



2021 ISACA Korea & Barun ICT Research Conference

- The MyData Era of Audit, Control & Governance



- 일시 : 2021년 12월 3일 (금) 09:00 ~ 16:10
- 장소 : Virtual Conference (Zoom)
- 주최: (사)한국정보시스템감사통제협회, 연세대학교 바른ICT연구소, 정보대학원
- 후원: (주)씨에이에스

기술에 가치를 더 해주는 회사



(주)씨에이에스(C·A·S)

Computer Assurance Services



IT 감리·감사 보증 서비스

- 씨에이에스(C·A·S)는 1995년 국내 최초 설립된 정보시스템 감리법인
- '감리 그이상의 서비스' ICT Audit·Assurance 서비스 분야 글로벌 리더 그룹
- ABCD(AI, Blockchain, Cloud, big Data)등 신기술과 SW보증 전문 서비스 기업

정보보호·개인정보 서비스

- 전문성과 독립성을 겸비한 정부지정 정보보호전문서비스 기업
- 개인정보 영향평가기관으로서 개인정보 통합 서비스 전문가 그룹
- 기반시설 취약점분석 및 모의해킹, 마이데이터 최고 수준 서비스 기업

IT컨설팅·데이터사업·GRC 솔루션 서비스

- PMO 및 ISP를 통한 디지털 전환을 선도하는 전문가 그룹
- 데이터기반 신기술로 고객에게 가치를 제공하는 기술법인
- ESGRC(환경,사회,거버넌스,리스크관리,컴플라이언스)솔루션 서비스



T. 02-786-3815
F. 02-2026-3818



<http://www.casit.co.kr>
webmaster@casit.co.kr



08507 서울시 금천구 가산디지털1로 168,
C동 1106호, 1206호 (가산동, 우림라이온스밸리)



(주)씨에이에스(C·A·S)
Computer Assurance Services

사회 : 김정중 (ISACA Korea 부회장)

시간	발표주제	발표자
09:00 ~ 09:30	Registration and Event Overview	
09:30 ~ 09:40	Welcome Remarks	김희영 (ISACA Korea 회장) 김범수 (바른ICT연구소 소장)
09:40 ~ 10:05	Keynote 1. UK General Data Protection Regulation Handling	David Rudd (ISACA UK Central England Chapter Committee Member)
10:05 ~ 10:30	Keynote 2. 마이데이터시대, 금융투자의 원칙과 전략	이남우 (연세대 국제대학원 객원교수)
10:30 ~ 10:50	Session 1. 금융 마이데이터와 데이터산업	성시호 (한국신용정보원 마이데이터지원센터 센터장)
10:50 ~ 11:10	Session 2. 데이터 3법 활용을 위한 개인정보보호정책 연구동향	복준영 (신구대학교 교수)
11:10 ~ 11:20	Break	
11:20 ~ 11:40	Session 3. Blockchain Essentials for Assurance	이동기 (EY한영회계법인 Director)
11:40 ~ 12:00	Session 4A. 악성댓글의 피해 규모 산정 방법 연구	김미예 (연세대학교 바른ICT연구소 연구교수)
	Session 4B. 자본시장 IT시스템 효율적 용량계획 모델	이국형 (한국거래소 IT전략부 과장)
12:00 ~ 14:00	Lunch	
14:00 ~ 14:30	APB Encore Session 1. Effective Data Protection and Security	
	The Importance of 'Smooth' Data Usage and the Protection of Privacy in the Age of AI, the IoT and Autonomous Robots	Fumio Shimo (Japan)
	Using Image Processing as Security Feature in Information Retrieval	Mohd Afizi bin Mohd Shukran (Malaysia)
14:30 ~ 15:00	APB Encore Session 2. COVID-19 and Responsible Use of Data	
	Contact tracing apps for self-quarantine in South Korea: Rethinking datafication and dataveillance in the COVID-19 age	Claire Seungeun Lee (USA)
	Data Privacy in the Philippines & COVID-19 response	Ivin Ronald D.M. Alzona (Philippines)
15:00 ~ 15:30	APB Encore Session 3. Data Governance Across Borders	
	Accountable and Trusted Transborder Data Flows by Building Convergence	Zee Kin Yeong (Singapore)
	Global Personal Data Protection Regulatory Support Services by KISA	Jiyun Kim (Korea)
15:30 ~ 16:00	APB Encore Session 4. Data Breach and Responsible Policies	
	Promoting Comparability in Personal Data Breach Notification Reporting	Suguru Iwaya (OECD)
	Does a Data Breach Harm Industry Peers? Evidence From the U.S. Retail Industry	Jaeyoung Park (Korea)
16:00 ~ 16:10	Closing Remarks	

목차

<u>Keynote 1.</u>	UK General Data Protection Regulation Handling David Rudd (ISACA UK Central England Chapter Committee Member)	5
<u>Keynote 2.</u>	마이데이터시대, 금융투자의 원칙과 전략 이남우 (연세대학교 국제학대학원 객원교수)	12
<u>Session 1.</u>	금융 마이데이터와 데이터산업 성시호 (한국신용정보원 마이데이터지원센터 센터장)	26
<u>Session 2.</u>	데이터 3법 활용을 위한 개인정보보호정책 연구동향 복준영 (신구대학교 교수)	37
<u>Session 3.</u>	Blockchain Essentials for Assurance 이동기 (EY한영회계법인 Director)	45
<u>Session 4A.</u>	악성댓글의 피해 규모 산정 방법 연구 김미예 (연세대학교 바른ICT연구소 연구교수)	56
<u>Session 4B.</u>	자본시장 IT시스템 효율적 용량계획 모델 이국형 (한국거래소 IT전략부 과장)	65
<u>APB Encore Session 1A.</u>	The Importance of `Smooth` Data Usage and the Protection of Privacy in the Age of AI, the IoT and Autonomous Robots Fumio Shimpo (Japan)	73
<u>APB Encore Session 1B.</u>	Using Image Processing as Security Feature in Information Retrieval Mohd Afizi bin Mohd Shukran (Malaysia)	77
<u>APB Encore Session 2A.</u>	Contact tracing apps for self-quarantine in South Korea: Rethinking datafication and dataveillance in the COVID-19 age Claire Seungeun Lee (USA)	84
<u>APB Encore Session 2B.</u>	Data Privacy in the Philippines & COVID-19 response Ivin Ronald D.M. Alzona (Philippines)	99
<u>APB Encore Session 3A.</u>	Accountable and Trusted Transborder Data Flows by Building Convergence Zee Kin Yeong (Singapore)	107
<u>APB Encore Session 3B.</u>	Global Personal Data Protection Regulatory Support Services by KISA Jiyun Kim (Korea)	112
<u>APB Encore Session 4A.</u>	Promoting comparability in personal data breach notification reporting Suguru Iwaya (OECD)	123
<u>APB Encore Session 4B.</u>	Does a Data Breach Harm Industry Peers? Evidence From the U.S. Retail Industry Jaeyoung Park (Korea)	130

● Keynote 1

UK General Data Protection Regulation Handling



David Rudd

(ISACA UK Central England Chapter Committee Member)

발표개요

- What is GDPR in the UK?
- Is the GDPR part of UK law?
- Current UK GDPR Position
- What are the 7 principles of GDPR?
- Current UK ISACA Activity
- What does this mean for UK GDPR Compliance

이력

- UK Government HM Revenue & Customs
- Chapter Lead for Information Governance Special Interest Group and GDPR
- Have ISACA UK led engagement with UK Information Commissioners Office

2021 ISACA Korea & Barun ICT Research Conference

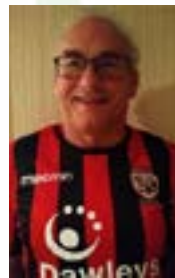
Midata in the UK and General Data Protection Regulation Handling

David Rudd | ISACA UK Central England Chapter

Confidential. For internal use only.



Biography and Role



- David Rudd
- Currently employed by UK Government Tax Authority
- ISACA CISA Certified since 2004
- ISACA UK Central England Chapter Committee Member
- Chapter Lead for Information Governance Special Interest Group covering GDPR
- Have led ISACA UK engagement with UK Information Commissioners Office (ICO)

Midata

- The overall aim of midata is to benefit the economy, by stimulating innovation and growth, as well as companies and consumers:
- **For the economy** - midata will encourage sustainable economic growth by boosting competition between companies in terms of value and service, and driving innovation.
- **For business** - midata will create opportunities for businesses through improved dialogue with consumers and increased trust, and the opportunity to provide innovative new personal information services and tools.
- **For consumers** - midata will allow consumers to access their data in a safe and secure way and make better decisions reflecting their personal wants and needs. New services made possible by midata will further assist consumers, whether it be in getting the best deal on their mobile phone contract or energy tariff, or managing their lives more efficiently.

The Midata vision of consumer empowerment

- the businesses, consumer bodies and regulators involved are all committed to working with Government to achieve its vision for midata, launched today. And all are endorsing the key principle that data should be released back to consumers.
- midata is a voluntary programme the Government is undertaking with industry, which over time will **give consumers increasing access to their personal data in a portable, electronic format.**
- Individuals will then be able to use this data to gain insights into their own behaviour, make more informed choices about products and services, and manage their lives more efficiently.

Who is involved in the UK

- Businesses and organisations that have so far committed to working in partnership with Government to achieve the midata vision are:
- Utility companies
- Credit and Loan agencies
- Banks
- Credit reference agencies
- Retailers

Midata Consumer Groups and Regulators

- The following consumer groups and regulators are working with midata to represent consumers' interests and concerns. As well as working towards potential benefits, their input plays an important role in identifying potential risks and helping determine how these can be addressed:
- Citizens Advice
- Communications Consumer Panel
- Consumer Focus
- **Information Commissioner's Office (ICO)**
- OFCOM
- Office of Fair Trading (OFT)

What is GDPR in the UK?

- The Data Protection Act 2018 is the **UK's implementation of the General Data Protection Regulation (GDPR)**. Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is: used fairly, lawfully and transparently.
- <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>

Is the GDPR part of UK law?

- The UK GDPR is the UK General Data Protection Regulation. It is a **UK law** which came into effect on 01 January 2021. It sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies.

What are the 7 principles of GDPR?

- The GDPR sets out seven principles for the lawful processing of personal data. Processing includes the
- Collection
- Organisation
- Structuring
- Storage
- Alteration
- Consultation
- Use, communication, combination, restriction, erasure or destruction of personal data.

Current UK GDPR Position

- ICO created Excel based toolkit to help businesses to self assess against the requirements of the UK GDPR legislation
- ISACA UK currently in consultation with ICO regarding legislative change
- Next steps involve direct ICO engagement
- Perception that many businesses struggle to meet GDPR requirements and report legislative breaches

Current UK ISACA Activity

- Set up round table events with external ISACA representatives
- ICO shared GDPR Evaluation toolkit and invited feedback
- Feedback received in writing and during round table events shared with ICO
- Revised toolkit produced and published by ICO

What does this mean for UK GDPR Compliance

- Greater understanding of how UK businesses can meet GDPR requirements
- Links into the ICO over consultation over UK legislative change
- Reduction in UK business GDPR breaches through improved data handling and risk assessment
- Greater UK business GDPR compliance
- UK businesses better placed to handle threats from AI and robotics

● Keynote 2

마이데이터시대, 금융투자의 원칙과 전략



이남우

(연세대학교 국제학대학원 객원교수)

발표개요

- 장기적인 기업가치 결정의 5가지 요소를 파악한 후 코리아 디스카운트 원인 및 애플과 삼성전자 시가총액이 5배나 차이 나는 이유를 분석해 본다.

이력

- 前 Merrill Lynch 한국 공동대표
- 前 Nomura HK 아시아 고객관리총괄대표

메타버스 시대 금융투자의 원칙과 전략

연세대학교 국제학대학원

이남우의 좋은주식연구소
이남우

2021.12

목차

- Introduction
- 주가를 결정하는 5가지 요소
- A small advice

이남우의 좋은주식연구소



반갑습니다!



- 연세대학교 국제학대학원 객원교수
- 메릴린치 한국 공동대표 및 Managing Director (싱가폴)
- 노무라 아태본부 고객관리 총괄 (홍콩)
- 삼성증권 초대 리서치센터장
- JP Morgan (홍콩), Vice President
- 저서: 좋은 주식 나쁜 주식
- 유튜브: 이남우의 좋은주식연구소



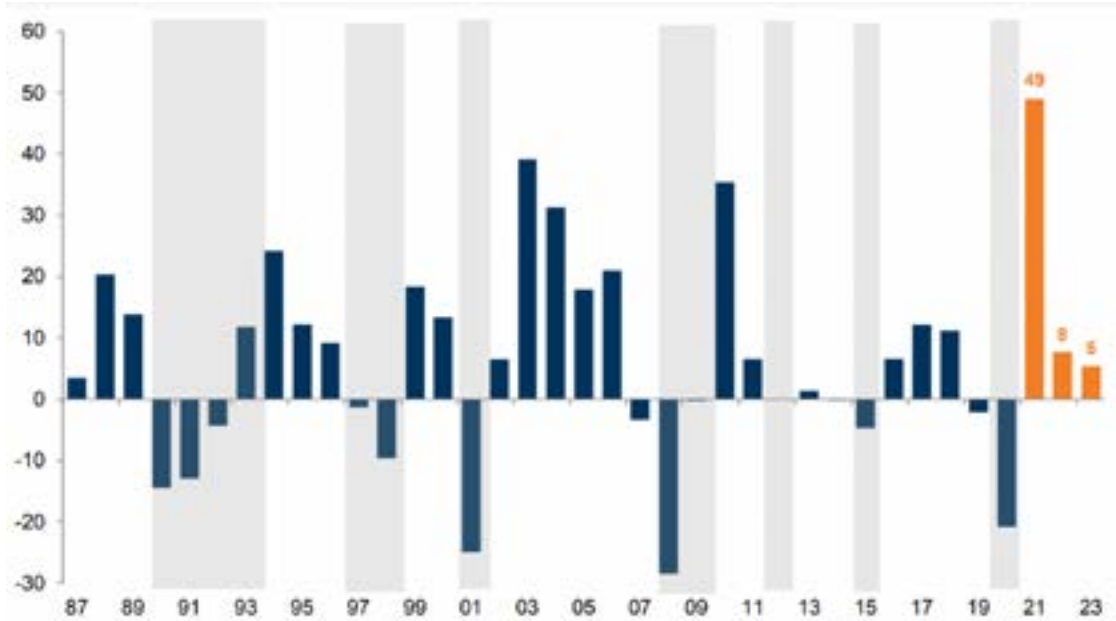
목차

- Introduction
- 주가를 결정하는 5가지 요소
 1. 이익성장률
 2. 배당과 자사주
 3. 재무구조
 4. 금리
 5. 거버넌스
- A small advice

이남우의 좋은주식연구소



전세계 이익증가율 22년 급격히 둔화 예상



Source: I/B/E/S, Datastream, Goldman Sachs Global Investment Research

자료: 골드만삭스

이남우의 좋은주식연구소



주식 매수는 상장사의 주인이 되는 것 'Fractional ownership'



이남우의 좋은주식연구소



미국 대기업 장기 수익성 추이 미국 증시 상승 핵심 요인

S&P 500 Profit Margin



이남우의 좋은주식연구소



업종별 성장성과 리스크 틀리다

표 2-12 MSCI(Morgan Stanley Capital International) ACWI(All Country World Index) 업종지수 연 상승률

	3년 평균	5년 평균	10년 평균
IT	24%	22%	18%
헬스케어	12%	7%	14%
경기 관련 소비재	10%	9%	14%
필수 소비재	5%	6%	10%
자동차 및 부품	6%	6%	8%
금융	-2%	4%	5%
전 세계 시장	7%	7%	10%

출처: MSCI

이남우의 좋은주식연구소



코스트코 (Costco): 효자 같은 주식



구독경제 모델
대표적 사례

출처: 2

$$\text{주식총수익률}(\%) = \text{주가변화율} + \text{배당수익률}^*$$

$$^*\text{배당수익률}(\%) = \frac{\text{지난 12개월간 받은 총 현금배당}}{\text{주가}}$$

이남우의 좋은주식연구소



안정 성장의 대명사: 10년간 주당순이익 연 12% 증가 + 2-3% 배당수익률



출처: 코스트코, 아우 파이낸스

이남우의 좋은주식연구소



주가 수준은 기업이익 성장률과 비례한다



출처: 야후 파이낸스

이남우의 좋은주식연구소



아마존: 확장성 있는 기업 주가 계속 오른다. 빅테크 중 제일 저평가!



출처: 아마존, 야후 파이낸스

이남우의 좋은주식연구소



아마존 장기 성장성 탁월함

표 3-7 아마존의 이익, 주가, PER

	매출액	영업이익	영업 현금흐름	주당 순이익	연평균 주가	연평균 PER
2010	342억 달러	14억 달러	35억 달러	2.53달러	137달러	54배
2011	481억 달러	9억 달러	39억 달러	1.37달러	201달러	147배
2012	611억 달러	7억 달러	42억 달러	-0.09달러	223달러	N/A
2013	745억 달러	7억 달러	55억 달러	0.59달러	296달러	502배
2014	890억 달러	2억 달러	70억 달러	-0.52달러	320달러	N/A
2015	1,070억 달러	22억 달러	119억 달러	1.25달러	485달러	388배
2016	1,360억 달러	42억 달러	172억 달러	4.90달러	699달러	143배
2017	1,779억 달러	41억 달러	184억 달러	6.15달러	960달러	156배
2018	2,329억 달러	124억 달러	307억 달러	20.14달러	1,567달러	79배
2019	2,805억 달러	145억 달러	385억 달러	23.01달러	1,780달러	77배
2020E*	3,725억 달러	189억 달러	495억 달러	34.90달러	2,682달러	77배
2021E**				48.60달러	3,257달러	67배
10년 평균 증가율	27%	30%	30%	34%	34%	

* 2020.12.31. 결산회계연도, 주당순이익 컨센서스 추정치
 ** 주가는 최근 주가, 주당순이익은 시장 컨센서스 추정치

이남우의 좋은주식연구소

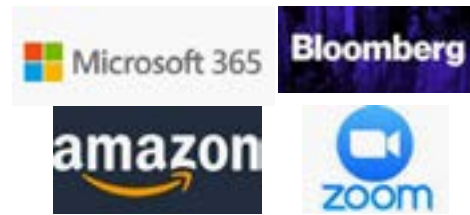

구독 경제: 21세기 소비 방식 Paradigm shift

- 물건을 “구매” “소유” 하는 것 아니고 일정 기간 “사용”에 대한 비용을 지불하는 개념.
 - 관련 상장사 높은 성장세 보이고 시장에서 프리미엄에 거래. “끈끈한 고객 관계”가 핵심.
 - Why? 시장은 불확실성 싫어함. 구독경제 모델은 미래 이익, 현금흐름 예측 가능성 높음.
- ⇒ 웅진코웨이가 3번이나 주인이 바뀐 이유. (MBK파트너스, 넷마블)
- ⇒ 방준혁의장 “신성장 동력 확보 위해 구독경제 1위인 코웨이 인수한다”

이남우의 좋은주식연구소


이남우 교수가 사용하는 구독경제 서비스

- 유튜브 (알파벳 지주사, 월간활성고객 2억명 이상)
- 넷플릭스 (가입자 2.1억명, 월13,500원)
- 신문 (온라인 국내 2개+해외 3개사)
- 블룸버그
- 마이크로소프트 365 (연 12만원, 가입자 2.5억명)
- 신용카드 (비자 11억명 회원, 마스타, 아멕스)
- 아마존 프라임 (2억명 이상 회원, 월13달러)
- 줌
- 쿠팡 (로켓와우 월 2,900원)
- 스타벅스
- 코스트코
- 우버 등등

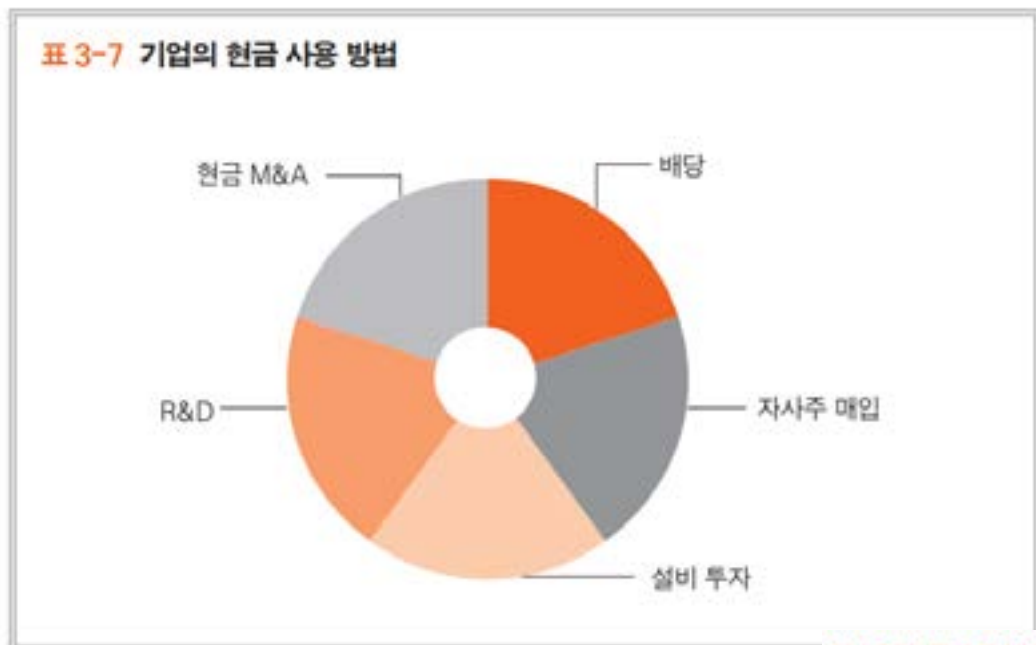


=> 디지털 구독서비스 중심

이남우의 좋은주식연구소



기업은 주주 위해 다양하게 현금 사용할 수 있다



이남우의 좋은주식연구소



전세계 시총 1위 애플의 주주친화 정책은 자사주 매입/소각이 핵심; 매년 80-90조원 소각

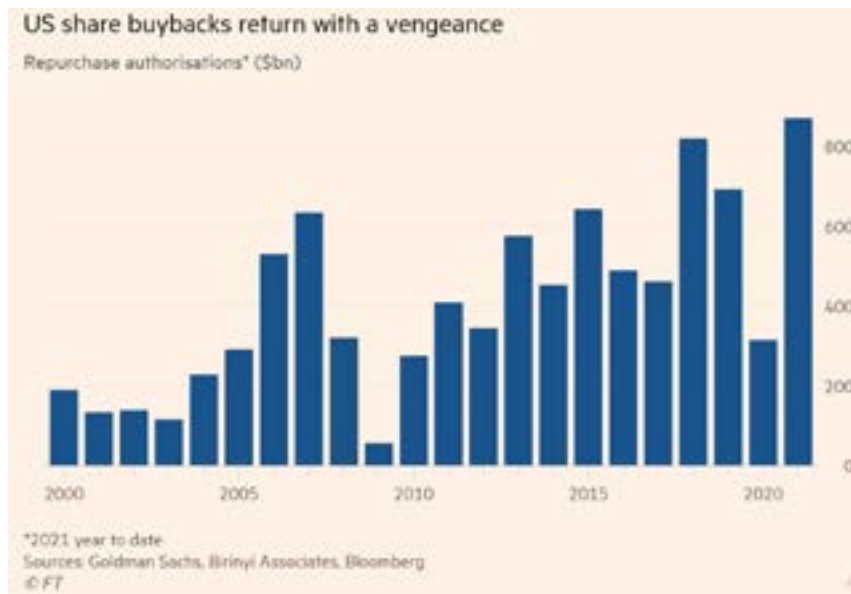


애플 시가총액: 2.2조 달러 (2,460조 원) vs. 한국 GDP: 1,920조 원

자사주는 매입 후 소각해야 모든 주주를 공평하게 대우하는 것임

이남우의 좋은주식연구소
YouTube

미국 자사주 매입 사상 최고치 주가 하락시 안전판 역할



이남우의 좋은주식연구소
YouTube

레버리지 효과 - 3가지 케이스

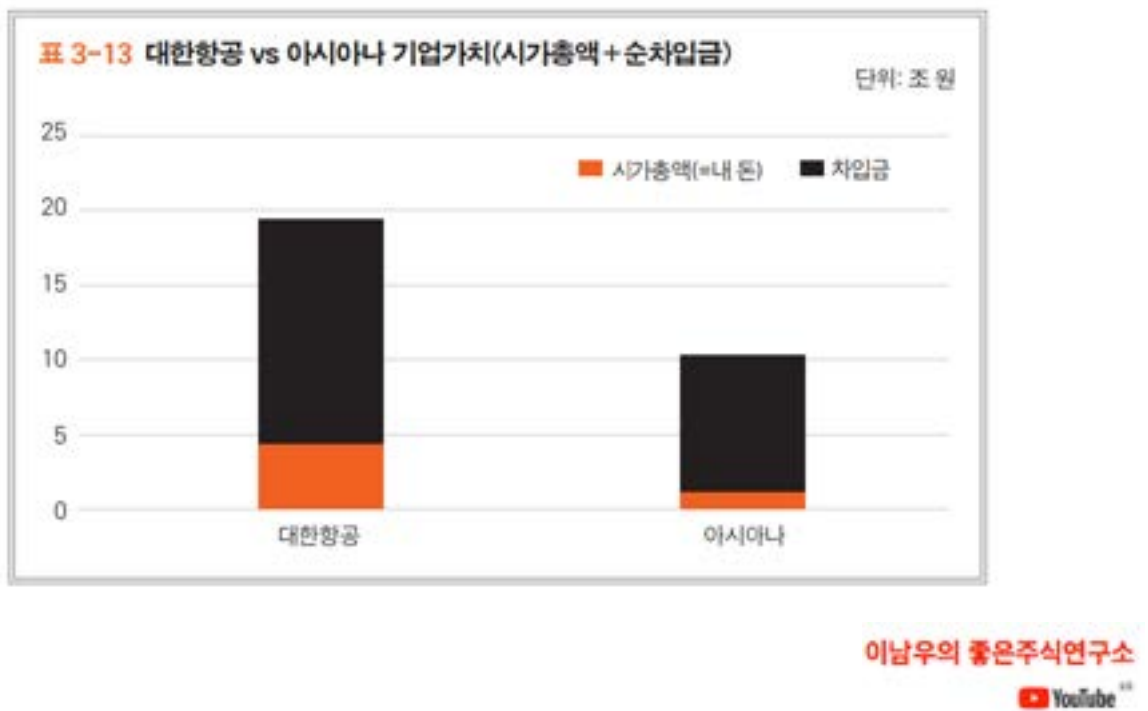
김씨 : 저축이 많고 유산도 물려받아 전액 현금으로 매수했다.

