

nCipher Security Webinar

조직 내 기밀 데이터 보호를 위해 충분한 노력을 하고 계십니까?



2020 글로벌 암호화 동향 보고서

6,400명이 넘는

다양한 업계 내 데이터 보안 전문가를 대상으로

17개국 및 지역 내 설문 조사 실시

최신 동향과 직관적인 정보를 확인해보세요.

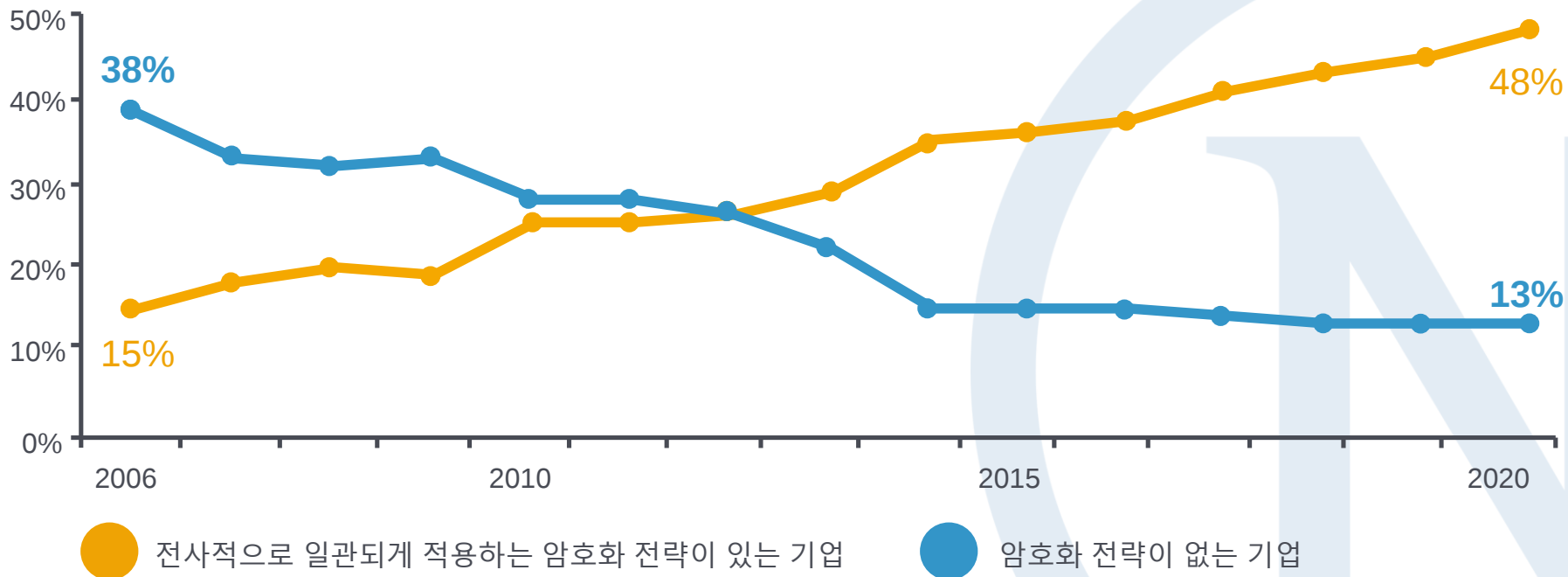


새롭게 떠오른 암호화 활용 동력 1위, 개인 정보.

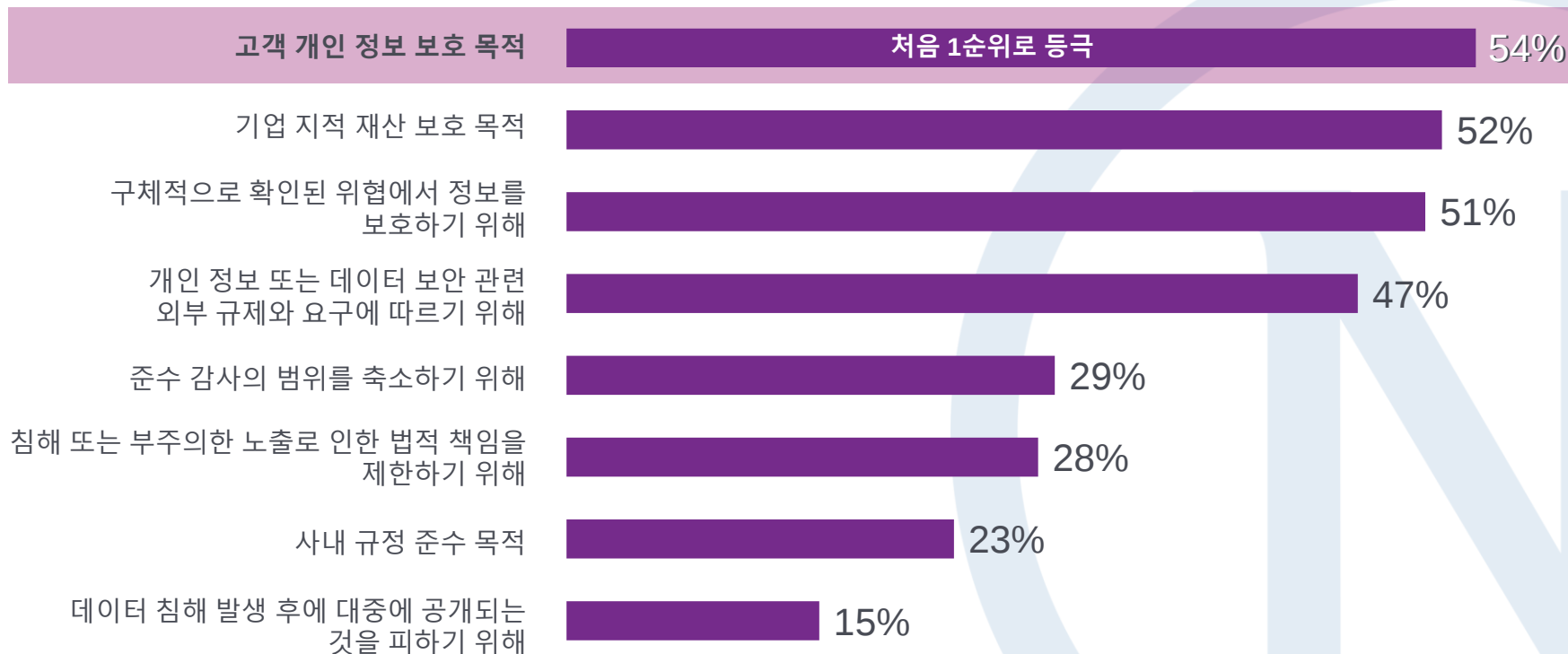
조사 결과, 단순히 규정을 준수하기 위함이 아니라, 고객 개인 정보를 보호하고자 하는 목적으로 암호화를 활용한다는 사실이 처음으로 밝혀졌습니다.

당사 연구는 다양한 선도 기업이 암호화 전략을 어떻게 적용하는지에 주목했으며, 무엇보다 빠르게 성장하는 활용 사례를 자세하고 직관적인 방법으로 제시합니다.

