민간 디지털 포렌식 업체의 데이터 유출 관리 연구

20200571 김희주
20211089 이은민

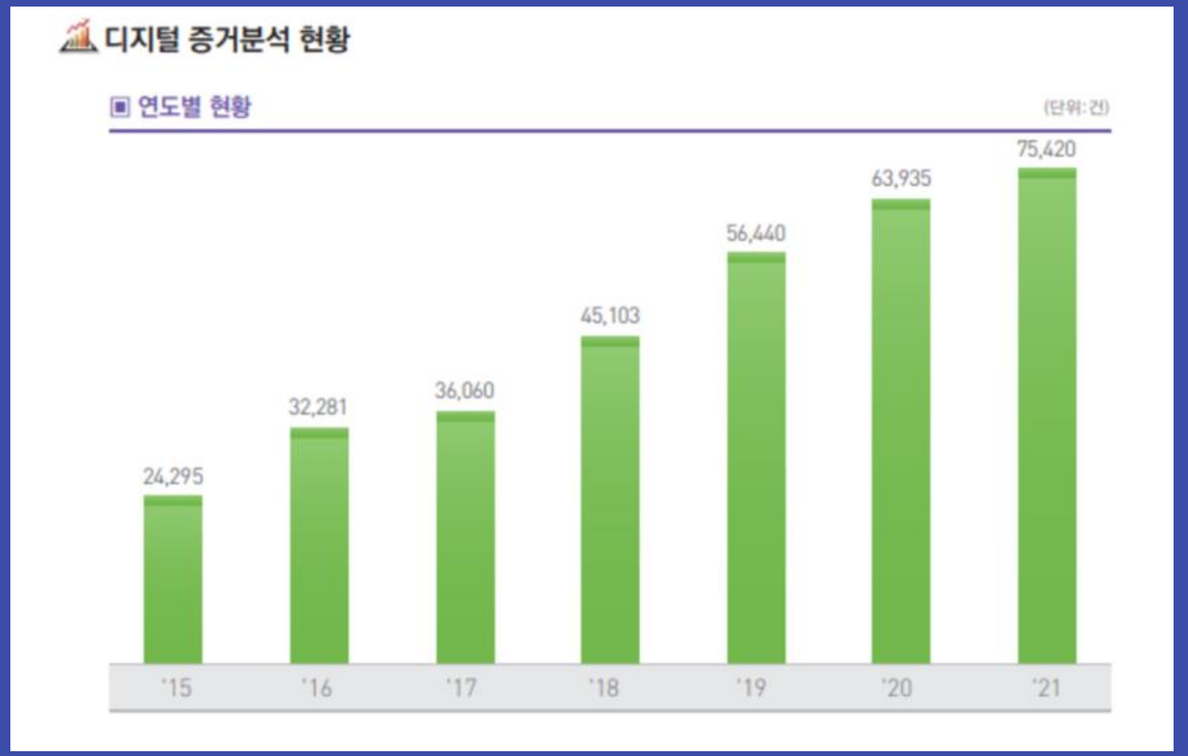
목차

1)
산업 보안에서 디지털 포렌식의 중요성

사이버 범죄의 증가 ▶
디지털 포렌식 수요 증가

사설 포렌식 업체에 의뢰하는 경우 ▶
프라이버시 보장의 어려움

(사례)
- 가수 정준영 버닝썬 사건
- 채널 A 뉴스 - 사설 포렌식의 두 얼굴



2)
국제 디지털 포렌식 표준 가이드라인

*국제형사기구(INTERPOL)의
국제 디지털 포렌식 가이드라인

분 야	필 수 항 목
Laboratory	a. 분석시설 규모(level)에 따른 조직도를 작성·구비 b. 연 단위 내부 감사 수행 c. 내·외부 불만 사항을 해결하기 위한 절차 수립 d. 문서화 업무에 대한 체계 구축
Facility and Environmental Condition	a. 시설 출입에 대한 접근통제 b. 분석시설(분석에 수행되는 공간)에 대한 출입목록 유지 - ID 카드 또는 생체인식 기술 활용 c. 분석시설 환경에 대한 정기적 모니터링 - 온도, 습도, 청결도(정리 상태) d. 안전에 관한 규칙 수립 e. 방문자 정책 수립 f. 정기적 시설의 정리
Equipment	a. 장비의 취급, 운반, 보관, 사용, 수리, 폐기 및 계획된 유지 보수 절차를 수립 b. 사용하기 전 장비가 사양에 따라 작동하는지 확인 c. 유지보수 프로그램 수행 d. 요구사항에 따른 펌웨어 업데이트(정기적 업데이트, 장비의 추가 구비 등) e. 장비의 보증문서, 설명서 및 license 유지 관리
Staff	a. 자격관리 ◦ 채용된 직원에 대한 직무기술서 작성 ◦ 신원의 확인 b. 전문성 개발 및 교육 ◦ 직원을 위한 교육 프로그램 수립 ◦ 신입사원 멘토 배정 ◦ 신규입용직원에 대한 역량평가 수행 ◦ 숙련도(기술수준) 유지를 위한 기존직원 평가 ◦ 회부 또는 실험실 간 숙련도(기술수준) 공유 ◦ 기술 자격증 구비 ◦ 기존 직원의 기술수준 유지 및 최신화를 위한 교육 시스템 구축(내부 세미나 등)
Forensic Method	a. 분석을 위한 SOP(Standard Operating Procedures 표준작업지침)를 수립 b. 최신 트렌드 및 기술발전을 고려하여 갱신 c. 도입할 디지털 포렌식 기술 또는 도구에 대한 검증 수행 d. SOP 외의 방법 또는 분석 시설에서 개발한 방법의 경우 검증 체계 구축 - 검증 후 활용 e. 국제적으로 통용되는 방법으로 디지털 증거 조작
Service Request	서비스 요청에 대한 정책과 프로세스 수립 후 이행 a. 요청 수락 또는 거부에 관한 프로세스 b. 요청사항 조정에 대한 프로세스 c. 정확한 요청사항을 요구하기 위한 프로세스(조사의 목적) d. 디지털 포렌식 분석 작업의 공식적 동의에 대한 합의 프로세스 e. 요청 문서화 ※ 부록 L : 인터폴의 디지털 포렌식 조사 요구사항 양식
