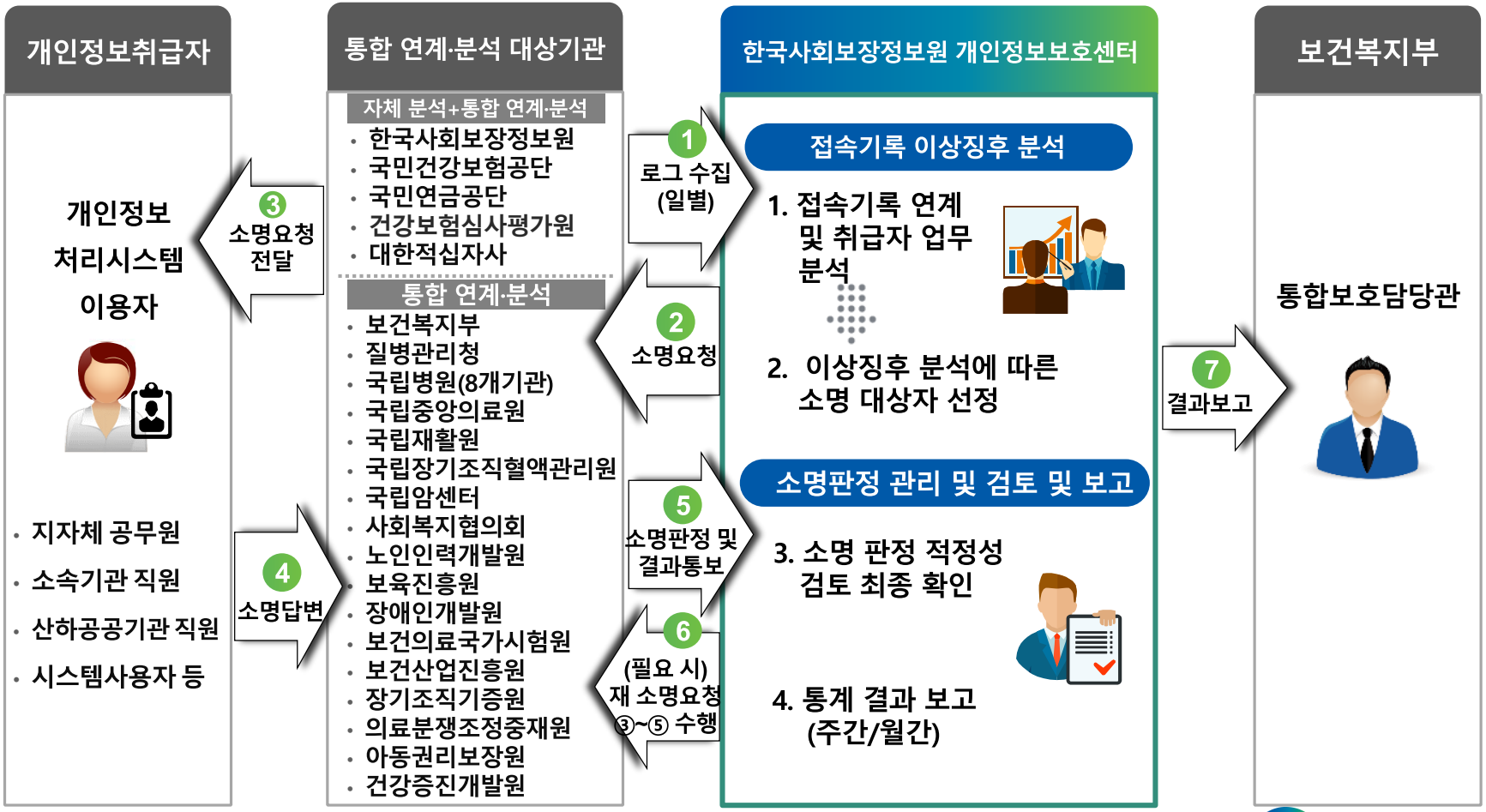
① 소명절차

접속기록 통합 연계·분석 절차 및 흐름도

3

▶ 약 35만명의 개인정보취급자의 접속기록 수집·분석·의심사례 추출 및 소명요청

▶ 개인정보취급자에게 소명전달·소명답변을 받아 최종 소명판정 후 결과 보고



보건복지부

SSiS 한국사회보장정보원

② 표준화된 접속기록 수집

