

# 국내외 핀테크 관련 기술 및 정책동향 분석을 통한 연구분야 발굴

Excavating research areas of FinTech through the  
analysis of its relevant technologies and policy trends at  
home and abroad

2016. 2.

수탁기관 : (재)한국디지털융합진흥원

## 제 출 문

한국인터넷진흥원 원장 귀하

본 보고서를 “국내외 핀테크 관련 기술 및 정책 동향 분석을 통한 연구분야 발굴”의 최종연구개발 결과보고서로 제출합니다.

2016년 2월 29일

수탁 기관 : (재)한국디지털융합진흥원

연구책임자 : 교 수 최 성(남서울대학교 컴퓨터학과)

참여연구원 : 교 수 노 시춘(남서울대학교 컴퓨터학과)

교 수 기 창진(남서울대학교 컴퓨터학과)

연구원 김 명 수((주)듀얼로그)

연구원 이 상덕((재)한국디지털융합진흥원)

연구원 김 두찬((재)한국디지털융합진흥원)

연구원 구 교광((재)한국디지털융합진흥원)

연구원 박 영진(남서울대학교멀티미디어학과)

연구원 최 유진(숙명여자대학교 중국어학과)



## 요 약 문

### 1. 제목 : 국내외 핀테크 관련 기술 및 정책 동향 분석을 통한 연구분야 발굴

### 2. 연구의 목적 및 중요성

클라우드 컴퓨팅 기술혁신은 기존 산업과 융합으로 새로운 일거리를 창출하고 있다. 특히 금융 분야에서는 IT기술과 결합되면서 핀테크라는 창조분야에서 일자리를 창출하고 있다. 전세계 다국적 거대 금융기관에서부터 벤처기업에 이르기까지 비즈니스와 생활 전반에 아우르는 금융의 혁신을 실시하고 있다.

본 연구에서는 금융분야의 핵심인 지급·결제, 송금, 대출, 투자 및 자산관리, 전자화폐, 금융정보 등 핀테크의 분야와 기존 서비스의 역할을 대체하거나 신규 시장을 개척한 주목할 만한 핀테크 스타트업 기업들의 환경 및 동향을 연구하였다.

IT환경변화와 더불어 금융 거래 환경의 변화를 인지하며 새롭게 등장하는 전자금융사기, 개인정보 유출 사고 등 다양한 금융 관련 보안 위협이 발생하고 있다. 이와 같이 핀테크에 대한 편리하다는 기대감과 달리, 본질적인 카드사 정보유출 사고 및 해킹 등으로 ICT 기술을 활용한 금융서비스의 안전성 확보에 있어서 우려가 높아지고 있다.

핀테크 산업의 발전과 진화는 정보보호와 동반 성장하지 않고는 불가

능하다. 규제 완화와 보안 강화의 최적의 물을 만들어야 한다. 핀테크 기업들의 불안정한 서비스로 대형 보안사고가 발생할 경우 핀테크 산업 발전에 악영향 줄뿐 아니라, 금융서비스의 근간인 신뢰가 무너지고 만다. 핀테크에서의 보안은 금융서비스와 기업의 생존을 결정하는 핵심 가치이다.

핀테크는 보안 대책이 뒷받침 되지 않으면 어떠한 보안 위협이 발생할지 모른다. 사용자의 접근성은 간편하게, 사용자의 안전성은 강화되어야 하는 양날의 칼과 같다. 그래서 편의성과 보안의 조화가 필요하다. 또한, 피해를 최소화할 수 있도록 법적 책임을 명확하게 하되 이해당사자간에 이해와 합의가 필요하다. 이렇게 핀테크 산업이 바람직하게 발전하고 금융 혁신을 이루기 위해서는 무엇보다 핀테크의 보안성 강화를 위한 기술이 필요하다.

### 3. 연구의 내용 및 범위

- 국내외 핀테크 관련 시장, 정책, 서비스 동향 분석
  - 국내외 핀테크 시장동향 및 트렌드 분석
  - 국내외 핀테크 정책동향 분석
  - 국내외 핀테크 서비스 및 스타트업 동향 분석
- 국내외 핀테크 서비스 보안기술 분석
  - 국내외 핀테크 서비스관련 보안위협 및 사고 사례분석(결제사기 등)
  - 모바일 기반 핀테크 서비스 보안기술 분석(FDS 등)
- 모바일 결제사기 대응기술 관련 연구 및 적용분야 도출
  - 모바일 기반 핀테크 보안기술 연구 분야 도출
  - 모바일 결제사기 대응기술 개발을 위한 적용분야 도출

#### 4. 연구결과

- 국내 핀테크 스타트업 지원 프로그램 및 정책 조사
  - 공공·민간부문에서 추진 중인 스타트업 지원 프로그램 조사
  - 국내 핀테크 분야 스타트업 지원 프로그램 활용 우수사례 조사
- 주요 국가(영국, 미국, 일본, 중국)의 스타트업 지원 프로그램 및 정책 조사
  - 정부 주도의 스타트업 지원 프로그램 운영 기관 및 지원정책 조사
- 핀테크 스타트업과 핀테크 보안 수요예측으로 핀테크산업육성 법률 및 핀테크보안 법안 입안시 기본자료로 제공
  - 공공 및 민간 컴퓨팅자원 활용으로 창조경제 스타트업기업 육성 효율화
- 모바일 결제사기 대응기술 관련 연구 및 적용분야 도출
  - 모바일 기반 핀테크 보안기술 연구분야 도출
  - 모바일 결제사기 대응기술 개발을 위한 적용분야 도출
  - 국내외 핀테크 서비스 관련 보안 위협 및 사고 사례 분석(결제사기 등)
  - 모바일 기반 핀테크 서비스 보안기술 분석(FDS 등)

#### 5. 활용에 대한 건의

- 핀테크산업 육성 법률 및 핀테크보안 법안 입안시 기본자료로 제공
- 공공 및 민간 컴퓨팅자원 활용으로 창조경제 스타트업기업 육성 효율화
- 핀테크 기업육성으로 안전하게 상거래를 할 수 있는 서비스가 전세계 언제 어디서나 가능
- 동일 가치사슬군(금융 기업간) 협업 및 비즈니스 공유가능으로 경제적 사회적 생산성향상 가능
- 창조경제시대에 맞는 핀테크산업 육성으로 금융업의 해외진출 및 일자리창출

## 6. 기대효과 (관련분야 예상파급효과)

- 핀테크 스타트업 창업 비용절감 및 유연성 확보
- 클라우드 기반 브러커 양성 및 블록체인, 비트코인 기술 전망
- 핀테크산업과 관련된 응용분야(Bio, IoT, Big data 등) 발굴
- 창의적인 중소, 벤처기업의 성장 생태계를 형성하고 핀테크 서비스 신규 수요에 대한 투자가 확대
- 빅데이터 등 신산업과 소프트웨어 및 IT 융합산업의 활성화를 통해 다양한 사업기회를 제공
- 핀테크 스타트업 도입의 ROI 제고 및 확산 가속화
- 핀테크 스타트업 생태계 활성화를 위한 정책자료로 활용
- 국내 핀테크 산업 육성을 저해하는 규제 개선 제언을 위해 활용 가능

# SUMMARY

**1. Title :** Excavating research areas of FinTech through the analysis of its relevant technologies and policy trends at home and abroad

**2. The purpose and significance of research**

The technology innovation of cloud computing is creating new jobs through its fusion with traditional industries. Particularly in the financial sector, its fusion with IT is creating new jobs in a creative sector called FinTech. Fintech is carrying out financial innovations across business and life in general, ranging large multinational financial institutions to ventures around the world.

In this research, sectors of FinTech – the core of financial sector, such as payment, remittance, loans, investment and asset management, electronic money, financial information, and etc. are studied. The environment and trends of remarkable FinTech start-up companies, replacing the role of existing services or pioneering new markets, are also studied.

Since electronic banking environment is being changed according to the changes of IT environment, various finance related security threats, such as electronic banking fraud, leakage of personal information from credit card companies, hacking and etc. are newly being emerged. These threats can put serious worries about the safety of financial services based on IT services and be critically against the expectation of the convenience of FinTech.

The evolution and development of FinTech industry is impossible without growth associated with information protection. The optimal rules of deregulation and increased security are supposed to be made. If a



large security incident is caused by a FinTech company as a result of its unsafe services, it may not only adversely affect the advance of the FinTech industry, but also result in the collapse of confidence – the backbone of the financial services. Security at FinTech is a core value that determines the survival of financial services and companies.

FinTech without security measures may cause security threats. As a double-edged sword, the accessibility of the user should be easy and the safety of the user should be strengthened. So the accessibility and safety of the user need to be in harmony. To minimize damage, liability issues between related parties should be cleared, understood, and agreed. In order that the FinTech industry develops desirably and achieves financial innovation, first of all, the technology for extra security of FinTech is necessary.

### **3. The content and scope of research**

- o FinTech related markets, policies, and services trend analysis at home and abroad
  - FinTech related market trends and trend analysis at home and abroad
  - FinTech policy trend analysis at home and abroad
  - FinTech service and start-up trend analysis at home and abroad
- o FinTech service security technology analysis at home and abroad
  - FinTech service related security threats and incidents case analysis at home and abroad(payment fraud, etc.)
  - Mobile-based FinTech service security technology analysis(FDS, etc.)
- o Excavating research and application areas related to technology against mobile payment frauds

- Excavating research areas on mobile based FinTech security technology
- Excavating application areas for technology against mobile payment frauds

#### **4. Results of research**

- o Investigation on Korean FinTech start-up support programs and policies
  - Investigation on start-up support programs being developed by the public and private sectors
  - Investigation on best practices on the utilization of Korean FinTech start-up support programs
- o Investigation on start-up support programs and policies in major countries (UK, USA, Japan, China)
  - Investigation on government-led start-up support programs operation agencies and support policies
- o Providing as basic data, when a Fintech Industry Development Act and a FinTech security bill are drafted, by forecasting a demand for FinTech start-ups and FinTech security
  - Making the promotion of Creative Economy start-up companies efficient by utilizing public and private computing resources
- o Excavating research and application areas on technology against mobile payment frauds related
  - Excavating research areas on mobile based Fintech security technology
  - Excavating application areas on technology development against mobile payment frauds
  - FinTech service related security threats and incident cases

- analysis at home and abroad(payment fraud, etc.)
- Mobile based Fintech service security technology analysis(FDS, etc.)