Evidence Handling	증거물(제출된 디지털 장비) 처리에 관한 정책 및 절차의 수립 a. 증거의 보존 b. 증거 라벨 표시 c. 증거 밀봉 d. 문서화 할 항목 유지관리 - 관리연속성 e. 분석되지 않은 증거 f. 증거의 확보 및 취급 간 주의사항 g. 저장 및 보존 ※ 부록 K 디지털 증거물 관리 양식
Forensic Result	a. 디지털 포렌식 결과를 보증할 기술 기록 유지 - 기록에는 프로세스를 수행한 검사자와 날짜를 표기해야 하며, 이전 기록의 수정사항이 반드시 추적되어야 함. b. 디지털 포렌식 결과에 대한 기술적(검증), 행정적 검토 수행 c. 요청자에 제공 전 포렌식 결과의 승인(내부검토) d. 디지털 포렌식 보고서에 대한 일반적인 형식 준수 ※부록 J: 디지털 포렌식 보고서의 공통 요구사항 양식(보고서 표준) e. 분석자의 의견진술 시 보고서에 명확하게 표기 f. 보고서를 수정하기 위한 절차 수립

* ISO 17025: 실험기관(laboratory, 시설) 운영 및
업무 절차 관련 국제 표준 중 일부

분 야		필 수 항 목
가. 조직구조	시설의 법적 실체	분석 시설의 공식적 등록 - 법률적으로 책임질 수 있는 조직인지 여부
	시험 활동의 수행 책임	자체에규 또는 가이드라인을 통해 처벌 조항 명시
	경영진	관리자(개인정보보호 책임자)의 실체 및 책임 사항 문서화
나. 자원	인적분야 (분석 담당자)	분석 담당자(개인정보처리자) 적격성 요구사항에 대한 문서화 - 일반요건(학력, 경력, 교육, 자격, 훈련, 기술지식 등)
		개인별 책임 및 의무 문서화
		권한에 대한 교육 - (작업, 수행, 검증) 특정활동 수행인원 구분
	시설 및 환경	DB 시스템 구축
		(위탁 데이터 이력관리 시스템) 운영으로 계약 종료 시 데이터 파기 입증
	장비	분석장비, 소프트웨어의 구비
		분석장비, 소프트웨어 적정성 - 법정에서 신뢰받는 장비, 소프트웨어
		분석장비 취급 절차 및 주요장비 기록 유지
다. 프로세스	의뢰 및 계약의 검토	의뢰 및 계약의 검토 절차 수립 - 요건의 규정 및 문서화
		적합성 진술 및 의사결정 규칙 - 고객 요구에 따른 합/부 판정양식 문서화
		계약변경사항의 고지
		의뢰, 입찰, 계약의 검토 기록 유지
	결과의 유효성 보장	관리연속성을 위해 분석 간 모니터링 - 사진, 영상, CCTV
		동일하거나 다른 방법을 사용한 반복 시험 또는 교정과 비교
		보고된 기존 결과와의 상관관계 비교 및 검토
		결과의 검토 및 승인 - 권한있는 인원에 의한 의견 및 해석과 문서화
	데이터 및 정보관리 통제	데이터 및 정보 접근성 구분 - 직원별 비밀취급인가 분류
		정보관리 시스템 이용 권한과 책임 문서화 - 관리자, 책임자