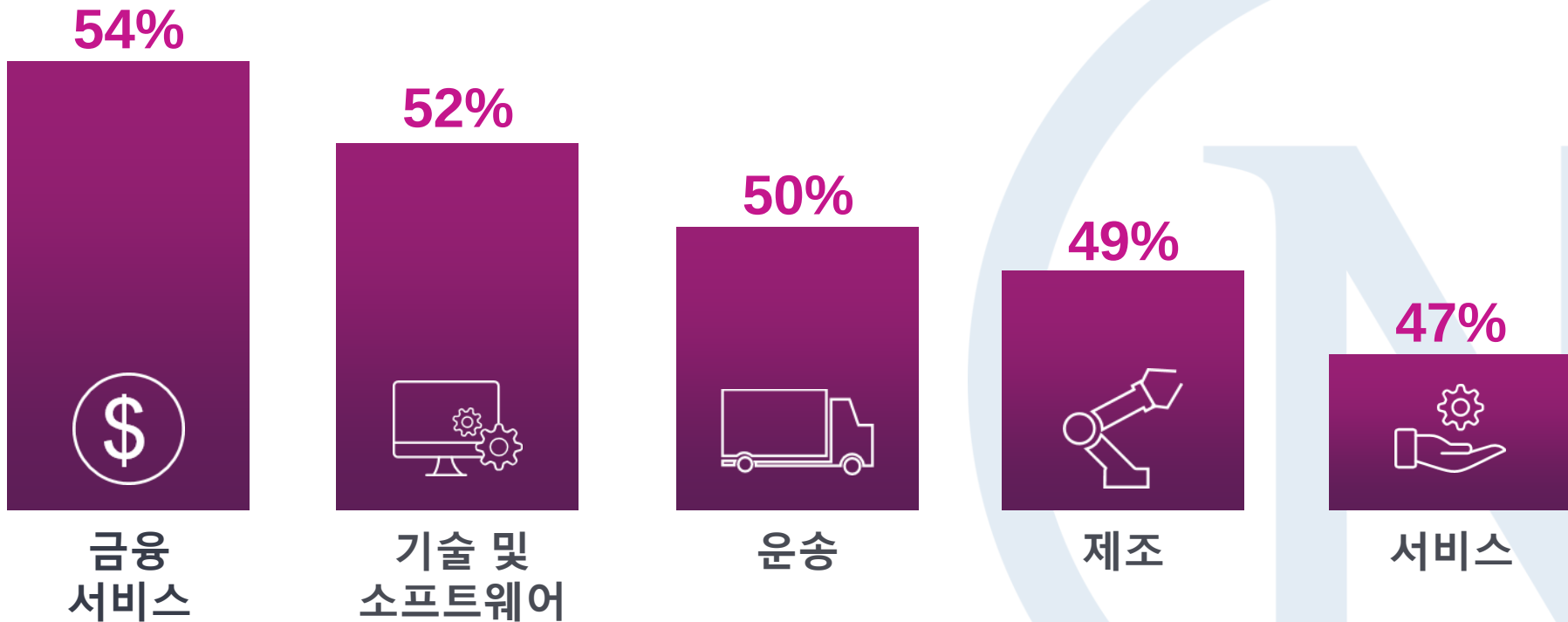
지난 15년간의 암호화 전략 추이



암호화 기술을 사용하는 주요 사유



암호화를 가장 많이 활용하는 대표 산업 분야 5가지



중요 데이터를 가장 크게 위협하는 요인

54%



직원의 과실

31%



시스템 또는
프로세스 오류

29%



해커

23%



임시직 또는
계약직 직원

20%



불순한
내부자

글로벌 암호화 동향 보고서

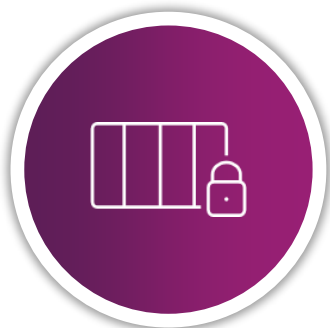
암호화로 선도하는 디지털 이니셔티브

디지털 이니셔티브 – 산업 전반에 이루어지고 있는 디지털 전환



가장 크게 증가한 암호화 활용 사례

클라우드



지난 3년간
컨테이너 암호화 18%
증가



지난 4년간
공공 클라우드 서비스
암호화 활용
21% 증가

IoT



지난 2년간
IoT 기기
암호화 11% 증가



지난
2년간 IoT 플랫폼,
데이터 저장소 암호화
12% 증가

가장 중요한 클라우드 암호화 기능 5가지

암호키 관리 표준인 KMIP 지원

67%

SIEM 통합과 로그 시각화 및 분석

62%

세분화된 액세스 컨트롤

60%

암호키 사용을 확인하는 감사 로그

55%

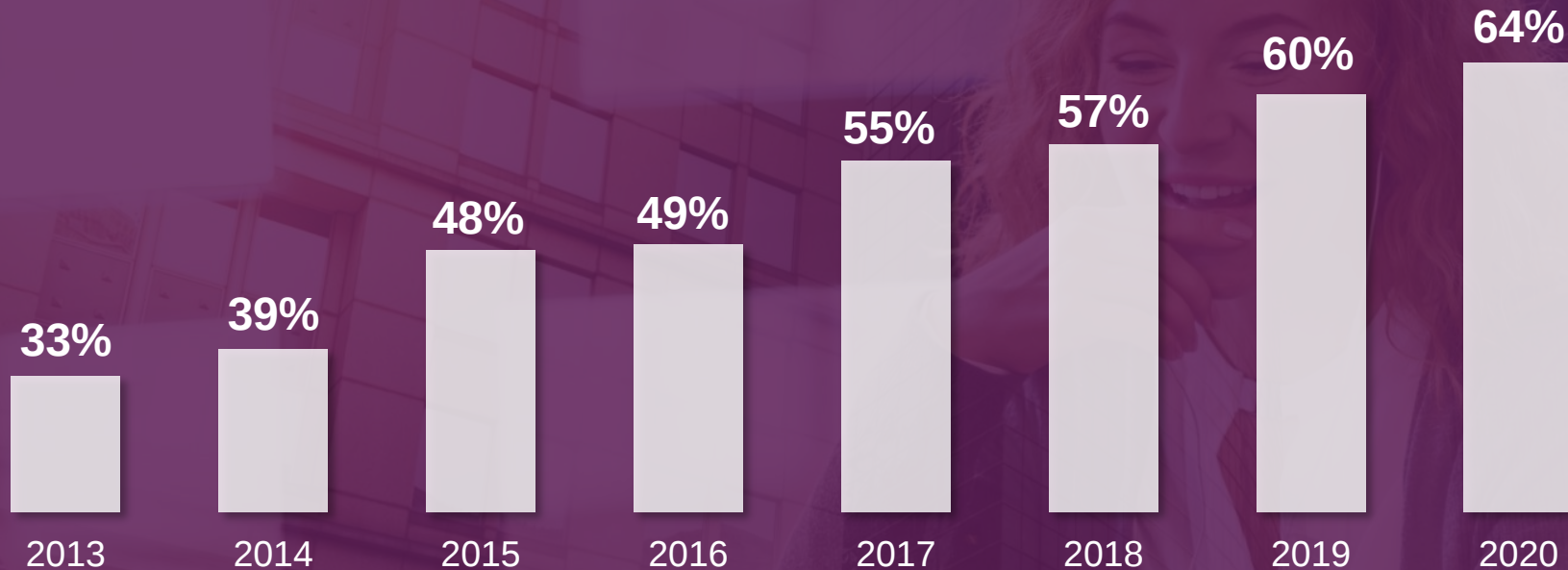
권한 계정 이용자 액세스 컨트롤

50%

글로벌 암호화 동향 보고서

하드웨어 보안 모듈(HSM)의 기능

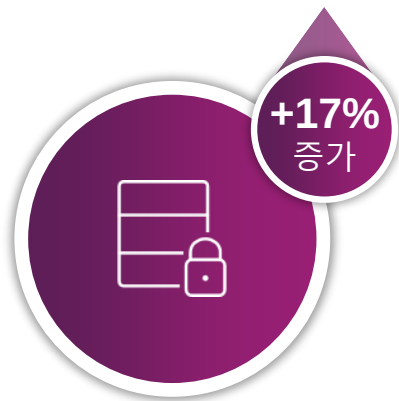
암호화 및 암호키 관리 영역에서 확대되는 하드웨어 보안 모듈(HSM)의 영향력