## **5. Suggestion for utilization of this research**

- o Use as a basic material for drafting a Fintech Industry Development Act and a FinTech Security Bill
- o Making the promotion of Creative Economy start-up companies efficient by utilizing public and private computing resources
- o Making secure commerce available anytime and anywhere all over the world by promoting FinTech companies
- o Making the improvement of economic and social productivity, in collaborating and sharing within the same value chain group(between financial institutions), possible
- o Expanding overseas operation and creating jobs in the financial sector by promoting FinTech industry in the Creative Economy period

## **6. Expected effects (Expected impacts in related fields)**

- o Securing cost savings and flexibility of FinTech start-up companies
- o Breeding up cloud based broker, and discovering Blockchain and Bitcoin technology perspectives
- o Excavating FinTech industry related application areas(Bio, IoT, Big data, etc.)
- o Forming growing ecosystems for creative small and medium-sized venture companies and expanding investment in new demand on FinTech services
- o Offering a variety of opportunities through new industries, such as

Big data, and the activation of software and IT convergence industries

- o Improving the ROI of FinTech start-ups introduction and accelerating proliferation of them
- o Utilizing as a policy data for activating Fin-Tech start-up ecosystems
- o Can be utilized as a proposal for regulation improvement inhibiting the promotion of domestic FinTech industries

# 목 차

제 1 장 서 론 .....	1
제 1 절 금융 핀테크 정의 .....	1
제 2 절 핀테크의 등장배경 .....	3
제 3 절 핀테크 비즈니스 서비스 .....	9
1. 핀테크 비즈니스 서비스 산업 구분 .....	9
2. 핀테크 비즈니스 서비스 모델 분류 .....	11
3. 핀테크 비즈니스 서비스 특성 .....	12
 제 2 장 국내외 핀테크 산업 동향 .....	14
제 1 절 현금없는 사회 선언 .....	14
제 2 절 국내 ICT기업의 핀테크 .....	16
1. 인터넷뱅킹 진출 .....	16
2. 국내 금융사의 핀테크 현황 .....	19
제 3 절 해외 핀테크 동향 .....	24
1. 글로벌 핀테크 투자현황 .....	24
2. 업종별 핀테크 해외사례 .....	27
제 4 절 국내 핀테크 정책 동향 .....	36
1. 금융위원회 핀테크 정책 .....	36

2 금융보안원 정책 .....	39
<b>제 3장 핀테크 기술 동향 분석 .....</b>	<b>41</b>
제 1 절 핀테크 기술동향 .....	41
1. 핀테크 기술핵심 .....	41
2. 핀테크 아키텍처 .....	47
3. 핀테크 보안기술 원칙 .....	50
4. 핀테크 인증기술 .....	51
5. 핀테크 서비스 품질관리 .....	54
6. 핀테크와 클라우드 .....	56
제 2 절 클라우드 컴퓨팅 서비스 기술 .....	59
1. 클라우드 컴퓨팅 서비스 개념 .....	59
2. 클라우드 컴퓨팅의 정의 .....	62
3. 클라우드 컴퓨팅의 특성 .....	64
제 3 절 클라우드 서비스 브로커리지(CSB) .....	66
1. 클라우드 서비스 브로커리지의 정의 .....	66
2. 클라우드 서비스 브로커리지의 분류 .....	67
3. 클라우드 서비스 브로커리지 기술 전망 .....	69
제 4 절 블록체인(분산장부)과 비트코인 기술 .....	72
1. 블록체인(Blockchain) .....	72
2. 금융 비즈니스 영역 : 8C .....	78
3. 비트코인 .....	85
4. 블록체인 기술의 핵심 .....	87
<b>제 4 장 핀테크(FinTech) 서비스 보안 .....</b>	<b>92</b>

제 1 절 핀테크 보안 개요 .....	92
1. 핀테크와 보안 .....	92
2. 핀테크 보안의 3요소 .....	93
제 2 절 FDS시스템 기본 구조 .....	94
1. FDS 시스템 구성과 기능 .....	94
2. 정보 수집 및 분석 .....	96
3. FDS시스템의 성능 목표 .....	97
제 3 절 데이터 수집 플랫폼 .....	98
1. 머신 데이터(machine data) .....	98
2. 비정형데이터 수집 플랫폼 .....	99
3. 오픈 소스 수집기 .....	101
제 4 절 데이터 분석 기술 .....	104
1. 분석 기술 유형 .....	105
2. 데이터 결합과 활용 기술 .....	105
3. 데이터 의미 분석 시맨틱 기술 .....	106
4. 대량의 데이터 분석 가공 기술 .....	106
5. 대용량 데이터의 저장과 관리기술 .....	110
제 5 절 금융사기 방지에 활용되는 기반기술 .....	112
1. Heuristics 방법론 .....	113
2. 빅데이터 기반 기계 학습(machine learning) .....	114
3. 인텔리전스(intelligence) 정보 변환 .....	118
제 6 절 사기방지 대응 환경 진단 .....	120
1. 개 관 .....	120
2. 정책동향 .....	120
3. 사기방지 인프라 구축 상황 .....	124
4. 금융권 FDS 구축동향 (2015년 기준) .....	128

제 7 절 사기탐지 적용 모델과 시스템 사례 진단 .....	131
1. 국내 사례 .....	131
2. 해외 사례 .....	134
제 8 절 사기탐지 알고리즘과 기술 진단 .....	139
1. 개 요 .....	139
2. 사기탐지에서의 지식공학(Knowledge Engineering) .....	140
3. 사기탐지 시스템과 빅데이터 .....	146
4. 사기탐지 알고리즘 적용시 참고사항 .....	152
제 9 절 도출되는 현안사항 .....	159
1. 금융사기 자체의 속성 .....	159
2. 사기 대응 정책과 관리제도 측면 .....	161
3. FDS 개발 방법론 측면 .....	162
4. FDS 운용 측면 .....	163
5. 사기탐지 알고리즘 자체의 특성 .....	167
 <b>제 5 장 핀테크 기술개발 분야 .....</b>	<b>169</b>
제 1 절 국내외 핀테크 서비스 보안 기술 분석 .....	169
1. 국내외 핀테크 서비스 관련 보안 위협 및 사고 사례 분석(결제사기 등) .....	169
2. 모바일 기반 핀테크 서비스 보안 기술 분석(FDS 등) .....	171
제 2 절 모바일 결제사기 대응기술 관련 연구 및 적용분야 도출 .....	207
1. 모바일 기반 핀테크 보안 기술 연구 분야 도출 .....	207
2. 모바일 결제사기 대응기술 개발을 위한 적용분야 도출 .....	218
제 3 절 연구 분야 발굴 .....	223
1. 분야 발굴 전제 .....	223
2. 분야 발굴 목표 .....	225



3. 연구분야 발굴 과정 .....	225
4. 연구작업 프레임워크 .....	227
제 4 절 연구분야 도출 .....	228
1. 분야 도출 .....	228
2. 발굴 분야 구성 .....	229
제 5 절 세부 연구분야 .....	232
1. 핀테크 거버넌스 보안 전략분야(A) .....	232
2. 핀테크 거버넌스 보안 전략분야(B).....	234
3. 핀테크 거버넌스 보안 전략분야(C).....	237
4. 핀테크 거버넌스 보안 전략분야(E).....	239
5. 핀테크 거버넌스 보안 전략분야(F).....	242
6. 핀테크 거버넌스 보안 전략분야(G).....	245
7. 핀테크 거버넌스 보안 전략분야(H).....	247
8. 핀테크 거버넌스 보안 전략분야(I) .....	250
9. 핀테크 거버넌스 보안 전략분야(J) .....	251
10. 핀테크 거버넌스 보안 전략분야(K) .....	252
11. 핀테크 거버넌스 보안 전략분야(L) .....	255
12. 핀테크 거버넌스 보안 전략분야(M) .....	258
13. 핀테크 보안 기술개발 분야(D 그룹1).....	260
14. 핀테크 보안 기술개발 분야(D 그룹1).....	263
15. 핀테크 보안 기술개발 분야(D 그룹1).....	265
16. 핀테크 보안 기술개발 분야(D 그룹1).....	268
17. 핀테크 보안 기술개발 분야(D 그룹1).....	270
18. FDS 알고리즘과 기술개발 분야(D 그룹2).....	273
19. FDS 알고리즘과 기술개발 분야(D 그룹2).....	275
20. FDS 알고리즘과 기술개발 분야(D 그룹2).....	277

21. FDS 알고리즘과 기술개발 분야(D 그룹2).....	280
<b>제 6 장 결론.....</b>	<b>284</b>
참고문헌 .....	286
부록 핀테크 관련 지원기관 .....	292

# Contents

<b>Chapter 1 Introduction .....</b>	<b>1</b>
Section 1 Definition of financial FinTech .....	1
Section 2 Background of FinTech appearance .....	3
Section 3 FinTech business service .....	9
1. Classification of FinTech business service industry .....	9
2. Classification of FinTech business service models .....	11
3. Characteristics of FinTech business model .....	12
 <b>Chapter 2 FinTech industry trends at home and abroad</b>	<b>14</b>
Section 1 Declaration of a society without cash .....	14
Section 2 FinTech trend of domestic ICT companies .....	16
1. Advance into internet banking .....	16
2. Current state of FinTech of the domestic financial institutions .....	19
Section 3 Trend of international FinTech .....	24
1. Current state of global FinTech investment .....	24
2. International cases of FinTech by industry .....	27
Section 4 Domestic FinTech Policy Trend .....	36