3) 디지털포렌식산업 육성 및 지원에 관한 법률안(2022.09.20)

> 디지털포렌식 산업 육청 추진을 위해 과학기술정보통신부장관(이하 과기정통부 장관)은 3년마다 디지털포렌식 산업 육성 기본 계획을 수립하고 실행 + 매년 해당 계획에 따라 실행 계획을 시행의 의무
국무총리 소속으로 디지털포렌식산업 육성위원회를 만들어 중요사항을 심의하고 과기정통부 장관은 디지털포렌식산업의 기술 개발을 위해 기술협력 및 인력, 정보 교류 사업을 추진의 의무 (안 제5조부터 8조까지)

> 디지털 포렌식산업육성을 위해 국가에선 사업자의 관리와 처벌을 통해 국민에게 믿음과 수준 높은 서비스를 지원하여야 한다. 이를 위해 디지털포렌식사업자는 과기정통부장관의 허가를 받아야 하고, 결격이 있을 시 해당 사업을 할 수 없다 (안 제9조 및 제10조)

3) 디지털포렌식산업 육성 및 지원에 관한 법률안(2022.09.20)

> 과기정통부 장관은 디지털포렌식 사업자가 부정한 방법으로 허가를 받거나 개인정보 보호 관련 법령을 위반할 경우, 허가를 취소하거나 영업 정지를 명할 수 있다 (안 제12조). 국가 및 지방자치단체는 재정 지원, 조세 감면, 창업 지원 등을 통해 디지털포렌식산업의 육성을 돕는다 (안 제13조부터 제 16조)

> 디지털포렌식산업의 기반을 조성하기 위해 국가에서 주도적으로 사업을 실시하는 법안을 제시하였다. 과기정통부장관은 디지털포렌식 산업의 육성을 위해 관계 중앙행정기관의 장과 협의하여 국내외 표준의 조사·연구·개발 등 표준화 사업을 추진할 수 있도록 한다 (안 제17조)

> 또한 과기정통부장관은 디지털포렌식산업의 육성을 위하여 전문인력 양성 교육프로그램의 개발 및 보급, 양성기관 지원 등 전문인력의 양성에 힘써야 한다 (안 제18조)

3) 디지털포렌식산업 육성 및 지원에 관한 법률안(2022.09.20)

> 과학기술정보통신부장관은 디지털포렌식산업의 육성 정책의 수립·시행에 필요한 기초 자료를 확보하기 위하여 디지털포렌식산업 실태조사를 매년 실시하고, 그 결과를 공개해야 한다 (안 제19조)

!해당 법안의 문제점!

1. “디지털포렌식”이 현행 정보보호산업의 진흥에 관한 법률1)(이하 “정보보호산업법”이라 한다) 의 “정보보호” 의미에 포함되므로 중복 입법의 우려
2. 산업 활성화 측면에서 과도한 진입장벽의 우려

4) 디지털 포렌식에서 정보유출을 규정하는 법령(1)

> 디지털 증거의 수집은 수사목적을 달성하는데 필요한 최소한의 범위에서 이루어져야 하며, 「형사소송법」 등 관계 법령에 따른 적법절차를 준수하여야 한다. (디지털 증거의 처리 등에 관한 규칙 제 9조).

> 전자정보를 압수 · 수색 · 검증할 경우에는 피의자 또는 변호인, 소유자, 소지자, 보관자의 참여를 보장하여야 한다(디지털 증거의 처리 등에 관한 규칙 제 13조).

4) 디지털 포렌식에서 정보유출을 규정하는 법령(2)

> 개인정보처리자는 개인정보가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적 · 관리적 및 물리적 조치를 하여야 한다.(개인정보보호법 제29조) -> 암호화 프로그램 사용

> 증거분석관은 분석을 의뢰한 경찰관에게 분석결과물을 회신한 때에는 해당 분석과정에서 생성된 전자정보를 지체 없이 삭제 · 폐기하여야 한다 (디지털 증거의 처리 등에 한 관한 규칙 제 35조 전자정보의 삭제 · 폐기).