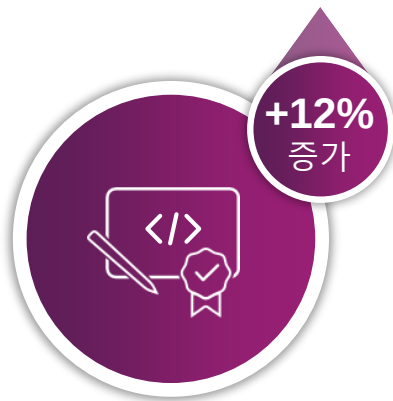
2020년 HSM의 주요 활용 사례 10가지



2016년 이후로 가장 크게 증가한 HSM 활용 사례



빅데이터 암호화



코드 서명



IoT 신뢰점
(Root of Trust)

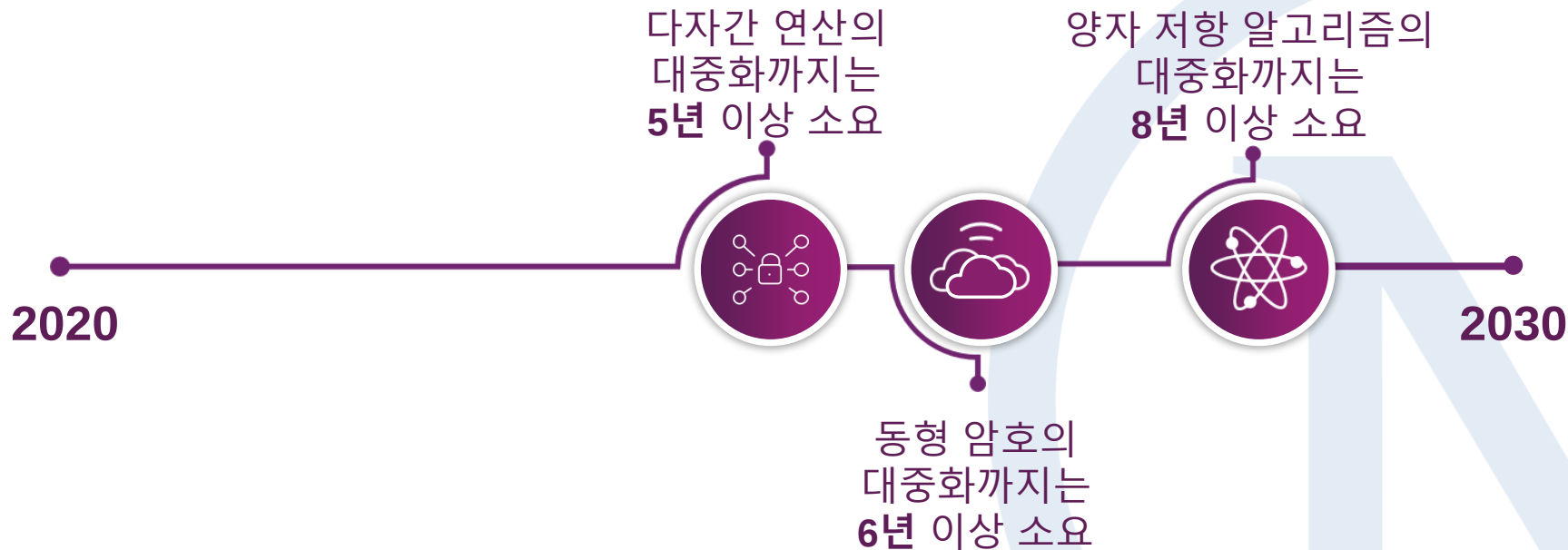


전자 문서 서명

글로벌 암호화 동향 보고서

암호화의 미래

최신 암호화 기술은 언제 대중화될 것인가? 기업의 예상시기



국내 개인정보 보호 최신 이슈

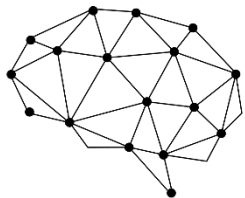
데이터 경제와 개인정보 보호



데이터 경제 정책 브리핑



공공 빅데이터 사업 협약



Cambridge
Analytica

캠브리지 애널리티카 社



글로벌 SNS 업체와 대통령의 스캔들

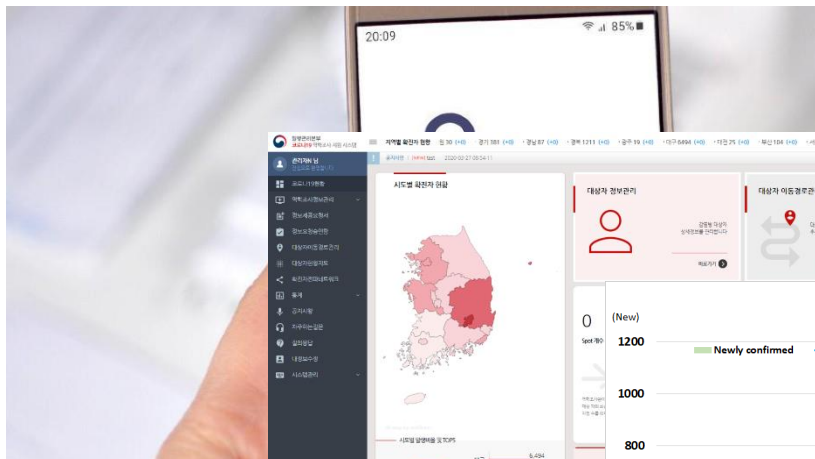


안면인식과 개인정보



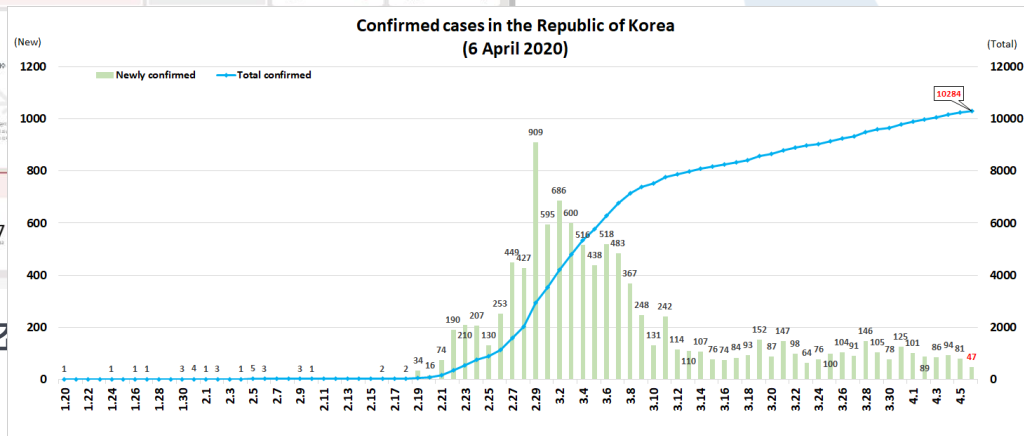
최고의 기술을 가진
sensetime 社

개인정보의 바람직한 활용 사례



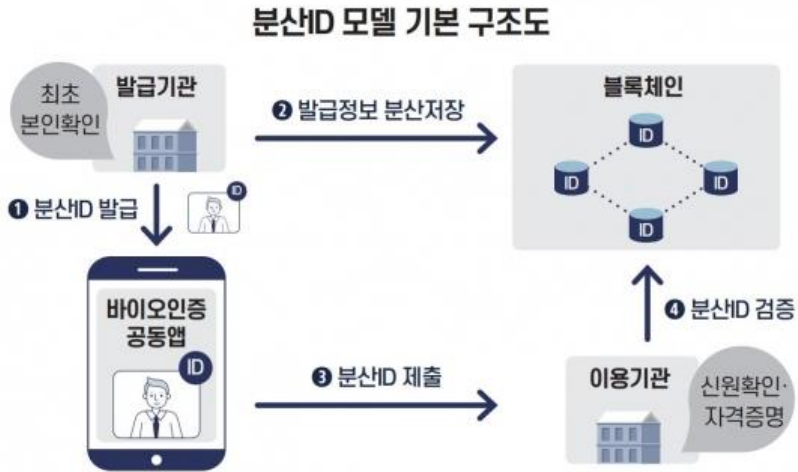
국

역학조

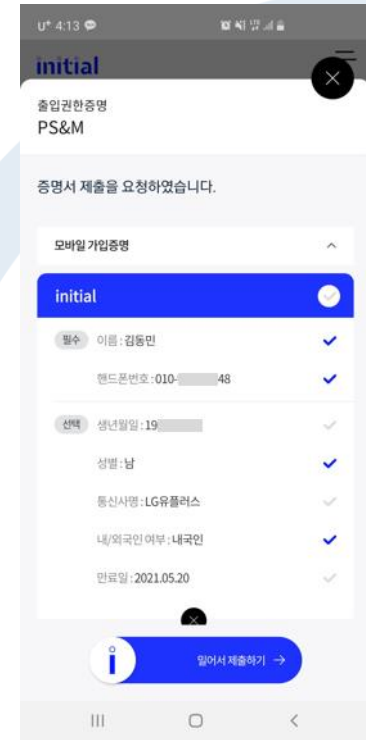


국내 개인정보 보호 최신 이슈

DID (Decentralized Identity / 탈중앙화 신원증명)

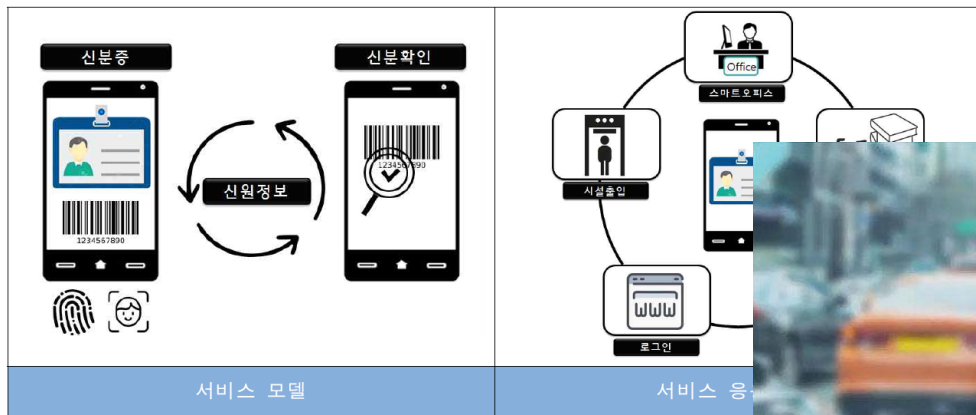


‘분산ID 모델의 실명확인 서비스’ (자료: 금융결제원)



이니셜 App

실제 적용되는 DID 기술



행안부 “블록체인 기반 모바일 신분증 서비스