<b>Chapter 4 FinTech Services Security .....</b>	<b>92</b>
Section 1 FinTech security overview .....	92
1. FinTech and security .....	92
2. Three elements of FinTech security .....	93
Section 2 Basic architecture of FDS system .....	94
1. FDS system configuration and features .....	94
2. Information collection and analysis .....	96
3. Performance objectives of the FDS system .....	97
Section 3 Data collection platform .....	98
1. Machine data .....	98
2. Unstructured data acquisition platform .....	99
3. Open source collector .....	101
Section 4 Data analysis technology .....	104
1. Types of analysis technology .....	105
2. Data bonding and utilization technology .....	105
3. Data semantics analysis semantic technology .....	106
4. Large amounts of data analysis processing technology	106
5. Storage and management technologies of large amounts of data .....	110
Section 5 Base technology utilized for preventing financial fraud .....	112
1. Heuristics methodology .....	113
2. Big data based machine learning .....	114
3. Intelligence Information conversion .....	118
Section 6 Environment diagnosis against fraud .....	120

1. Overview .....	120
2. Policy trend .....	120
3. Fraud prevention infrastructure building status .....	124
4. FDS building trends of financial institutions (2015) .....	128
Section 7 Fraud detection application models and system cases diagnostics .....	131
1. Domestic cases .....	131
2. Overseas cases .....	134
Section 8 Fraud detection algorithms and technology Diagnostics .....	139
1. Overview .....	139
2. Knowledge engineering in fraud detection .....	140
3. Fraud detection system and Big data .....	146
4. Reference for applying fraud detection algorithm .....	152
Section 9 Derived current issues .....	159
1. Properties of the financial fraud itself .....	159
2. Policy against fraud and management system aspects .....	161
3. FDS development methodology aspects .....	162
4. FDS operation aspects .....	163
5. Characteristics of fraud detection algorithm itself .....	167
 <b>Chapter 5 FinTech Technology Development Areas .....</b>	<b>169</b>
Section 1 Analysis of FinTech services security technology at home and abroad .....	169
1. Case analysis of FinTech related security threats and incidents at home and abroad(payment fraud, etc.) .....	169

2. Mobile based FinTech services security technology analysis(FDS, etc.) .....	171
Section 2 Excavating research and application areas on related technology against mobile payment fraud reaction	207
1. Excavating mobile based FinTech security technology research areas .....	207
2. Excavating application areas for development of technology against mobile payment fraud .....	218
Section 3 Excavating research areas .....	223
1. Prerequisite of excavating areas .....	223
2. Goal for excavating areas .....	225
3. Research areas excavation process .....	225
4. Research work framework .....	227
Section 4 Deriving Research areas .....	228
1. Process of deriving research areas .....	228
2. Structure of excavated areas .....	229
Section 5 Detailed research areas(No. 1~ No. 20) .....	232
1. FinTech Governance Security Strategy Area(A) .....	232
2. FinTech Governance Security Strategy Area(B) .....	234
3. FinTech Governance Security Strategy Area(C) .....	237
4. FinTech Governance Security Strategy Area(E) .....	239
5. FinTech Governance Security Strategy Area(F) .....	242
6. FinTech Governance Security Strategy Area(G) .....	245
7. FinTech Governance Security Strategy Area(H) .....	247
8. FinTech Governance Security Strategy Area(I) .....	250
9. FinTech Governance Security Strategy Area(J) .....	251

10. FinTech Governance Security Strategy Area(K) .....	252
11. FinTech Governance Security Strategy Area(L) .....	255
12. FinTech Governance Security Strategy Area(M) .....	258
13. FinTech Security Technology Development Area(D group1) .....	260
14. FinTech Security Technology Development Area(D group1) .....	263
15. FinTech Security Technology Development Area(D group1) .....	265
16. FinTech Security Technology Development Area(D group1) .....	268
17. FinTech Security Technology Development Area(D group1) .....	270
18. FinTech Algorithm and Technology Development Area(D group2) .....	273
19. FinTech Algorithm and Technology Development Area(D group2) .....	275
20. FinTech Algorithm and Technology Development Area(D group2) .....	277
11. FinTech Algorithm and Technology Development Area(D group2) .....	280

## Chapter 6 Conclusion .....284

References

Appendix FinTech related support institutions



## 그림 목차

(그림 1-1) 핀테크 산업의 개념도 .....	1
(그림 1-2) 전세계 핀테크 시장 규모 .....	2
(그림 1-3) 해외 ICT 기업 금융업 확대 방향 .....	5
(그림 1-4) 전 세계 핀테크 기업의 금융업종 진출 .....	10
(그림 2-1) CNN보도, 현금없는 사회를 위한 준비 국가 .....	14
(그림 2-2) 글로벌 핀테크 사업영역별 투자 비중(%) .....	25
(그림 2-3) 금융위의 글로벌 핀테크 육성정책 .....	37
(그림 2-4) 금융보안원의 금융 IT·보안 10대 이슈 전망 .....	40
(그림 3-1) : 금융 서비스와 핀테크 간의 관계 .....	42
(그림 3-2) 핀테크의 ICT기술 분야(예) .....	42
(그림 3-3) 현행 금융 서비스 모델 .....	46
(그림 3-4) 현행 차세대 시스템 아키텍처 .....	47
(그림 3-5) 핀테크 아키텍처 구성 .....	48
(그림 3-6) 포스트 금융 시스템의 아키텍처 구성 .....	49
(그림 3-7) 본인 인증 방법 별 안정성 비교 .....	52
(그림 3-8) 금융 거래 내역 모니터링 프로세스 .....	53
(그림 3-9) 인터넷 전문은행의 변화 형태 .....	55
(그림 3-10)인터넷 전문은행의 Application Architecture 수립 원칙 (예) .....	56
(그림 3-11) 클라우드 기반 플랫폼 .....	58
(그림 3-12) 핀테크 보안기술 개념도 .....	58
(그림 3-13) 클라우드 컴퓨팅 개념도 .....	61
(그림 3-14) 클라우드 컴퓨팅의 특성(NIST의 구분) .....	65
(그림 3-15) 클라우드 서비스 브로커리지 개념도 .....	67

(그림 3-16) 클라우드 서비스 브로커리지 분류 .....	68
(그림 3-17) 클라우드 서비스 활용 기업 경쟁력 제고 .....	70
(그림 3-18) 클라우드 서비스 아키텍처 .....	71
(그림 3-19) 비트코인의 네트워크 프로세스 .....	74
(그림 3-20) 공인된 제3자 공인기술 vs 블록체인 기술 .....	75
(그림 3-21) 블록체인의 작동 프로세스 .....	77
(그림 3-22)블록체인위조가 어려운 이유 .....	77
(그림 3-23) 금융 8C .....	79
(그림 3-24) Ripple의 해외송금 서비스개요 .....	85
(그림 3-25) IoT에 의한 블록체인의 다양한 구성 방법 .....	91
(그림 4-1) 금융업무 사고 탐지 프로세스 .....	95
(그림 4-2) 이상금융거래탐지시스템 업무 흐름도 .....	97
(그림 4-3) Data Mining Approaches for Intrusion Detection .....	108
(그림 4-4) NELL 시스템의 구조 .....	115
(그림 4-5)금융권 침해대응 모니터링 체계 .....	122
(그림 4-6) 이상 금융 거래 탐지·대응 시스템의 세부 구조 .....	128
(그림 4-7) Zero Touch Fraud Detection & Analysis .....	137
(그림 4-8) The Architecture of Detection Phase .....	138
(그림 4-9) expertsystem에서의 Knowledge-base 구조 .....	142
(그림 4-10) 최적해를 찾아가는 휴리스틱 경로(Romania with step costs in km) .....	145
(그림 4-11) 빅데이터의 전형적인 워크로드 .....	152
(그림 4-12) 머신러닝 개념도 .....	154
(그림 4-13) 칼리스타 플룩하트의 얼굴 인식 과정 .....	156
(그림 4-14) Deep Learning in Android Malware Detection, March 08 2014 , by Lyq, analysis .....	158

(그림 5-1) 전 세계 데이터 유출/침해 통계 .....	171
(그림 5-2) 핀테크 서비스와 보안기술 구조 .....	172
(그림 5-3) IC Tagging 인증 방식 .....	183
(그림 5-4) FIDO 구분 .....	185
(그림 5-5) DB서버 내부의 암호화 .....	193
(그림 5-6) PCI Security Council .....	205
(그림 5-7) 생체인증 사례 .....	207
(그림 5-8) 2채널 분할 입력 .....	211