이씨 : 저축이 부족해 5억 원을 대출받아 매수했다.

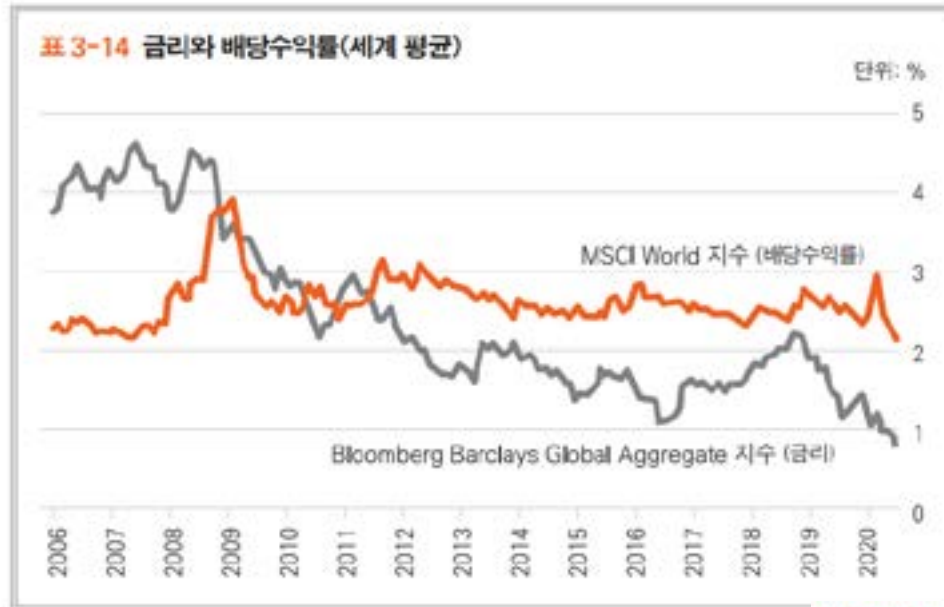
박씨 : 자녀들 사교육비로 저축이 부족해서 7억 5,000만 원을 대출받아 매수했다.



재무구조가 불량한 기업은 빚이 주가를 결정한다



주가는 금리와 반대로 간다 하지만 현 금리 수준은 역풍이라 할 수 없다



출처: 파이낸셜 타임스

이남우의 좋은주식연구소



기업거너번스: 코리아 디스카운트 진짜 이유?

1. 자본집약적 비즈니스 모델: 기업 이익을 경기에 민감하고 예측 어렵게 만든다.
2. 취약한 기업거버넌스: 한국 기업거버넌스 아시아 순위 12개국 중 9위.
3. 정부의 과도한 간섭: 한국 4대 금융지주사 PBR 중국 공산당 소유 4대 중국은행 보다 낮음.
4. 급격히 둔화되는 내수 증가율: 장기성장성 훼손.

이남우의 좋은주식연구소



목차

- Introduction
- 주가를 결정하는 5가지 요소
- A small advice

이남우의 좋은주식연구소
YouTube

성공 투자의 3가지 요소

- 지적 호기심
 - 섬세하게 관찰하는 능력
 - 신제품을 직접 체험하고자 하는 부지런한 자세
-
- “전기차, 자율주행 등 미래 mobility 알고 싶으면 테슬라 모델 Y 또는 모델 3 시승해봐라”
 - 주식 투자는 ‘좋은 기업’을 적당한 가격에 사서 기다리는 시간과의 싸움이다.



이남우의 좋은주식연구소
YouTube

[Email: cdc_advisor@yonsei.ac.kr](mailto:cdc_advisor@yonsei.ac.kr)

FB: Namuh Rhee (이남우)

이남우의 좋은주식연구소
YouTube

● Session 1

금융 마이데이터와 데이터산업



성시호

(한국신용정보원 마이데이터지원센터 센터장)

발표개요

- 국내 마이데이터 산업을 주도하고 있는 금융분야 마이데이터 운영 준비사항 및 국내 타산업과 해외사례를 설명한다.

이력

- 한국신용정보원 마이데이터지원센터 센터장


2021.12.3.

금융 마이데이터와 데이터산업

마이데이터 지원센터
성시호 센터장

 한국신용정보원
Korea Credit Information Services



 한국신용정보원
Korea Credit Information Services



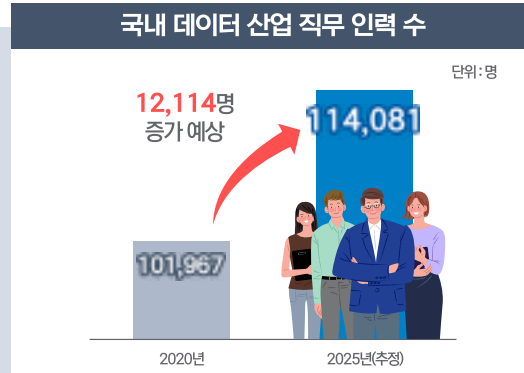
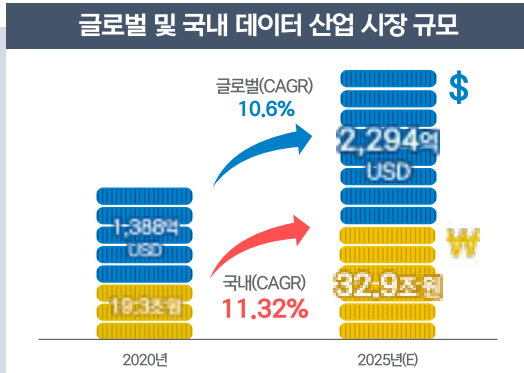
I 데이터산업과 국·내외 마이데이터 현황

01 세계 데이터 산업의 흐름



데이터 기반 모든 산업분야에서 디지털전환(DT)이 일어나는 4차산업혁명이 진행 중

- 데이터는 '21세기의 원유', 데이터를 얼마나 잘 활용하는지가 **혁신 역량과 성과**를 좌우
- 데이터 산업은 **정보처리·분석기술을 업무에 활용하는 산업**을 총칭하며 고속 성장 중
- 특히 **마이데이터**는 데이터 산업 중 세계적으로 초기 단계로 **급 성장이 예상**되는 분야



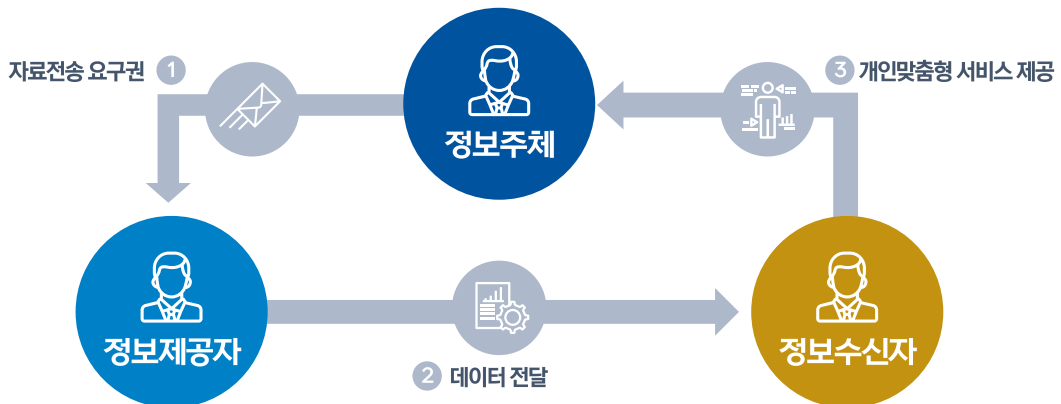
(참조) MarketsandMarkets(2020), 한국데이터산업진흥원(2021)

02 마이데이터란?



“마이데이터”는 정보주체가 본인정보를 적극 관리·통제하고 주도적으로 활용하는 것을 의미

- 가명 처리된 데이터 활용은 제한적으로 **정보주체 동의**를 통한 적극적인 방식인 **마이데이터**에 관심
- **‘나에 대한 데이터는 내가 주인이며 내가 관리한다’**는 정보주체의 인식 확산
- 신용, 자산, 건강관리 등에 주도적으로 활용하고, **‘자료전송 요구권’**이 핵심 기반





03 해외 마이데이터 산업 현황 (1/2)



개인정보를 기반으로 하는 마이데이터는 금융산업을 중심으로 확산 중

- 개인정보 중 **보건, 교육, 에너지, 이동통신, 금융정보** 등을 포함
- 특히, 전세계적으로 금융분야 중 은행을 중심으로 한 **'오픈뱅킹'** 정책이 추진 중

마이데이터

- EU GDPR 제정
- 영국 Mi Data
- 미국 Smart Disclosure
- 일본 정보이용신용은행제도

오픈뱅킹

- EU PSD2 시행
- 싱가포르 API Playbook
- 영국 Open Banking
- 홍콩 Open API Framework
- 호주 Open Banking
- 일본 은행법 개정
- 미국 제3자 API 접근활용

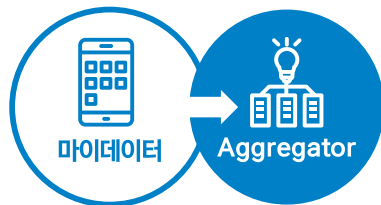


03 해외 마이데이터 산업 현황 (2/2)



마이데이터 산업의 비즈니스 모델은 크게 Aggregator와 PFM으로 구분 가능

- **Aggregator** (여러 회사의 상품이나 서비스 정보를 모아 제공하는 회사)
- **PFM** (Personal Finance Management, 개인자산관리)



04 국내 마이데이터 산업 현황 (1/3)

국내 마이데이터 산업은 금융을 중심으로 전 분야로 점진적 발전 중

• 운영가능 수준에 따라 '마이데이터 발전 로드맵'은 0~4단계로 구분

3단계 **금융 분야**

1.5단계 **공공 분야**

1.5단계 **통신 분야**

1단계 **의료 분야**

0단계 **조회**
개인정보 조회가능 수준

1단계 **저장**
정보조회 및 다운로드 가능 수준

2단계 **전송요구**
타기관으로 전송가능 수준

3단계 **대리 활용**
대리인을 통한 통합조회가능 수준

4단계 **전분야 확산**
정보주체 데이터 통제가능 수준 (25년~)

(참조) 4차산업위원회, '마이데이터 발전 종합정책'(21.6.11.)

04 국내 마이데이터 산업 현황 (2/3)

금융분야 본인신용정보관리업 분허가 기관(52개사) 준비 현황을 분석한 결과,

• 다수 기관은 '종합자산관리 & 맞춤형 상품추천'에 집중
• 일부 기관은 '보험상품', '금융투자', '대출비교' 등 **특화된 분야**로 준비

대분류

마이데이터 사업자 비즈니스 모델

비즈니스 모델	개수
PFM	48
Aggregator	4

중분류

마이데이터 사업자별 비즈니스 모델

중분류	개수
자산관리, 상품추천	27
금융투자(특화)	6
보험(특화)	5
대출비교(특화)	4
DATA제공	4
신용평가모형(특화)	2
모빌리티(특화)	2
소상공인(특화)	1
라이프스타일(특화)	1



04 국내 마이데이터 산업 현황 (3/3)

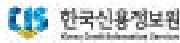


마이데이터 관련 일반법(개인정보보호법)과 산업 분야별 개별법 개정안이 추진 중

국내 마이데이터 관련 법률 제·개정 현황

법률명	주무부처	추진현황	관련 법령
신용정보법	금융위원회	개정 완료 (’20.2월 공포)	<ul style="list-style-type: none"> 전송요구권 신설(제33조의2) 본인신용정보관리업 신설(제2조의9의2)
민원처리법	행정안전부	개정 완료 (’20.10월 공포)	<ul style="list-style-type: none"> 민원인 요구에 따른 본인정보의 민원처리간 공동이용(제10조의2)
전자정부법		개정 완료 (’21.6월 공포)	<ul style="list-style-type: none"> 정보주체 본인에 관한 행정정보 제공요구권 (제43조의2)
데이터산업진흥 및 이용촉진에 관한 기본법	과학기술정보통신부	개정 완료 (’21.10월 공포)	<ul style="list-style-type: none"> 개인데이터 이동의 요구(제12조)
개인정보보호법	개인정보보호위원회	정부입법예고 완료 (’21.5월)	<ul style="list-style-type: none"> 개인정보 전송요구권(제35조의2) 개인정보관리 전문기관 지정(제35조의3)

9



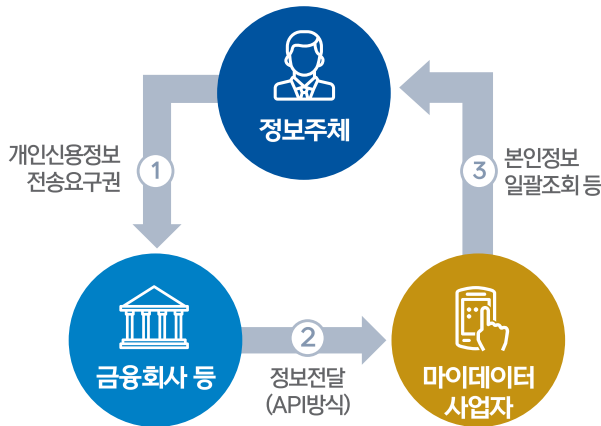
II 금융 마이데이터 산업

10

01 금융 마이데이터 운영 개요



신용정보법 '개인신용정보 전송요구권'은 개인의 데이터 주권 확립을 가능하게 하는 권리



정보주체(A씨)가 '개인신용정보 전송요구권'을 행사

- 필요한 정보 항목을 선택하여 금융회사로 하여금 해당정보를 마이데이터 사업자에 제공할 것을 요구

금융회사는 A씨의 정보를 마이데이터로 전달

- 표준화된 전산처리방식(API)을 통해 정보전달
- 정보주체의 인증정보는 암호화하여 안전하게 전달

A씨는 마이데이터 사업자를 통해 본인신용정보 일괄조회 서비스 제공

- 은행, 카드, 보험, 금투, 전자금융 등의 금융정보를 통합조회하고, 기타상품추천, 컨설팅 등의 서비스 제공

11

02 금융 마이데이터 산업 구성



① 정보주체 ② 마이데이터사업자 ③ 정보제공자 ④ 중계기관 ⑤ 마이데이터지원센터로 구성



12



03 금융 마이데이터 참여자 - ② 마이데이터 사업자



본인신용정보관리업 허가·신청기관은 지속적으로 증가될 것으로 예상

- 본 허가 획득 완료기관은 총 52개사
- 예비 허가 획득 (6개사) 및 예비 허가심사 중 (9개사)

본인신용정보관리업 허가 현황

※'21.11.12.기준

업권	본허가완료	예비허가완료	예비허가심사중	합계
은행, 여신전문	18	1	1	20
보험, 금융투자	8	4	4	16
상호금융, 저축은행	2	0	0	2
CB	2	0	0	2
핀테크, IT	22	1	4	27
전체	52	6	9	67

13



03 금융 마이데이터 참여자 - ③ 정보제공자



법령상 신용정보제공기관은 보유한 정보주체의 신용정보를 제공할 의무

- 약 550여개 기관이 'API 자체 구축' 또는 '중계기관'을 통한 정보 제공을 준비
- * 상호금융(3,500개 기관)은 개별 조합을 대표하여 중앙회를 통해 정보 제공

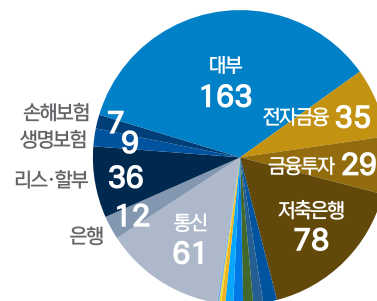
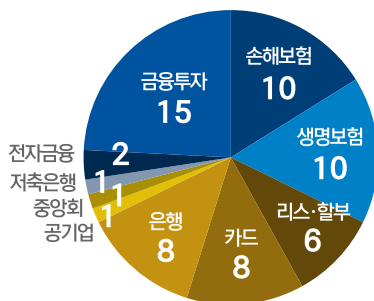
※'21.11월기준

API 직접 구축

65개 기관

중계기관 이용

490개 기관



공기업(7), 외국은행(5), 중앙회(5), P2F(5), CB(4), 카드(2), 채권인수(1), 종합금융(1)

14



참고 금융업권 별 전송 대상 정보



정보제공항목(490여개), API 항목(70여개)



은행

수신계좌, 투자 상품, 대출상품, 개인형 IRP



카드

카드 기본, 포인트, 청구·결제 및 리볼빙, 승인상세, 대출상품, 선불카드



금융투자

보유계좌, 잔액, 거래내역, 개별상품, 연금계좌, 개인형 IRP



보험

보험계약, 자동차보험, 대출상품, 보장(담보), 개인형 IRP



할부금융

대출계약, 대출잔액, 거래내역, 운용리스 계약 및 거래내역



전자금융

선불발행, 선불거래, 결제수단 등록, 결제내역



기타

통신, 대부, 보증보험, P2P업권의 거래관련정보



03 금융 마이데이터 참여자 - ④ 중계 기관



중·소형 금융기관을 위해 법령상 지정된 중계기관이 신용정보 전송역할을 지원

- 상호금융 등 일부 중계 기관은 다른 중계 기관을 통해 연결 가능

중계기관 리스트

기관명	중계기관 수행 업권	비고
한국신용정보원	보험, 카드, 리스/할부, 공공	
금융결제원	은행, 중앙회 (상호금융 포함)	
저축은행중앙회	중앙회에 전산위탁 운영하는 경우	저축은행 (80여개)
농·축협중앙회	중앙회에 전산위탁 운영하는 경우	조합 (1,300여개)
수협중앙회	중앙회에 전산위탁 운영하는 경우	조합 (90여개)
산림조합중앙회	중앙회에 전산위탁 운영하는 경우	조합 (40여개)
신용협동조합	중앙회에 전산위탁 운영하는 경우	조합 (150여개)
새마을금고중앙회	중앙회에 전산위탁 운영하는 경우	금고 (1,300여개)
행정정보공동이용망 연계 공공기관	행정정보공동이용망 연계 공공기관	
코스콤	증권, 자산운용, 선물, 전자금융, 대부	
한국정보통신진흥협회	통신업권	통신사



III 향후 마이데이터 산업 변화 및 전망

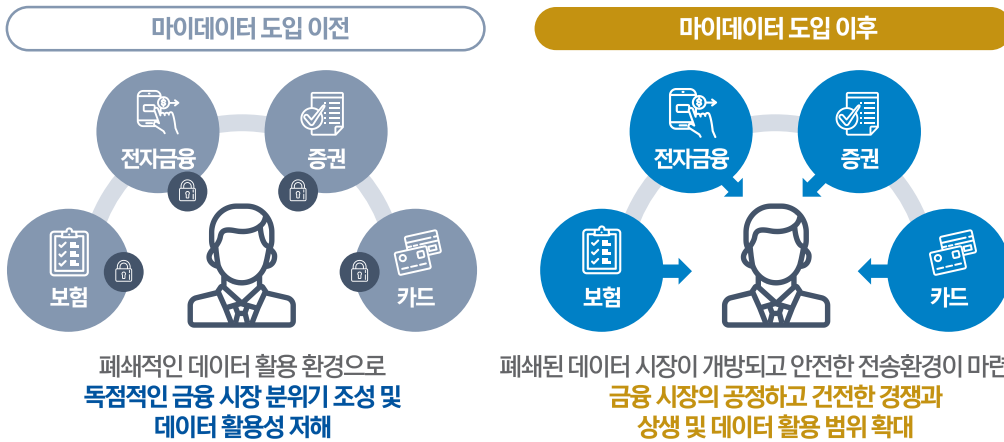
17



01 금융 마이데이터 도입에 따른 변화

개방적인 데이터 정책으로 공정하고 건전한 시장조성 및 데이터 활용범위 확대 예상

- 안전하고 편리한 데이터 이동 환경조성으로 정보주체는 안심하고 신용정보 전송요구를 시행



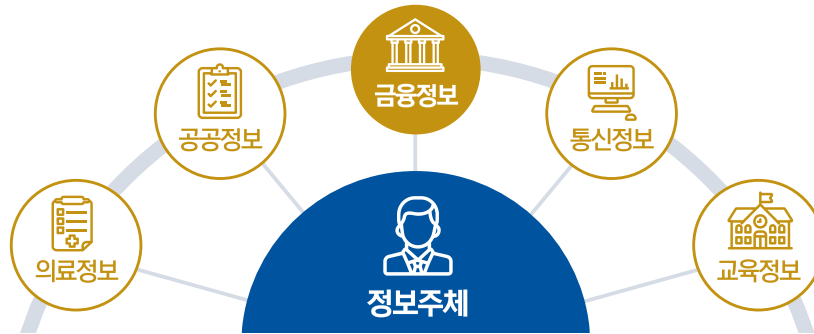
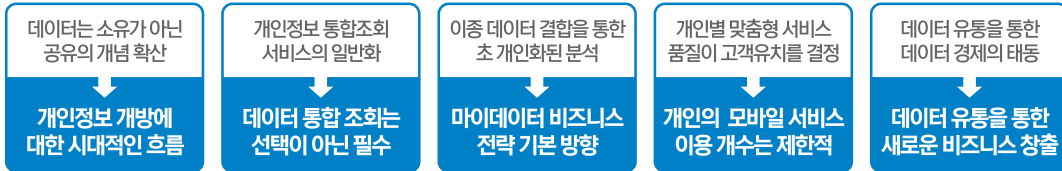
18



02 다양한 산업으로 마이데이터 확산



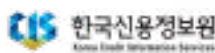
금융정보를 넘어 모든 개인정보를 대상으로 본격적인 ‘마이데이터 시대’로의 전환



19

감사합니다

2021.12.3.



● Session 2

데이터 3법 활용을 위한 개인정보보호정책 연구동향



복준영
(신구대학교 교수)

발표개요

- 2020년 데이터 3법의 국회 통과로 개인정보의 산업적 활용이 가능해짐에 따라 개인정보보호정책의 연구동향을 파악하고 데이터 3법 관련한 산업적 활용과 미래 연구 방향을 제시한다.

이력

- 신구대학교 스마트사무경영과 교수
- ISACA Korea 부회장
- 前 풀무원 ECMD 미래전략실장
- 前 CJ푸드빌 복합화사업본부장
- 前 삼성물산 마케팅/영업 그룹장
- 前 SK텔레콤 마케팅전략 및 u-City 추진단 기획부장

2021 ISACA Korea & Barun ICT Research Conference

데이터 3법 활용을 위한 개인정보보호정책 연구동향 고찰

복준영 | ISACA 사업부문 부회장
신구대학교 스마트사무경영과

Confidential. For internal use only.