□ (단기목표) 안정성 및 신뢰성 확보를 통한 단계적 확대

○ 공무원증, 장애인증, 운전면허증 등 신분증 시범사업 추진

- 신분증의 디지털화에 대한 다양한 사회적 우려를 해소하기 위해 공무원증, 장애인증 등 소규모 신분증을 대상으로 안정성 검증 후 단계적으로 확대 추진



모바일 운전면허증 화면 (자료 : SBS)

실제 적용되는 DID 기술

< 2020년 블록체인 공공선도 시범사업 선정 과제 >

분야	제안기관	과제명	컨소시엄명
치안	경찰청	블록체인 기반 디지털 증거 관리 플랫폼 구축	이노트리, ㈜마크애니
농업	농촌진흥청	블록체인 기반 노지작물 생산·유통 관리 플랫폼 구축	㈜이지팜
사회안전망	보건복지부	블록체인 기반 복지급여 중복수급 관리 플랫폼 구축	데일리블록체인, 메타빌드(주), ㈜매직에코
식품안전	식품의약품안전처	블록체인 기반 식품안전 데이터플랫폼 구축	㈜LGCNS, ㈜블루시스, ㈜솔리데오시스템즈
의료	강원도	블록체인 기반 강원도형 만성질환 통합 관리 플랫폼 구축	아이콘루프, ㈜유비플러스, 이드웨어
인증	경상남도	분산신원증명(DID) 기반 지역공공 서비스 플랫폼 구축	라온시큐어(주), ㈜에드뱅크
교통	세종특별자치시	블록체인 기반 자율주행자동차 신뢰 플랫폼 구축	㈜LGCNS, ㈜언맨드솔루션, 라온화이트햇(주), 라온시큐어(주)
	한국도로공사	블록체인 기반 상호신뢰 통행료 정산 플랫폼 구축	㈜핑거, 하나은행
환경	부산광역시	블록체인 기반 상수도 스마트 수질 관리 시스템 구축	㈜인텔리코드, 아이에스테크놀로지, ㈜코드박스
	제주특별자치도 (다년도)	블록체인 기반 전기차 배터리 Life Cycle 관리시스템 구축	㈜LGCNS, ㈜인포마인드, ㈜대은, ㈜민테크