## 표 목차

[표 1-1]	해외 ICT기업의 금융업 진출현황 .....	4
[표 1-2]	해외 IT 기업의 국내 금융서비스 제공 현황 .....	5
[표 1-3]	금융보안 규제환경 변화 .....	7
[표 1-4]	비대면 금융 실명확인 방법 비교 .....	8
[표 2-1]	국내 ICT 업계 금융서비스 현황 .....	18
[표 2-2]	카카오 금융서비스 내용 .....	19
[표 2-3]	국내 핀테크의 분야별 추진현황 .....	21
[표 2-4]	현 핀테크 업무 범위 .....	22
[표 2-5]	기존은행과 인터넷 전문은행 비교 .....	23
[표 2-6]	영미중의 핀테크 도입 현황 .....	26
[표 2-7]	해외은행들의 온라인, 모바일 경쟁력 강화 사례 .....	28
[표 2-8]	설립 주체별 해외 인터넷전문은행 현황 .....	29
[표 2-9]	해외 은행들의 핀테크 육성방안 .....	29
[표 2-10]	혁신적인 해외 핀테크 기업 사례 .....	33
[표 2-11]	주요 국가의 핀테크 특징과 투자현황 .....	35
[표 3-1]	모바일 결제 기술 .....	43
[표 3-2]	대출을 위한 빅데이터 분석 활용 .....	44
[표 3-3]	빅데이터 활용 사례 .....	45
[표 3-4]	보안의 3요소 .....	50
[표 3-5]	클라우드 컴퓨팅과 다른 컴퓨팅 방식의 비교 .....	60
[표 3-6]	다양한 클라우드 컴퓨팅의 정의 .....	63
[표 3-7]	클라우드 컴퓨팅 전 세계 시장 규모 .....	64
[표 3-8]	클라우드 컴퓨팅의 5가지 본질적 특징 .....	66
[표 3-9]	Gmail과 비트코인 구조 비교 .....	78

[표 3-10]	블록체인 기술의 장점 .....	84
[표 3-11]	블록체인을 활용한 자산거래사례 .....	85
[표 3-12]	이베이와 오픈바자의 비교 .....	90
[표 4-1]	핀테크 보안의 3요소 .....	94
[표 4-2]	FDS 기능 요건 .....	96
[표 4-3]	머신 데이터위치와 정보속성 .....	99
[표 4-4]	부정위험 탐지를 위한 데이터 분석방법 .....	110
[표 4-5]	금융권 FDS 구축 현황(' 15. 3월말 기준) .....	129
[표 4-6]	금융권의 이상금융거래 탐지시스템(FDS) 고도화 로드맵 .....	129
[표 4-7]	주요 미국은행의 이상금융거래 탐지시스템(FDS) 특성 비교 .....	135
[표 4-8]	알고리즘 방식과 빅데이터 방식의 비교 .....	149
[표 4-9]	사기탐지 알고리즘 진화방향 .....	152
[표 4-10]	인공지능의 원리를 사용하는 데이터 처리 알고리즘	157
[표 4-11]	FDS 이해관계자 식별과 관심사항 .....	163
[표 5-1]	신종 전자금융 보안사고 유형 .....	180
[표 5-2]	정보시스템 보안 도메인 .....	181
[표 5-3]	TEE의 장점 .....	184
[표 5-4]	FIDO 지문인증의 특징 .....	185
[표 5-5]	개발기술 사양 .....	208
[표 5-6]	클라우드 보안가이던스의 핵심영역 .....	218

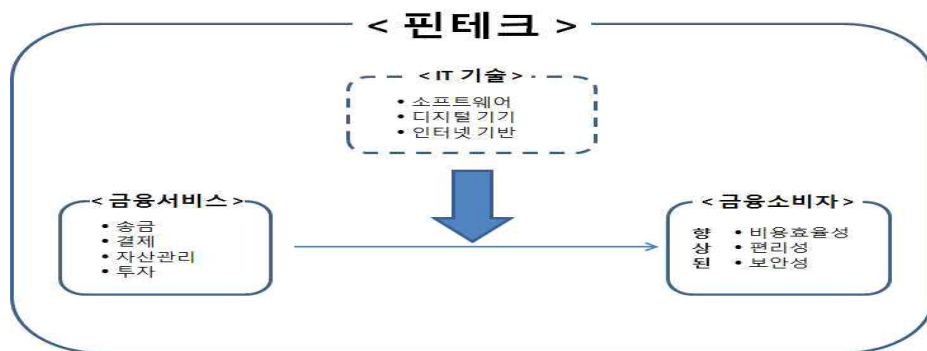
# 제 1 장 서론

## 제 1 절 금융 핀테크 정의

2015년도부터 ICT업계와 금융업계의 공통된 관심사는 핀테크(FinTech)였다. 금융(financial)과 기술(technology)의 합성어인 핀테크(FinTech)는 금융업은 물론 인터넷 모바일 산업에도 큰 파장을 몰고 왔다. 핀테크로 진행되는 금융 디지털화 융합은 기존 금융산업의 비즈니스 모델과 프로세스의 ‘파괴적 혁신’이라는 측면에서 주목해야 한다.

핀테크가 금융산업에 미칠 파장과 관련해 혁신적인 주장 중 하나는 2015년 2월 미국 비즈니스 인사이더라는 온라인경제신문의 기사이다.

‘조만간 은행이 필요치 않게 된다(Soon, You Won't Need A Bank)’라는 이 기사는 핀테크 스타트업들의 빠른 성장으로 기존 은행 지점창구에 갈 필요성이 없어져가고 있다고 보고 있다.



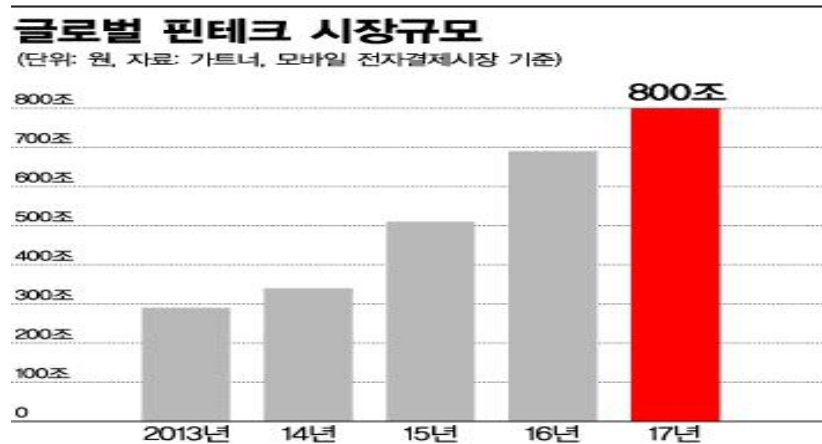
(그림 1-1) 핀테크 산업 개념도

사실 인터넷 전용 은행을 통해 계좌개설, 송금, 선불카드 발급 등을 활용하고, 해외 송금, P2P 대출, 모기지론, 크라우드펀딩 등 다양한 영역의 전문 핀테크 기업의 서비스를 활용하면, 은행을 이용하지 않아도 된

다는 것이다. 비즈니스 인사이더는 핀테크 기술의 빠른 성장과 스타트업들의 잇단 등장으로 은행 업무의 대부분을 핀테크 기업이 대체되고 있다고 보고 있다.

최근 핀테크 산업이 주목받는 이유는 모바일 트래픽이 큰 폭으로 증가함과 동시에 모바일 채널을 통한 금융거래 또한 빠른 속도로 늘어나는 등 관련 산업이 발전할 수 있는 기반이 형성되고 있기 때문이다.

글로벌 모바일 결제시장 규모는 2011년 1059억 달러에서 2017년 7210억 달러로 6년 동안 약 7배 성장할 것으로 전망된다.



(그림 1-2) 전세계 핀테크 시장 규모

이처럼 모바일 결제시장이 급속하게 확장되면서 송금 및 지급결제의 수단으로서 스마트폰의 비중 역시 큰 폭으로 늘어나게 되고, 관련 신기술 개발과 새로운 서비스 출시도 잇따르고 있다. 국내에서는 대형 ICT기업을 중심으로 송금과 지급결제 중심의 핀테크 서비스가 잇달아 등장하고 있지만 해외와 같은 핀테크 기업들의 다양한 서비스 상용화 실적은 전무한 상황이다. 핀테크 산업이 이처럼 빠른 속도로 성장하고 있지만 국내 기업들의 대응은 상대적으로 미진한 것으로 평가받고 있다.

국내 핀테크 산업을 올바르게 육성하기 위해서는 글로벌 핀테크 산업이

어떤 방향으로 발전하고 있는지, 향후 주목받을 분야가 무엇인지 예측해 볼 필요가 있다. 특히 이미 선두주자로 평가받는 주요 핀테크 영역별 선두주자들의 핵심 경쟁력을 제대로 분석함으로써 국내 핀테크 산업 발전을 위한 시사점을 얻는 것도 중요하다. 이에 본 연구의 1장에서는 핀테크의 정의, 2장에서는 국내외 핀테크 동향, 3장에서는 클라우드 및 핀테크 기술 동향을 중심으로 살펴보았다. 그리고, 4장, 5장에서는 핀테크 보안기술과 FDS보안기술에 중점적으로 연구하였으며, 6장에서는 핀테크 보안기술 연구 20분야를 발굴 하여 제시하였다.

## 제 2 절 핀테크(FinTech) 등장배경

글로벌 IT기업들이 금융(financial)과 정보통신기술(information communication technology)을 결합한 핀테크(FinTech) 시장을 형성해 가고 있다. 핀테크에 대한 개념적 정의는 글로벌 IT기업들이 폭넓은 사용자 기반을 바탕으로 정보통신기술과 송금, 결제, 자산관리 등 각종 금융서비스를 결합한 새로운 유형의 금융서비스를 의미한다.<sup>1)</sup> 또한 핀테크는 금융서비스와 관련한 소프트웨어를 새롭게 만들거나 운용성과를 향상시킬 수 있는 모든 기술적인 과정을 포함하는 의미이며, 의사결정, 위험관리, 포트폴리오 재구성, 준법관련 업무, 성과관리, 시스템통합, 온라인 이체와 지불 등 금융기관 업무의 전반에 영향을 주는 기술들을 종합한다. 따라서 핀테크는 금융서비스의 운용성과를 제고시킬 수 있으며, 모바일 정보기술 환경과 결합하여 금융거래의 확산이 가속화 되고 있다.

---

1) 삼성증권, FinTech란 무엇인가, 2014. 10., p.3.