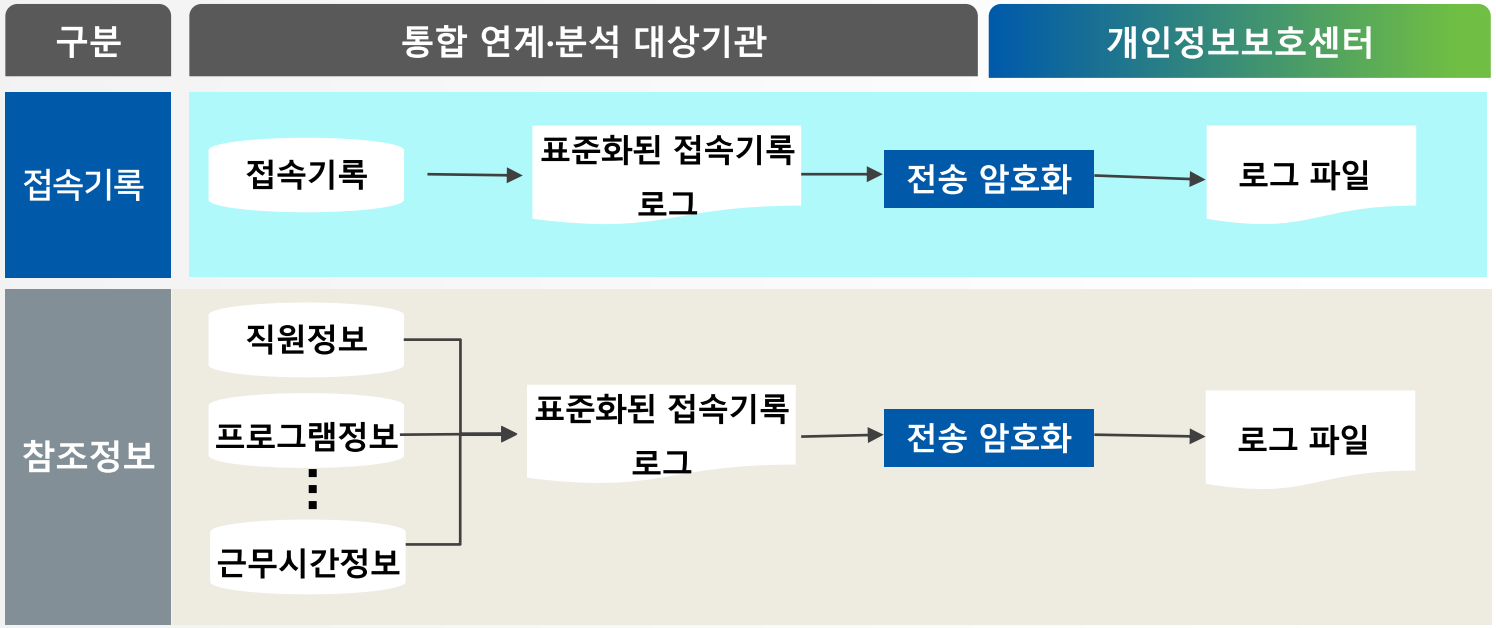
3

▶ 접속기록 생성 규칙을 적용하여 표준화된 접속기록 로그형식에 따라 일 단위로 생성
▶ 표준화된 접속기록은 암호화하여 일 단위로 전송(기본정보)

로그파일 생성규칙

- 일단위로 파일 생성
- 항목별 구분자 : Tab
- 첫 번째 속성 로그 구분자 : Space
- 텍스트 파일로 로그 기록(문자세트 EUC-KR)
- 표준화된 접속기록 형식에 따른 로그 생성