발표자 소개



복 준 영

- 現) ISACA 사업부문 부회장
- 現)신구대학교 스마트사무경영과 마케팅교수
- 現) 한국외식산업정책학회 부회장
- 풀무원 계열사 대표/풀무원 ECMD 미래전략실장
- CJ 푸드빌 복합화 본부장
- 삼성물산 마케팅 그룹장
- SK텔레콤 마케팅전략팀/u-City사업추진단 부장

Table of Contents

1. 연구목적과 배경
2. 데이터 3법 개정
3. 연구방법
4. 연구결과
5. 시사점
6. 향후 데이터 3법의 활용

1. 연구 목적과 배경

데이터 3법의 개정 (2020년 1월 9일)

- 데이터3법(개인정보보호법·정보통신망법·신용정보법 개정안)의 법제화 및 8월부터 시행
 - 기술적 처리(비식별화)를 통해 가명·익명 정보를 산업적 연구, 상업적 통계 목적으로 **개인동의 없이 활용**.
 - '생존하는 개인을 식별하는 일체의 정보'
 - 해당 정보만으로는 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 개인을 알아볼 수 있는 모든 정보
 - 시민단체는 개인정보보호에 관한 안전조치에 대한 우려감을 나타내고 있는 실정
- <시민단체의 우려>
- 개인정보에 관한 자기결정권 침해
 - 기업의 이윤추구 목적으로 통제장치 없이 개인정보(질병, 신용정보)를 무분별하게 사용(헌법 10조, 17조 위법사항)
 - 정보주체로서의 정보이용 열람권, 삭제요구권 등이 부재
 - 기업이 가명정보+익명정보를 결합하여, 판매, 활용하는지에 대한 감시 등으로부터 배제

'개인정보보호' 정책 연구동향

- 2011년 9월 개인정보보호법 시행
 - 공공기관의 개인정보보호에 관한 법률로 규제
 - 금융기관 등 민간부문의 개인 정보보호 규정은 없거나, 자율규제 명목으로 존재
- 개인정보 유출사고의 심각성
 - 행정처분이 완료된 정보유출 사고 건수만 해도 2020년 상반기 1,302만 건으로 폭증
 - 관련 정책 연구는 일부 기술적연구에 국한됨.



2. 데이터 3법 개정

개인정보보호법

- 주요특징
 - 가명정보의 제도화
(기존) “해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는”
(개정) 익명정보는 「개인정보보호법」을 적용하지 않음.
“다른 정보의 입수 가능성” 등 기준을 제시
 - 개인정보 정의, 민감정보·주민등록번호 처리제한, 개인정보 처리위탁, 안전조치의무, 개인 정보보호책임자 지정, 정보주체의 권리, 손해배상, 개인정보보호 인증 등의 규정은 모두 삭제

정보통신망법

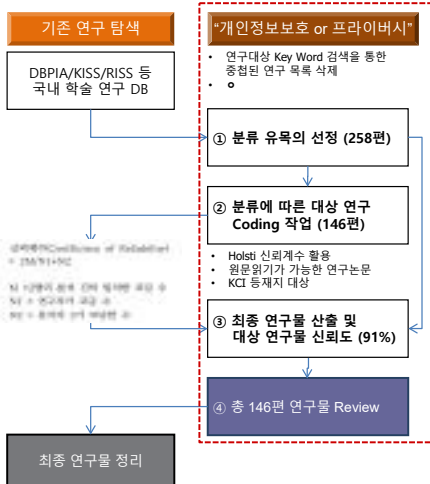
- 정보통신망법 내 개인정보 관련 다른 법령과의 유사·중복 조항 정비와 협치(거버넌스) 개선
- 정보통신망 이용촉진 및 정보보호 등에 관한 법률
- 개인정보 규정(제4장)을 삭제하여 이 중 「정보통신망법」에만 있는 조항들은 「개인정보보호법」내 특례규정으로 편입
- 정보통신망법」의 단말기 접근권한에 대한 동의, 주민등록번호 처리 관련 본인확인기관의 지정 등 규정은 삭제되지 않고 여전히 존치

신용정보법

- 「신용정보의 이용 및 보호 등에 관한 법률」
- 개인정보보호법」과의 정합성, 가명정보의 도입 등을 내용으로 하여 개정
- 추가정보를 사용하지 아니하고는 특정 개인을 알아볼 수 없도록 처리(가명처리)한 개인신용정보로서 가명정보의 개념을 도입(제2조제15호, 제16호 신설)
- 그리고 통계작성(시장조사 등 상업적 목적의 통계작성을 포함), 연구(산업적 연구를 포함), 공익적 기록보존을 위해서 가명정보를 신용정보주체의 동의 없이도 이용하거나 제공할 수 있도록 규정(제32조제6항 제9의2, 제9의4).

	기안	안건번호
제1차	신용정보법 일부개정법률안(신용정보법 일부개정법률안)	신용정보법 일부개정법률안(신용정보법 일부개정법률안)
제2차	신용정보법 일부개정법률안(신용정보법 일부개정법률안)	신용정보법 일부개정법률안(신용정보법 일부개정법률안)
제3차	신용정보법 일부개정법률안(신용정보법 일부개정법률안)	신용정보법 일부개정법률안(신용정보법 일부개정법률안)

3. 연구 방법



연구 방법 절차

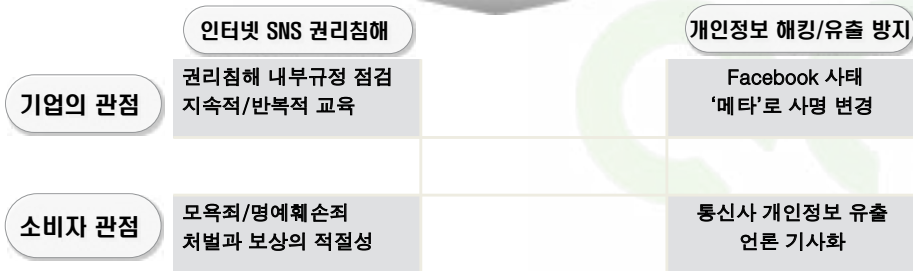
- 2011 - 2020년까지 10년 간 국내 "개인정보보호" 정책에 관한 연구**
 - 한국연구재단 학술 등재지에 등재된 논문
 - 석·박사 논문, 보고서, 서평, 답론 등을 제외
- "연구 동향" 파악의 목적과 활용**
 - "연구 동향"을 파악하는 목적은 특정 분야의 연구 성과를 고찰하고 현재와 미래 흐름을 파악
 - 비교적 길지 않은 학문분야 일수록 후속연구의 정체성 및 타당성 문제에 관하여 연구자들 사이에서의 심도 있는 검토 가 요구
- '동향 연구' 및 '고찰 연구'에서 활용하는 '내용분석기법'**
 - 기존 연구를 분류 유목에 따라 분류하여 해당 연구의 내용을 Review
 - 분류 유목의 기준 선정이 중요(연구시기, 연구목적, 연구방법, 연구결과 등)

4. 연구 결과

연구 동향 측면

2013 년 이후 구글, 페이스북, 전자상거래 등 사이버 이용자 활용 빈도가 높아짐에 따라 인터넷 SNS 관련 개인정보보호 취급방침, 권리 침해, 확인수단 등에 관한 연구가 활발

2014년 카드3사의 개인정보유출사건을 계기로 금융과 핀테크, 빅 데이터, 사물인터넷 중심의 개인정보 보완과 해킹, 유출방지 및 형사적 손해배상과 처벌의 적정성 등에 관한 연구가 본격화

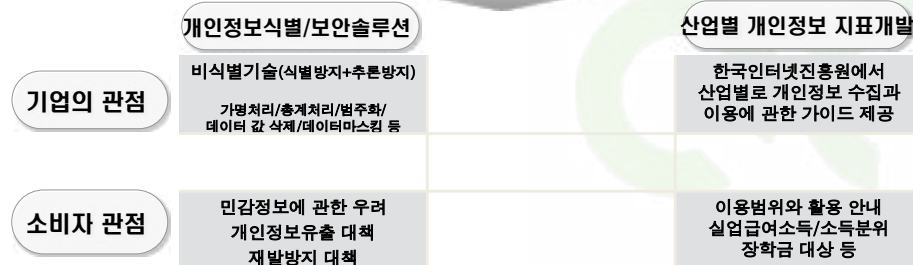


4. 연구 결과

연구 성격 측면

개인정보의 식별기능 대안과 인증 및 정보보안 솔루션 모듈의 경우, 공공데이터를 활용한 모델링과 로그데이터를 활용한 시뮬레이션

특정 산업분야별로 개인정보수집범위, 인증, 평가 등에 적용할 수 있는 지표 개발

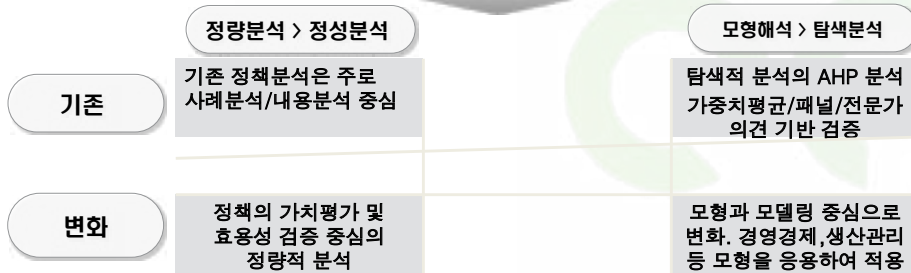


4. 연구 결과

연구 방법 측면

공공부문 및 비영리부문의 개인정보보호의 효율성 측정에 유용한 자료 포락 분석 (Data Envelopment Analysis)을 활용

품질 모형인 Kano 모델로 측정항목을 분류하거나 Timko의 고객만족계수 도출을 통해 개인정보보호 프로그램의 신속성을 측정



5. 시사점

주민번호 등 민감정보 수집과 활용에 대한 형사적 처벌 규제 완화

미국, EU, 일본 등의 해외 사례를 통한 추가적인 정책 규제 완화 필요성

모델링을 통한 민감 정보의 식별에 관한 보완적 대안을 제시

개인정보의 자기결정권 및 잊혀질 권리 측면에서 더욱 명확한 조건과 상황의 설정이 필요

개인정보보호정책에 있어 보호대상자인 국민들의 인식과 태도의 변화가 필요

개인정보를 수집, 활용하는 기업 또는 기관이 최소의 민감 정보를 수집 혹은 수집 종류의 변화 필요성

개인정보의 로그 및 쿠키 데이터를 수집, 입력하여 안전성을 검증을 통해 주민번호 등 민감 정보를 대체

해외사례(EU, 미국, 일본 등)를 통한 개방된 공공데이터를 활용 및 모델링 강화

개인정보를 취급 사이트와 모바일 애플리케이션의 식별번호 분석을 통한 모델링 검증

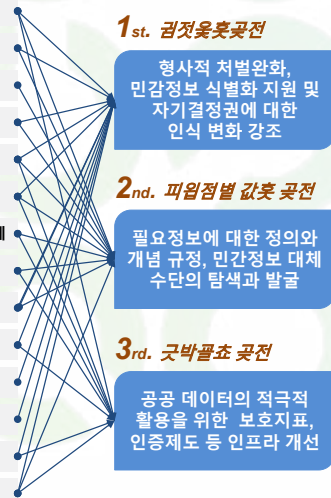
출입국관리소에 보관되어 있는 약 9천만건의 안면인식 데이터와 2022년까지 순차적 공개의 활용

개인정보의 제도적, 운영 관리수준에 따른 인증, 평가, 보호지표를 개발을 위한 인증제도 활용

DNA, 영상 및 안면인식, 바이오 생체 및 위치정보 등 개인의 민감 정보에 관한 기준 마련 필요성

개인정보 시스템 기반 업무 수행 지원 및 교육 등 전문성 강화 방안 마련

개인정보 인프라 및 역량에 대한 홍보 기능 강화를 통해 기관/기업의 인지도·신뢰도 제고



6. 향후 연구 방향

데이터 3법의 활용 방향		향후 과제 방향
1 대내외 개인정보 환경 진단	<ul style="list-style-type: none"> • 산업별로 개인에 관한 필요정보 활용에 관한 활동 점검 • 필요정보의 익명/가명 데이터 전환이 가능한지, 자료 융합과 비교 분석으로도 해당 데이터의 식별이 가능한지 확인 • 정책위배에 관한 법률적 해석을 사전에 검증 • 개인정보를 다루는 기관의 종사원 인식 수준과 영향 분석 (기존 해킹 및 보안사고로 인한 안전 불감증) 	개인정보보호팀 또는 전담조직 구성
2 사용자 데이터 안정성 방안 마련	<ul style="list-style-type: none"> • 제공 데이터 고객을 대상으로 한 각 분야별 위험 요인 도출 • 안전인식, DNA 등 고도화된 민감 개인 정보의 조합, 융합으로도 개별 인식이 불가능한 해결 방안 마련 (로그기록, 쿠키 등 활용) 	<ul style="list-style-type: none"> • 고객CS 부서, 마케팅/영업 등 고객 개인정보를 취급하는 부서를 대상으로 개인정보활용에 대한 정기/수시점검 • 익명/가명 데이터 수집과 가공을 전담조직에서 담당하고, 개방된 공공데이터 수준과 비교/점검 • 해당 기관과 조직에서만 사용가능한 개인정보 데이터를 정의하고 표준화
3 데이터 3법의 전략적 활용	<ul style="list-style-type: none"> • 개방된 공공데이터를 활용한 정보 활용 모델링 구축 • 산업별로 대·내외 환경변화, 조직 전략 등을 반영한 지속가능한 성과 창출이 가능한 전략 및 실행과제 수립 • 익명성/가명 자료가 조직내 전략적 활용에 어떻게 활용되는지 조직/기관별로 정의한 후, 자료 탐색과 수집, 데이터 처리에 대한 고민과 연구가 필요 	개인정보 데이터 모델링 및 방법론 개발
4 정보 활용에 관한 목표/성과 추정을 통한 세부정책 개발	<ul style="list-style-type: none"> • 중장기 데이터 활용에 관한 고제 설정/시행으로 전략적 활용에 대한 세부 정책 개발 : 아직까지 개인 정보(주민등록 번호 처리 관련 본인확인기관 지정 등 규정)에 관한 제한 조치 존재 • EU GDPR*등 국제적 데이터 법제와의 정합성 제고로 전세계 데이터 경쟁에 참여할 수 있는 기반 마련 <p><small>* General Data Protection Regulation (일반 개인정보보호법)</small></p>	<ul style="list-style-type: none"> • 해외 및 국내 개방 공공데이터의 수준을 파악 • 필요 개인 정보에 관한 블록체인 기술, 암호화 기술 등을 활용, 개인정보 데이터 모델링(학계와 공동) • 원천 데이터의 폐기 및 관리 등에 관한 규정 마련 • 접근 종사원 제한, 한정을 통한 인적 교육관리 강화

6. 향후 연구 방향 : 친환경 차량충전소 가명정보 결합 사례

지자체(차량등록데이터)-민간(차량이동데이터) 간 가명정보 결합을 통해 친환경 차량 충전 인프라 수요예측 및 최적 입지 분석모델을 개발하여 데이터 기반의 과학적 행정을 구현

- (주요 데이터) 차량등록데이터(지자체), 차량이동데이터(네비게이션)
- (가명정보 결합) 개인정보를 가명정보 처리 후 결합, 수요예측 분석모델 개발
- (데이터 활용 활성화) 데이터 3법 개정 이후, 지자체 최초 가명정보 결합 통해 NEEDS를 반영한 맞춤형 정책 개발 등 데이터 활용 정책 홍보 가능
- (표준분석모델 구축) 향후 행정안전부 친환경 차량 인프라 입지선정 표준분석모델로 선정 및 타 지자체 확산 가능
- (스마트 그리드 사업 초석) 스마트도시 기본계획 내 지자체 입주업체 대상 전기차 스마트 그리드 사업 추진의 초석

감사합니다.

● Session 3

Blockchain Essentials for Assurance



이동기
(EY한영회계법인 Director)

발표개요

- 블록체인 및 가상자산 최신 동향을 살펴보고, 블록체인 개념의 개요와 감사/통제 관점에서 고려할 사항을 알아본다.

이력

- ISACA Korea 부회장
- EY Global Blockchain SMR
- 한국감사협회(IIA) CIA 위원회 부위원장
- 한림국제대학원대학교 컴플라이언스&윤리 전공 겸임교수

2021 ISACA Korea & Barun ICT Research Conference

Blockchain Essentials for Assurance

이동기 | 부회장
ISACA Korea - Digital Audit 교육부문
EY한영회계법인

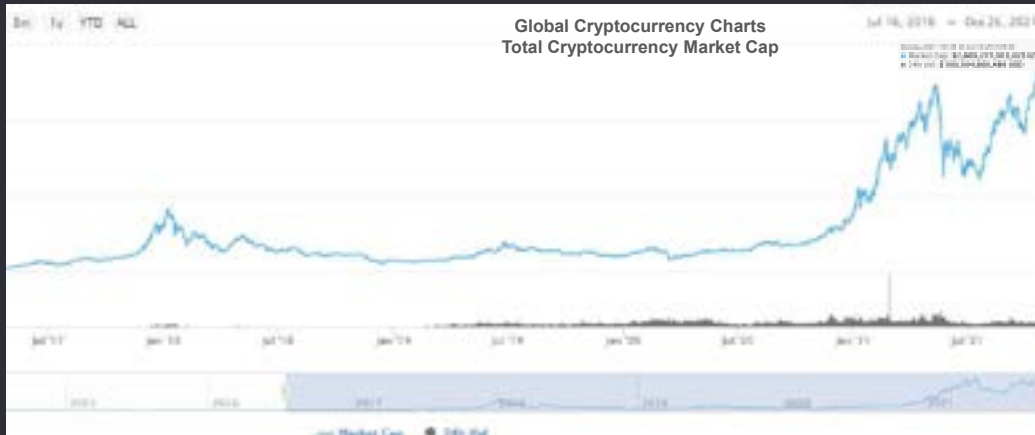
Confidential. For internal use only.



Introduction

Accelerated development of cryptocurrency market

- ▶ Cryptocurrency market worldwide has grown enormously.



2



Accelerated development of cryptocurrency market



- ▶ In the next year or two, you can expect many technology and financial services companies to explain their plans to enter the blockchain market.

In nearly every case, they will cite the low penetration of the technology in their industry or market as evidence that it's "early days yet" and they have "plenty of time" to formulate their strategy and leverage their legacy market position.

It isn't. They don't.

- Paul Brody, EY Global blockchain leader.

3



Business Opportunity & Risk Management

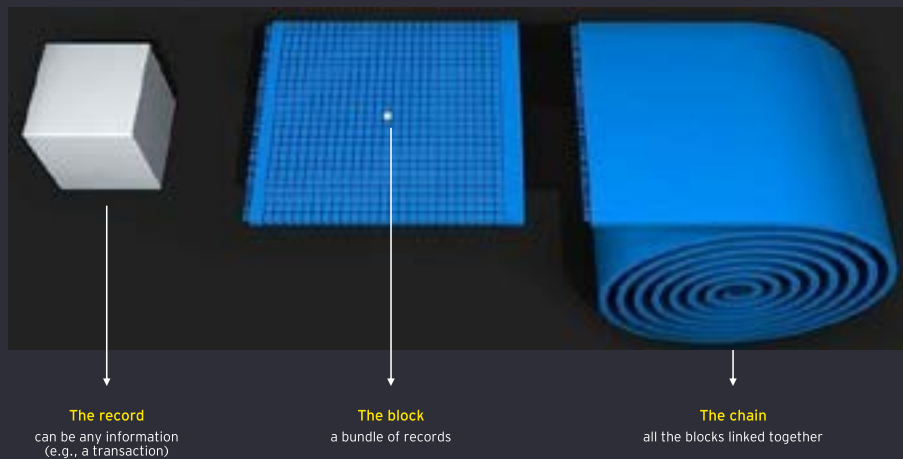
Blockchain technology is being applied in various industries, including finance and supply chain. The articles highlight the benefits of blockchain, such as increased transparency and security, and its potential to revolutionize traditional business processes.

이름	피해금액	날짜	내용
에이치비	437억	2021-09-27	8.8048%의 21487% 등의 손실
피에프	196억	2021-09-25	해당 금액
에이치비	896억	2021-09-25	해당 금액
에이치비	947억	2021-09-19	해당 금액
블록체인	6,824억	2021-09-18	다양한 가상자산 시장 피해
우호인	2,947억	2020-09-18	해당 금액

"한국은행의 '분산원장 기술의 현황 및 주요 이슈' 보고서를 보면, 2009~2015년 세계 가상자산 거래소 중 3분의 1이 해킹을 당했고, 그중 절반이 손해를 견디다 못해 사업을 접었다. 문제는 해당 거래소가 문을 닫으면 피해는 투자자들에게 돌아간다는 점이다." - 중앙일보 (2019.12.14)

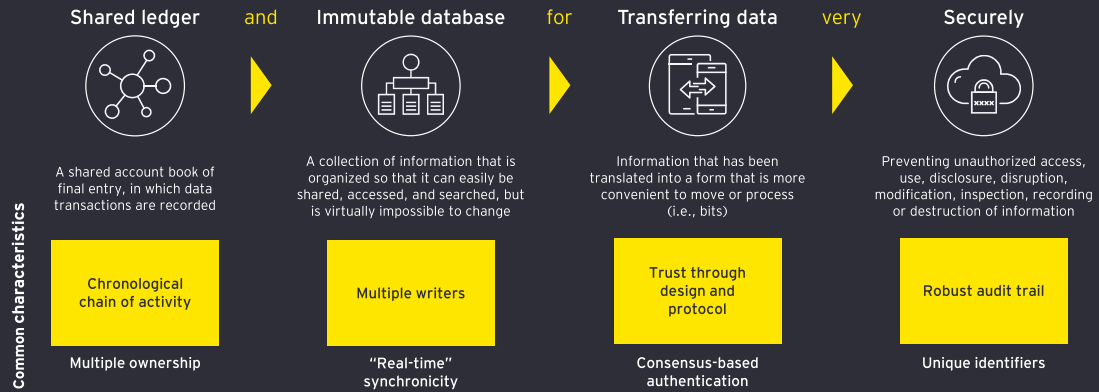
발행 시기	거래소명	피해 규모	피해 원인	결과	발생 국가
9월	에이치비	607억 원	해킹	폐업	일본
4월	피에프	300억 원	기타발 가상자산소트 부정	폐업	한국
4월	에이치비	400억 원	기타발 가상자산소트 부정	폐업	한국
2월	에이치비	1,000억 원	해킹	폐업	미국
11월	블록체인	6,824억 원	해킹	폐업	일본
11월	에이치비	1,000억 원	해킹	폐업	한국
12월	에이치비	400억 원	해킹	폐업	한국
1월	에이치비	200억 원	해킹	폐업	한국

Why is it called "blockchain"?



What is blockchain?

- ▶ Blockchain is a distributed infrastructure technology held collaboratively, which enables a decentralized exchange of trusted data. It uses cryptography to allow each participant on the network to update the ledger in a secure way without the need for a central authority or intermediary.

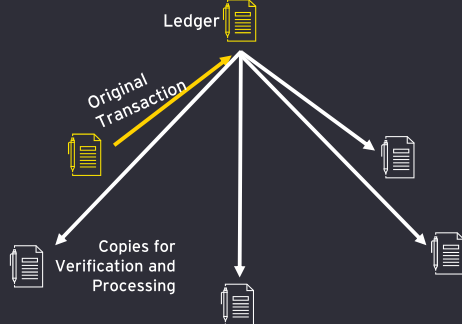


6



Consensus ensures all nodes have the same ledger

- ▶ Consensus enables agreement on one version of the blockchain ledger of transactions.
- ▶ The ideal consensus mechanism would be difficult/expensive to perform, but easy/cheap to verify.
- ▶ Proof of work is the model used by Bitcoin and requires work to be performed by miner nodes which can be easily verified by other network participants.



7





Audit considerations

9 EY EMEA Blockchain Summit

Auditing considerations for digital assets

Understand the business, Blockchain ecosystem consists of 5 Pillars

- ▶ Entities may engage in various activities in the blockchain ecosystem.

Entities that hold and/or transact using digital assets

Includes asset managers, private investment funds, high frequency traders

Entities that hold and/or facilitate trading of digital assets on behalf of customers

Exchanges are the main medium of buying and selling cryptocurrency
Custodians hold cryptocurrency on behalf of their customers

Entities that create digital assets for sale or distribution to third parties

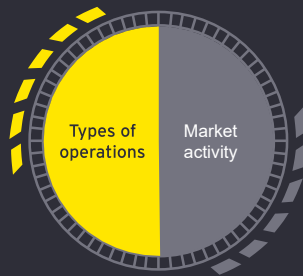
Issuance of Stablecoin backed by basket of stable assets

Entities that use blockchain-based business models

Includes miners, payment service providers, platform providers and wallet software providers

Traditional entities that operate or participate in blockchain processes and/or consortiums

Any company implementing an enterprise or inter-enterprise blockchain solution or using a blockchain for internal processes



9



Auditing considerations for digital assets Understanding blockchains

From a speech by Kathleen Hamm, PCAOB Board member, 2 November, 2018:

“

In the case of blockchain, if an audit client uses it for business or operational activities, the auditor must understand the information systems, including the related business processes, relevant to financial reporting and how the use of blockchain affects the client's flow of transactions. Blockchain does not magically make information contained within it inherently trustworthy. Events recorded in the chain are not necessarily accurate and complete.

<https://pcaobus.org/News/Speech/Pages/what-auditors-need-to-know-blockchain-other-emerging-technologies.aspx>

”

Key takeaway:

Regulators expect auditors to have a sufficient understanding of the technology.