DID

DID

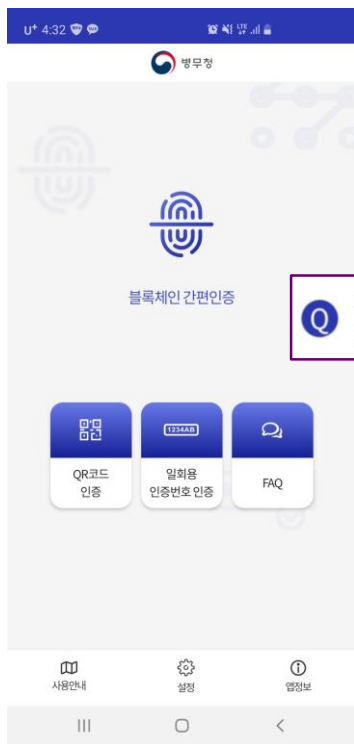
DID

DID

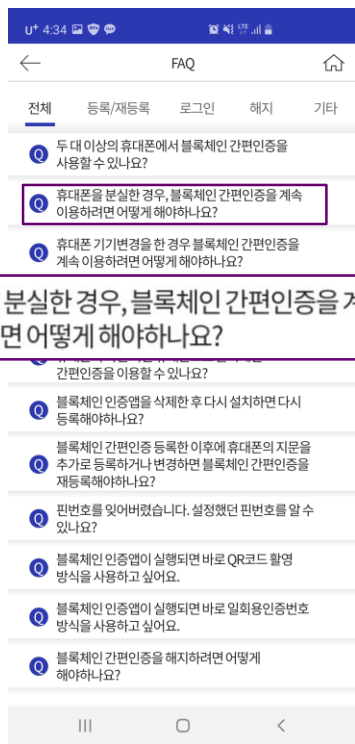
DID

자료 : 과학기술부

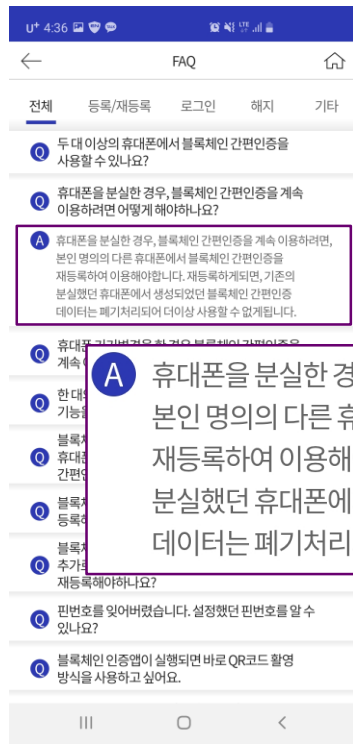
블록체인이 대비해야 할 단말기(개인키) 분실



병무청 블록체인
간편인증 App



FAQ



A 휴대폰을 분실한 경우, 블록체인 간편인증을 계속 이용하려면, 본인 명의의 다른 휴대폰에서 블록체인 간편인증을 재등록하여 이용해야 합니다. 재등록하게 되면, 기존의 분실했던 휴대폰에서 생성되었던 블록체인 간편인증 데이터는 폐기처리되어 더이상 사용할 수 없게 됩니다.

블록체인이 대비해야 할 단말기(개인키) 분실

아이디로그인

아이디

비밀번호

로그인

회원가입

아이디찾기

비밀번호찾기

휴대전화인증 로그인

휴대전화인증 로그인

휴대전화인증으로 로그인을 하시려면 먼저 회원가입 후 휴대전화 번호를 등록하셔야 합니다.

일반적인 회원정보 찾기 절차

고객	customer		
논리 이름*	물리 이름*	데이터 타입	널 허용
🔑 고객번호	customer_UID	NUMBER	N-N
● 아이디	customer_id	VARCHAR2(20)	NULL
● 비밀번호	customer_pw	VARCHAR2(20)	NULL
● 이름	customer_name	VARCHAR2(20)	NULL
● 전화번호	customer_tel	NUMBER	NULL

고객정보 테이블

Kevin 사용 이력

아이디	Log
Kevin	1번 아이템 구매
Kevin	3번 아이템 구매
Kevin	1번 아이템 사용

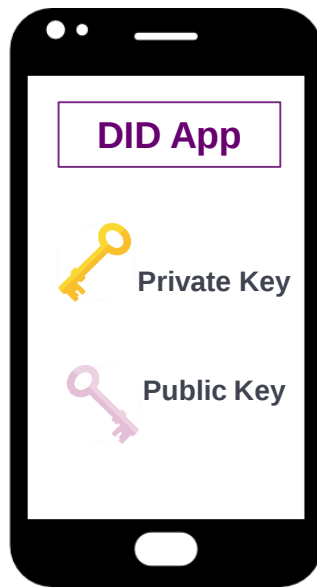
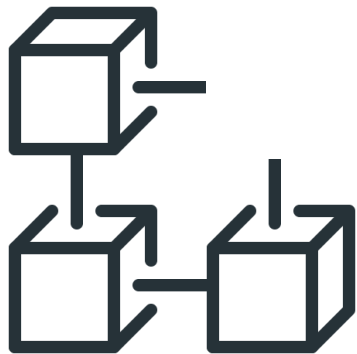
David 사용 이력

아이디	Log
David	5번 아이템 구매
David	7번 아이템 구매
David	7번 아이템 사용

통합 사용 이력

고객번호	아이디	Log
000001	Kevin	1번 아이템 구매
000001	Kevin	3번 아이템 구매
000001	Kevin	1번 아이템 사용
000001	David	5번 아이템 구매
000001	David	7번 아이템 구매
000001	David	7번 아이템 사용

블록체인이 대비해야 할 단말기(개인키) 분실



신원인증 요청



인증 확인

신원
인증기관

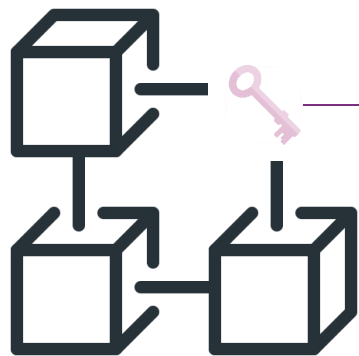
분산ID 발급 요청



발급 승인

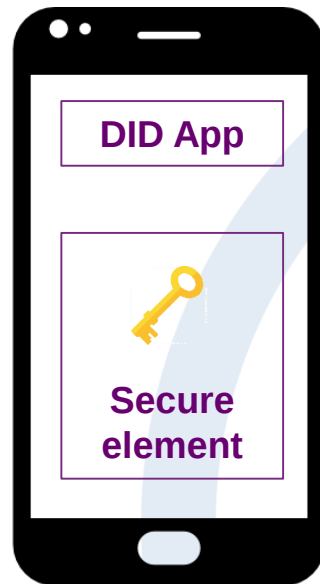
DID
발급기관

블록체인이 대비해야 할 단말기(개인키) 분실



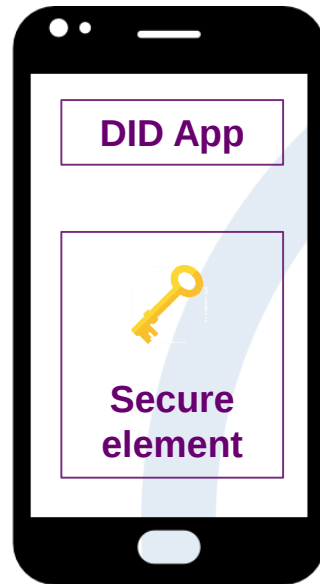
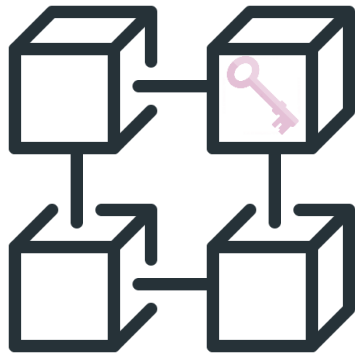
 Private Key