4) 디지털 포렌식 사설 업체에 위탁된 데이터 보호 방안에 관한 연구 (1)

1. 블록체인 기반

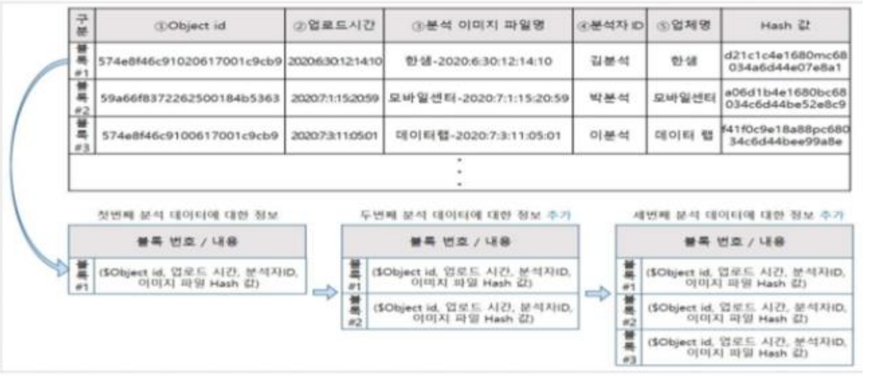
* 퍼블릭 블록체인이란?

인터넷을 통해 참여한 사용자 모두에게 공개되며 함께 운용되는 거래장부,
따라서 누구나 블록체인 상의 데이터를 읽고, 쓰고, 검증할 수 있으며
데이터 조작 또한 불가 -> 무결성 보장

* 시나리오

1) 분석 대상의 데이터를 이미징 한 파일에 object id[19]와 upload 시간, 분석 이미지 파일명, 분석자 ID, 업체명, 이미지 파일의 해시값을
산출
2) 해당 값들을 블록체인의 블록에 저장
3) 분석 대상이 추가될 때마다 이전 블록에 새로운 블록이 연결되기 때문에 분석 데이터에 대한 이력 저장

블록체인을 사용하여
위탁된 데이터의 분석을 개시하고,
이 담당자가 누구인지 식별하여
책임을 부여하는 목적



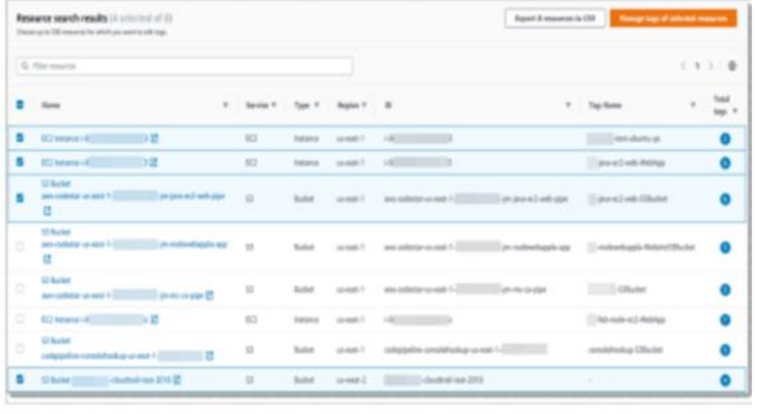
〈Figure 1〉 Blockchain-based consigned data history management system

4) 디지털 포렌식 사설 업체에 위탁된 데이터 보호 방안에 관한 연구 (2)

2. 클라우드 기반

* 시나리오

1) 사설 업체에게 수정 권한을 제외한 읽기, 쓰기 권한만을 부여하고 클라우드 상의 DB에 분석 기기에 대한 정보를 등록
2) 이후 읽기, 쓰기를 시도할 때마다 태그 기록을 남김



데이터 처리에 대한 이력을 태그 기록으로 남길 시

개인정보 처리자와 책임자가 각자의 책임을 이행하므로 최종적으로 데이터의 파기까지 입증이 가능

2) 시나리오

시나리오 1

중소기업에서 기술 유출이 되서 포렌식 의뢰

사설 포렌식 업체에서 2차 유출

시나리오 2

중소기업의 기술관리자가
개인 기기 포렌식 의뢰

사설 포렌식 업체에서 개인정보 유출

1) 관련 개념

* 마스킹(masking)이란?

last_name	first_name	ssn	gender	state
Smith	Bob	123-45-6789	M	CA
Doe	Jane	098-76-5432	F	PA
King	Stephen	888-67-5309	M	WI
Savage	Randal;	135-24-6789	M	FL
Downer	Debbie	918-55-4680	F	NC