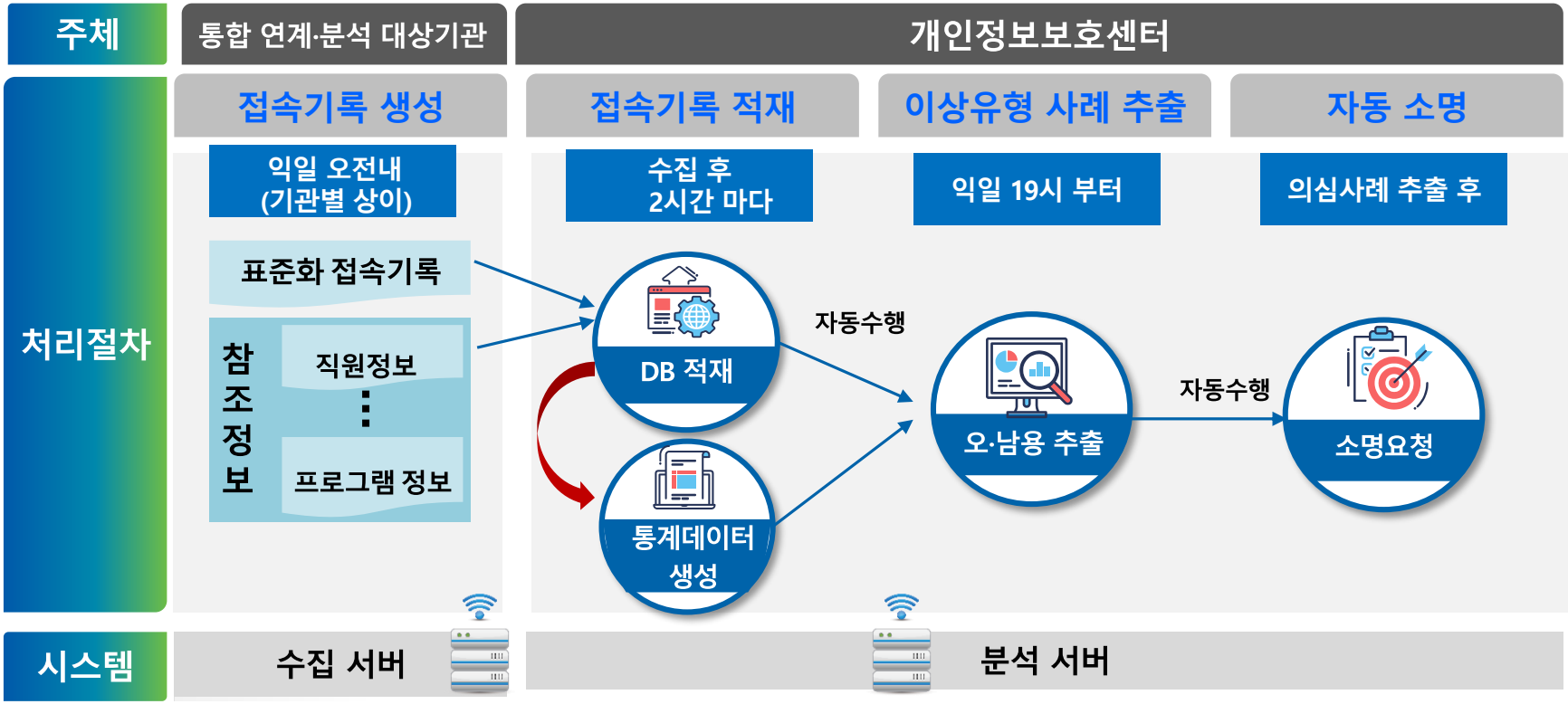
로그 수집절차



③ 이상유형 추출

▶ 수집한 로그 파일(RAW)을 DB에 적재 후 정상 적재 여부 점검

▶ 00개 추출기준(00개 세부기준)을 적용, 이상유형 추출 (추출기준은 지속적 개선)



- 다차원 분석을 통한 추출 조건 개선
- 기관별 특성에 맞는 추출 조건 개발(예, 병원은 24시간 업무가 많아 업무시간 외 조회 추출을 적용하지 않음)