10



Auditing considerations for digital assets Risk assessment

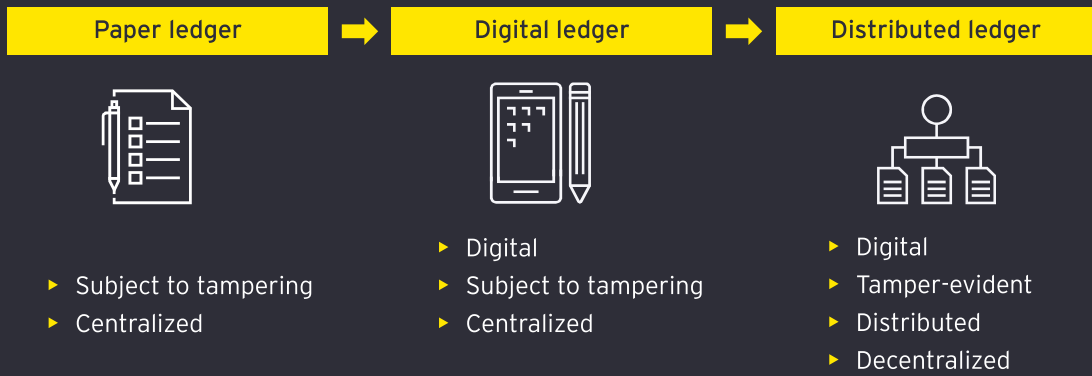
- ▶ The risks associated with digital assets vary, depending on how an entity holds these assets and/or transacts with them. Example risks include:
 - The entity's business purpose for holding and/or transacting digital assets
 - The types of digital assets held and/or transacted by the entity (e.g., bitcoin, ether)
 - Whether the entity maintains custody of its digital assets or whether a third party has custody of the assets
 - Whether a third party that has custody of the assets stores them in segregated or commingled public addresses, and whether the third party has an appropriate service organization control (SOC) report
 - How the entity transacts with its digital assets (e.g., trades peer-to-peer on the blockchain, trades on a digital asset exchange) and whether such transactions are traceable to the blockchain

11



Auditing considerations for digital assets

Risk assessment, Blockchain - digitization of business processes and the audit



12



Auditing considerations for digital assets

Risk assessment, Blockchain Architecture

- ▶ Enterprises must consider the potential disruption caused by integrating blockchain with their existing systems and processes.



* source: Generic Blockchain Reference Architecture Model, Blockchain Framework and Guidance (2020), ISACA





13



Auditing considerations for digital assets

Risk assessment, Implementation risks

Risks involved in implementing blockchain impact various functions of an organization. Some common examples include:

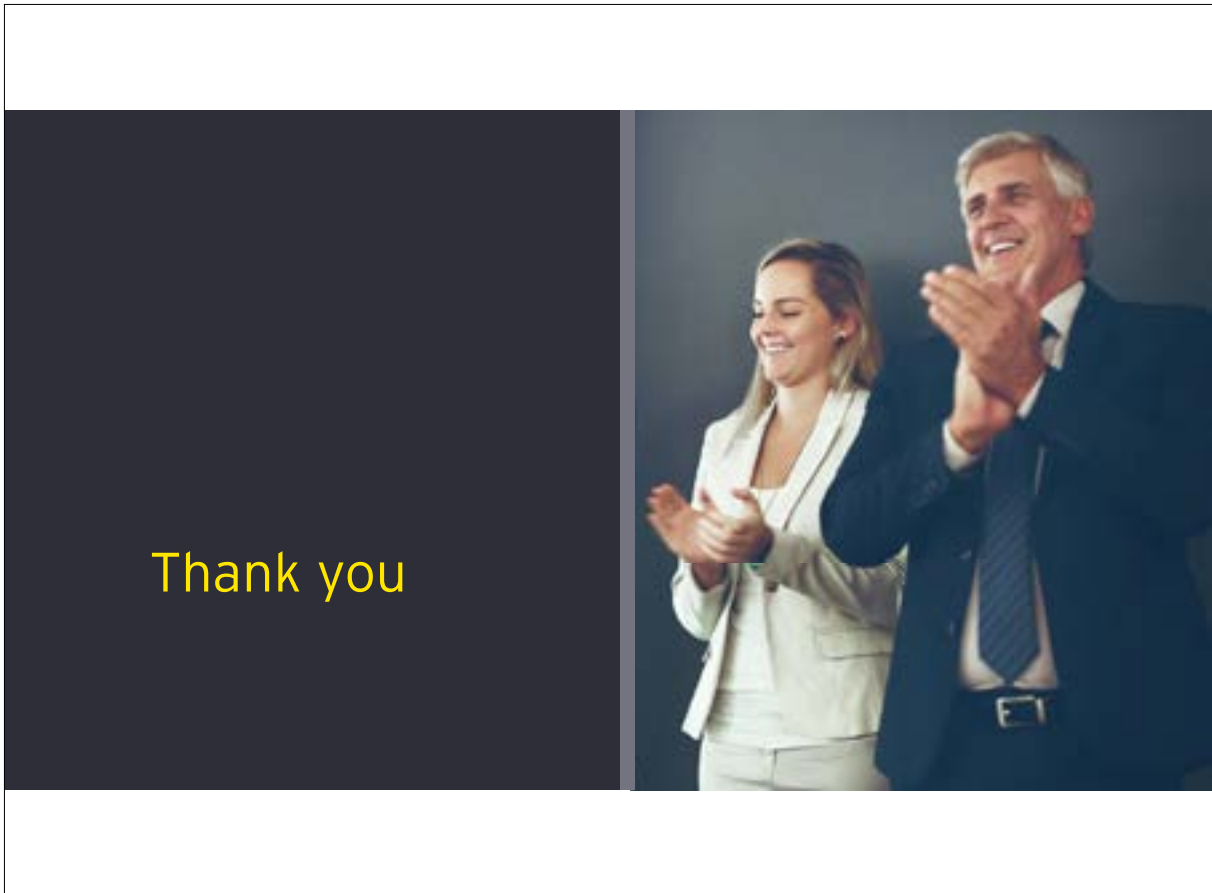
- ▶ **Data** - Benefits of blockchain technology can only be unleashed if the underlying information processed on blockchain is reliable and relevant. It is critical to develop supporting processes and controls to ensure quality of data. How are legacy IT systems interfaced with the blockchain, as inputs and receiving outputs? 
- ▶ **Technology** - Blockchain is rapidly evolving and requires many key choices among various emerging technological solutions. It is critical that a rigorous governance structure exists around blockchain implementation projects. 
- ▶ **Compliance** - Opportunities created by blockchains to transact with pseudonymous parties, share data and autonomously execute contracts introduce new legal and regulatory compliance risks. 
- ▶ **Financial reporting** - Distributed ledgers require new solutions to effectively support financial reporting by an organization participating in newly connected marketplaces. Internal controls must be considered surrounding the reliability of information in the blockchain and the reconciliation between the blockchain and financial reporting systems. 

Coordination between cross-functional teams consisting of operations, technology, legal and finance executives is critical for a successful implementation. It is also critical that an entity identifies, hires and retains appropriate resources with unique expertise in cryptography, programming and networking. Availability of these resources is a significant obstacle to successful adoption.

Auditing considerations for digital assets

Continuing topics

Proper internal controls in place and functioning as designed	<ul style="list-style-type: none"> ▶ Business process internal controls, such as segregation of duties ▶ IT internal controls, such as access to private keys 			
Custody of assets	<ul style="list-style-type: none"> ▶ Who holds the keys? Client? Third-party custodian? Exchange? 			
Know your customer (KYC) and anti-money laundering (AML)	<table border="1" style="width: 100%; text-align: center;"> <tr><td>Process</td></tr> <tr><td>Technology</td></tr> <tr><td>Legal, risk and compliance</td></tr> </table>	Process	Technology	Legal, risk and compliance
Process				
Technology				
Legal, risk and compliance				



Why CISA at this moment?

▶ 재무보고 내부통제 (내부회계관리제도)를 위한 IT Professional 수요 증가 (risk, control and audit)

상장회사수 및 시가총액 추이

단위: 개, 조원

	2016	2017	2018	2019	2020	2021	
상장회사수	총계	1,824	1,922	1,887	1,835	2,117	2,268
	비금융회사수	775	775	779	774	788	800
	금융회사수	1,049	1,147	1,108	1,061	1,329	1,468
시가총액	총계	1,107.3	1,468.2	1,713.0	1,889.4	1,733.0	2,281.0
	비금융회사	1,102.3	1,281.2	1,308.0	1,889.4	1,884.0	1,879.3
	금융회사	5.0	187.0	405.0	0.0	249.0	401.7

내부회계관리제도 검토 및 감사

자본시장과 금융투자업에 관한 법률
주식회사 등의 외부감사에 관한 법률

상장기업

적용연도 및 자산총액 기준	내부회계관리제도 감사대상 사업연도	
	개별기준	연결기준
2조 이상	2019년	2022년
5천억 이상 2조 미만	2020년	2023년
1천억 이상 5천억 미만	2022년	2024년
천세 주공상업법인	2023년	2024년

▶ 내부회계관리제도 도입규준
▶ 내부회계관리제도 감사기준

2020년말 기준 상장회사 2,268개사

Why CISA at this moment?



▶ ISACA Korea's Offering "CISA exam Prep Course (CISA 시험 준비반)"



CISA 준비반 1기(案) : 오프라인 - Coming Soon!!!
- 주 1회 (8시간) * 5주 완성 or
- 주 2회 (4시간) * 5주 완성

▪ 상장사 내부회계관리제도 감사도입으로 인한 CISA 수요 증가

▪ 국내 유일 ISACA Accredited Trainer(국제 공인강사) 직강

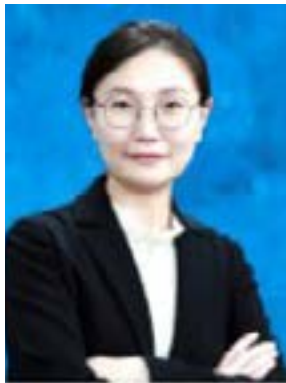
▪ Big4회계법인, Tech기업 등 현직 Trainer 문제 해설

▪ 취업, 이직 등 경력관리를 위한 멘토링

▪ ISACA 협회 공식 수험서 제공
(한글번역본: 이론서 + 문제풀이/해설)

End of Document

악성댓글의 피해 규모 산정 방법 연구



김미예

(연세대학교 바른ICT연구소 연구교수)

발표개요

- 악성 댓글은 개인의 정신과 신체적 건강에 부정적 영향을 미칠 뿐 아니라, 이로 인해 사회적 비용까지 유발한다. 본 연구는 악성 댓글이 미치는 사회 경제적 비용을 추정하고자 피해규모 산정 방법을 연구하여, 대략적인 악성댓글의 피해 규모를 파악하고자 한다.

이력

- 경영학 박사



악성 댓글의 피해는 어떻게 계산할 수 있는가?

연세대학교 바른ICT연구소

김미예 연구교수

CONTENTS

- 1 악성 댓글 현황
- 2 사회적 비용 추정을 위한 방법
- 3 비용 항목 도출

악성 댓글, 연예인을 넘어 일반인에게로..

1. 악성 댓글 현황

"내가 할 어떻게 해야..." 괴로워했던 선미, 결국 결단 내렸다

2019.11.14

SNS가 너무 괴로웠던 선미, SNS가 "내가 할 어떻게 해야..."

자살을 고민 중이었던 선미, 결국 SNS가 "내가 할 어떻게 해야..."

카따-떼카-와이파이 셔틀... 'SNS 감옥' 탈출구가 없다

뉴스 | 1월 14일

여고생 죽음 내몬 SNS 협박..

2021.01.14 14:00

연예뉴스 댓글 막으니 인스타그램·유튜브가 악플 사라지대로

3

사용자가 인식하는 악성 댓글 비중은?

1. 악성 댓글 현황

댓글 유형

구분	빈도	퍼센트
악성댓글	108	53.5
질문댓글	12	5.9
논리적 댓글	13	6.4
비평적 댓글	69	34.2
합계	202	100.0

(이제홍 2013)



(한국리서치 주간리포트 2021.1.20)

4

악플러의 책임과 규제 관련 법령

형법상 명예훼손죄(제307조)

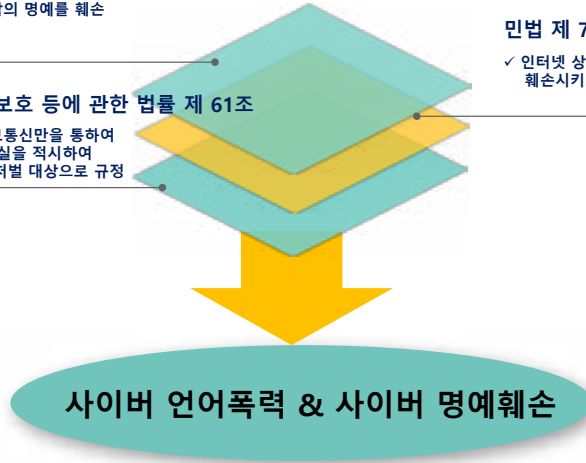
✓ 공언히 사실을 적시하여 사람의 명예를 훼손

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제 61조

✓ 사람을 비방할 목적으로 정보통신망을 통하여 공언히 사실, 또는 허위의 사실을 적시하여 타인의 명예를 훼손한 자를 처벌 대상으로 규정

민법 제 750조

✓ 인터넷 상에서 악성 댓글을 달아 사람의 명예를 훼손시키고 모욕을 가하는 행위로 인격권 침해



5

악플이란?

사이버 언어폭력

• 인터넷, 휴대전화, 문자 서비스 등을 통해 욕설, 거친 언어, 인신 공격적 발언 등을 하는 행위

사이버 명예훼손

• 사실여부와 상관없이 다른 사람/기관의 명예를 훼손하는 글을 인터넷, SNS 등에 올려 누구나(블록정 다수) 볼 수 있게 하는 행위

악성 댓글

• 인터넷 상 댓글 창에서 사실 여부와 상관없이 다른 사람의 명예를 훼손하는 글이나 인신 공격적 발언 등 악의적인 (Malicious) 내용을 다룬 댓글

6

1. 악성글 현황

피해 경험은 어느 정도인가?

[표 2-3-6] 성별·2020년 사이버폭력 피해 경험

구분	사례수	전체	언어 폭력	명예 훼손	스토킹	성폭력	신상보유	따돌림	갈취	강요
전체	(1,500)	62.7	36.0	28.3	39.8	32.6	25.1	24.4	21.9	22.7
남성	(770)	70.4	43.5	35.5	44.4	36.9	30.9	31.1	27.7	28.2
여성	(730)	54.5	28.1	20.7	35.0	25.9	19.1	17.4	15.8	16.8
20대	(329)	67.8	53.6	38.8	37.6	35.3	32.1	30.7	29.9	32.7
30대	(338)	65.7	39.8	35.7	46.3	38.1	30.9	32.7	30.7	31.1
40대	(410)	61.5	32.5	23.6	39.6	30.3	22.6	21.1	18.9	17.8
50대	(423)	57.4	22.7	18.8	35.6	28.4	17.5	16.1	11.7	12.9

(방송통신위원회 2020)

7

1. 악성글 현황

어떠한 내용으로 피해를 받는가?

[표 2-3-7] 성별·사이버폭력 피해 대응법 채택 내용

구분	사례수	피해 내용								기타
		사생활 침해	신상보유	성폭력	스토킹	언어 폭력	명예훼손	따돌림	갈취	
전체	(940)	27.1	22.7	22.2	21.1	19.3	14.6	12.5	4.7	
96.0% (901명)은 신고, 20.0% (188명)은 신고 후 대응법 채택	(412)	30.4	23.9	26.8	25.2	21.7	18.7	13.3	3.1	
95.0% (901명)은 신고, 20.0% (188명)은 신고 후 대응법 채택	(296)	31.2	23.1	26.4	23.4	30.4	10.4	12.8	0.6	
개인 홈페이지	(234)	28.5	31.5	24.6	28.8	21.1	14.2	15.7	2.8	
개인 휴대전화	(207)	42.7	33.3	15.9	16.5	20.0	14.7	10.5	7.1	
이메일주소 받기	(84)	25.4	28.4	48.2	40.0	10.2	44.2	7.2	0.8	
언어인계급	(81)	24.8	38.8	15.8	21.3	25.6	28.3	27.7	2.9	
기타	(9)	5.7	0.0	0.0	5.7	0.0	5.7	19.0	69.6	

(방송통신위원회 2020)

8

1. 악성 댓글 현황

피해 후 심리는 어떠한가?

[표 4-2-15] 피해 후 심리
(사이버몰매 피해 경험자, 단위: %, "그렇다"·"매우 그렇다" 응답 비율)

구분 (사례수)	전체 (940)	연령대별				성별	
		20대 (223)	30대 (222)	40대 (252)	50대 (243)	남성 (542)	여성 (398)
상대방에게 복수 욕구	45.0	45.3	47.8	48.4	40.7	44.1	46.3
우울, 불안, 스트레스	41.2	39.6	43.8	43.8	37.5	38.1	45.4
사람 교제 어려움	37.0	35.1	36.8	40.9	34.7	35.1	39.6
예전 일도 하기 싫음	34.7	31.2	35.3	40.2	31.8	31.1	39.6
자살, 자해 욕구	21.6	29.2	21.5	21.2	15.3	20.2	23.6
별 생각 없음	43.0	39.6	40.0	45.5	46.3	42.9	43.1

(방송통신위원회 2020)

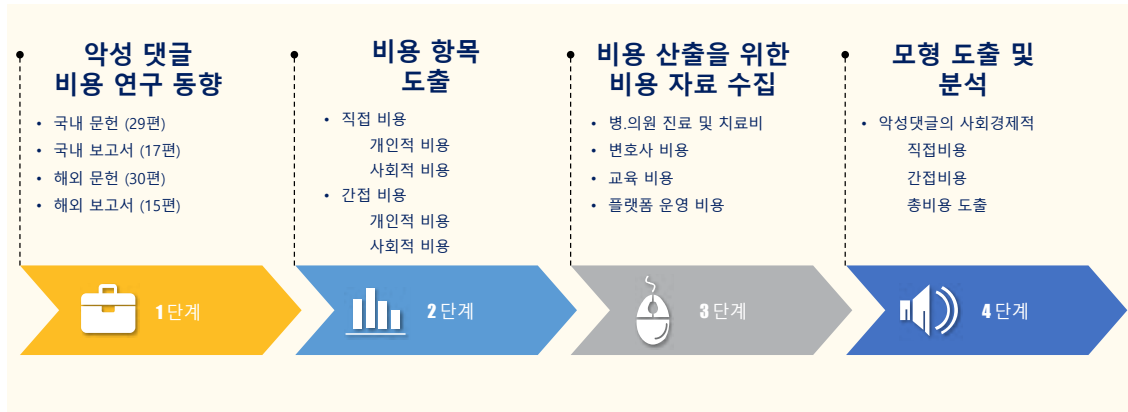
2. 비용 추정 방법

악성 댓글로 인한 사회적 비용 계산



2. 비용 추정 방법

어떻게 측정하는가?



11

2. 비용 추정 방법

악성댓글의 비용 항목 도출_호주



2018 The economic cost of bullying in Australian schools

The consequences of bullying are felt at the time of the incident and long into the future through reduced **economic potential, negative health and social consequences, and pressures on the health and social service systems.**

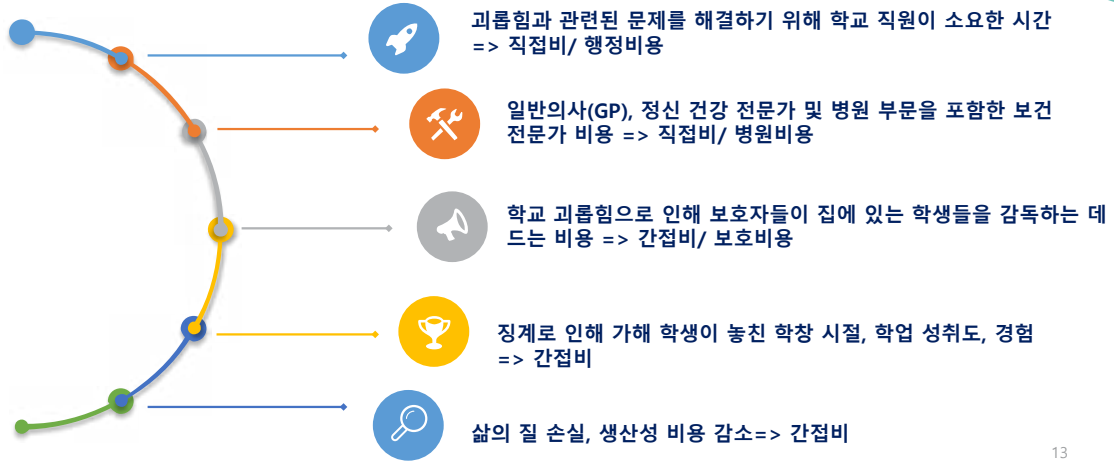
Table 1: Economic costs that will be experienced during school years for new school starters in 2018

Economic cost domain	Costs experienced during school years for new school starters (millions)
Senior staff time spent on bullying	3307
Cost of absenteeism for students at issue	4181
Primary and secondary health services	51
Mental health services use	348
Police involvement	41
Total	8328

12

2. 비용 추정 방법

악성댓글의 비용 항목 도출_호주



13

2. 비용 추정 방법

악성댓글의 비용 항목 도출_뉴질랜드



2018 Cyberbullying in New Zealand, estimating societal costs

TABLE 3: QUANTIFYING THE COST OF CYBER-BULLYING

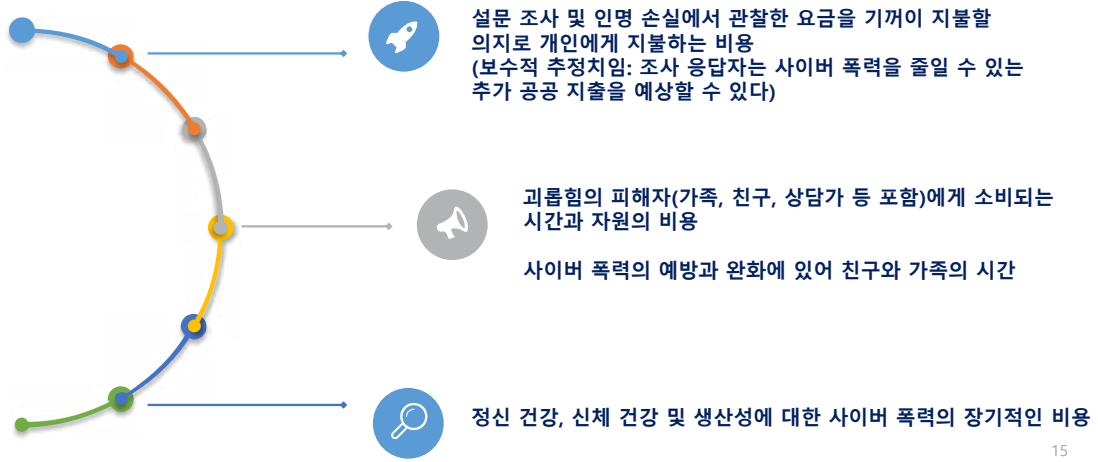
	2018, \$m	Notes
Personal cost	38	
At willingness to pay for victims of cyberbullying	75	Willingness to pay for each victim
Cost of lost TV	3	Statistical value of life, Australian data on loss of life related to bullying
Cost of interventions	368	
Friends & family	337	At average earning rate
Teachers, counsellors, etc	11	At marginal cost of report time
Medicines, online, etc	2	At marginal cost of service
Police	2	Estimate based on Australian bullying study
Education, justice, etc	6	Funding for NetSafe, etc
Long term health & productivity impact	N/A	Unquantified due to insufficient information
Total costs	444	Total annual cost of cyberbullying

Source: Sense Partners

14

악성댓글의 비용 항목 도출_뉴질랜드

2. 비용 추정 방법



15

어떤 비용 항목을 구성할 수 있을까?

3. 비용 항목 도출



16

● Session 4B

자본시장 IT시스템 효율적 용량계획 모델



이국형
(한국거래소 IT전략부 과장)

발표개요

- 증권사를 포함한 자본시장 참여 기업들의 IT시스템 필요용량을 다양한 머신러닝을 활용하여 예측하고 그 결과를 비교 분석한다.