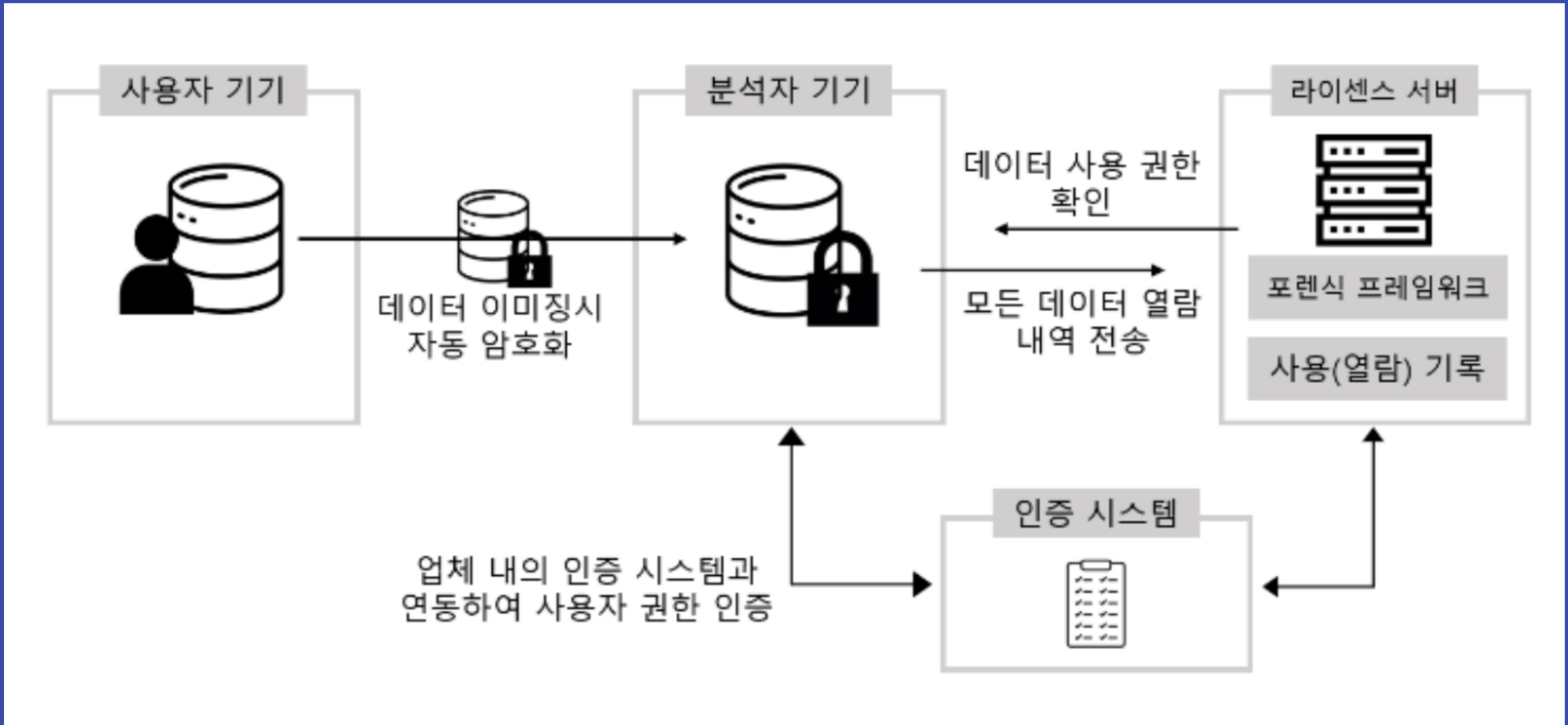
→

last_name	first_name	ssn	gender	state
Smith	Bob	xxx-xx-xxxx	M	CA
Doe	Jane	xxx-xx-xxxx	F	PA
King	Stephen	xxx-xx-xxxx	M	WI
Savage	Randy	xxx-xx-xxxx	M	FL
Downer	Debbie	xxx-xx-xxxx	F	NC