4 통합 연계·분석 추출기준 유형

3

▶ 00개 추출기준(00개 세부기준) 운영 중

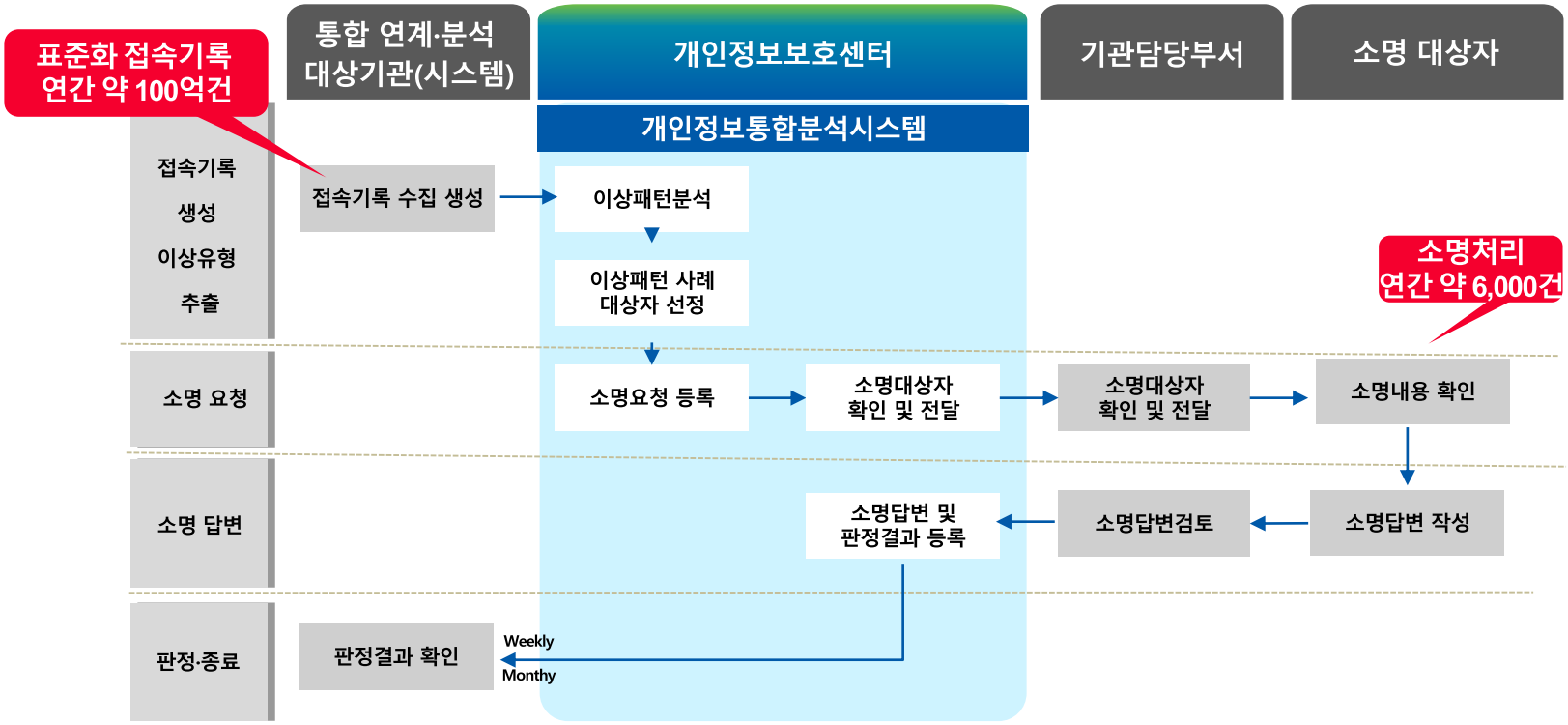
▶ 통합 연계·분석 대상기관의 일정기간(최대 6개월) 표준화된 접속기록을 분석, 의심사례 추출

순번	추출기준 유형	세부기준
1	**사용자ID 공유**	사용자ID 공유(동시접속)
		동일ID로 많은 PC 접속
		동일ID를 사용하여 타지역에서 접속
⋮	⋮	⋮