이력

- 한국거래소 IT전략부 과장

01 용량계획의 새로운 접근

초기 과다 투자를 통해 과용량의 IT시스템을 구축하여 장기간 사용하는 방식에서 벗어나, 효율적인 용량 조절이 가능한 IT시스템 구축 방식 필요

» 머신러닝을 활용한 용량계획 모델 개발 및 효용 검증

- 트랜잭션의 규모를 결정하는 '호가(주문)건수'를 예측
- (일별) 투자자수, 거래 종목수, 호가건수, 체결건수, 거래량, 회원사 거래증거금 등

COVID-19 및 개인투자자 참여 급증 등 투자 환경의 변화는 주문 및 거래량 급증(동학개미운동)으로 이어짐

» 개인 투자자 심리, 행동을 반영하는 변수를 포함하여 IT시스템 용량계획 마련 필요

- 코스피200 변동성지수(VKOSPI) 이용

⇒ 정확한 용량계획이 매우 중요하고 사람들의 심리에 매우 민감한 자본시장 IT시스템 대상

2

01 참고(자본시장 심리지수)

국내 자본시장에서 소비자의 심리와 관련된 지표는 코스피 200 변동성 지수임

[코스피 200 변동성 지수(VKOSPI, 공포지수)]



* KRX 발표, 실시간, 수치형

- ✓ 한국의 유가증권시장(KOSPI)에 상장되어 있는 200개 종목을 기초자산으로 하고 있는 KOSPI200 옵션 가격을 이용하여 미래 변동성에 대한 시장의 기대치를 나타내는 실시간 지수
- ✓ 주식시장의 변동성이 클 것이라 예상하는 투자자가 많아 질수록 변동성 지수가 상승하고, 반대로 변동성이 작을 경우 변동성 지수가 하락
- ✓ VKOSPI는 경제학 분야에서 주가 변동성에 대한 투자자 심리를 반영하는 것으로 입증된 변수

3

02 연구 방법

(용량 계획 모델 개발) 국내 특정기업의 용량산정 방법을 토대로 다양한 머신러닝 기법을 활용하여 용량 예측을 수행

- ✓ 기준일 시점 기준으로 과거 x일간의 데이터를 이용하여 기준일 이후 y일간의 필요할 호가(주문)건수의 최대치를 일별로 예측하여 실제 호가건수와 비교
- 연속형 수치의 예측이므로 R2, MAE, MAPE, MPE 등 지표 확인

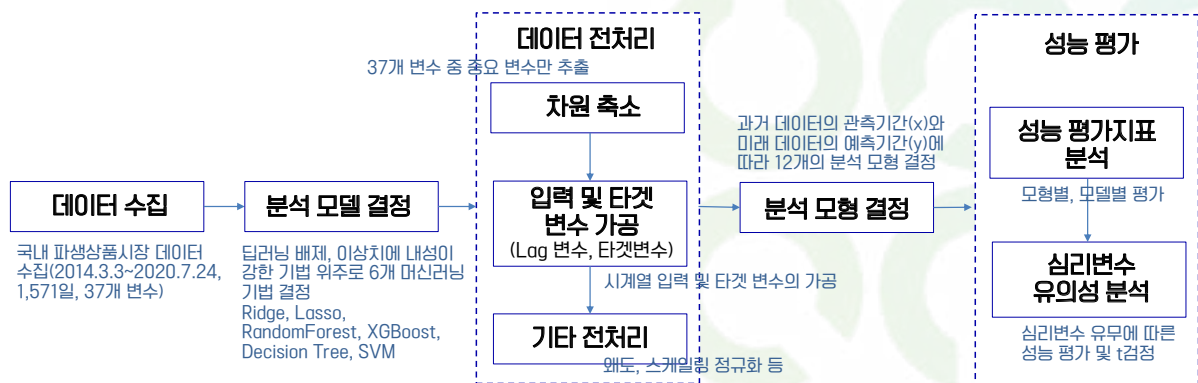
(심리변수 유의성 확인) 상기 예측모델에서 사람의 심리를 반영한 요인을 용량산정에 반영하지 않았을 경우와 반영하였을 경우의 용량 예측을 수행하여 성능 비교 및 t-검정 실시

- 심리지수를 반영한 용량 계획 모델의 성능이 더 높은지 확인
- t-검정을 위한 표본들은 동일한 시퀀스의 데이터를 이용하여 동일한 타겟변수를 예측한 값이며, 한 표본에는 VKOSPI 변수를 포함하고, 다른 한 표본에는 VKOSPI 변수를 제외한 입력을 사용토록 한 것만 제외하고 모두 동일토록 처리하여 변수의 제외 전후 처리를 비교하는 대응표본 t-검정 예정

4

02 연구 방법

(연구 절차)



5

02 연구 방법

(분석 모델) 데이터 특성을 고려한 머신러닝 모델 결정

- ✓ 연구의 목적은 호가건수 이상치를 잘 예측하는 것
- ✓ 적은 데이터 양(영업일 기준 1571개, 약 7년치)과 다수의 이상치가 존재
- ✓ 따라서 적은 데이터에도 성능이 좋고, 이상치에 내성이 강한 분석 기법 결정

머신러닝 기법	
Regression 계열	Linear Regression(Ridge)
	Linear Regression(Lasso)
	SVM(Regression)
Decision Tree 계열	Decision Tree(Regression)
앙상블 계열	Random Forest(Regression)
	XGB Tree Ensemble(Regression)

1) Ridge, Lasso : 경사하강법을 이용하여 Mean Squared Error(평균제곱오차)가 최소화되도록 목적함수를 설정하는데 Lasso와 Ridge는 MSE에 L1, L2 페널티를 추가하여 목적함수를 변경함으로써 과적합을 어느정도 탈피할 수 있는 모델

2) RandomForest, XGBoost : 하나의 모델을 이용할 경우, 학습 데이터를 너무 잘 학습하는 과적합이 발생할 수 있기 때문에, 여러개의 모델들을 사용하여 종합적으로 판단하는 모델

3) Decision Tree : RandomForest와 XGBoost의 기본이 되는 모델로, 이상치에 대한 성능 차이를 비교하기 위함

4) Support Vector Machine : 표본 공간 내 클래스간 분류를 위해 선형회귀와 유사하게 벡터를 설정하되, 벡터의 두께를 나타내는 마진을 주어 분류하는 모델로, 과적합을 탈피할 수 있는 메커니즘은 없으나 성능이 매우 뛰어난 것으로 알려져 있어, 본 연구에서 이상치에 대한 성능 차이를 비교하기 위함

6

02 연구 방법

(평가 지표)

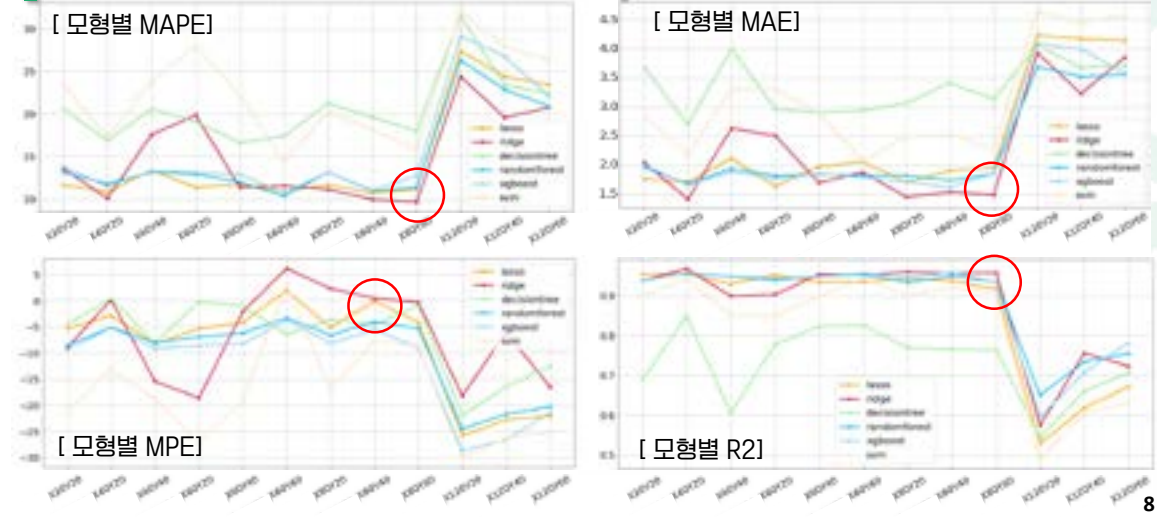
- ✓ MAE(Mean Absolute Error) : 예측값과 실제값의 모든 차이의 합을 의미
- ✓ MAPE(Mean Absolute Percentage Error) : MAPE를 백분율로 변환한 값
- ✓ MPE(Mean Percentage Error) : 모델이 과소 예측 또는 과대 예측 여부를 확인하기 위해 사용
* 음수일 경우 과대 예측, 양수일 경우 과소 예측을 의미하며 본 연구는 시스템의 용량계획을 예측하는 것으로 과소 예측을 회피하고, 최소 수준의 과대 예측을 하여야만 의미있는 모형이 될 수 있음

평가 지표	계산식
MAE	$\frac{1}{n} \sum_{i=1}^n (\text{예측값} - \text{실제값})$
MAPE	$\frac{1}{n} \sum_{i=1}^n \left(\frac{ \text{실제값} - \text{예측값} }{\text{실제값}} \right) \times 100$
MPE	$\frac{1}{n} \sum_{i=1}^n (\text{실제값} - \text{예측값}) \times 100$

7

03 연구 결과(성능)

(모형별 성능) 모형 9-1(x 80일, y 60일)이 최적의 성능을 나타냄



8

03 연구 결과(성능)

(모델별 성능) 과적합에 강한 모델이 전반적으로 우수한 성능을 보이며 Ridge가 최적의 성능을 보임

✓ 연구의 목적상 이상치가 존재하는 데이터의 특성에 따른 것

모형 9-1	Ridge	
	Test set	Training set
R2	0.9082	0.9073
MAE(건수)	1,493,032	1,175,366
MAPE(%)	9.65	8.74
MPE	-0.32	-1.14

모형 9-1	Lasso	
	Test set	Training set
R2	0.9177	0.9425
MAE(건수)	1,254,248	1,866,084
MAPE(%)	11.16	11.09
MPE	-4.71	-3.60

모형 9-1	Decision Tree Regressor	
	Test set	Training set
R2	0.6581	0.8378
MAE(건수)	3,589,260	2,814,066
MAPE(%)	23.69	18.10
MPE	-14.78	-6.65

모형 9-1	Support Vector Regressor	
	Test set	Training set
R2	0.9083	0.9310
MAE(건수)	2,299,528	2,292,674
MAPE(%)	15.78	15.87
MPE	-8.72	-3.48

모형 9-1	RandomForest	
	Test set	Training set
R2	0.9377	0.9441
MAE(건수)	1,820,411	1,590,680
MAPE(%)	11.29	9.41
MPE	-5.00	-3.68

모형 9-1	XGBboost	
	Test set	Training set
R2	0.9336	0.9788
MAE(건수)	1,862,303	1,194,277
MAPE(%)	11.71	8.22
MPE	-9.04	-2.92

9

03 연구 결과(심리지수 유의성)

- (성능) 심리지수를 포함한 모형과 포함하지 않은 모형간 R2 0.0183, MAPE 3.03% 성능 차 발생
 - ✓ 심리지수 미포함시, MPE 또한 양수를 나타내어 실제값 대비 과소예측 경향

Edge	Test set	
	모형 1-1	모형 1-2
R2	0.9582	0.9399
MAE(건수)	1,495,037	1,333,795
MAPE(%)	9.65	17.48
MPE	-0.39	6.45

- (t-검정) 심리지수를 포함한 모형과 포함하지 않은 모형의 테스트 데이터 예측결과 간 통계적으로 유의미한 차이 있음

- 한 표본에는 VKOSPI를 입력 변수로 포함하고 다른 표본에는 VKOSPI를 제외한 후, 동일한 시퀀스의 테스트 데이터를 이용하여 동일한 날짜의 호가(주문)건수를 예측하였으므로, 대응표본 통계량 검증 필요
- 정규성(Shapiro Wilk)을 만족하지 않아, 순위값을 이용한 비모수적 방법(Wilcoxon)을 사용하였으며 $p < 0.01$ 수준에서 두 표본간 유의미한 차이가 있음

10

04 과다한 IT 투자에서 현명한 IT 투자로...

(연구결과 및 토의)

- ✓ COVID-19 기간을 포함한 실증데이터를 이용하여 개발하였으며, 실무에서 활용 가능한 높은 성능과 안정성을 보유한 용량계획 모델 개발(Ridge R2 0.9582, MAPE 약 9.65%)
- ✓ 기업의 비용효율성을 최대한 높이되, IT시스템 용량 변경에 수반되는 실무적 제약을 고려한 최적의 x(관측 기간 80일), y(예측기간 60일) 값 제시
- ✓ 심리지수 VKOSPI를 포함할 경우, 의미있는 성능강화가 나타남을 입증 (성능, t-검정)함으로서, IT시스템의 용량계획에도 심리지수가 활용될 수 있음을 확인

(연구의 의미)

- ✓ 기존 수요예측 연구에서 거의 다루지 않았던 IT시스템의 용량계획에 머신러닝을 활용
- ✓ 자본시장 도메인에서 공통적으로 사용할 수 있는 용량계획 모델 개발, 기업의 비용효율성 증대 기여
- ✓ 심리지수가 IT시스템 용량계획에 중요한 변수임을 입증함으로서, 심리지수가 다양한 수요예측에 적극적으로 활용될 수 있음을 보여주고, 더 나아가 다양한 투자자 심리 데이터 가공, 지수화 확대 및 활용 촉진

11

감사합니다.



The Importance of 'Smooth' Data Usage and the Protection of Privacy in the Age of AI, the IoT and Autonomous Robots



Fumio Shimpo

(Professor of Faculty of Policy Management at Keio University / Japan)

발표개요

- The emerging technologies of AI and autonomous robots are forcing us to consider not only improvements in the development of their industrial use but also further urgent research into the ethical and legal issues. In the future, autonomous robots equipped with AI will become more widespread in our society and such robot acquisition of data may lead to data confidentiality issues which we are not able to solve just by focusing solely on AI-data acquisition issues. This presentation focuses on the possibilities of privacy violation and the issues which should be considered related to handling personal data and focuses on an introduction to the Japanese Personal Information Protection Act, the mutual adequacy findings between Japan and the EU, the Data Free-Flow with Trust (DFFT) initiative and future legal discussions about the increasing use of AI. Finally, I will point out the need to both clarify and streamline any related future regulations.

10th Asia Privacy Bridge (APB) Forum

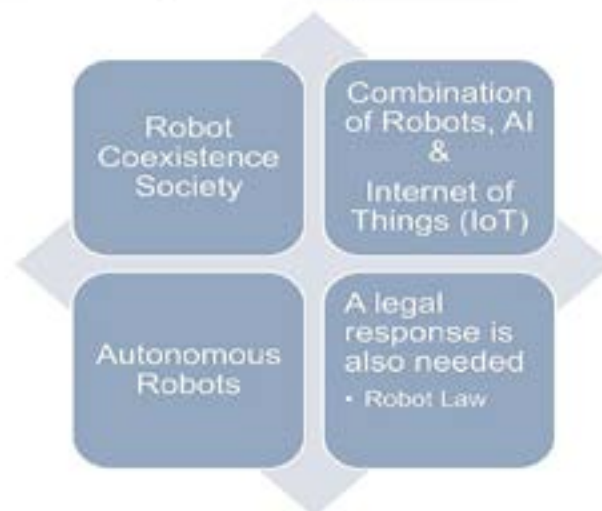
hosted by the Barun ICT Research Center of Yonsei University, Seoul, Korea
September 9th (Thursday)

The Importance of `Smooth` Data Usage and the Protection of Privacy in the Age of AI, the IoT and Autonomous Robots







Dr. Fumio SHIMPO

Professor
Keio University
Faculty of Policy Management

The Relationship Between Robots, Artificial Intelligence and the Internet of Things



Can AI be Used to Improve Human Moral Decision-making?

-  1. AI and robots are expected to be used in the future in improving quality of our life
-  2. Dramatically accelerated by the use of AI with 'open data' sources
-  3. It is likely that AI will be useful for understanding and investigating in detail past case studies
-  4. Improper use of such AI and robots could lead to 'Big Brother' risks
-  5. Decision-making will be changed drastically by using AI
-  6. It will also play an important role to improve human moral decision-making

2

Possible Future Problems regarding AI

- Foresee-ability of the Occurrence of Accidents
- Ensuring the Controllability and Transparency
- Legal Responsibility
- Legal Implications for using AI and Robots
 - Issues related to Civil Code
 - AI machine learning and the protection of intellectual property
 - Fintech
 - Trolley Problem
 - Collecting massive amounts of information
 - AI in business transactions and recommending products
 - AI profiling transactions

3

Reducing the Possibilities of Privacy Violation by AI Use



Using Image Processing as Security Feature in Information Retrieval



Mohd Afizi bin Mohd Shukran

(Professor in Department of Computer Science at the National Defence University of Malaysia / Malaysia)

발표개요

- Until recently, IR was an area of interest restricted mainly to librarians and information experts. A single fact changed these perceptions—the introduction of the Web, which has become the largest repository of knowledge in human history. Due to its enormous size, finding useful information on the Web usually requires running a search. And searching on the Web is all about IR and its technologies. Thus, almost overnight, IR has gained a place with other technologies at the center of the stage.

GUEST SPEAKER

USING IMAGE PROCESSING AS SECURITY FEATURE IN INFORMATION RETRIEVAL

Professor Ts. Dr Mohd 'Afizi Mohd Shukran



1

Modern Information Retrieval

- ▶ IR deals with the representation, storage, organization of, and access to information items
 - ▶ Types of information items: documents, Web pages, online catalogs, structured records, multimedia objects
- ▶ Early goals of the IR area: indexing text and searching for useful documents in a collection
- ▶ Nowadays, research in IR includes:
 - ▶ Modeling, Web search, text classification, systems architecture, user interfaces, data visualization, filtering and languages

2

IR at the center of the stage

- Until recently, IR was an area of interest restricted mainly to librarians and information experts
- A single fact changed these perceptions—the introduction of the Web, which has become the largest repository of knowledge in human history
- Due to its enormous size, finding useful information on the Web usually requires running a search
- And searching on the Web is all about IR and its technologies
- *Thus, almost overnight, IR has gained a place with other technologies at the center of the stage*

3

Content Based Image Retrieval

- ▶ Idea: identify and extract features related to image contents
- ▶ The problem: **content-based image retrieval** is the task of retrieving images based on their contents
- ▶ Query-by-example (QBE):
 - ▶ user supplies an image and the system finds other images that are similar to it
 - ▶ ignores semantic information associated with images
- ▶ Best ranking functions based on image properties that are not affected by variables
 - ▶ pose, camera focal length and focus, lighting, camera viewpoint, and motion

4

Swarm Intelligence In Information Retrieval

- ▶ Recently, a family of nature-inspired algorithms, known as *Swarm Intelligence* (SI), has attracted several researchers from the field of e-learning and information retrieval.
- ▶ The collective and social behaviour of living creatures motivated researchers to undertake the study which today is known as *Swarm Intelligence*.
- ▶ *Application of swarm intelligence to distributed visual information retrieval distributed over networks.*
- ▶ *Using ant-like or bee-like agents to crawl the network and to retrieve relevant images*
 - ▶ *Agents movements are influenced by markers stored on the hosts. These markers are reinforced to match the distribution of relevant images over the network.*

5

Concept of Swarm Intelligence

- ▶ SI systems are typically made up of a population of simple agents (an entity capable of performing/executing certain operations) **interacting locally with one another and with their environment.**
- ▶ Biological creatures, such as schools of fish and flocks of birds, clearly display structural order, with the behaviour of the organisms so integrated that even though they may change shape and direction, they appear to move as a single coherent entity such as **Particle Swarm Based Optimizers (PSO), Ant Systems and Artificial Bee Colony (ABC)**

6

Swarm Intelligence for Content Based Image Retrieval

- ▶ Image retrieval using swarm intelligence
 - ▶ The proposed pattern recognition technique use a correlation based feature selection algorithm in order to achieve higher detection accuracy rate than hand-coded signature approaches and payload-based anomaly detection techniques.
 - ▶ Develop a real-time detection algorithm that will improve the retrieval accuracy by detecting colour scheme such as RGB and YUV of the images
 - ▶ Profiles for the normal and for the attack patterns will be developed for the classification of network traffic as normal or attack based on geometric structure of network connections.

7

Artificial Bee Colony (ABC) for Swarm Intelligence (Cont.)

- ▶ The ABC algorithm was proposed by Karaboga – it simulates the foraging behaviour of a honeybee colony to solve multidimensional and multimodal optimization problems.
- ▶ ABC algorithm is a machine learning based NIDS.
- ▶ In the machine learning process, classification rule is crucial to identify the correct class in a population.
- ▶ The aim of classification rule is to find a set of rules which can identify the specific class from different groups.

8

CONCLUSION

- ▶ Biology-inspired algorithms such as GA and swarm based approaches like Ant Colonies have been successfully used in Information Retrieval particularly in Content Based Image Retrieval (CBIR).
- ▶ From the best of our knowledge, previous researchers have never applied the ABC algorithm in CBIR.
- ▶ Classification approach based on the swarm intelligence algorithm are effective in feature extraction process and retrieval accuracy.

9

REFERENCES

- ▶ D. Karaboga and B. B. Akay, "An artificial bee colony (abc) algorithm on training artificial neural networks," Erciyes University, Engineering Faculty, Computer Engineering Department, Technical Report TR062005, 2005.
- ▶ D. Karaboga and B. Basturk, "On the performance of artificial bee colony (ABC) algorithm," *Applied Soft Computing*, vol. 8, pp. 687-697, 2008.
- ▶ Y. Rui, T. S. Huang, M. Ortega, "Weighted support vector machine for classification," *IEEE Transaction on Circuits and Systems for Video Technology*, vol. 8, pp. 644-655,¹⁰ 2004.

THANK YOU

11

Contact tracing apps for self-quarantine in South Korea: Rethinking datafication and dataveillance in the COVID-19 age



Claire Seungeun Lee

(Professor, School of Criminology & Justice Studies,
University of Massachusetts Lowell / USA)

발표개요

- This study examines contact tracing mobile applications (hereafter, contact tracing apps) for those who were subject to self-quarantine through the lenses of dataveillance and datafication. Using an Internet ethnography approach, self-quarantined Korean individuals' blog entries were analyzed. The research argues that the application functions as a datafication tool that collects the self-quarantined people's information and performs dataveillance on the self-quarantined people. This research further offers insights for various agreements/disagreements at different actors (i.e. the self-quarantined, their families, contact tracers/government officials) in the process of contact tracing for COVID-19. This study also provides insights into the implications of information and technology as they affect datafication and dataveillance conducted on the public.

Contact tracing apps for self-quarantine in South Korea: rethinking datafication and dataveillance in the COVID-19 age

Claire Seungeun Lee, Ph.D.

Assistant Professor

University of Massachusetts Lowell



Table of contents



Background



Research aims
& questions



Framework




Data &
methods



Results



Concluding
remarks



This research is based on the following publication

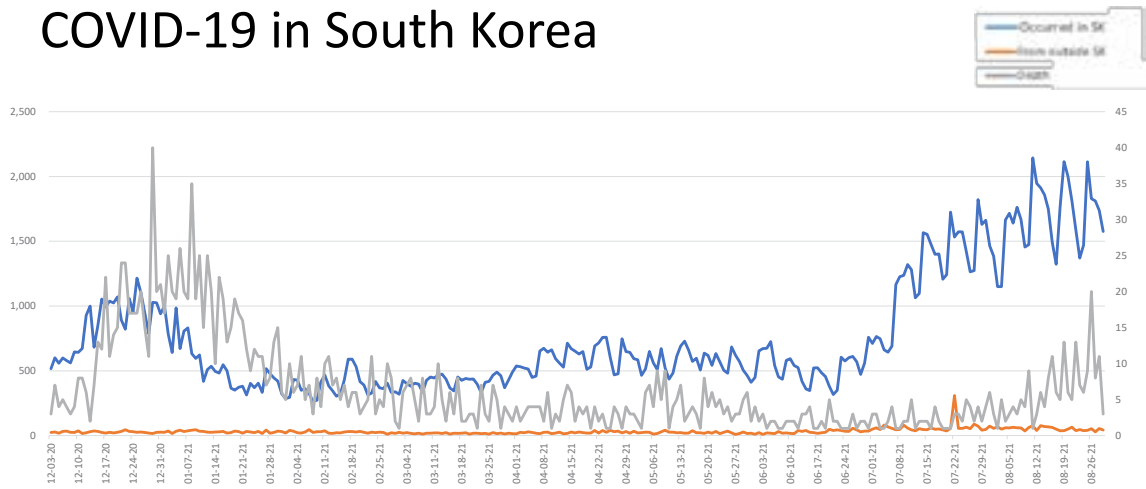
- Lee, C.S. (2021). "Contact tracing apps for self-quarantine in South Korea: rethinking datafication and dataveillance in the COVID-19 age", *Online Information Review*, 45(4): 810-829.



Background

- COVID-19 was first documented in China, and the virus was soon to be introduced to its neighbor – South Korea – on January 20, 2020.
- South Korea, one of the earliest countries to initiate a national pandemic response to COVID-19 with fairly substantial measures at the individual, societal and governmental level, is an interesting example of a rapid response to the disease in the Global South (Lee, 2020).