[표 1-1] 해외 ICT기업의 금융업 진출현황

업종	기업	주요내용
플랫폼	 (미)	- 전자지갑 '구글월렛'('11), 이메일 기반 송금('13. 5) 등 출시 - 영국 내 전자화폐 발행 허가, 소액대출업체 '렌딩클럽' 투자('14)
	 (미)	- 전자지갑 '패스북' 출시('12) 및 아이폰5 이후 모델 기본 탑재
SNS	 (미)	- 아일랜드 내 전자화폐 발행 승인('14. 4), 및 EU 내 효력 발생 - 해외송금 기업인 '아지모(영)' 등과 제휴 추진('14. 4)
	 (중)	- 지급결제서비스 '텐페이'('13. 9), MMF '리차이통'('14. 1) 출시 - 중국 정부의 민영은행 시범 사업자 선정('14. 3)
통신 서비스	 (미)	- AT&T 모바일과 공동으로 모바일 지급결제 서비스 '아이시스 (ISIS)' 출시('12)
	 (케냐)	- 지급결제 및 전자화폐 서비스 'M-페사' 출시('07) - 'M-페사'에 예금 및 무담보대출 서비스 추가('12)
검색	 (중)	- 온라인 전용 MMF '바이파' 출시('13. 10) - 중국 정부의 민영은행 시범 사업자 선정('14. 3)
전자 상거래	 (중)	- 지급결제서비스 '알리페이'('03), 소액대출 '알리파이낸스'('11), 온라인 전용 MMF '위어바오'('13. 9) 출시 - 중국 정부의 민영은행 시범 사업자 선정('14. 3)
	 (미)	- 자사 사이트 내 지급결제 서비스 '페이팔' 출시('98) - 자사 선불카드인 'My Cash' 출시('12)
	 (미)	- 자사 사이트 내 지급결제 서비스 '아마존페이먼트' 출시('14. 6)

핀테크는 소비자들의 금융생활과 금융시장에 지각변동을 일으킬 수 있을 만큼 폭발적인 영향력을 나타낼 수 있으며, 기존의 금융기관과 달리 IT업체들은 인터넷 기술을 이용하여 간편하고, 다양한 금융서비스 상품을 개발하여 소비자들에게 제공함으로써 기존 금융기관에 위협이 된다. 국내 금융기관들 역시 핀테크 부상에 촉각을 기울이고 있으며, 자신들의 전통적 고유 사업에 미칠 영향을 분석하여 대응방안을 마련하여 진행하고 있다.

[표 1-2] 해외 IT 기업의 국내 금융서비스 제공 현황

해외 IT 기업	소속국가	국내 제휴회사(제휴시기)	주요 금융서비스
아마존(amazon)	미국	하나은행(' 13. 4)	.한국인 대상 해외 소액송금(건당 \$1,000, 연간 \$10,000 한도)
알리바바(Alibaba)	중국	- 하나은행(' 14. 6) - 이니시스(' 12. 10) - 롯데면세점(' 14. 4)	중국인의 한국 On-Off Line 가맹점 내 위안화 직접 지급결제
텐센트(Tencent)	중국	-다날( '14. 4) -신세계면세점( '14. 6)	중국인의 한국 On-Off Line 가맹점 내 위안화 직접 지급결제

(\* 주 : KDB산업은행, ICT업계의 금융업 진출에 따른 시장영향 분석, 산업이슈, 2014. 7.)

이는 ICT기업을 중심으로 한 비금융기관의 금융업종 진입이 기존 금융기업들의 고유 시장의 잠식으로 이어질 때 금융기업 고유 사업에 위협적인 요소가 될 수 있기 때문이다.



(\* 주 : 산업은행경제연구소, 교보증권 리서치센터)

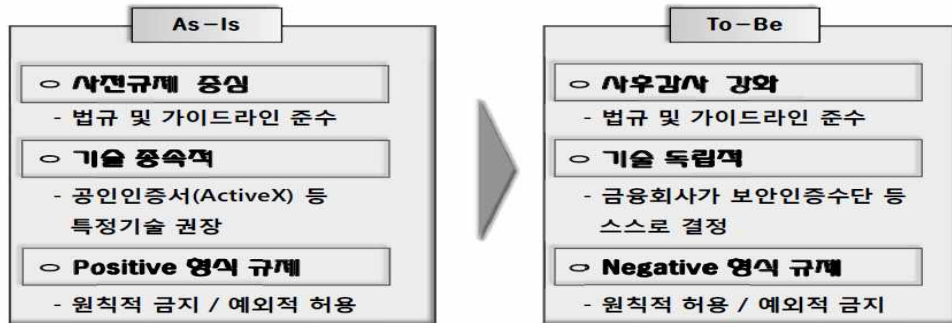
(그림 1-3) 해외 ICT 기업 금융업 확대 방향

미국의 경우 ICT기업 등 비금융사가 2020년에는 기존 금융권 시장의 30%를 잠식할 것으로 예상하고 있다. 2013년 세계 핀테크 열풍은 30억 달러에 달하는 투자 규모로 이어져 핀테크 기업에 대한 투자는 약 1년 만에 200% 가까이 급증했다. 연평균 투자증가율은 31%로 전체 벤처기업에 대한 연평균 투자증가율 7%를 크게 상회하는 것으로 나타났다.

국내의 경우에는 비금융기관의 금융업 참여에 대한 규제로 인해 시장 잠식의 속도가 느리지만 소액결제와 송금을 중심으로 비금융사의 시장 확대가 이루어지고 있으며, 기존 금융사의 수수료 수입은 지속적으로 감소할 것으로 추정된다. 이와 반대로 핀테크의 긍정적 영향에 대한 전망도 있는데, 이는 ICT기업들이 다양한 고객 접점 및 정보를 활용하여 소비자들의 인식 변화와 이용률 확대로 전체 금융시장 규모가 확대되고 있다.

금융벤처 열풍이 불면서 국가마다 핀테크 열풍이 불고 있고, 국내도 새로운 비즈니스 모델의 핀테크 기업들이 등장하고 있다. 간편 결제서비스를 표방하는 각종 ‘페이’ 서비스가 범람하고, 비대면 채널을 기반으로 하는 인터넷 전문은행인, “카카오다움 콘소시움”과 “KT콘소시움”이 인가를 받았다. 빠르면 금년 가을부터 서비스 예정이다. 그동안 점포를 기반으로 이뤄졌던 금융서비스가 사람을 마주하지 않고 온라인 접속을 통해 가능해졌다. 이와 더불어 최근 금융업계도 보안 규제 패러다임이 사전 규제에서 사후 감사로 자율보안으로 바뀌어져야 한다.

[표 1-3] 금융보안 규제환경 변화



(\* 주 : IBK기업은행)

자율 보안 키워드 속에는 금융회사가 보안인증 수단 등을 스스로 결정할 수 있다는 것이다. 공인인증서와 액티브X 등 특정 기술을 권장했던 과거와 달리 이제는 다양한 기술을 선택할 수 있는 자율성이 주어지게 된다. 비대면 금융서비스를 위한 실명 확인 방법으로 금융회사가 기존 대면 방식에서 다양한 방식을 택할 수 있는 길이 열려졌다.

[표 1-4] 비대면 금융 실명확인 방법 비교

유형	비대면 금융 실명확인 방법	사례
기본정보 수집 및 부가인증	1) 인터넷뱅킹 접속 및 계좌개설 신청서 작성(이름, 주소, 사회보장번호, 운전면허증, 고용정보 등 입력) 2) 입력 정보를 토대로 금융회사가 신용평가기관에 고객 신원조회 의뢰 3) (부가인증절차) 신원조회 후 고객에게 전화해 고객이 입력한 정보 및 신원조회 과정에서 습득한 정보에 대해 고객에게 질문하고 답변 확인 4) 계좌 개설 및 고객 요청에 따라 체크카드 및 직불카드 우편 송부	미국 Charles Schwab Bank
실명확인증표 수집	1) 인터넷뱅킹 접속 및 회원가입 후 기본정보 입력(이름, 생년월일, 휴대폰번호, 운전면허증 번호, 이메일 주소 등) 2) 온라인으로 실명확인증표 정보 입력(2개 이상) 3) 금융회사는 각 실명확인증표 발급기관을 통해 입력한 정보의 진위 여부 확인 4) 확인 완료 및 계좌 개설	호주 UBank
기본정보 수집 후 거래매체 송부 시 실명확인증표 확인	1) 인터넷뱅킹 접속 후 계좌개설신청서 작성(이름, 주소, 휴대폰번호, 이메일 주소 등 입력) 2) 금융회사는 고객이 입력한 주소로 본인 한정 우편을 통해 현금카드, 보안카드 등 거래매체 송부 3) 고객은 배달원에 사진이 부착된 실명확인증을 제시해 배달원으로부터 본인임을 확인받고 우편물 수취(수일 소요) 4) 금융회사는 배송 완료 여부를 확인해 거래 허가 (수일 소요)	일본 Seven Bank
실명확인증표를 수집·검증 후 실명확인증표 상 주소로 거래매체 송부	1) 인터넷뱅킹 접속 후 계좌개설신청서 작성(이름, 주소, 휴대폰번호, 이메일 주소 등 입력) 2) 실명확인증표를 금융회사에 송부 ①스마트폰앱을 이용해 운전면허증 정보 자동입력, ②인터넷뱅킹 사이트에서 운전면허증, 카드형 건강보험증을 촬영해 인터넷뱅킹 사이트에 업로드, ③운전면허증, 건강보험증, 여권, 연금수첩, 주민등록증, 인감등록증 등을 우편 발송 3) 금융회사는 실명확인증표를 확인하고 증표상의 주소로 현금카드 및 보안카드를 송부 4) 우편 수취 및 거래 개시	일본 Jibun Bank

(\* 주 : 금융연구원)

이미 비대면 금융서비스를 도입해 운영하고 있는 해외에서는 신분증 사본, 우편, 영상통화, 계좌이체 등 다양한 비대면 확인 방식을 활용하고 있다. 다만, 자금세탁 방지를 위해 여러 단계를 거쳐 확인한다. 기본 정보를 수집한 후 해당 정보를 이용해 고객 신원을 조사하고 부가적인 인증방법을 택하거나 이름, 주소, 휴대폰 번호, 이메일 주소 등의 정보를 수집한 다음 우편을 통해 본인 여부를 확인하는 방법 등을 활용한다. 국

내에선 해외에서 검증된 비대면 확인 방식을 우선 허용하고 다중확인을 통해 정확성을 제고한다는 방침이다.