5 소명 처리 상세흐름도

3

▶ 소명 요청을 받은 후 20일 이내 답변 등록



- 표준화 접속기록이란? 통합 연계·분석을 위해 대상기관 개인정보처리시스템에서 지정된 화면에 대한 접속기록 및 참조 정보를 개인정보보호센터가 정한 기준에 맞게 생성한 로그

4 표준 접속기록 분석 실적 및 주요개인정보 오·남용 의심 유형

1 오·남용 의심 유형 추출 비율(2016년~2019년)

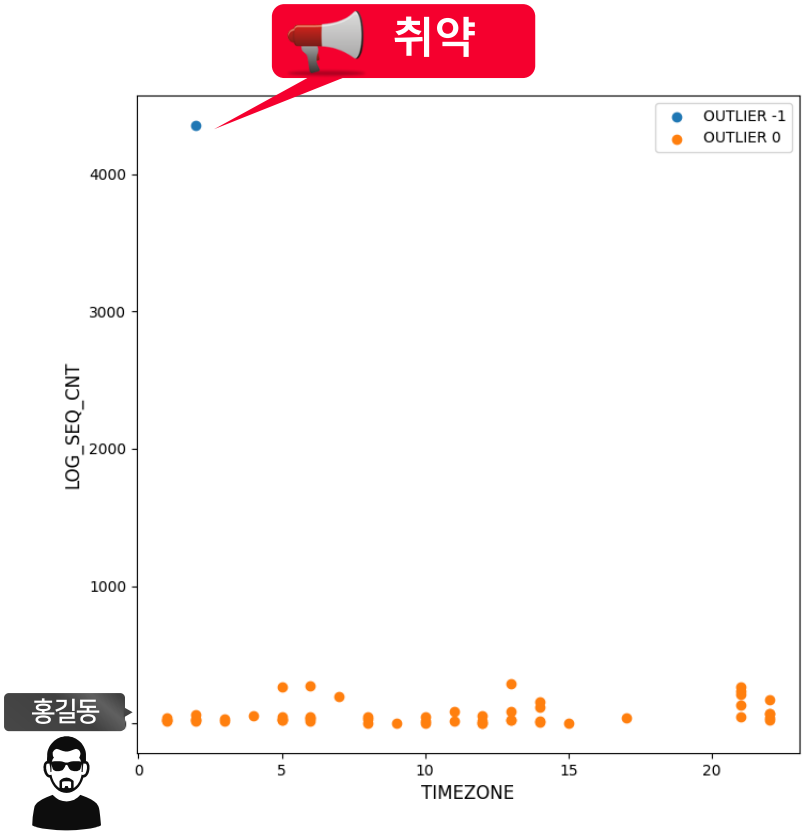
4

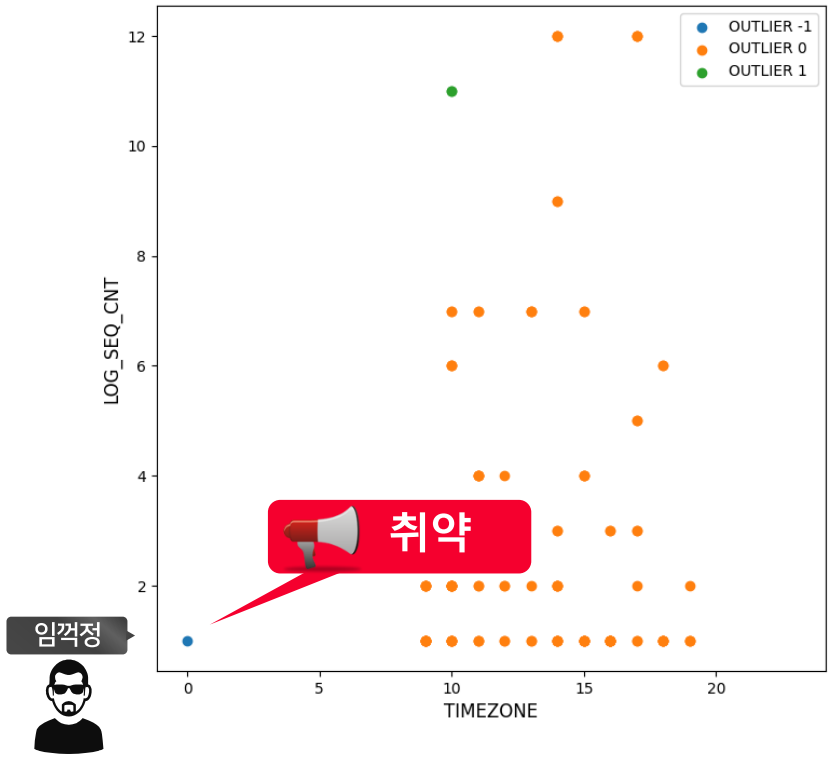
- **사용자ID 공유 및 타 지역 접속 54.91%**
  사용자ID 공유, 대표ID 사용(개별ID 미발급), 동일IP에서 다수 ID 접속 등
- **호기심 및 특정업무 처리**
  특정업무를 이용한 개인정보처리(호기심 조회), 성명을 이용한 주민등록번호 조회 등