COVID-19 in South Korea

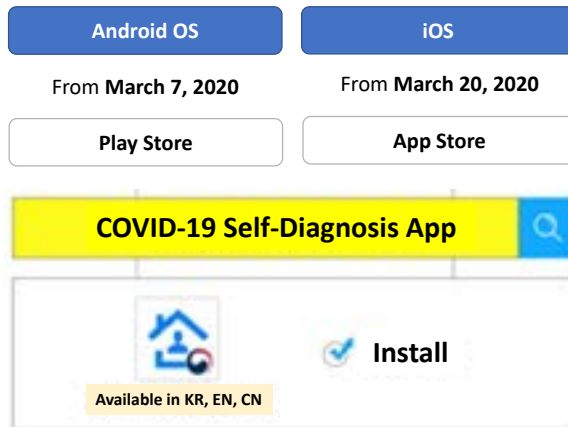


- As of 8/29/2021, 248,568 individuals were contracted with COVID-19 (235,117 individuals (95%) had the virus inside South Korea, the rest were from outside of the country).

Self-quarantine in South Korea

- Self-quarantine in the context of COVID-19
 - self-isolation for those who were international or domestic passengers by air and, thus, were suspected to be infected with the virus as a result of said travel.
- Since May 15, 2020, those who have traveled back to South Korea from other countries needed to follow stringent rules upon their arrival at Incheon Airport.

The COVID-19 Self-Diagnosis App



- Individuals installed the COVID-19 Self-Diagnosis App on their smartphone to report their temperature before walking through immigration.
- The Self-quarantine Safety Protection App, which aims to keep the government updated with recent travelers' self-diagnoses of their health conditions (e.g. high fever, cough, sore throat, dyspnea) twice a day, is for those who entered South Korea from overseas and keeps all self-recorded data private. People's manual input information does not go public.

The current research

- This study explores **a contact tracing mobile app** for those who practice self-quarantine named the Self-quarantine Safety Protection App through a lens of **dataveillance and datafication**.
 - This research examines what contact tracing means to those who experienced contact tracing in different roles, as well as how they make sense of their contact tracing experiences.
- This study uses an **Internet ethnography** approach to collect and analyze data.
 - In the COVID-19 pandemic era, this method is particularly useful to gain access to those who are affected by the situation.

Self-tracking applications and contact tracing apps in the COVID-19 era

- Self-tracking health applications, in particular those used to track and monitor the spread of COVID-19, inherently depend upon the accurate input of different types of personal data.
- **Contact tracing apps**
 - **For use by infected individuals**
 - As of 2020, 48 countries, not including South Korea, used COVID tracking (for infected individuals) utilizing Bluetooth, Location, Google/Apple and DT-3T technologies (Gilmor, 2020). Applications for contact tracing function as a way of keeping track of movement and these reshape ways in which people live and move and interact with each other (Aouragh et al., 2020; Kitchin, 2020). Contact tracing mobile devices can be used on a proximity-sensing base (Xia and Lee, 2020). Singapore’s TraceTogether is such an example (e.g. Goggin, 2020; Lee and Lee, 2020).
 - **For the self-quarantined** who have potentially, but are not confirmed to have, contracted the virus.
 - South Korea’s tracing applications include a feature that monitors movement to prevent those who are on the tracking radar from taking unauthorized leave from their designated quarantine location (“mudan ital bangji”).

Figure 1. The quarantine processes of Korean and foreign nationals upon arrival to South Korea



Source(s): Ministry of Health and Welfare (2020b)

Framework: Datafication and dataveillance

Datafication

- “a legitimate means to access, understand and monitor people’s behavior with data” (van Dijck, 2014, p. 198)
- Datafication is used to understand how self-diagnosis and personal information data that are stored in the App are datafied.

Dataveillance

- Continuous surveillance through the use of data (Lee, 2019; van Dijck, 2014).
- How people’s data is used as a tool in the process of surveilling and socially controlling people during this coronavirus pandemic.

A large graphic featuring a stylized tree with various digital and social media icons as leaves and branches, including a laptop, house, people, globe, music notes, and gears.

Internet ethnography

- Internet ethnography is a fairly new methodology, compared to traditional ethnography, in that it has only existed since the invention of the Internet and is based on online observations, interviews and content analysis of what is happening in cyberspace (Sade-Beck, 2004).
- The authentic public documentation of people’s lived experiences makes it a beneficial approach for collecting data.


#NETNOGRAPHY #WEB2.0

Data & methods

- The data were collected and derived from publicly accessible web forums and blogs in South Korea.
- The data were collected from May 15 to July 31, 2020, as May 15 is when the South Korean government's self-quarantine measures for inbound travelers took effect (Ministry of Health and Welfare, 2020a).
- I conducted a keyword search of COVID-19-related keywords ("i.e., COVID-19," "corona," "coronavirus") with keywords related to "self-tracking" (i.e. "jaga keokli" ("self-isolation)," "keokli" ("isolation"), "jaga keokli application" ("self-isolation app")) on Naver's blog entries and online cafes threads.
- These sites are extensively written in Korean, but as the focus of this research is on Korean citizens' understanding of the COVID-19 self-tracking applications, I paid attention to the possibility that some threads may be written in languages other than Korean and excluded them from the data set.

Data collection (con't)

- The data collected were available publicly, which means the original posters allow others to read, copy and paste without any requisite permission. While online information and data available on the Internet are usually considered public (Beneito-Montagut, 2011), in order to avoid potential ethical issues, I removed all personally identifiable information. Following a protocol of using screen captures from the Internet (Beneito-Montagut, 2011), all the images collected and obtained from Naver were anonymized and any personal/identifiable information was removed.



Data analysis

- To analyze data, they were first saved into an Excel file. The data were individually imported and analyzed using NVivo software.
- In the process of manual data coding/collection, various themes and codes emerged from the data and were noted.
- Codes and themes were created from initial readings of each data entry, and analyses of the data were produced along these identified codes and themes.
- A second person and I coded all of the data separately and then regrouped to check and code a sample of the data to verify our coding was consistent and reliable. The resulting intercoder reliability was 0.86, which is considerably reliable (Landis and Koch, 1977).



Self-quarantined Koreans' experiences with
the self-protection COVID-19 application



Datafication of self-quarantined information

- Blogger A, who came back to South Korea on July 2, 2020, wrote,

“The App is mandatory for those who returned to South Korea. I have to diagnose my health at 10 in the morning and 7 in the evening and save the information in the App. My information from the self-quarantine period is captured in the App. It’s like a diary” (Jeeyoung, July 2, 2020).



Self-quarantined’s information in the Self-Protection COVID-19 App

Dataveillance through one’s own personal, biometric, health and location data

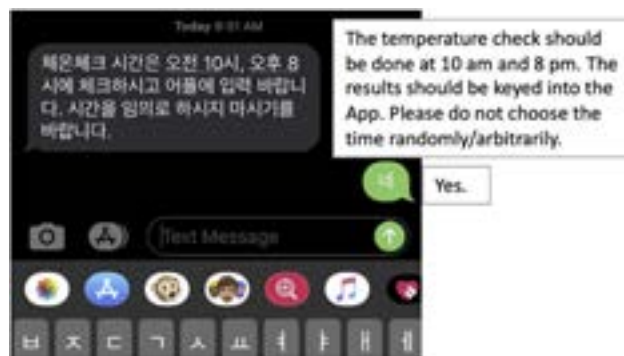
- While datafication and dataveillance are interrelated mechanisms for the Self-Protection COVID-19 App, some self-quarantined Koreans’ public opinions show disagreement and tensions in places where dataveillance was noticed.



Users’ agreement on personal & location tracking information

Passive dataveillance via personal data

- By default, the user must enter their personal information into the App. At least within the bounds of this Internet ethnographic study, almost no one seemed to care, nor seriously attempted to withhold their personal information from the App.
- Blogger XX commented,
“you know, as our very first step, I need to put all my personal information [in here]. I do not feel comfortable about this, but what can I do? I came back to my country from abroad, so there is no way out. If I do not do this, police might target me. .” The sense that the information requested via the App is highly personal, yet inescapable is no coincidence. Indeed, some of the personal data collected through the App are clearly classified as personal information.
- In the Korean Personal Information Protection Act, enacted in 2014, personal information refers to information that identifies a particular individual by his or her full name, resident registration number and/or image. In reality, available personal information becomes public data via datafied applications. In doing so, the application and the government become agents of dataveillance.



Dataveillance via (missing) health data

Dataveillance via the application's GPS

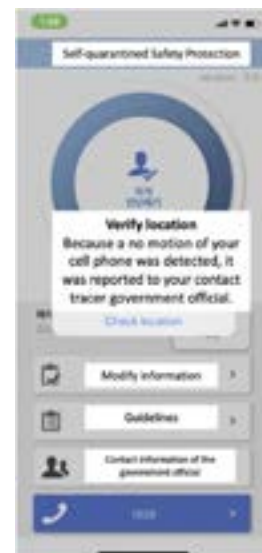
- A notification popped up on blogger C's phone that alerts,

"The App has used your location 2 times in the background over the past three days. Do you want to continue to allow background location use?"
- This feature
 - Whereabouts about the self-quarantined person recently was and is currently located at, reminding users of the importance and omniscience of the GPS function of the App.



Dataveillance via the application's "untraceable" GPS location

- If self-quarantined individuals leave their designated isolation place or accidentally or intentionally turn off the GPS function of the App, the App sends the following message and it notifies the contact tracers. Nara wrote that "I unexpectedly got a call from my contact tracer. He asked me where I am. I said that I am at home (I was thinking . . . I am doing self-quarantine properly) until he notified me that my GPS [for the App] turned off. I did not know about that." "I realized that I have been watched by someone. I totally forgot about that" (Nara, June 25, 2020).

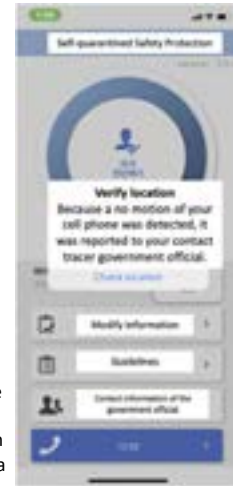


Dataveillance via the application's "untraceable" GPS location

Dataveillance through the App was happening in accordance with datafication of users' information on the App. The notification in Figure warns, "Your phone's motion was not detected for some time, it was reported to your contact tracer/case worker." The blogger Minho who posted this image complained, "It is troublesome. Just because I am self-quarantining, I do not always hold onto my phone (If I take a nap or use the computer, two or three hours just fly by)" (Minho, July 5, 2020).

When your eyes should be open, according to South Korean standards. . . day and night. If your phone is just lying still for about three hours, the App thinks you left the phone behind and went out. When there is an alert message from the App such as, "Nomotion was detected for some time, please check in," you must check, "Verify" or "Yes."

Like him, some passengers who traveled back to South Korea from Europe or the USA also experienced the effects of the time difference. They also need to adjust to the Korean time zone and might take a long nap after arriving. However, when the App's location tracking alert pops up, if individuals do not act immediately for whatever reason, it assumes that the user left the phone at home and went out. While being assigned to use the App may not be worrisome for some self-quarantined Korean citizens, the types and levels of data collection contents and the process required to collect it may pose some anxiety for them and create a tension between the App (the government) and the self-quarantined citizens.



Conclusion: Summary

- This paper shows how self-reporting applications function as a multifaceted technology in the COVID-19 era by combining a qualitative analysis of stories, which were obtained from the web.
- Datafication is used to understand how self-diagnosis and personal health and location data, which are stored in the App, are datafied.
- Dataveillance is a mechanism of how people's data are used as a tool of and process of surveilling and socially controlling the self-quarantined during the coronavirus pandemic.

Conclusion: Summary

- The actors
 - **the self-quarantined** are becoming increasingly familiar with how the App works and what implications the App might have for their data and lives.
 - **the contact tracers** (government officials) fulfill their duties and take responsibility for dataveillance of the self-quarantined people. They need to make sure the self-quarantined in their areas are observing the mandated guidelines.
- The data provided by the self-quarantined
 - symptom/nonsymptom data and location tracking data are particularly important for the purposes of datafication and dataveillance of the self-quarantined by both the App users themselves and the contact tracers.
- Datafication and dataveillance practices concerning the App have concerns and implications for privacy infringement.

Implications

- In regard to datafication/dataveillance, the coercive aspect of the App's required installation and usage makes it difficult for individuals to opt out of reporting and storing their data. From these individuals' perspectives, datafication and dataveillance are the products that follow from this App's existence.
- This aspect of such applications may be more relevant to critiques of the existing Personal Information Protection Act (Korea Legislation Research Institute, 2014), although most of the South Korean bloggers in this research normatively accept the compulsoriness of the App.



Claire S. Lee, Ph.D.
Claire_Lee@uml.edu



Data Privacy in the Philippines & COVID-19 response



Ivin Ronald D.M. Alzona

(Executive Director, National Privacy Commission / Philippines)

발표개요

– The National Privacy Commission (NPC) has been an active participant in the COVID-19 response of the Philippines as the data privacy authority of the country. The Commission believes that the fundamental right to privacy must always be upheld amid the pandemic, and data protection must not be sacrificed.

The discussion will present the initiatives of the Commission, such as but not limited to NPC Public Health Bulletins, FAQs, policies, in ensuring data privacy and protection during COVID-19 response.

DATA PRIVACY

In the PHILIPPINES &

COVID-19 RESPONSE

Atty. Ivin Ronald D.M. ALZONA

Executive Director
National Privacy Commission



NPC_DIT_PPF-V1.0, R0.0, 05 May 2021

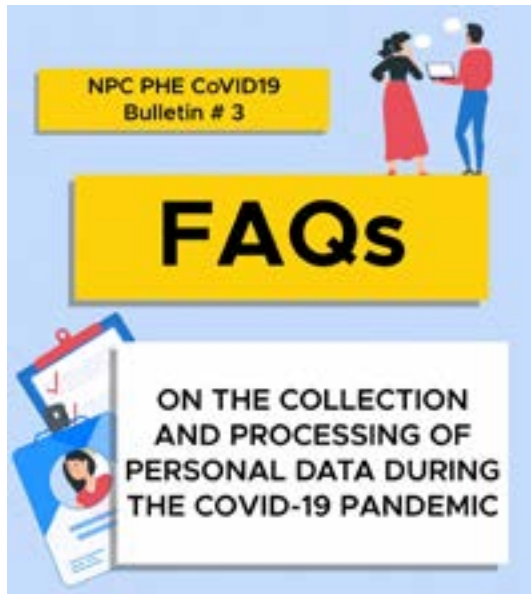
The Data Privacy Act of 2012 (DPA) is not a hindrance to the COVID-19 response.

NPC PHE BULLETIN No. 7: Official Statement of the National Privacy Commission on Calls for Patients to Waive Privacy Rights, Publicly Disclose Health Status



DATA PRIVACY IN THE PHILIPPINES & COVID-19 RESPONSE

2021



A On monitoring of persons entering offices/ buildings

B On employees; collection of personal data

C On contact tracing; persons under investigation



A On return to work

B On work from home



NPC & DOH Joint Memorandum Circulars



DATA PRIVACY IN THE PHILIPPINES & COVID-19 RESPONSE

2021

NPC PHE BULLETINS

19

Issued from February 2020 to May 2021



DATA PRIVACY IN PHILIPPINE'S COVID-19 RESPONSE

2021

NATIONAL PRIVACY COMMISSION
NPC PHE BULLETIN No. 8: On COVID-19-related apps, digital tools and solutions in this time of pandemic
NPC PHE Bulletin No. 12: Press Statement of Privacy Commissioner Raymund Enriquez Liboro on the collection of personal data to aid in contact tracing relevant to the COVID-19 response
Developers of LGUs' Contact-Tracing Apps Enjoined to Act as Privacy Watchers

PROTECTING PATIENT DATA FROM UNAUTHORIZED DISCLOSURE

GUIDELINES FOR ESTABLISHMENTS ON THE PROPER HANDLING OF CUSTOMER AND VISITOR INFORMATION FOR CONTACT TRACING

PERSONAL DATA PROCESSING FOR THE COVID-19 VACCINATION PROGRAM

NATIONAL PRIVACY COMMISSION

DATA PRIVACY IN THE PHILIPPINES & COVID-19 RESPONSE 2021

RESPONSE TO SOCIAL ISSUES

NATIONAL PRIVACY COMMISSION
Statement by Privacy Commissioner Raymund Enriquez Liboro on "Social Vigilantism" in the time of COVID-19
April 2, 2020 | 3:03 PM GMT+0800 LAC
Date: December 12, 2020

NATIONAL PRIVACY COMMISSION
NPC PHE BULLETIN No. 9: NPC Supports DILG's bid vs discrimination of COVID-19 frontliners
April 23, 2020 | 8:52 PM GMT+0800 LAC
Date: December 12, 2020

NATIONAL PRIVACY COMMISSION

DATA PRIVACY IN THE PHILIPPINES & COVID-19 RESPONSE 2021

ADAPTING TO QUARANTINE RESTRICTIONS



DATA PRIVACY IN THE PHILIPPINES & COVID-19 RESPONSE

2021

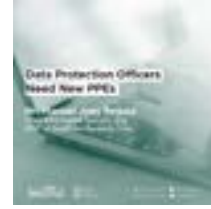
DPO JOURNAL



DATA PRIVACY IN THE PHILIPPINES & COVID-19 RESPONSE

2021

KNOWLEDGE SHARING BY PRIVATE SECTOR



DATA PRIVACY IN THE PHILIPPINES & COVID-19 RESPONSE

2021

JOURNAL RELEASES ON health



DATA PRIVACY IN THE PHILIPPINES & COVID-19 RESPONSE

2021

SOCIAL MEDIA REMIND ERS

Hindi porke't viral ay totoo
at dapat nang i-share,
lalo na kung may
personal data na kasama.



Everytime you feel like
sharing unverified or
speculative information,
wash your hands instead.



DATA PRIVACY IN THE PHILIPPINES & COVID-19 RESPONSE

2021



✉ ivin.alzona@privacy.gov.ph

🖱 privacy.gov.ph

THANK YOU!

Accountable and Trusted Transborder Data Flows by Building Convergence

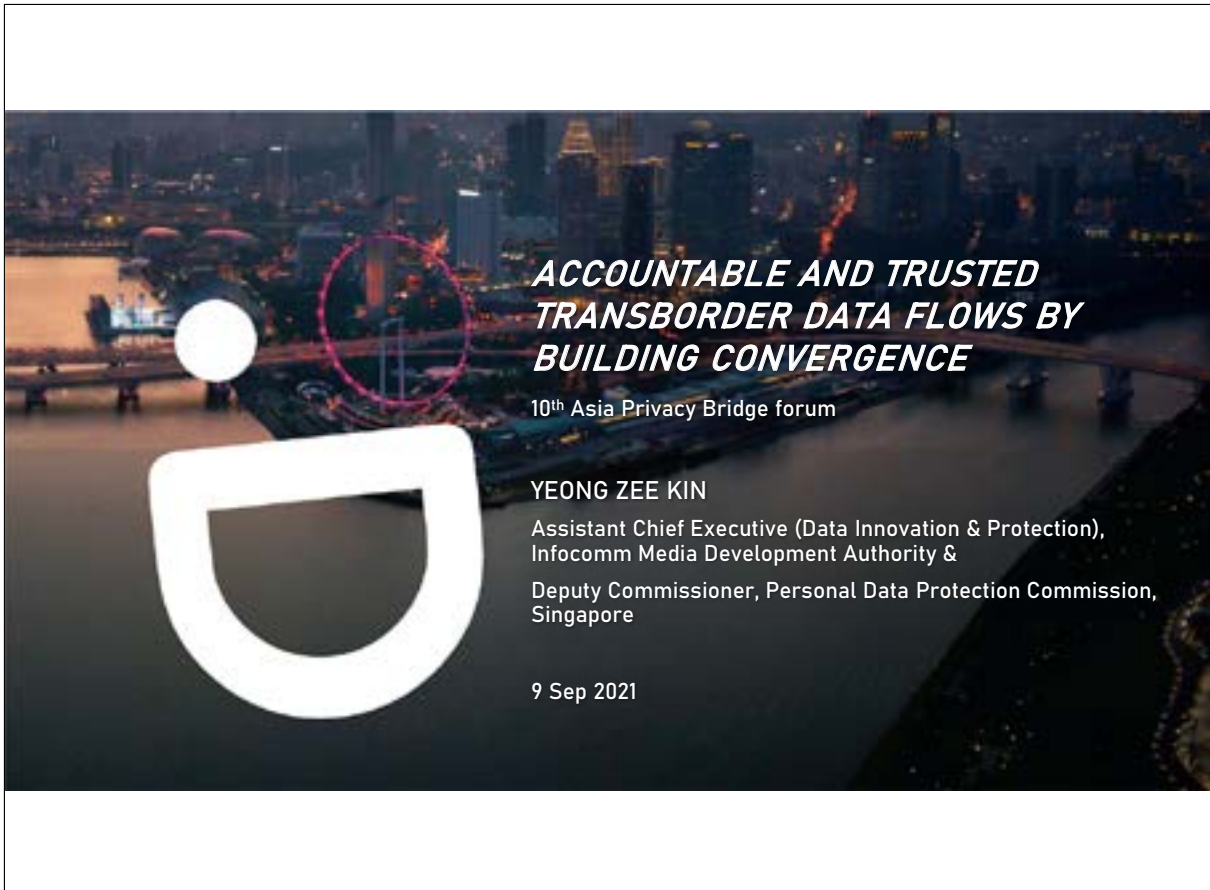


Zee Kin Yeong

(Deputy Commissioner, Personal Data Protection Commission / Singapore)

발표개요

- Singapore released a Model AI Governance Framework, a companion Implementation and Self-Assessment Guide for Organisations, and two volumes of Compendium of Use Cases to help industry implement trustworthy AI systems. As a logical next step, PDPC Singapore is developing a Minimum Viable Product (MVP) for AI governance testing. This MVP is a practical way forward to operationalise AI ethics principles, and it allows companies to be more transparent about their AI systems in order to build trust with their stakeholders.







***ACCOUNTABLE AND TRUSTED
TRANSBORDER DATA FLOWS BY
BUILDING CONVERGENCE***

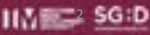
10th Asia Privacy Bridge forum

YEONG ZEE KIN
Assistant Chief Executive (Data Innovation & Protection),
Infocomm Media Development Authority &
Deputy Commissioner, Personal Data Protection Commission,
Singapore

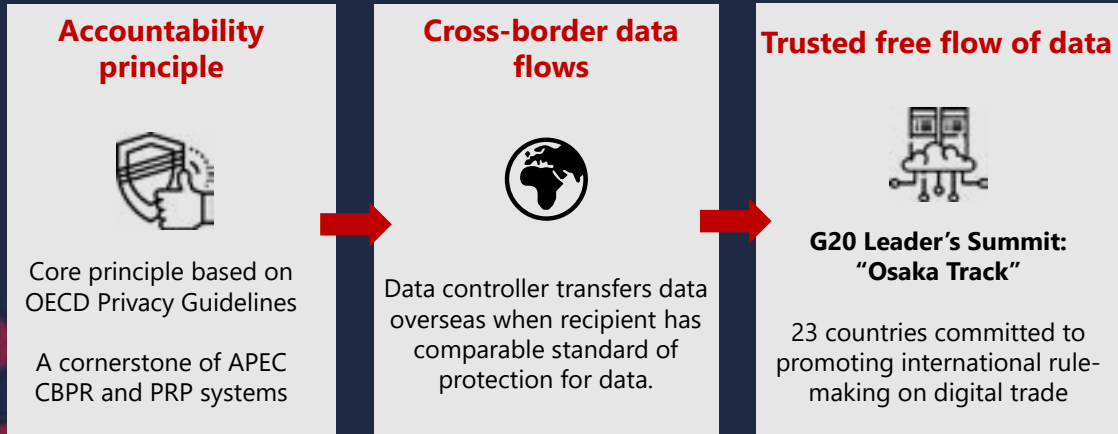
9 Sep 2021

Facilitating Data Flows in Era of Digitalisation

Data - a non-rivalrous resource	Accelerated digitalisation
 <p>Different organisations can benefit from working on respective copies of the same dataset.</p>  <p>Data therefore should not be hoarded within national borders.</p>	 <p>Digitalisation led to exponential increase in data generation and data flows.</p>  <p>Digital economies should build common standards to support safe transborder data flows.</p>

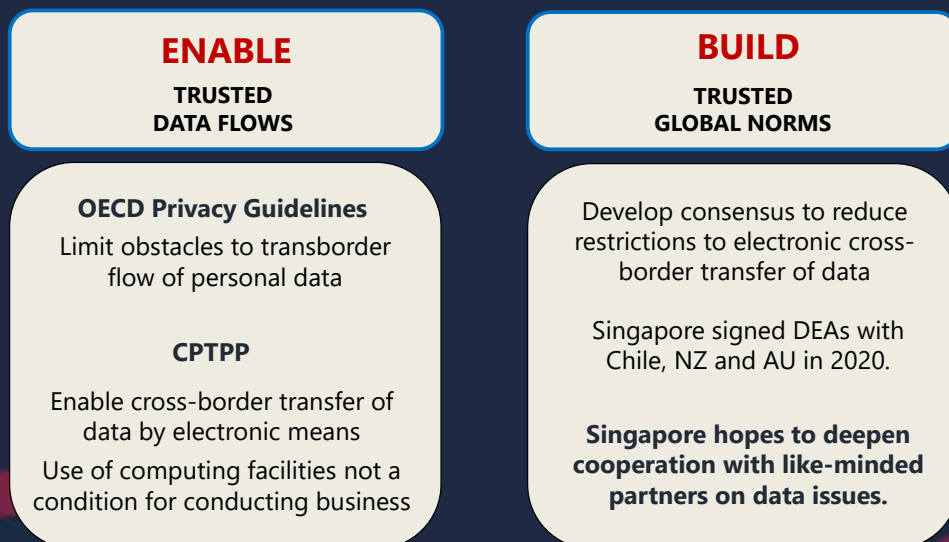


Accountability: Trusted Cross Border Data Flows



IIIM SG:D

Building Convergence for Data Flows: Digital Economy Agreements



IIIM SG:D

Building Convergence for Data Protection: APEC CBPR, ASEAN MCCs

CONSENT



Adequate for residual circumstances

Not ideal for recurrent transfers, i.e., service providers change periodically

CONTRACTS



E.g. EU SCCs, ASEAN MCCs, BCRs

Businesses impose data protection and security requirements on recipient.