금융위원회는 ①실명확인증표 사본 제출 ②영상통화 ③접근매체(예: 현금카드) 전달시 확인 ④기존계좌 활용 등 실명확인 정확도가 높은 4가지 방식을 제시했다. 비대면 확인방식의 실명확인 정확도 확보를 위해 이중 확인을 의무화하고, 다중확인을 권고사항으로 운영할 계획이다. 더불어 스마트 기기와 본인 확인 관련 기술을 접목해 회사별로 창의적이고 다양한 방식을 활용할 수 있도록 문을 열어줬다.

### 제 3 절 핀테크 비즈니스 서비스

#### 1. 핀테크 비즈니스 서비스 산업 구분

핀테크 비즈니스 서비스 분야에는 크게 지급 결제서비스 분야, 대출 분야, 전자화폐 분야, 그리고 금융정보 분석 분야로 구분할 수 있다.

첫번째로, 지급 결제서비스는 핀테크의 대표적인 서비스이다. 이 지급 결제방식에는 간편결제와 송금 분야가 있는데 국내에서는 간편결제가 송금분야보다 주 관심사가 되고 있다. 해외에서는 송금과 간편결제는 같은 서비스로 인식되고 있는데 이 차이는 전자지갑과 전자화폐에 대한 인식의 차이 때문에 발생한다. 해외에서는 페이팔과 알리페이의 경우 충전식 전자지갑을 이용해서 온라인 오프라인 결제를 제공한다. 그러나 국내에서는 모든 금융서비스가 은행에서 개설한 통장을 중심으로 연계되어 있어 전자지갑의 필요성을 크게 느끼지 못하고 있고, 모든 거래의 중심이 신용카드와 체크카드를 이용한 방식이기 때문에 전자지갑보다는 간편결제에 더 많은 관심이 쏠리고 있다.



(그림 1-4) 전세계 핀테크 기업의 금융업종 진출

앞으로 핀테크 활성화를 위해 정책과 규제의 완화가 대폭 이루어지면, 이 규제 완화의 틈새를 이용한 판매자의 의도적인 사기행위의 발생을 막기 위한 결제시스템 자체의 보호장치가 필요하다. 이 보호장치로 해외의 페이팔이나 알리페이는 제3자 결제시스템 방식을 사용한다. 국내에서 지급결제 분야는 전자지갑을 활용한 간편결제 및 송금 패턴으로 바뀌기 전까지 간편 결제서비스에 국한될 가능성이 높다. 이런 측면에서 현금 또는 신용카드를 이용한 충전 방식인 알리페이 보다는, PG(payment gateway, 전자결제대행)사와 연계되어 신용카드 대신에 사용이 가능한 애플페이나 삼성페이가 쉽게 시장에 정착할 것으로 예상된다. 국내 금융권에서도 중국 관광객에 대한 수요 때문에 알리페이나 애플페이가 수용되고 있으며, 앞으로 가속화 될 것이다.

두번째로, 대출 분야는 국내에서 가장 전망이 기대되는 핀테크 분야이다. 이는 미국의 렌딩클럽(Lending Club)과 같은 P2P 대출 서비스이다. P2P 대출은 금융 잉여자원을 활용한다는 측면에서 공유경제 컨셉과도 같다. 공유자원의 활용을 금융이라는 대상으로 확대한다면 투자자와 소

비자를 연계하는 공유경제 플랫폼을 제공한다. 국내에서는 소상공인 전문 P2P 대출 스타트업 기업인 '핀다', 고금리 제2 금융권 대출을 전환해주는 전환대출 전문기업인 '피플펀드', 건축중인 건물을 담보로 건축자금 대출 전문 기업인 '테라펀딩' 등이 등장하였다. P2P 대출 서비스는 단순히 투자자와 대출이 필요한 사람을 연계하는 서비스가 아니라 우선 대출자에 대한 신용도를 평가하는 것이 핵심 경쟁력이다. 투자자의 경우 기존 은행금리보다 높은 투자이익을 거둘 수 있다는 장점이 있지만, P2P 대출기업의 안정성과 신뢰를 어떻게 확보할 것인가는 여전히 숙제로 남아있다. 핀테크 활성화를 위해서는 규제를 완화해야 하지만, P2P 대출과 같은 경우 투자자 보호를 위한 사후 감시와 감독이 필요한 분야이기도 하다.

세번째 핀테크 분야는 전자화폐 분야이다. 전자화폐는페이팔과 같이 지급결제를 위한 수단으로 사용되기도 하지만, 그 자체로 가상화폐 역할을 하기도 한다. 대표적인 가상화폐인 비트코인(Bitcoin)이다. 비트코인은 가상화폐이면서 동시에 결제플랫폼이다. 아직은 다양한 상거래가 가능할 만큼 활성화 되어있지 않지만, 페이팔이 비트코인 결제를 지원하면서 점차 거래 대상이 넓혀지고 있다. 여전히 비트코인이 기존 화폐 체계보다 보편성이 떨어지는 것이 사실이지만, P2P 기반 분산 데이터베이스와 공개키 암호방식으로 거래가 수행되는 특성 때문에 각국의 중앙은행들과는 달리 통화량을 임의로 제어할 수 없다. 그래서 비트코인은 상대적으로 인플레이션에 강하다. 여전히 탈세나 불법 자금으로 활용될 우려가 존재하나 기존 금융시스템의 문제에 대응할 수 있는 유일한 화폐체계이다.

마지막으로, 금융정보 분석 분야는 개인들에게 은행·카드·증권·보험 등 복수개의 금융서비스를 통합시킨 자산관리 서비스를 제공하는 분야로써, 향후 핀테크 스타트업 기업들이 금융 규제에 비종속적으로 서비스를 시도해 볼 수 있는 분야이다.

## 2. 핀테크 비즈니스 서비스 모델 분류



핀테크 비즈니스 서비스는 대부, 지급 결제 및 전자결제(Electronic Billing), 개인재무 및 자산관리(Personal Finance/Asset Management), 자금이체 및 송금 (Money Transfer/Remittance), 디지털 화폐(Digital Currency), 금융기관용 툴(Financial Institutional Tools) 제공, 지분투자형 크라우드펀딩(Equity crowdfunding)의 7가지 모델로 분류할 수 있다. 현재 벤처캐피탈의 투자가 많이 이뤄지고 있는 분야는 지급 결제서비스이다.

### 3. 핀테크 비즈니스 서비스 특성

핀테크 기업의 서비스 특성은, 기존 금융기관 서비스에 비교하여, 핀테크 기업의 서비스를 이용하는 금융고객의 관점에서 보면 크게 수수료 절감, 서비스 이용 용이성 증대, 빠르고 간편한 서비스의 3가지를 들 수 있다.

첫번째 특성으로, 핀테크 기업은 기존 금융산업의 수수료체계를 붕괴시키고 있다. 영국의 트랜스퍼 와이즈라는 해외송금 회사는 기존 은행의 해외송금 수수료를 10분의 1 수준으로 낮췄고, 세계 최대의 P2P 온라인 대부회사인 미국의 렌딩클럽은 대출금리는 개인 신용도에 따라 상이하지만 약 7% 수준으로 금융기관보다 금리가 낮추었다.

두번째 특성으로, 기존 금융기관에 비해 핀테크 업체들이 제공하는 금융서비스의 용이성이 높다는 것이다. 퍼스널 캐피탈은 평균 자산보유액이 10만~200만달러 수준의 자산가를 대상으로 온라인 자산관리 서비스를 제공하고 있다. 또 미국의 온라인 은행인 뱅킹 업은 사회적 약자를 대상으로 계좌 개설 및 선불카드 발급 서비스를 제공하고 있다. 이처럼 핀테크 기업들은 기존 금융서비스가 제대로 미치지 못한 영역에 서비스를 제공하면서 인기를 모으고 있다.

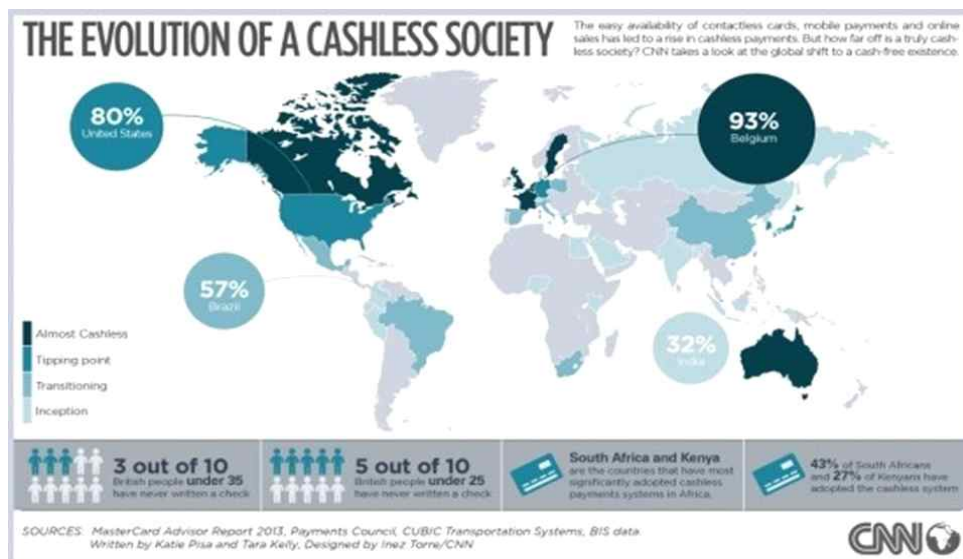
마지막 특성으로, 빠르게 서비스를 이용할 수 있다는 점도 핀테크 회

사들의 강점으로 떠오르고 있다. 소규모 자영업자 등을 대상으로 한 대부회사인 온테크는 통상 2~3주 정도 걸리던 대출심사 기간을 단축해 인기를 얻고 있다. 최근 인기를 모으고 있는 간편 결제서비스 핀테크 회사들도 빠르고 간편한 서비스를 강점으로 내세우며 빠르게 성장하고 있다.