2 추출조건 유형별 대표 오·남용 사례

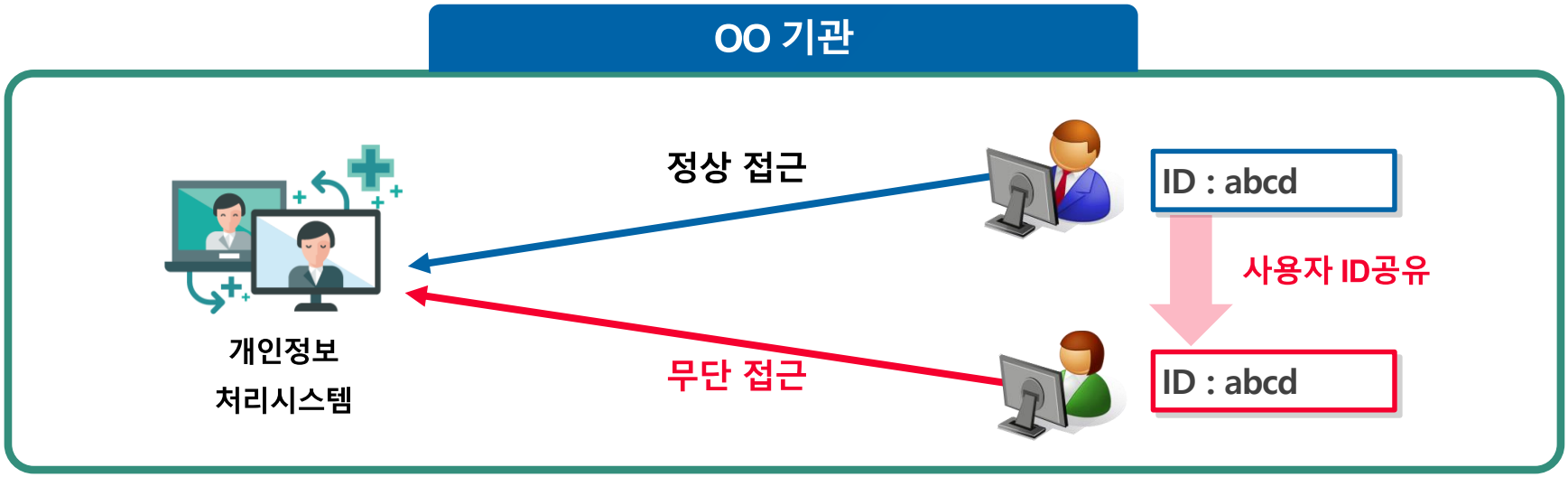
구분	추출조건 유형	대표 사례(예시)
1	사용자ID 공유	• **계정이 발급되지 않은 기간제 근로자와 계정을 공유하여 사용하는 경우** • 계정이 발급되지 않은 공익근무요원과 계정을 공유하여 사용하는 경우 • 계정이 발급되지 않은 업무보조자와 계정을 공유하여 사용하는 경우 • 퇴직자/휴직자/전보자의 계정을 공유하는 경우
.	.	.
.	.	.
.	.	.
.	.	.
.	.	.
.	.	.