Intra-group transfers: Support centralisation of corporate functions within MNC

CERTIFICATIONS



APEC CBPR and PRP systems:

Intra- & inter-company transfers between certified companies in participating countries

ASEAN to build certification system as part of ASEAN Cross-Border Data Flows Mechanism

Concluding Remarks

NEW AREAS

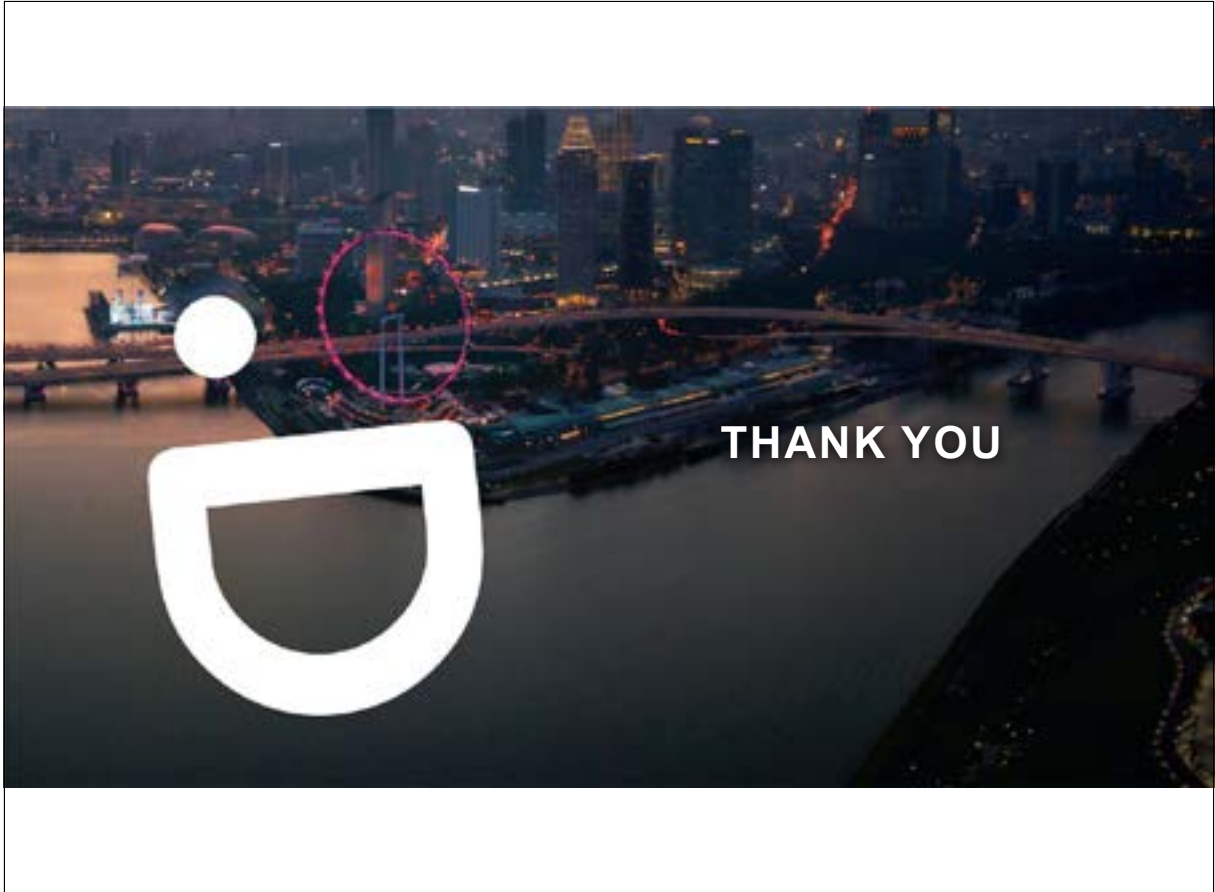


Ability for law enforcement to request for and access data across borders more easily.

FOCUS



Convergence for data flows and data protection through international rules and agreements key to maximising potential of data.



Global Personal Data Protection Regulatory Support Services by KISA



Jiyun Kim

(Deputy General Researcher, Korea Internet & Security Agency / Korea)

발표개요

- Introduce KISA's Global Personal Data Regulatory Support Services that provide beneficial information and analyses concerning global personal data protection-related issues, laws, and systems for helping Korean companies enter into overseas markets.

Personal Information Protection in Korea

– Introduction of Korea Internet & Security Agency (KISA) –



CONTENTS

- 0 1** Personal Information Protection Laws and Governance in Korea
- 0 2** Introduction of Korea Internet & Security Agency (KISA)



01 Personal Information Protection Laws and Governance in Korea – Constitutional Basis

Fundamental Right I

The right to privacy is a fundamental right and protected by constitution

'The right to privacy is a fundamental right which prevents the state from looking into the private life of citizens, and provides for the protection from the state's intervention or prohibition of free conduct of private living. Concretely, the privacy protection is defined as protecting and maintaining the confidential secrecy of an individual; ensuring the inviolability of one's own private life; keeping from other's intervention of such sensitive areas as one's conscience or sexual life; holding in esteem one's own personality and emotional life; and preserving one's mental inner world'. *Constitutional Court, 2003. 10. 30. 2002Hun-Ma518*

Fundamental Right II

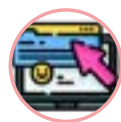
The right to control one's own personal information is a fundamental right

'The right to control one's own personal data is a right of the subject of the information to personally decide when, to whom or by whom, and to what extent his or her information will be disclosed or used. It is a basic right, although not specified in the Constitution, existing to protect the personal freedom of decision from the risk caused by the enlargement of state functions and info-communication technology.' *Constitutional Court, 2005. 5. 26. 2004Hun-Ma190 (Consolidated)*

01 Personal Information Protection Laws and Governance in Korea – Definitions



Personal Information



ID



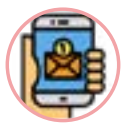
Account Number



Address



Name



Phone Number



Photo



Resident Registration Number



Other Information

Keywords of Personal Information

- 1 Living Individual
- 2 Identifiable if combined

Types of Personal Information

- 1 Financial Information
- 2 Unique Identification Number
- 3 Location-based Information
- 4 Sensitive Information
- 5 Biometric Information

01 Personal Information Protection Laws and Governance in Korea – Rights

Rights of Data Subject

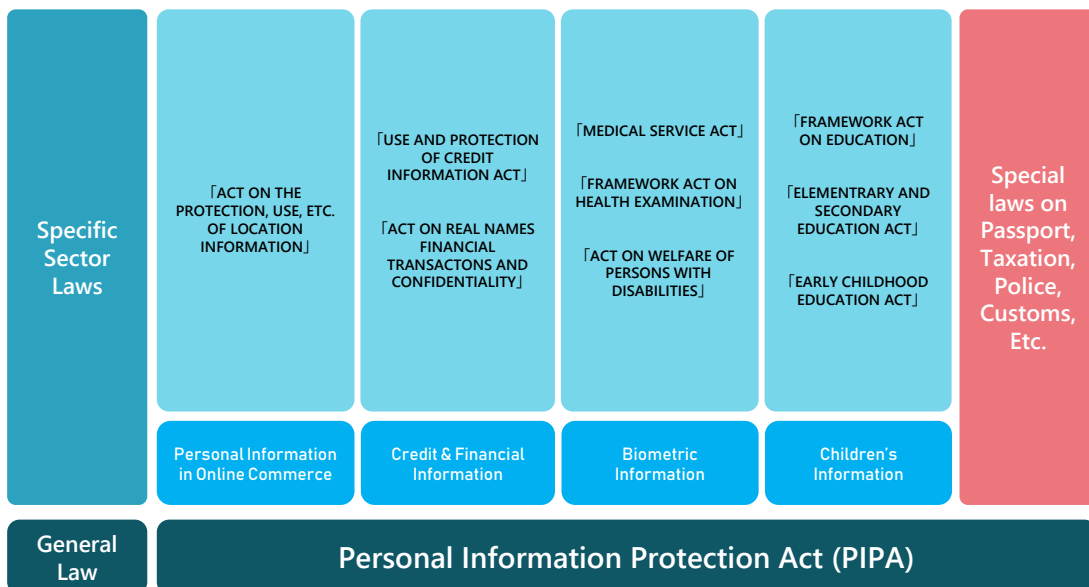
- 1 Right to be Informed
- 2 Right to Decide Consent-Related Matters
- 3 Right to Access
- 4 Right to Erasure
- 5 Right to Redress



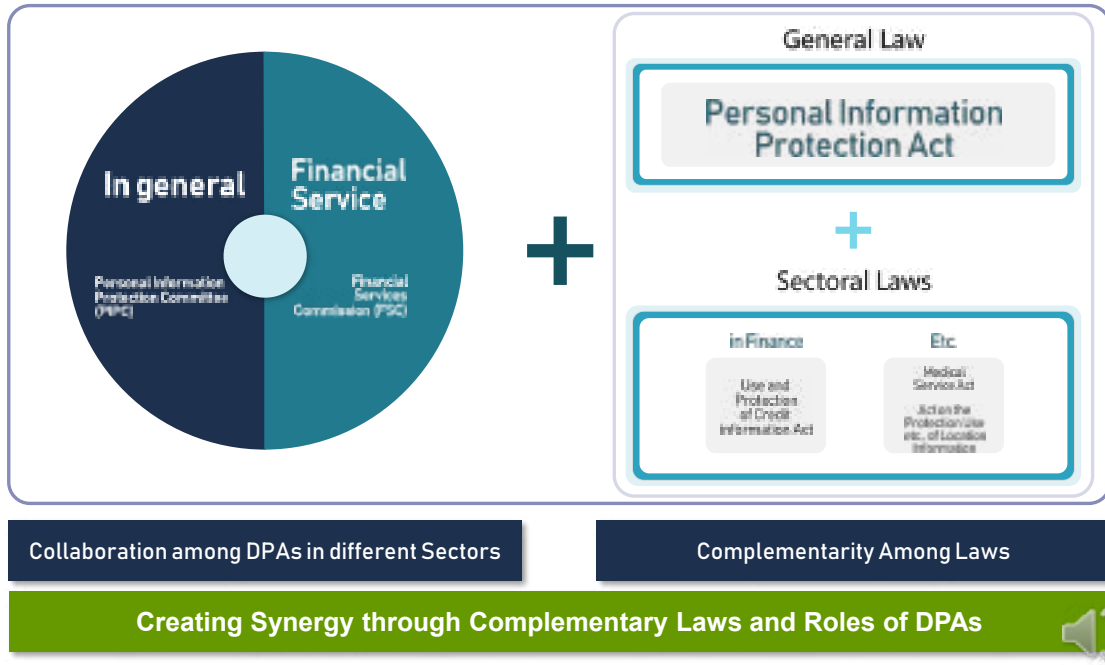
Personal Information Protection Act (PIPA)



01 Personal Information Protection Laws and Governance in Korea – Laws



01 Personal Information Protection Laws and Governance in Korea – Governance

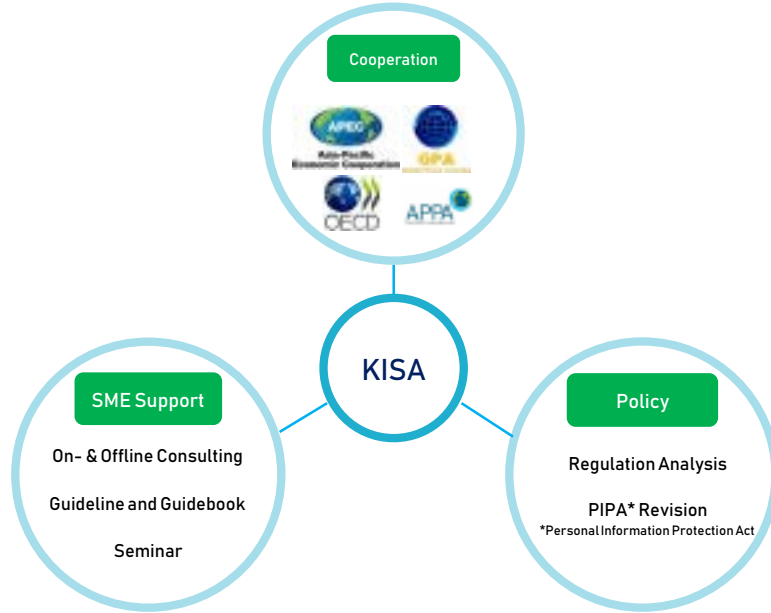


01 Personal Information Protection Laws and Governance in Korea – Video

Video – Introduction of Data Protection in Korea

02 Introduction of Korea Internet & Security Agency – Our Service

Korea Internet & Security Agency (KISA) Global Data Protection Regulation Compliance Service Summary

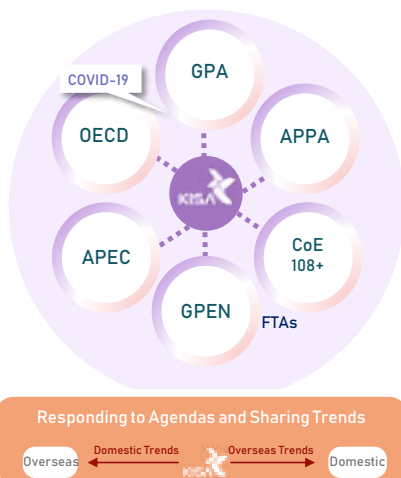


02 Introduction of Korea Internet & Security Agency – Our Service

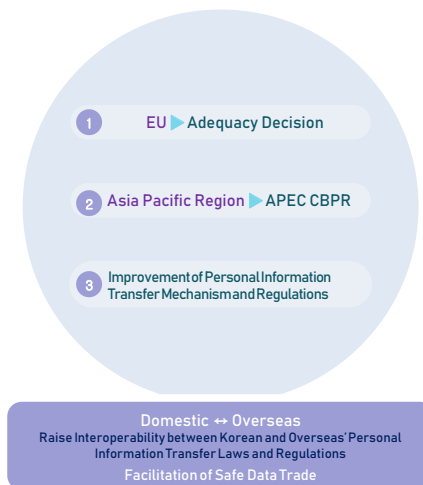
Global Data Protection Regulatory Support Service I

Development of International Cooperation and Interoperability between Korean and Global Regulations

International Cooperation



Regulation Interoperability

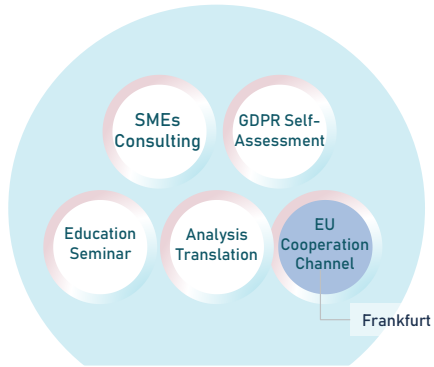


02 Introduction of Korea Internet & Security Agency – Our Service

Global Data Protection Regulatory Support Service II

Support Global Data Protection Regulation Compliance for SMEs

Support Global Data Protection Regulation Compliance



Aiming to provide One-Stop Global Data Protection Regulation Compliance Support Service

Currently providing information about personal information protection laws and regulations of 36 countries (EU: 27, U.S., U.K., China, Japan, Etc.)

<Global Compliance Support Service>



Personal Information Protection International Cooperation Center
(www.privacy.go.kr/pic)

<EU Region Compliance Support Service>



GDPR Compliance Support Center
(www.gdpr.kisa.or.kr)

02 Introduction of Korea Internet & Security Agency – Our Service

Global Data Protection Regulatory Support Service II

Support Global Data Protection Regulation Compliance for SMEs

<GDPR Compliance Support Service>



GDPR Compliance Self-Assessment Tool



GDPR Translation



GDPR Summary



Guidebook

02 Introduction of Korea Internet & Security Agency – Our Service

Global Data Protection Regulatory Support Service II

Support Global Data Protection Regulation Compliance for SMEs

<Global Data Protection Regulation Compliance Support Service>

Law & Governance



Global DPA List

Country	Law	Authority	Website
USA	California Consumer Privacy Act (CCPA)	California Information Privacy Protection Authority	https://www.cccpa.org/
UK	General Data Protection Regulation (GDPR)	Information Commissioner's Office (ICO)	https://ico.org.uk/
France	General Data Protection Regulation (GDPR)	Commission Nationale de l'Informatique et des Libertés (CNIL)	https://www.cnil.fr/
Germany	General Data Protection Regulation (GDPR)	Bundesbeauftragte für die Datenverarbeitung (BfDI)	https://www.bfdi.bund.de/
Spain	Organic Law of Data Protection (LOPD)	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/
Italy	General Data Protection Regulation (GDPR)	Garante per la Protezione dei Dati Personali	https://www.garanteprivacy.it/
Japan	Act on the Protection of Personal Information (APPI)	Personal Information Protection Commission (PPC)	https://www.ppc.go.jp/
South Korea	Personal Information Protection Act (PIPA)	Personal Information Protection Commission (PIPC)	https://www.kisa.go.kr/

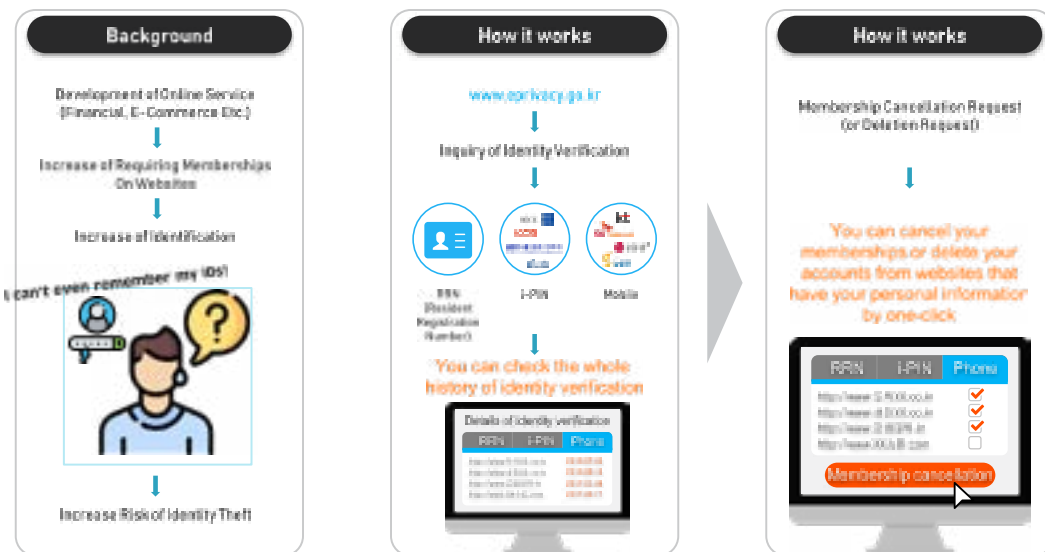
GDPR Summary



02 Introduction of Korea Internet & Security Agency – Our Service

ePrivacy Clean Service

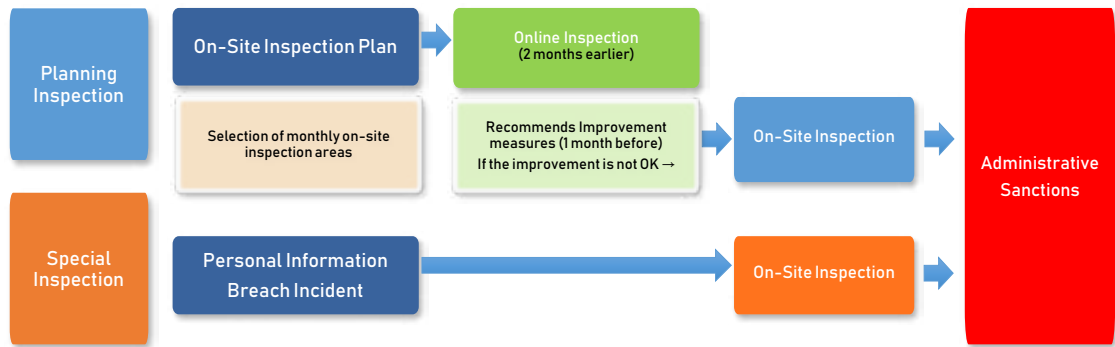
Service that helps data subjects to easily manage their personal information scattered on the Internet in one place



02 Introduction of Korea Internet & Security Agency – Our Service

Data Management Inspection
 On-site Inspection of Personal Information Management and Protection in Organizations

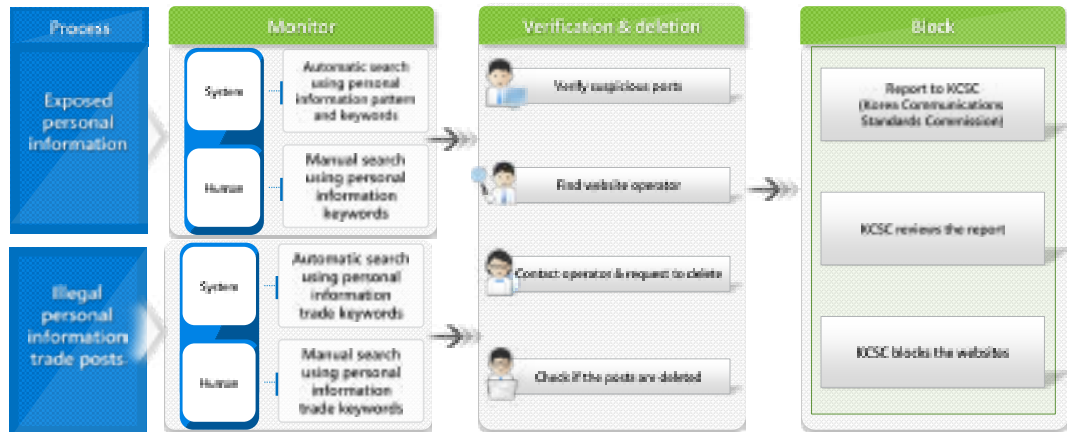
<Inspection Process>



02 Introduction of Korea Internet & Security Agency – Our Service

Personal Information Breach Monitoring
 24/7 Monitoring of Illegal Personal Information Transaction or Exposed Personal Information

<Monitoring Process>



02 Introduction of Korea Internet & Security Agency – Our Service

Personal Information Breach Monitoring

24/7 Monitoring of Illegal Personal Information Transaction or Exposed Personal Information

<Monitoring Process and Criteria Example>

Classification	Public Sector	Private online sector
Target websites	≒ 180,000	≒ 3,600,000
Direct	Search items	8 items(resident registration number, foreigner registration number, passport number, driver license number, bank account number, credit card number, health insurance number, mobile phone number)
	Search method	Search bot browses and does web crawling in target websites
	Interval	A group(1 day), B group(3 days), C group(1 week), D group(2 weeks)
Indirect	Search items	8 items + illegal personal information trade posts
	Search method	5 portals(Google, Naver, Daum, Bing, Yahoo) + 5 SNS(Twitter, Facebook, Instagram, Weibo, VK)
	Interval	2 days

02 Introduction of Korea Internet & Security Agency – Our Service

118 Data Breach Report Center

24/7 Data Breach Report Center for Illegal Spam, Phishing, Personal Information Breach, Hacking, and Virus, Etc.

<118 Data Breach Report Center>



02 Introduction of Korea Internet & Security Agency – Our Service

Education and Public Relations

Raise of Public Awareness about Personal Information Protection and KISA Service through On- and Offline Campaigns

<Education and Public Relations>

TV Public Service Announcement



Offline Education



Online Education for Kids



Outdoor Advertisement
(Baseball Stadium)



Outdoor Advertisement
(Supermarket)



Animation

Thank you for listening

For more information

Please Contact gdpr@kisa.or.kr / iprivacy@kisa.or.kr

or visit www.kisa.or.kr / www.privacy.go.kr/pic



Promoting comparability in personal data breach notification reporting



Suguru Iwaya

(Policy Analyst, Science, Technology and Innovation Directorate at the OECD)

발표개요

- The OECD project on “Promoting Comparability in Personal Data Breach Notification Reporting” aims at improving the evidence base for security and privacy policy making through the comparable data collection by Privacy Enforcement Authorities (PEAs). The presentation will show some of the project’s findings about the trends of personal data breach notification regulations and data collection by PEAs in light of the trends of breaches during the COVID-19 pandemics.