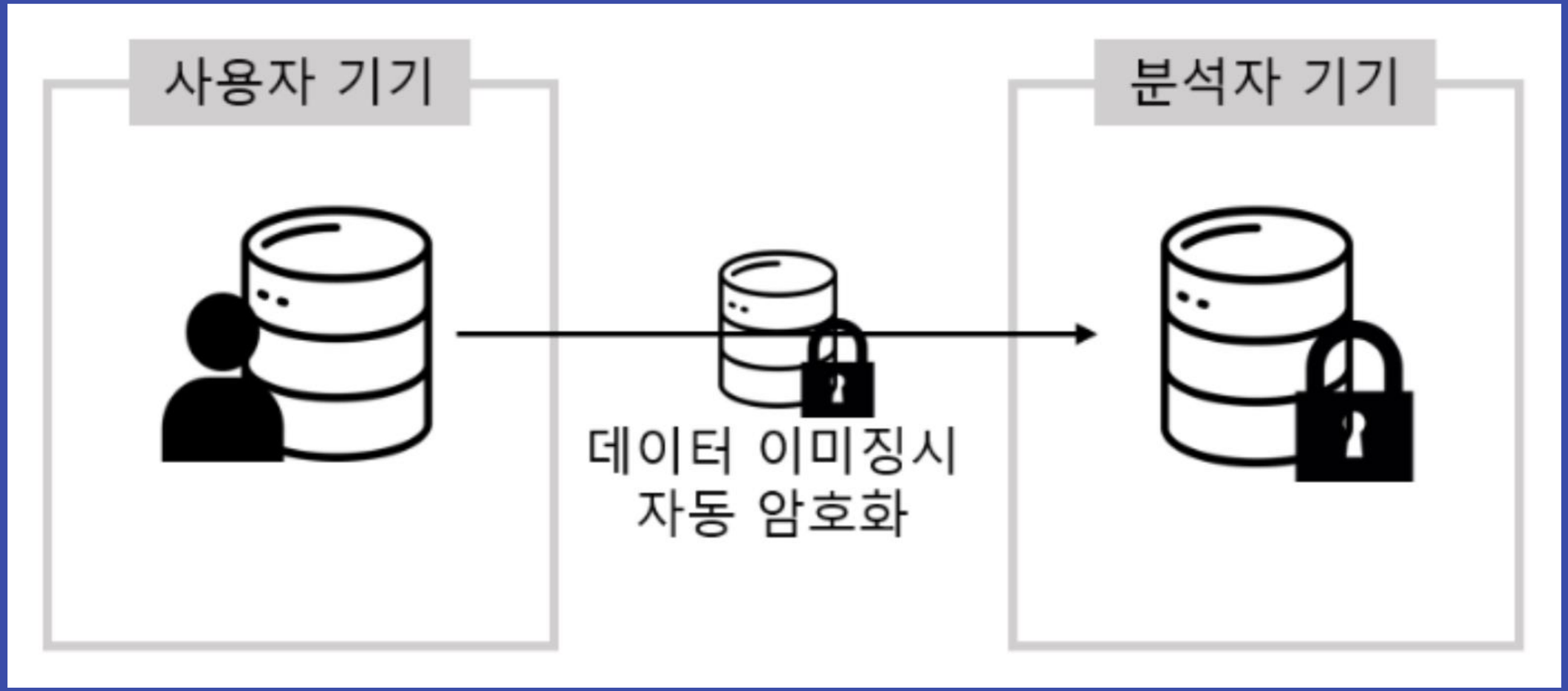
* 워터마킹(watermarking)이란?

* 제어 알고리즘이란?