 Public Key

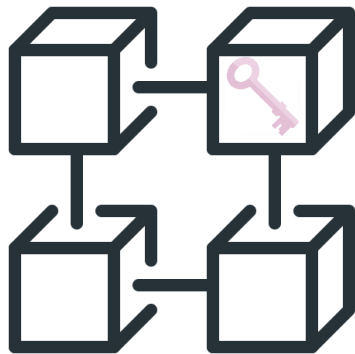


Public Key	Log
12345678	1번 아이템 구매
12345678	3번 아이템 구매
12345678	1번 아이템 사용

블록체인이 대비해야 할 단말기(개인키) 분실



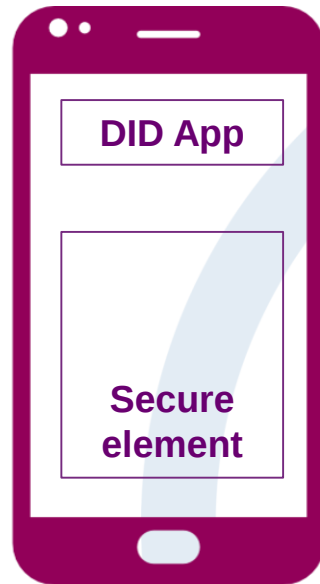
블록체인이 대비해야 할 단말기(개인키) 분실



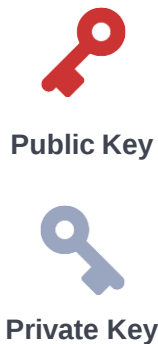
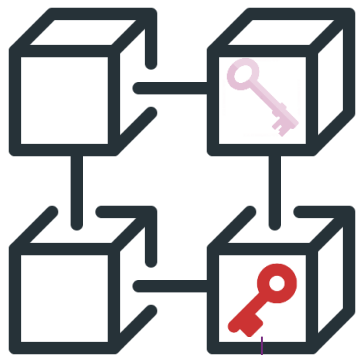
Public Key



Private Key



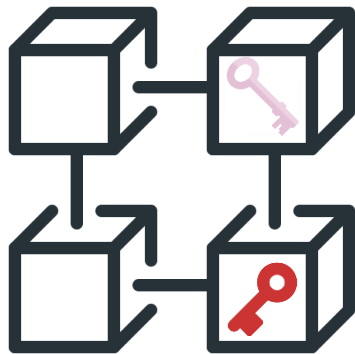
블록체인이 대비해야 할 단말기(개인키) 분실



Public Key	Log
12345678	1번 아이템 구매
12345678	3번 아이템 구매 ✗
12345678	1번 아이템 사용

Public Key	Log
abcdefgh	5번 아이템 구매
abcdefgh	7번 아이템 구매
abcdefgh	7번 아이템 사용

블록체인이 대비해야 할 단말기(개인키) 분실



Bitcoin Address



SHARE

19PXg2Ljftt9hRj4R9xYjprS5w43ZhreSB

Private Key



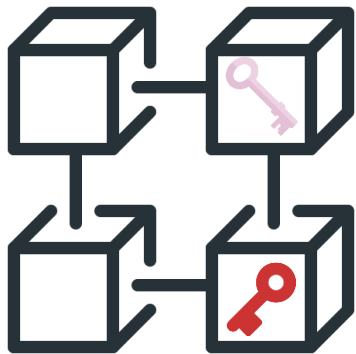
SECRET

KxJ1XNGePRvbnfp1qFHGHCVtXF8662NnbVvkn6EgGtYt6Xzh9yPY



Key 를 종이에 인쇄하여 안전한 금고에 보관

블록체인이 대비해야 할 단말기(개인키) 분실

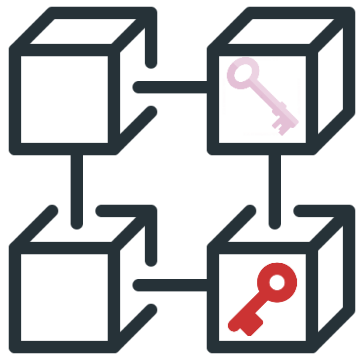


- | | | | |
|----|----------------|-----|----------------|
| 1. | <i>army</i> | 7. | <i>garbage</i> |
| 2. | <i>van</i> | 8. | <i>claim</i> |
| 3. | <i>defense</i> | 9. | <i>echo</i> |
| 4. | <i>carry</i> | 10. | <i>media</i> |
| 5. | <i>jealous</i> | 11. | <i>make</i> |
| 6. | <i>true</i> | 12. | <i>crunch</i> |

12개의 단어를 순서대로 입력하여 복원 (니모닉)



블록체인이 대비해야 할 단말기(개인키) 분실



신원
인증기관

Secure Channel 백업

HSM (Hardware Security Module)



X 50,000,000

국내 개인정보 보호 최신 이슈

데이터 3법 (개인정보 보호법·정보통신망법·신용정보법)

I 데이터 경제 3법

자료: 각 부처

법률명	소관부처	규제완화 주요내용
개인정보보호법	행정안전부	- 가명정보를 상업적 목적으로 활용 가능 - 개인정보 관리 개인정보보호위원회로 일원화
신용정보법	금융위원회	- 가명정보 금융분야 빅데이터 분석 및 이용 가능 - 가명정보 주체 동의없이 이용 및 제공 허용
정보통신망법	과학기술정보통신부 방송통신위원회	- 온라인상 개인정보보호 규제 감독 권한 개인정보보호 위원회로 변경

데이터 경제 3법 (자료: 대한금융신문)

개인정보 비식별화의 필요성

- 1. 31. (금) 신종코로나바이러스감염증 확진

○ 장O순 (58세, 화성시 오산동 거주, 자영업, 김O동의 母)

- 1. 19. (일) 김O동 화성시 자택 방문

- 1. 21. (화) 김O동의 기침, 미열 증상으로 화성시보건소 방문 후 능동감시자 분류

- 1. 22. (수) ~ 1. 30. (목) 능동감시 이상 없음

- 1. 30. (목) 김O동 발열 발생 / 화성시보건소 방문

- 1. 31. (금) 신종코로나바이러스감염증 확진

□ 향후 계획

○ **경찰, 확진자 '개인정보' 공개**

○ 접촉자 확인 점검결과 보고(2. 1.)