PROMOTING COMPARABILITY OF PERSONAL DATA BREACH NOTIFICATION REPORTING

Suguru Iwaya, Policy Analyst, Digital Economy Policy Division, STI, OECD



Project's background

- Based on the Ministerial Declaration on the Digital Economy in 2016
- Aims at evidence base for security and privacy policy making through compatible DBN reporting
- Survey questionnaire was circulated with the support from the GPA, APPA and EDPB from June 2019 to February 2020



Survey from June 2019 to February 2020

- The survey provides a wide range of information:
 - A. General questions and authority profile
 - B. Authority's funding and resources
 - C. Personal data breach notification reporting law, jurisdiction and exemptions
 - D. Personal data breach annual reporting
 - E. Number of personal data breach notifications received
 - F. Personal data breach notification by sector
 - G. The nature and type of the personal data breach incident
 - H. The types of personal data affected
 - I. Monetary fines and other penalties
 - J. Measures taken to prevent or mitigate risk and impact evaluation
 - K. Use of PDBN data
- Total of 35 countries that participated in the survey:
 - 32 OECD members (including 24 States reporting for the United States) and 3 non-members

3



What is data breach notification (DBN) ?

- Data breach
 - The general term 'data breach' refers to security incidents that impact on **non-personal data** as well as on **personal data**.
 - A 'personal data breach' can be described broadly as being a breach of security that leads to the unintended or unauthorised destruction, loss, alteration, disclosure of, or access to personal data.
- Personal Data breach notification
 - The regulatory requirements that require organisations to notify **the authority** and/or to **the affected individuals** following a personal data breach.
 - These requirements are **mandatory** or **voluntary**.
 - The **window** through which the authority and individuals can obtain information on data breaches.

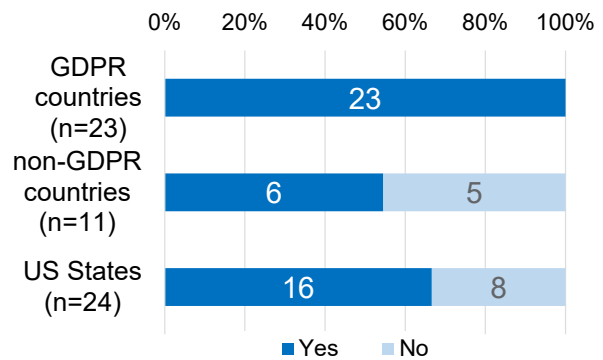
4



Trend towards mandatory PDBN reporting

- Trend towards mandatory personal data breach notification to the authority.
- In some jurisdictions mandatory PDBN reporting apply differently depending on the sector
- Thresholds to notify are generally based on a risk-based approach
- There are variations in mandatory PDBN reporting to data subjects

Number of countries that answered they have mandatory PDBN reporting to one or more authorities



Internationally comparable data metrics

Total number of data breaches reported to the authority

Nature of causes

- Malicious or non-malicious
- Internal or external
- Human error

Specific causes

- Loss of IT equipment
- Mailing
- Hacking
- Technical error
- Theft
- Improper disposal of documents
- Unauthorised access

Types of data breached

- Personal credential data
- Sensitive data
- Financial data

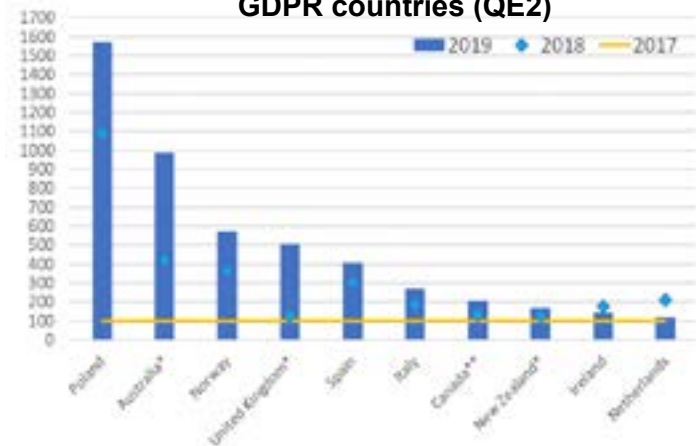
Information on encryption of data breached



Total number of data breaches reported to the authority

- Number of PDBNs generally increased from 2017 to 2019.
- Significant increase can probably be attributed to introduction of mandatory PDBN.

Change in the number of PDBNs from 2017 to 2018 and from 2018 to 2019 in GDPR countries (QE2)



* Numbers of PDBNs in 2017 are normalised to 100. Numbers of PDBNs in 2018 and 2019 are compared against this normalised value. To avoid overrepresentation of changes from small numbers, data less than 50 was eliminated from the calculation.

7



Recent trends of the total number of DBs

- Both increase and decrease in the number of PDBNs were observed.
 - e.g. DBNs reported in 2020 increased by 10% (Irish Data Protection Commission, 2021)
 - e.g. DBNs reported in 2020 decreased by 26% (UK ICO, n.d.)
- Impacts of mega breaches are increasing.
 - e.g. while the number of publicly disclosed breaches shrank by 48% in 2020, the number of records increased by 141% compared to 2019 (RiskBased Security, 2021)
- Other complementary indicators such as number of DBNs that meet the reporting threshold and number of the affected data subjects have gained importance.

8



Nature of causes

- Internationally comparable data items on nature of causes of DBs reflect the high-level trend of DBs
 - Malicious or non-malicious
 - Internal or external
 - Human error
- High-level trend continues after the survey period
 - e.g. Common causes of DBs: ‘email error’, followed by ‘other’, ‘website error’, ‘hacking’ (Privacy Commissioner New Zealand, 2020)
 - e.g. are malicious attack (52% of breaches), system glitch (25%), and human error (23%) (Ponemon Institute and IBM Security, 2020).
 - e.g. From November 2019 to October 2020, the top actions that caused data breaches were ‘hacking’, ‘social’, ‘error’, and ‘malware’ (Verizon, 2021).

9



Specific causes

- Internationally comparable data items on specific causes
 - Loss of IT equipment
 - Mailing
 - Hacking
 - Technical error
 - Theft
 - Improper disposal of documents
 - Unauthorised access
- Specific causes may need to be complemented by the explanation on the current threat environment.
 - the inclusion of “unauthorized disclosure” to reflect misdelivery and misconfiguration
 - An explanation to “theft” to clarify that it involves the theft of credentials through social engineering or reuse of stolen credentials for phishing

10



Types of data breached

- Internationally comparable data items on the types of data breached
 - Personal credential data
 - Sensitive data
 - Financial data
- The comparable data items capture the threat environment
 - e.g. “Personally Identifiable Information” is the top that 80% of breaches involved (Ponemon Institute, 2020); Top 2 were “Names”(46%) and Email (32%) in 2020 (Risk Based Security, 2021)
 - e.g. Medical data, financial data steadily increased since 2018 (Risk Based Security, 2021)
- “unknown” is enhancing the presence in the types of data breached

Does a Data Breach Harm Industry Peers? Evidence From the U.S. Retail Industry



Jaeyoung Park

(Research Professor, Graduate School of Information
at Yonsei University / Korea)

발표개요

- This study demonstrates that a data breach that occurs due to an industry-wide problem is likely to decrease the shareholder value of industry peers. Additionally, it has been shown that the data breach risk contagion effect is stronger for industry peers that have visibly disclosed data breach risk in their 10-K report before the data breach.

10th Asia Privacy Bridge Forum 2021

Does a Data Breach Harm Industry Peers? Evidence from the U.S. Retail Industry

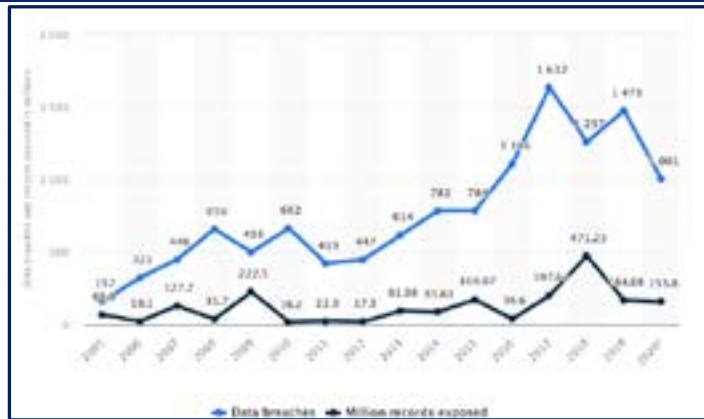
September 9, 2021

Jaeyoung Park

Postdoctoral researcher, Yonsei University



Data Breaches



Company	Date of Breach Disclosure	Cost of Breach
Home Depot Inc	September 2014	\$ 298,000,000
Target Corp	December 2013	292,000,000
TDK Companies Inc. ¹	January 2007	220,000,000
Heartland Payment Systems	January 2009	147,000,000
Arthen, Inc.	February 2015	115,000,000
Global Payments Inc	March 2012	114,200,000
Equifax Inc. ²	September 2017	87,500,000
RSA Security (EMC Corp)	March 2011	66,300,000
Ubiquiti Networks, Inc.	August 2015	56,100,000
Mondelez International, Inc. ²	June 2017	54,000,000

Source: <https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/>

www.AuditAnalytics.com
 1) Expanded population of breaches to 2007
 2) New disclosure of cyber-related costs/estimates

Source: <https://blog.auditanalytics.com/ranking-the-equifax-data-breach-updated/>

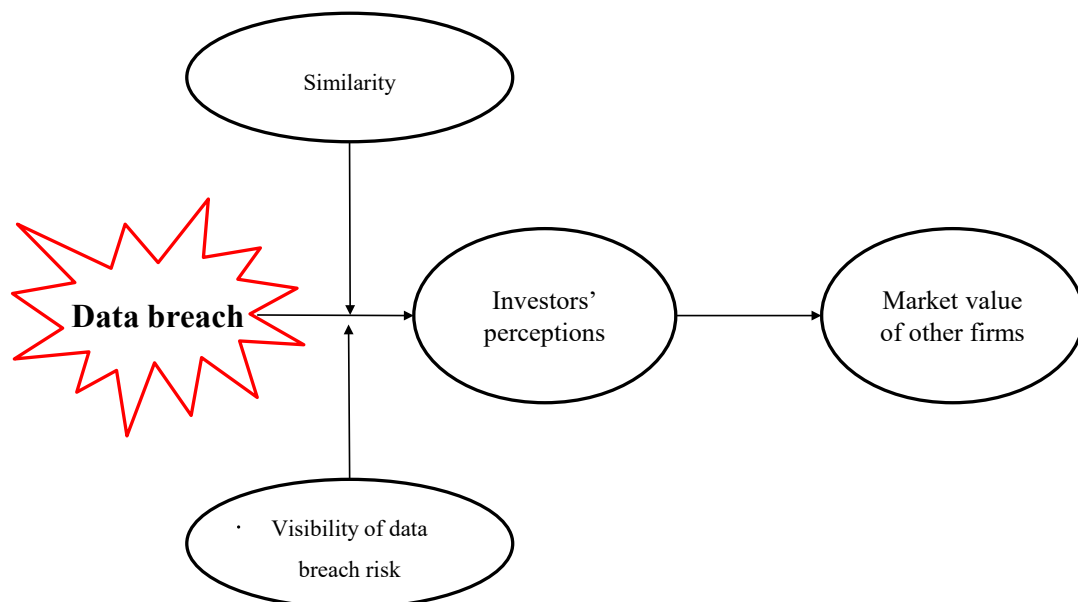


Investors' Perspective

- ❑ Most investors consider **cybersecurity** to be a critical component of risk oversight and they are engaging with portfolio companies to better understand how cybersecurity risk is governed and managed.
- ❑ A considerable body of research have explored **how investors react to security issues (events)**.
 - ✓ **Information security investment** leads to 1.36 percent increase of abnormal returns for firms (Chai et al, 2011); **ISO 27001 certification announcements** are associated with positive abnormal market value creation (Deane et al., 2019).
 - ✓ **Data privacy breach announcement** negatively affects the market value of the firm in general, although the negative impact is different across industries and type of breaches (Acquisti, et al., 2006; Malhotra & Malhotra 2011; Tripathi & Mukhopadhyay, 2020).
- ❑ Although previous research has demonstrated how a data breach can generate negative consequences to *the breached firm*, there is a lack of understanding of how a data breach at one firm affects *other firms* that have not been breached.

Guilt by association (“contagion effect”) vs. Gain by misfortune (“competition effect”)

Conceptual Framework of a Data Breach Spillover



Theoretical Background: Information Transfer

- ❑ **Information transfers** are said to occur if announcements (events) made by one group of firms contemporaneously affect the returns of another group of non-announcing firms (Schipper, 1990). e.g., bankruptcy (Lang & Stulz, 1992), accounting restatements (Gleason et al., 2008), financial misconduct (Paruchuri & Misangyi, 2015), or even environmental problems (Barnett & King, 2008).
- ❑ This effect can occur if information released by a firm has important implications for the **future profitability of other non-announcing competitors**.
- ❑ The information transfer effect typically arises among **intra-industry firms** rather than among completely unrelated companies, and it exists when information released by one firm affects **the performance of other non-announcing competitors** in the same industry (Szewczyk, 1992; Guo, 2017)
- ❑ There were negative mean abnormal returns among **Internet firms that were not attacked**: the competitors were presumed to be in a similar situation to the announcing firm owing to **industry commonalities** (Ettredge & Richardson, 2003).

Theoretical Background: Cybersecurity Risk Disclosure

- ❑ The SEC issued a disclosure guidance regarding **cybersecurity in 2011**.
 - ✓ According to the guidance, public companies should disclose the risks of cyberattacks or security breaches in their SEC filings if such incidents “are among the most significant factors that make an investment in the company speculative or risky” (SEC, 2011).
 - ✓ Cybersecurity risk disclosure provides investors with **useful information** about firms’ cybersecurity risks, and it may be positively associated with **the market valuation**.



10-K Report

TABLE OF CONTENTS

PART I	
Item 1	Business
Item 1A	Risk Factors
Item 1B	Unresolved Staff Comments
Item 2	Properties
Item 3	Legal Proceedings
Item 4	Mine Safety Disclosures
Item 4A	Executive Officers
PART II	
Item 5	Market for the Registrant's Common Equity, Related Stockholder Matters and Issuer Purchases of Equity Securities
Item 6	Selected Financial Data
Item 7	Management's Discussion and Analysis of Financial Condition and Results of Operations
Item 7A	Quantitative and Qualitative Disclosures About Market Risk
Item 8	Financial Statements and Supplementary Data
Item 9	Changes in and Disagreements with Accountants on Accounting and Financial Disclosure
Item 9A	Controls and Procedures
Item 9B	Other Information
PART III	
Item 10	Directors, Executive Officers and Corporate Governance
Item 11	Executive Compensation
Item 12	Security Ownership of Certain Beneficial Owners and Management and Related Stockholder Matters
Item 13	Certain Relationships and Related Transactions, and Director Independence
Item 14	Principal Accountant Fees and Services
PART IV	
Item 15	Exhibits, Financial Statement Schedules
SIGNATURES	

An Example of Item 1A in 10-K Report (Target corporation)

Competitive and Reputational Risks
Our continued success is dependent on positive perceptions of Target which, if eroded, could adversely affect our business and our relationships with our guests and team members.
 We believe that one of the reasons ...

Information Security, Cybersecurity, and Data Privacy Risks
If our efforts to provide information security, cybersecurity, and data privacy are unsuccessful or if we are unable to meet increasingly demanding regulatory requirements, we may face additional costly government enforcement actions and private litigation, and our reputation and results of operations could suffer. -> "subcaption"
 We regularly receive and store information about our guests, team members, vendors, and other third parties. We have programs in place to detect, contain, and respond to data security incidents. However, because the techniques used to obtain unauthorized access, disable or degrade service, or sabotage systems change frequently and may be difficult to detect for long periods of time, we may be unable to anticipate these techniques or implement adequate preventive measures. In addition, hardware, software, or applications we develop or procure from third parties may contain defects in design or manufacture or other problems that could unexpectedly compromise information security, cybersecurity, and data privacy. Unauthorized parties may also attempt to gain access to our systems or facilities, or those of third parties with whom we do business, through fraud, trickery, or other forms of deceiving our team members, contractors, and vendors.

Legal, Regulatory, Global and Other External Risks
The COVID-19 pandemic has affected our business in many different ways, and may continue to amplify the risks and uncertainties facing our business and their potential impact on our financial position, results of operations, and cash flows.
 The COVID-19 pandemic has ...

Examples of Cybersecurity Risk in the 10-K

Subcaptions of “low visible data breach risk” (no “data or information” keyword)

Bob Evans Farms: “We rely heavily on information technology and any material failure, interruption, or security breach in our systems could adversely affect our business.”

McDonald’s: “Information technology system failures or interruptions or breaches of network security may interrupt our operations.”

Subcaptions of “high visible data breach risk” (“data or information” keyword)

Barnes & Noble: “The Company faces data security risks with respect to *personal information*.”

Big Lots: “If we are unable to secure *company, employee, and customer data*, our systems could be compromised, our reputation could be damaged, and we could be subject to penalties or lawsuits.”

Method: Event Data (2013-2017)

- ❑ Data breaches related to **Point of Sale (POS)** in the U.S retail industry (SIC code 52-59), which allows us to test for the data breach risk contagion effect, because the POS system can be seen as a common vulnerability (risk) that almost all retail firms have.
- ❑ Data source: the LexisNexis database and data breach related databases such as Privacy Rights Clearinghouse (privacyrights.org)

Table 1. List of Breached Firms

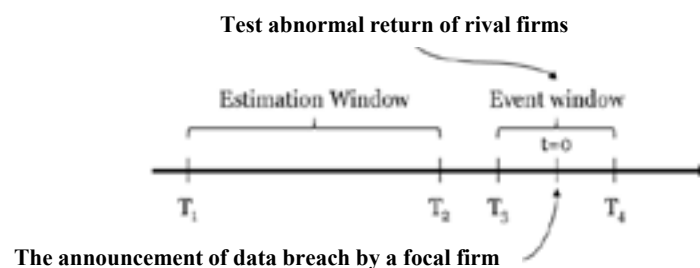
Event date	Event Firms	SIC	Asset [m\$]	Employee	Revenue [m\$]	Market value [m\$]
20131219	Target	5331	48,163	361,000	73,301	38,982
20140305	Sally Beauty Holdings	5990	1,950	26,450	3,622	4,300
20140902	Home Depot	5211	40,518	365,000	78,812	106,053
20141021	Staples	5940	11,175	83,008	23,114	8,591
20150302	Natural Grocers by Vitamin Cottage	5411	189	2,346	520	366
20150504	Sally Beauty Holdings	5990	2,030	27,470	3,753	4,233
20150615	Fred's	5331	649	9,148	1,970	613
20160511	Wendys	5812	4,108	21,200	1,870	2,933
20160519	Noodles & Company	5812	240	10,600	455	254
20170619	The Buckle	5651	580	8,600	974	1,028

Method: Sample (industry peers)

- ❑ Data source: COMPUSTAT from WRDS
- ❑ All non-breached firms with **the same two-digit SIC code** as breached firms.
- ❑ Standard Industrial Classification (SIC) codes are four-digit numerical codes assigned by the U.S. government to business establishments to identify the primary business of the establishment. The first two-digit of the SIC code indicates the major industry group, a definition widely used in the previous studies (e.g., Wang and Wang, 2019).
- ❑ After excluding any observations with confounding events at the time of the data breach or missing variables, I ended up with **310** samples of non-breached firms.

Method: Event Study

- ❑ The event study can offer insights in contexts where it would be more difficult to utilize alternative metrics of performance (Sorescu et al., 2017).
- ❑ Assuming efficient information processing of the breach announcement, the event window ought to be as short as possible (McWilliams and Siegel 1997). **CAR (-1,1)** is used as our dependent variable.



Method: Definition of Variables

Table 2. Definition of Variables

Variable	Definition	Source
Dependent variable		
CAR (-1,1)	The cumulative abnormal return for the industry peers in the three days surrounding the data breach event	Eventus from WRDS
Independent variable		
Visible data breach risk	Dummy variable, equal to 1 if "data" or "information" keywords are included in the subcaptions related to security risks in Item 1A of 10-k filings at the end of the fiscal year before the data breach, 0 otherwise.	EDGAR
Similarity	Dummy variable, equal to 1 if the non-breached firm's four-digit SIC code is the same as the breached firm, 0 otherwise. For example, when a breached firm is Target (SIC code 5331), Costco Wholesale (SIC code 5399) is coded as 0, and Walmart (SIC code 5331) is coded as 1.	Compustat from WRDS
Control variable		
Prior performance	The ratio of net income to total assets (Compustat annual item: NI/AT)	Compustat from WRDS
Firm size	Natural log of total assets in millions (Compustat annual item: AT)	Compustat from WRDS
Growth	The ratio between the book and the market value of firm's equity (Compustat annual item: CEQ/MKVALT)	Compustat from WRDS
Massive breach	Dummy variable, equal to 1 if non-breached firms is sample of the Target or Home Depot breach is, 0 otherwise.	PRC
Past breach	Dummy variable, equal to 1 if non-breached firms experience data breach(es) prior to the breach, 0 otherwise.	PRC

Results: Data Breach Risk Contagion Effect

- the CAAR for the 3-day event window (-1,1) was -0.68% and was statistically significant ($p < 0.001$). It suggests that a data breach is likely to decrease industry peers' shareholder value.
- Evidence of the negative spillover effect of data breach or the data breach risk contagion effect

Table 3. Impact of Data Breach on Abnormal Stock Returns for Industry Peers

Event window	SIC sample (N = 310)		
	CAAR (%)	Uncorrected Patell Z	Generalized Sign Z
(0, 0)	-0.42	-3.077**	-3.464***
(-1, 0)	-0.64	-3.705***	-3.805***
(-1, 1)	-0.68	-3.320***	-2.669**
(-1, 2)	-0.72	-2.844**	-2.555**
(0, 1)	-0.45	-2.536**	-3.578***
(0, 2)	-0.49	-2.035*	-1.874*

Note. The symbols †, *, **, and *** denote statistical significance at the 10, 5, 1, and 0.1% levels, respectively, using a generic one-tail test.

Results: The Role of Similarity

- ❑ The market values of industry peers with high similarity significantly decreased, while those of industry peers with low similarity did not.
- ❑ In an event window of (-1,1), for example, the CAAR of the former was -1.602% and it was statistically significant ($p < .001$), whereas the latter was 0.173% and it was not statistically significant.
- ❑ The differences between groups were statistically significant for various event windows.

Table 4. Comparison Between Industry Peers by Similarity

Event window	Low similarity (N = 158)		High similarity (N = 152)		Difference test
	CAAR (%)	t-value	CAAR (%)	t-value	
(-1, 0)	0.126	.313	-1.480	-5.523***	3.295***
(0, 1)	0.160	.520	-1.077	-4.304***	3.108***
(-1, 1)	0.173	.407	-1.602	-4.786***	3.269***

Note. CARs are calculated using the market model. The symbols *** denote statistical significance at the 0.1% levels.

Results: The Role of Cybersecurity Risk Disclosure

- ❑ The market values of industry peers with high visible data breach risks significantly decreased, while those of industry peers with low visible data breach risks did not.
- ❑ In an event window of (-1,1), for example, the CAAR of the former was -1.223% and it was statistically significant ($p < .001$), whereas the latter was 0.267% and it was not statistically significant.
- ❑ The differences between groups were statistically significant for various event windows.

Table 5. Comparison Between Industry Peers by Data Breach Risk Disclosure

Event window	Low visible data breach risks (N = 118)		High visible data breach risks (N = 187)		Difference test
	CAAR (%)	t-value	CAAR (%)	t-value	
(-1, 0)	0.293	.580	-1.194	-4.881***	2.942**
(0, 1)	0.124	.329	-0.743	-3.237***	2.085*
(-1, 1)	0.267	.524	-1.223	-3.903***	2.638**

Note. CARs are calculated using the market model. The symbols *, **, and *** denote statistical significance at the 5, 1, and 0.1% levels.

Discussion

- ❑ One firm's data breach harms the market value of industry peers.
 - ✓ This study provides additional evidence for the data breach risk contagion effect, indicating one firm's loss is also its competitor's loss.

- ❑ The data breach risk contagion effect is stronger for non-breached firms with high similarities to a breached firm, compared to those with low similarities.

- ❑ The data breach risk contagion effect is stronger when the risk of data breaches is visibly disclosed in industry peers' 10-K report.
 - ✓ The market response to cybersecurity risk disclosures offers mixed results.
 - ✓ This study adds new evidence to the effect of cybersecurity risk disclosure.

***Thank you for your attention.
Any questions or comments?***