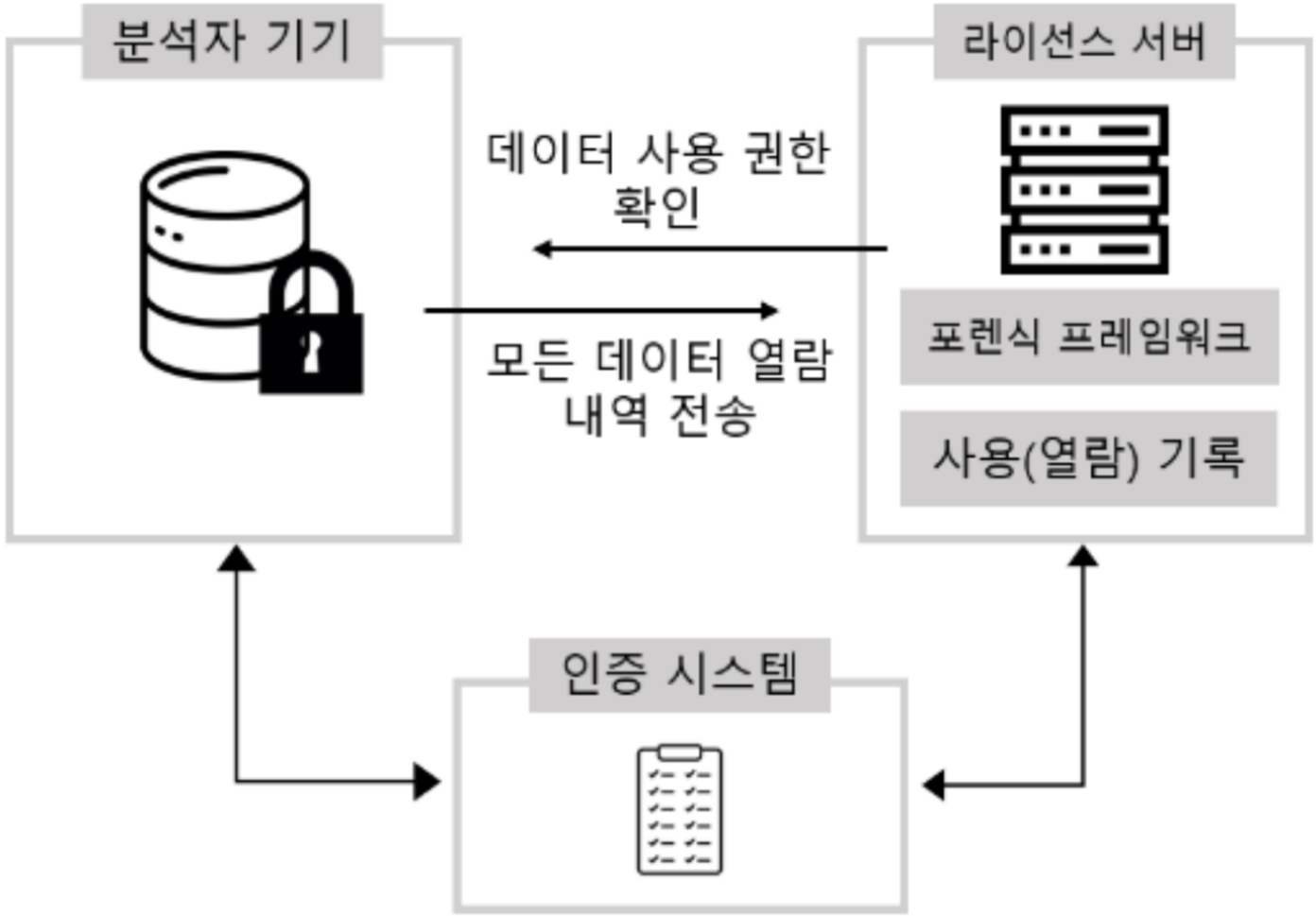
3) 아이디어_전체 플로우


사용자 기기
분석자 기기
라이센스 서버
데이터 사용 권한
확인
데이터 이미징시
자동 암호화
모든 데이터 열람
내역 전송
포렌식 프레임워크
사용(열람) 기록
인증 시스템
업체 내의 인증 시스템과
연동하여 사용자 권한 인증