강북 #6 (남, 93년생)	5/10	이태원 클럽 방문	가족 3명 (음성, 자가격리 중)	서울의료원
- 5월 7일(목) 10:05~11:00 출근 마스크 착용 버스, 지하철 - 5월 7일(목) 11:00~21:30 타구 소재 직장 마스크 착용 - 5월 7일(목) 21:30~23:24 퇴근/자택 도착(수유2동) 마스크 착용 버스, 지하철 - 5월 8일(금) 10:06~11:00 출근 마스크 착용 버스, 지하철				

강북 #5	3/12	해외접촉 (필리핀)	가족 2명 (음성, 격리해제)	퇴원(완치)
중앙방역대책본부 지침에(2020.4.12.)의거 공개기간 이후의 공개정보 삭제 ※ 공개기간 : 확진자가 마지막 접촉자와 접촉한 날로부터 14일				

개인정보

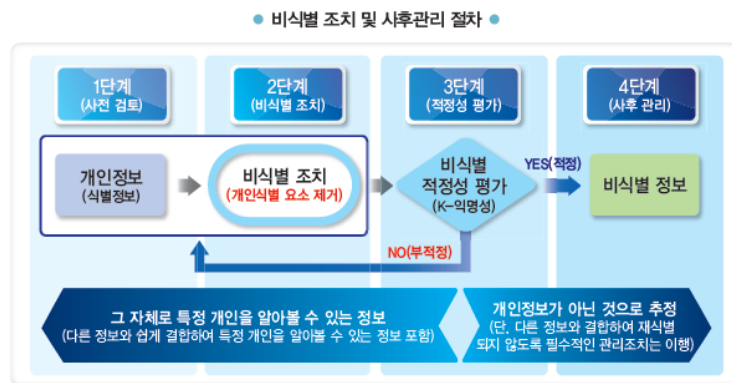
- 5월 10일(일) | 08:30~15:10 이송 전 자택 대기
 - 5월 10일(일) | 15:10~16:00 서울의료원 이송 | 119 구급차
 - 5월 10일(일) | 16:00 서울의료원 격리병상 입원
- ※ 역학조사 결과에 따라 강북구접촉자는 모두 검사하였고 자택 및 주변 일대 방역 소독도 완료하였습니다.

COVID-19 확진자 동선 공개 사이트

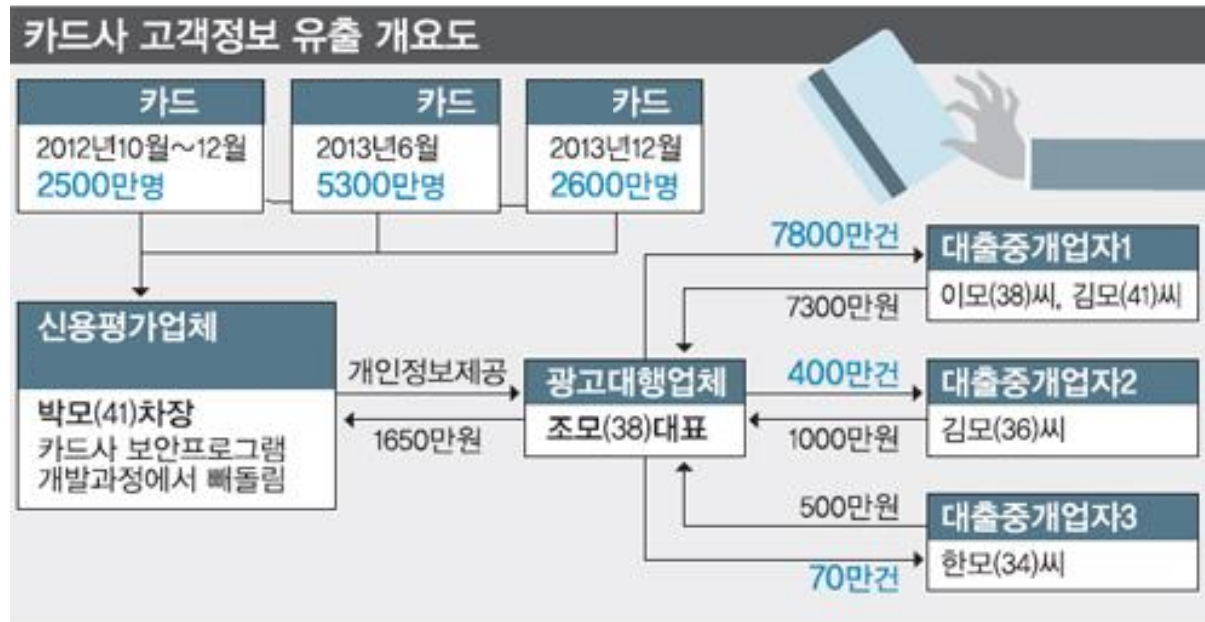
개인정보 비식별화 방법

● < 예시 > 비식별 조치 방법 ●		
처리기법	예시	세부기술
가명처리 (Pseudonymization)	● 홍길동, 35세, 서울 거주, 한국대 재학 → 임꺽정, 30대, 서울 거주, 국제대 재학	① 휴리스틱 가명화 ② 암호화 ③ 교환 방법
총계처리 (Aggregation)	● 임꺽정 180cm, 홍길동 170cm, 이공위 160cm, 김말위 150cm → 물리학과 학생 키 합 : 660cm, 평균키 165cm	④ 총계처리 ⑤ 부분총계 ⑥ 라운딩 ⑦ 재배열
데이터 삭제 (Data Reduction)	● 주민등록번호 901206-1234567 → 90년대 생, 남자 ● 개인과 관련된 날짜정보(합격일 등)는 연단위로 처리	⑧ 식별자 삭제 ⑨ 식별자 부분삭제 ⑩ 레코드 삭제 ⑪ 식별요소 전부삭제
데이터 범주화 (Data Suppression)	● 홍길동, 35세 → 홍씨, 30~40세	⑫ 감추기 ⑬ 랜덤 라운딩 ⑭ 범위 방법 ⑮ 제어 라운딩
데이터 마스킹 (Data Masking)	● 홍길동, 35세, 서울 거주, 한국대 재학 → 홍○○, 35세, 서울 거주, ○○대학 재학	⑯ 임의 잠음 추가 ⑰ 공백과 대체

개인정보 비식별 조치 방법
(자료 : 개인정보 비식별 조치 가이드)