## 제 2 장 국내외 핀테크 산업 동향

### 제 1 절 현금없는 사회 선언

최근 화폐제도가 근본적으로 변화하며, 요동을 치고 있다. 2016년 1월2일, CNN에서 보도한 위의 기사는 2016년은 ‘현금 없는 사회’ 를 알리고 있다. IT분야를 선도하는 유럽의 덴마크, 스웨덴, 노르웨이가 현금 없는 사회로 진출하기 위한 발 빠른 움직임을 보이고 있고, 아시아에선 역시 IT분야를 선도하고 있는 대한민국도 ‘현금 없는 사회’ 로 가기 위한 준비를 한다고 한다. 현금없는 사회를 이끌고 있는 전자 결제시스템인 유럽의 모바일페이, 아시아의 삼성페이, 미국의 애플페이는 서로 경쟁하며 시장을 넓혀가다가 결국에는 이 모든 것을 통합한 전세계적인 전자 결제시스템이 탄생될 것이다.



(그림 2-1 ) CNN보도, 현금없는 사회를 위한 준비 국가

전세계를 통합한 전자 결제시스템이 탄생하면 이에 대한 결제(혹은 인증)

수단도 현재의 스마트기기에서 몸 안에 이식하는 베리칩으로 옮겨가게 된다. 현금 없는 사회 끝에 베리칩 사회가 있는 것이다. “누구든지 이 표를 가진 자 외에는 매매를 못하게 되는” (계 13:17) 현금이 사라진 베리칩 시대가 눈앞에 와 있는 것이다. 물건을 사고파는 과정에서 현금 사용을 제한하려는 계획을 세우고 있는 덴마크는 세계 최초로 수표와 동전을 폐기하는 국가가 되어가고 있다. 덴마크 정부는 2016년 1월부터 대부분의 가게에 현금 출납기를 폐기 하였다고 한다. 병원과 약국 그리고 우체국과 같은 필수적인 공공 서비스 분야에서는 현금을 사용할 수 있지만, (이를 제외한 가게에 현금 사용을 금지하는) 계획은 법제화의 길을 가고 있다고 한다. 덴마크는 스칸디나비아 반도의 이웃 국가인 노르웨이 스웨덴과 함께 전세계에서 전자화폐를 선도하는 국가 중 하나이다. 비즈니스 그룹들은 이것이 비용절감에 도움이 되며, 현금 강탈과 같은 안전문제를 근본적으로 해결할 수 있다고 보고하고 있다.

현금없는 사회는 더 이상 “꿈같은 이야기가 아니라, 조만간 실현될 하나의 비전이다” 라고 덴마크 은행연합회는 말하고 있다. 현재는 덴마크의 모든 소매점들이 현금을 받아주고 있지만, 이것이 많은 덴마크의 상점들이 디지털 결제를 막아내지는 못하고 있다. 인구의 40%가 Danske Bank(DNSKY)의 MobilePay를 통해 돈을 이체하거나 가게나 온라인에서 쇼핑을 할 때 사용하고 있다. 노르웨이와 스웨덴의 상황도 덴마크와 유사하다고 한다.

최근 한국은행도 동전 사용을 최대한 줄여 ‘동전 없는 사회(coinless society)’를 만드는 방안을 추진한다고 발표하였다. 이는 핀테크 기술을 활용해 동전을 카드 등 다른 결제 수단으로 대체해 관리 비용을 줄이겠다는 취지다. 한국은행은 지난 1월12일 이런 내용을 포함해 지급결제 분야의 중장기 과제를 담은 ‘지급결제 비전(vision) 2020’을 발표하였다.

한국은행은 우선 영국 스웨덴 등이 운영 중인 현금 없는 사회 모델을 연구해 우리나라에서 ‘동전 없는 사회’의 도입 가능성을 검토하기로 했다. 이 국가들은 버스 등 대중교통을 이용할 때 현금을 낼 수 없도록 하고 있다. 또 다른 유럽 국가들은 자금 세탁 방지 등을 목적으로 100만~500만원 이상 금액을 거래할 경우 현금이 아닌 수표나 계좌이체 등의 수

단을 이용하도록 법으로 규제하고 있다.

한국은행의 '동전 없는 사회'의 도입 검토 방식은 동전으로 받게 되는 거스름돈을 선불카드에 충전해 주는 방식이다. 예컨대 9500원짜리 물건을 살 때 현금 1만 원을 냈다면 거스름돈 500원을 고객에게 주지 않고 해당 금액만큼 고객의 카드에 충전을 해주는 것이다. 한국은행 관계자는 “신용카드와 모바일기기 등 현금을 대체할 수단이 늘어나고 있는 만큼 그 중간 단계로 먼저 동전 사용을 줄여 보자는 취지”라며 “다만 동전 사용을 아예 금지하는 상황은 염두에 두지 않고 있다”고 전했다.

이렇듯 선진국에서도 IT기술에 의한 현금 없는 사회에 진화하면서 금융 비즈니스의 기회가 찾아오고 있다.

## 제 2 절 국내 ICT기업의 핀테크 동향






핀테크가 주목 받는 이유는 최근 모바일 디바이스 사용이 급증했고 모바일을 통한 금융거래가 늘어나면서 관련 산업이 발전할 수 있는 여건이 형성되었기 때문이다. 글로벌 ICT 기업들은 모바일 네트워크 기반으로 다양한 형태의 핀테크 서비스를 제공하고 있다. 초기 핀테크 기반 서비스는 지급결제, 송금/전자화폐, 편당, 자산관리와 같이 기존 금융서비스에 국한된 형태가 많았다. 하지만, 다양한 ICT기술을 접목시키며 새로운 아이디어의 핀테크 서비스가 나타나고 있다. 글로벌 은행들은 핀테크의 중요성을 인식하고 관련 기업에 대한 투자와 지원을 하고 있으며, 우리나라도 인터넷 은행을 확정하는 등 핀테크 산업은 확대되고 있다.

### 1. 인터넷뱅킹 진출

글로벌 ICT기업들의 국내·외 금융시장 진출에 의한 새로운 금융수익

실현 기회의 확대와는 달리 국내의 경우 비금융기관의 기존 금융기업의 규제 장벽으로 인하여 금융업 진출 및 서비스 혁신은 대단히 어려운 실정이다. 국내의 경우 전자금융 거래법(2007. 1.)에서 비금융기관은 여·수신, 증권, 보험 등의 일반 금융업무 영위가 불가하며, 금융위원회의 허가 하에서 전자화폐 발행 및 관리 업무 수행이 가능하고 등록에 의한 전자자금 이체, 직불전자지급수단 발행 및 관리, 선불전자지급수단 발행 및 관리, 전자지급결제 대행, 결제대금 예치, 그리고 지급인이 수취인에게 지급해야 할 자금내역의 전자고지 및 자금수수·정산을 대행하는 전자고지 결제에 대해서만 가능하다. 또 다른 금융서비스 혁신의 제약 요인으로서는 공인인증서의 사용 등 복잡한 규제에 있다. 이와 같이 국내 ICT기업들의 금융업 진출에 대한 제약 및 현실적 시장진입의 어려움과 달리 주요 해외 ICT 기업들은 비금융기관의 금융업 규제에 대한 완화추세로 금융업 진출이 활발한 가운데 확장추세에 있다. 예를 들면, 일본은 비금융기관의 금융업 진출을 허가제가 아닌 등록제로 운영하고 있으며, 중국은 오히려 정부차원에서 ICT기업을 포함한 비금융기관의 금융업 진출의 장려와 ICT기업을 포함한 주요 기업에 대해 민영은행설립 시범사업권을 부여하였다. 유럽의 경우 패스포팅(Passporting) 규정에 따라 EU 중 한 국가에서 비금융기관의 금융업 허가 시 EU전체에서 금융업 수행이 가능하도록 되어 있다.

[표 2-1] 국내 ICT 업계 금융서비스 현황

업종	기업	주요 금융서비스
SNS		<ul style="list-style-type: none"> <li>- 카카오톡 기반의 송금·결제서비스 '뱅크월렛카카오' 출시('14. 11)</li> <li>- 카카오톡 기반의 주식 정보제공 및 매매서비스 '카카오 증권플러스' 출시(주식매매 기능은 '14년 하반기 추가)</li> </ul>
제조		<ul style="list-style-type: none"> <li>- 신용카드사와 연계해 전자지갑서비스 '삼성월렛' 출시('13. 5)</li> <li>- 멤버십카드 및 신용카드 정보 등록 후 간편결제 기능 제공</li> </ul>
통신		<ul style="list-style-type: none"> <li>- 3사 모두 전자지갑 출시</li> <li>• SKT '스마트월렛'('10), KT '모카월렛'('12), LGU+ '스마트월렛'('11)</li> <li>- 은행·신용카드사와 연계해 스마트폰의 바코드, QR(Quick Response)코드, NFC 등으로 온·오프라인 결제기능 제공</li> </ul>
		
		

(\* 주 : KDB산업은행, ICT업계의 금융업 진출에 따른 시장영향 분석, 산업이슈, 2014. 7.)