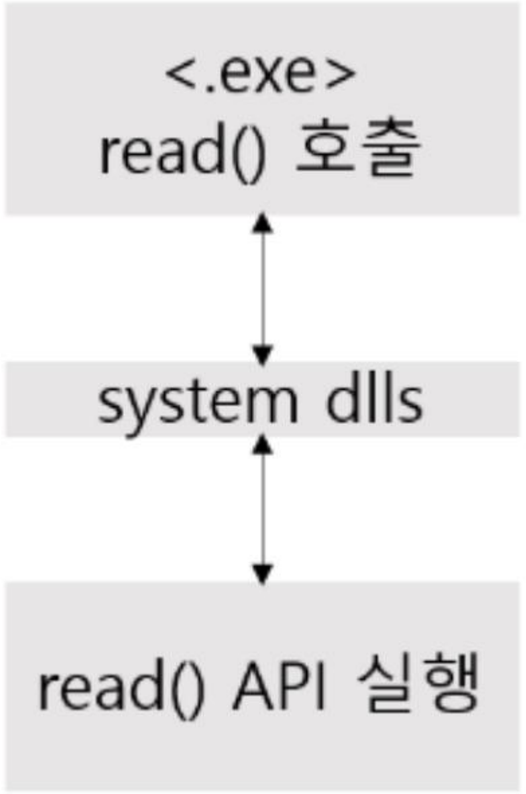
4) 아이디어_(1)이미징



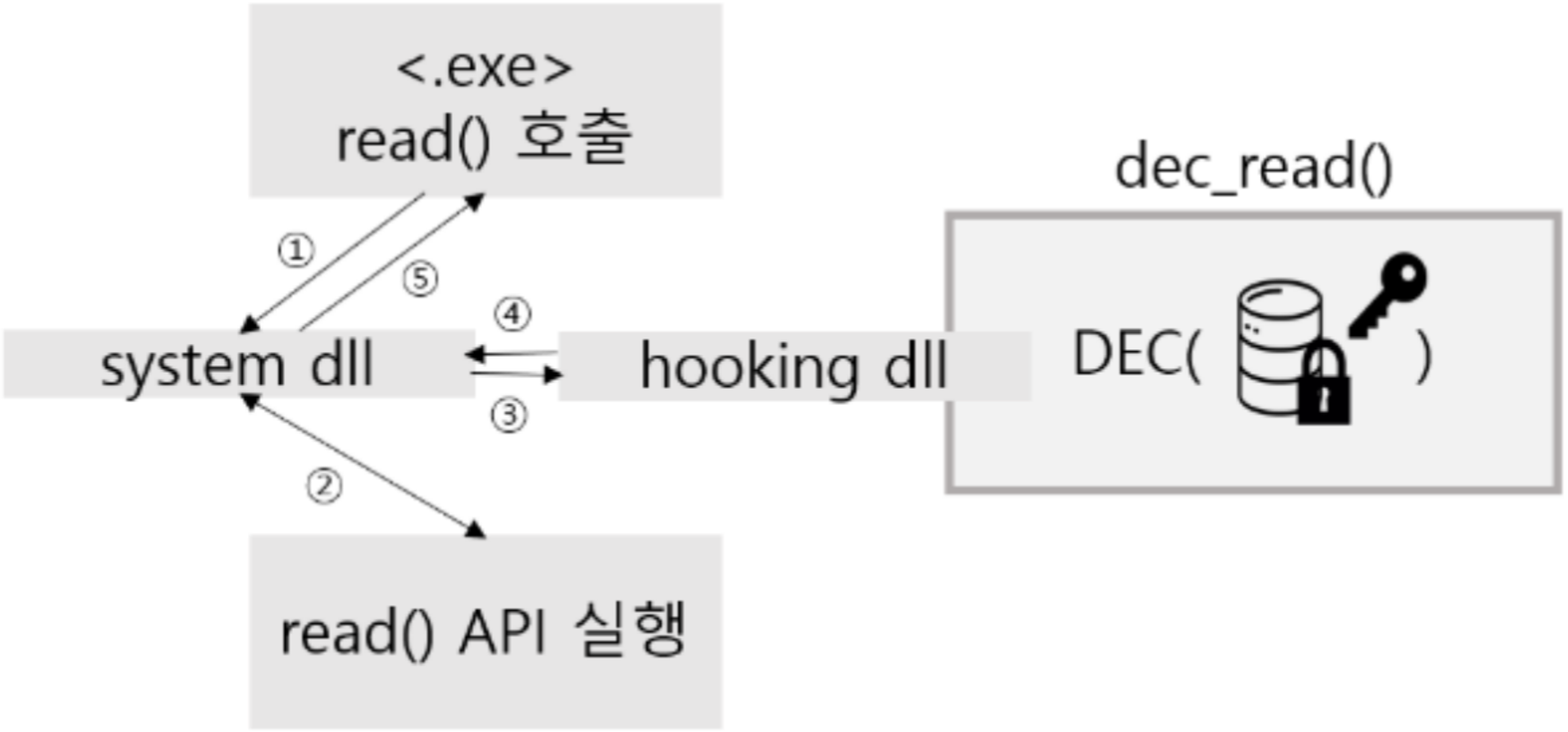
5) 아이디어_(2) 인증 및 접근



6) 아이디어_(2) 제어 알고리즘



정상적인 프로세스



제안하는 제어 알고리즘의 프로세스

7) 법률적 제안 내용

01 처벌 강화 ▶ 정보 유출 시 강한 처벌 (개인정보보호법 제 59조, 영업기밀보호법 참고)

02 요구 조건 강화 ▶ 디지털 포렌식 업체를 개업하거나 운영할 시 최소한의 요구조건 필요

03 중앙 집중 관리 시스템 ▶ 국가에서 직접 민간 디지털 포렌식 업체 관리 - 업체별로 고유 번호 부여 > 민간 디지털 업체는 이를 의무적으로 포렌식 할 때 워터마크로 삽입함으로써 정보 유출 시 추적 가능

Thank you!

발표 들어주셔서 감사합니다 :)