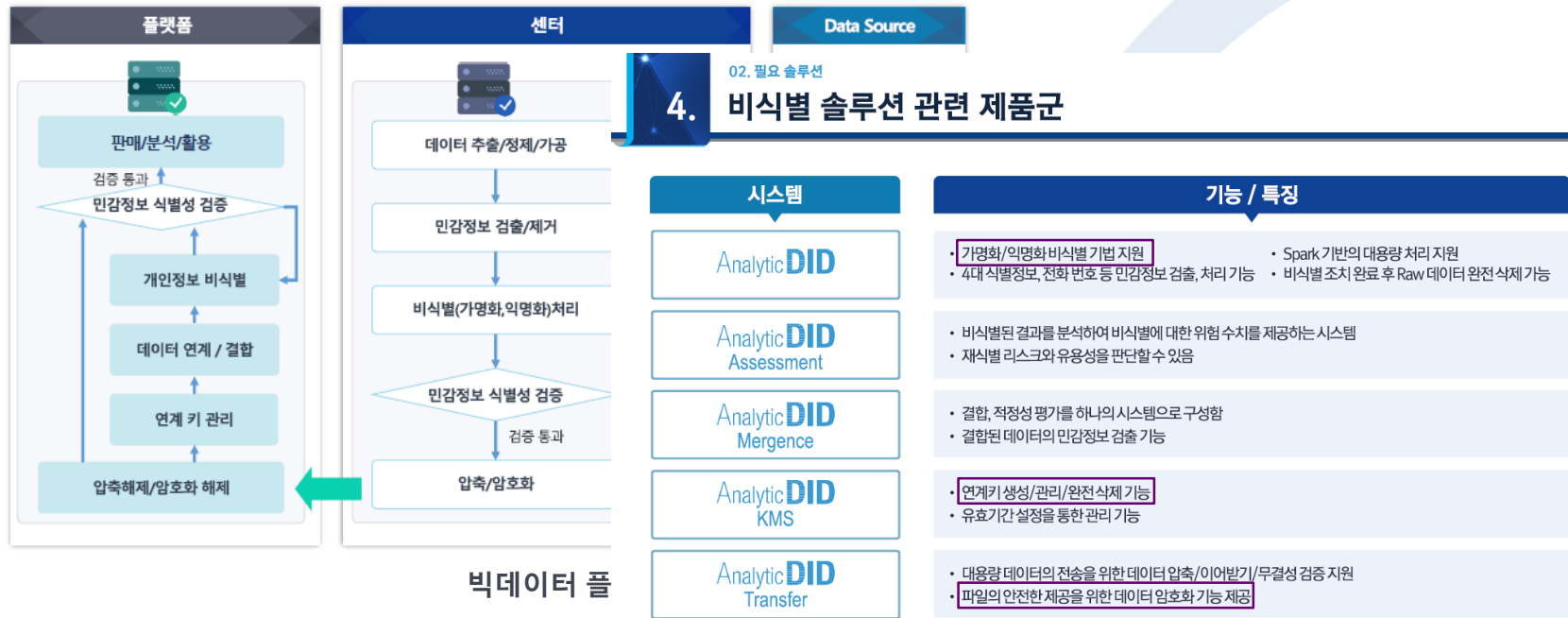
개인정보 비식별 조치 및 사후관리 절차



2013년 카드사 개인정보 유출 사고 (자료 : 세계일보)

II. 사례

빅데이터플랫폼 구축사례



비식별 솔루션 관련 제품군 (자료:Fasoo)

비식별 정보의 공개와 재식별 시 제재

② 암호화(Encryption)

- 정보 가공시 일정한 규칙의 알고리즘을 적용하여 암호화함으로써 개인정보를 대체하는 방법, 통상적으로 다시 복호가 가능하도록 복호화 키(key)를 가지고 있어서 이에 대한 보안방안도 필요
- 일방향 암호화(one-way encryption 또는 hash)를 사용하는 경우는 이론상 복호화가 원천적으로 불가능
 - ※ 일방향 암호화는 개인정보의 식별성을 완전히 제거하는 것으로, 양방향 암호화에 비해 더욱 안전하고 효과적인 비식별 기술에 해당
- 적용정보 : 주민등록번호, 여권번호, 의료보험번호, 외국인등록번호, 사용자 ID, 신용카드번호, 생체정보 등

나. (비식별 정보의 활용) 비식별 정보는 개인정보가 아닌 정보로 추정되므로 정보주체로부터의 별도 동의없이 해당 정보를 이용하거나 제3자에게 제공할 수 있습니다.

- 다만, 개인정보가 아닌 것으로 추정되더라도 불특정 다수에게 공개되는 경우에는 다른 정보를 보유하고 있는 누군가에 의해 해당 정보주체가 식별될 가능성이 있으므로 비식별 정보의 공개는 원칙적으로 금지됩니다.

2 재식별 시 제재

가. 비식별 정보를 재식별하여 이용하거나 제3자에게 제공한 경우에는 개인정보의 목적 외 이용·제공에 해당하여 5년 이하의 징역 또는 5천만원 이하의 벌금형에 처해집니다 (개인정보 보호법 제18조제1항 위반, 정보통신망법 제24조 및 제24조의2 위반, 신용정보법 제32조 및 제33조 위반)

※ 정보통신망법 적용 사업자는 위반행위 관련 매출액의 3% 이하 과징금이 추가 부과될 수 있음

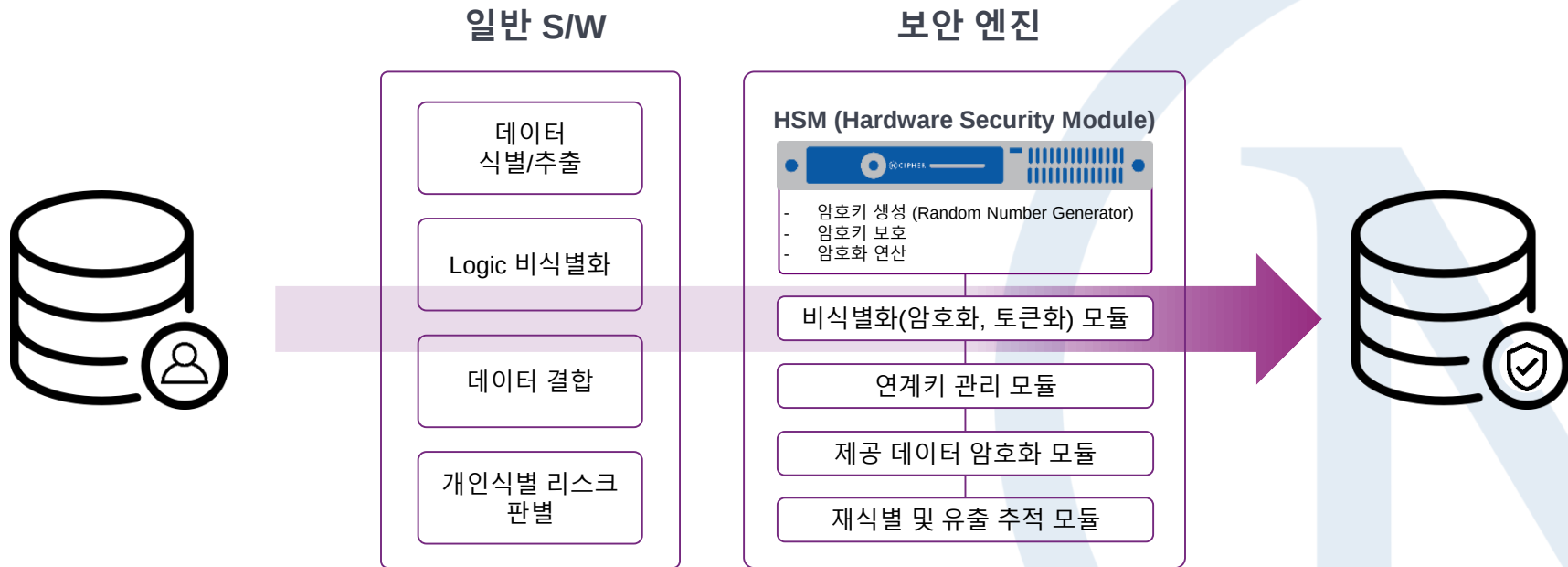
- 예를 들어, 비식별 정보를 제3자에게 제공하면서 비식별 조치 요령을 공유하거나 공개되어 있는 알고리즘으로 암호화하여 쉽게 복호화될 수 있도록 정보를 제공하는 경우 등이 이에 해당 할 수 있습니다.

나. 비식별 정보를 처리하는 자(비식별 정보를 제공받은 자 포함)가 해당 정보를 이용하는 과정에서 재식별하게 된 경우에는 해당 정보를 즉시 처리중지하고 파기하여야 합니다.

- 추가적 비식별 조치없이 재식별된 정보를 보관하는 경우 5천만원 이하의 과태료가 부과됩니다 (개인정보 보호법 제15조 제1항 위반, 정보통신망법 제22조제1항 위반, 신용정보법 제15조 제2항 위반)

※ 정보통신망법 적용 사업자는 5년 이하 징역 또는 5천만원 이하 벌금형에 처해지며, 위반행위 관련 매출액의 3% 이하 과징금이 추가 부과될 수 있음

개인정보 비식별화 시스템 구성





AN ENTRUST DATACARD COMPANY