▶ 개인정보취급자의 평소 업무 처리 시간과 업무처리량의 분포 범위를 벗어날 경우 개인정보 이상처리로 추출





▶ 사용자 ID를 공유 하여 권한이 없는 개인정보취급자에게 개인정보가 열람되는 사례

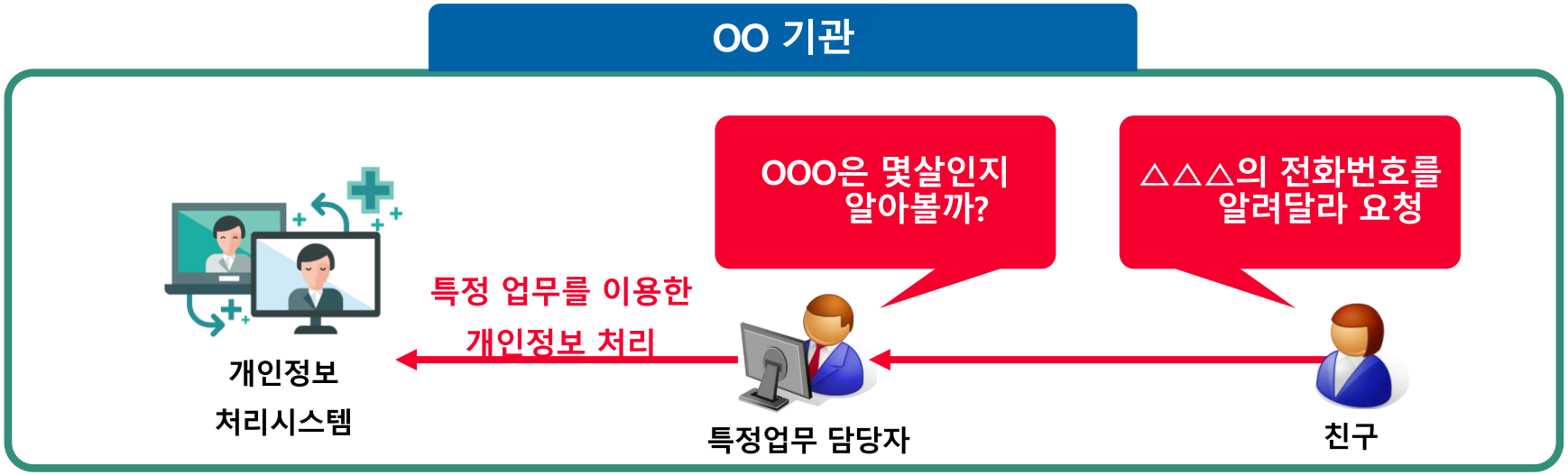


사례

출장 시 업무공백을 메우기 위해 사무실 내 직원에게 계정(ID)을 공유하여 개인정보 처리시스템을 사용하는 경우

※ 사용자 ID공유는 하나의 계정(ID)을 2명의 직원이 공유하는 것이 일반적, 3명 이상 공유하는 경우도 나타남

▶ 개인정보처리시스템을 이용하여 특정 업무를 처리하는 개인정보취급자가 호기심 또는 타인의 부탁에 의해 무단으로 타인의 개인정보 조회



사례

지인 또는 담당 업무와 관련이 없는 직원의 요청으로 제3자의 개인정보를 업무와 무관하게 조회하는 경우 개인정보처리시스템에서 개인정보를 조회하는 경우

5 향후 운영 방향

향후 운영 방향

개인정보취급자의 개인정보 오·남용 예방을 통한 개인정보보호 강화

통합 연계·분석 대상 기관 정비

- 통합 연계·분석 대상 개인정보 처리시스템 선정기준 마련
- 업무특성, 개인정보처리 시스템 환경에 맞는 추출기준 적용

개인정보보호 역량 제고

- 신규 기관 및 공공기관 개인정보 관리수준 진단 미흡기관 컨설팅 강화
- 개인정보보호 담당자의 전문 역량 제고 강화 프로그램 운영

추출기준 및 품질정비

- 표준된 접속기록 품질(수집, 적재율 등) 개선
- 개인정보 오·남용 판정기준 정비

감사합니다.