[표 2-1]에서처럼 국내 ICT업계의 경우 해외 주요 ICT기업들과 달리 소극적인 시장 대응으로 내수 위주의 전자지갑(Wallet) 서비스 및 은행 등 금융기관과 연계한 스마트폰의 바코드, QR(Quick Response)코드, NFC 등의 결제서비스 상품을 출시하고 있는 정도이다. 이 같은 최소한의 시장진입 마저도 모바일 사용자들의 낮은 저변확산과 이용불편성 등이 시장 확대 저해요인이 되고 있다.

최근 카카오톡은 SNS기반의 금융서비스 카카오페이를 출시하였는데 이는 카카오톡 애플리케이션(앱 응용프로그램)에 신용카드 정보를 등록해 놓은 뒤 인터넷 쇼핑몰 등에서 물건을 살 때 비밀번호 입력만으로 간단히 결제할 수 있는 서비스이다. 카카오페이 서비스는 30만원 이상 결제할 때는 공인인증서가 필요해 다소 불편한 점도 있다. 이외에도 카카오톡 금융서비스는 [표 2-2]에서처럼 2014년 11월에 송금 및 결제서비스 관련 뱅크월렛카카오를 출시하였으며, 주식관련 서비스인 증권플러스 기능을 보강하였다.

[표 2-2] 카카오 금융서비스 내용

구분	제휴기관	주요 기능	
증권 플러스	주요 증권사(대신,미래에셋, 삼성,키움 등 4개 증권사)	정보제공	－주식 종목 및 시황정도 실시간 제공 －카카오톡 이용자간 정보 교류
		주식매매	－카카오톡과 연동한 실시간 주식매매
뱅크 월렛 카카오	금융결제원 및 주요은행(기업,국민, 외환,수협,농협,우리, SC,신한,씨티,대구,부산,전북,제주,경남,우정사업본부 등 15개 은행	현금충전	－최대 50만원 한도, 금액소진 시 자동충전
		송금	－카카오톡 ID기반 일 최대 10만원 송금(송금완료시 메시지 표시, 송금취소 가능) －건당 수수료100원(예정)
		현금출금	－NFC기반 자동입출금기(ATM)에서 출금
		결제	－NFC기반 온라인·모바일 쇼핑물 소액결제

카카오톡은 기존 은행 모바일뱅킹과 비교할 때 송금절차가 축소되어 있으며, 결제정보의 저장, 익숙한 사용 환경 등의 편의성 증가를 통해 기존 금융기관 서비스에 비해 차별화 되어 있다. 또한 SNS의 특성인 네트워크 효과로 단기간 내 서비스 확산에 대한 잠재력을 보유하고 있다.

## 2. 국내 금융사의 핀테크 현황

급격한 성장세를 보이고 있는 해외 핀테크 산업과 달리 국내의 핀테크 산업은 답보수준에 머물러 있는 상태이다. 한국은 IT 인프라는 잘 갖추어져 있으나, 세계 100대 핀테크 기업 중 국내기업은 단 한 곳도 없는 상황이다. 최근 지급결제 분야에서 다음과 네이버 등의 대형 ICT업체들이 송



금 및 지급 결제시장에 진입하였으나 괄목할만한 성과를 내놓지 못하고 있는 실정이다. 과도한 진입장벽과 규제로 국내의 핀테크 산업은 뒤쳐진 상태이다. 이유는 여신전문금융업법 등 금융관련 법률은 금융업 진입 조건을 엄격하게 규정하고, 금융위원회와 금융감독원 등 여신 감독기관의 심사를 통과해야 금융업 허가가 가능하다. 또한 대기업의 금융 진출에 따른 경제 불균형을 우려한 금산분리 원칙에 따른 금융규제로 핀테크 등 금융과 타 산업의 융합이 정체되어 있다. 그래서 최근, 정부의 적극적인 핀테크 육성 의지에 따라 핀테크에 대한 금융회사들의 관심과 참여가 증대되고 있으며, 핀테크 산업 육성 전략 등 각종 지원책을 통해 핀테크 산업이 활성화될 것으로 기대된다. 사례로서는 기업은행은 홍채인식을 통한 비대면 인증을 추진하고, 우리은행은 집단지성을 이용한 사기방지 솔루션 개발 착수, BC 카드는 빅데이터와 인공지능을 활용해 소비자의 구매의사를 예측, 마케팅에 활용하는 시스템 개발 중에 있다.

[표 2-3] 국내 핀테크의 분야별 추진현황

분야	국내 현황
지급결제	•카드사 및 PG사 등의 간편 결제서비스 출현
송금	•금융회사를 통하지 않고 비금융회사의 플랫폼을 활용한 온라인송금 서비스 출현
예금·대출	•인터넷 전문은행 2곳 선정
투자자금모집	•투자형 클라우드 펀딩법안 국회 통과예정
자산관리	•온라인 투자자문 등에 대한 제도적 제약은 없음 •온라인 펀드슈퍼마켓 도입 완료
보험	•개별 보험회사 홈페이지를 통한 온라인 보험 가입 •온라인 보험 슈퍼마켓 도입 추진 중
기타	•(빅데이터) 빅데이터 가이드라인 마련 및 통합신용정보집중기관 설립 추진 중 •(보안·인증) 핀테크 보안업체 및 금융회사 간 제휴확대, 스마트 OTP 출시 준비, 금융보안원 설립 등

(\* 주 : Pixabay)

국내에는 신용카드사, 오픈 마켓, PG사가 각각 공인인증서가 적용되지 않는 소액결제에 대해 최근 간편 결제서비스를 제공해 왔으며, 금융당국의 공인인증서 사용 의무화 폐지와 간편결제 도입을 위한 규제 완화 이후 카드사와 신용정보 보관이 가능해진 PG업체의 서비스 확대가 추진되고 있다.

[표 2-4] 현 핀테크 업무 범위

구분	내 용	비 고
전자금융업자 (전금법)	전자화폐 발행·관리	금산법 28①
	전자자금이체업무	금산법 28②
	직불전자지급수단의 발행·관리	금산법 28②
	선불전자지급수단의 발행·관리	금산법 28②(T-money)
	전자지급결제대행(Payment Gateway)	금산법 28②
	결제대금예치업(에스크로계좌)	시행령 § 15③
	전자고지결제업	시행령 § 15③
전자금융 보조업자 (전금법)	정보처리시스템으로 신용카드업자의 신용카드 승인 및 결제 그 밖의 자금정산	카드VAN社
	정보처리시스템으로 은행의 자금인출업무, 환업무 및 그 밖의 업무를 지원	은행VAN社
	전자금융업무와 관련된 정보처리시스템을 금융회사·전자금융업자를 위해 운영	정보시스템운영업체 (우리FIS)
	1호~3호 사업자와 제휴·위탁·외부주문에 관한 계약을 체결하고 정보처리시스템 운영	위 세 업체의 용역업체
은행법상 금융전 산업 준용	금융회사 업무 관련 자료처리, 전송 프로그램 제공 및 관리	은행업감독규정시행세칙 § 35 i.
	금융회사 업무 관련 전산시스템 판매 또는 임대	은행업감독규정시행세칙 § 35 ii.
	금융회사 업무 관련 자료 중계·처리하는 부가통신 업무	은행업감독규정시행세칙 § 35 iii.
최근 新경향	(금융데이터 분석) 고객과 관련된 다양한 금융 데이터를 수집·분석	신용정보분석 개발, 빅데이터 개발
	(금융소프트웨어) 스마트 기술을 이용한 혁신적 금융업무·서비스 관련 소프트웨어 제공	금융모바일앱, 인터넷뱅킹, 금융보안 등
	(금융플랫폼) 금융기관 개입 없이 자유롭게 금융거래할 수 있는 거래기반 제공	회원제 증권정보제공업 등

핀테크에 대한 추진 방향, 사업 영역, 분류, 서비스 내역 등에 대한 해석이 이해관계 주체에 따라 다양하며 시장을 바라보는 시각도 다른 것 같다. 국내 금융환경의 특수성도 있지만 금융 기반의 핀테크나 기술기반의 테크핀이나 보안 기반의 핀테크나 등 정의도 각기 다르다.

핀테크 기업이 접근하기에는 각종 규제, 보수적인 금융 환경, 금융기관

별로 적용하는 핀테크 기술 등이 다르기 때문에 접점을 찾기가 어렵다는 문제도 있습니다. 공인인증서와 ActiveX 문제, 인증기술인 일회용비밀번호생성기(OTP, One Time Password) 등 일부 접근매체에 집중되어 있다 보니 단순 간편결제 분야 위주로 발전하고 있다.

우리나라는 금융분야에 대한 높은 규제장벽으로 금융과 IT와의 융합이 느리게 진행되어 왔으나 최근 들어 IT업체의 금융업 진출에 위협을 느낀 국내 은행들이 ICT업체와 제휴를 본격화하는 양상을 보이고 있다.

[표 2-5] 기존은행과 인터넷 전문은행 비교

분야	기존은행	인터넷 전문은행
인터넷 금융거래	인터넷을 보조적 영업채널로 간주(조회 및 이체거래)	인터넷을 주 채널로 영업하며, 모든 거래가 인터넷을 통하여 이루어짐
영업 기반 지역	지역 점포를 중심으로 해당 지역 기반을 두고 있는 고객 중심	해당 국가 또는 전세계
영업시간	인터넷뱅킹의 조회, 이체를 제외하고 영업시간 제외 (09:00~18:00)	24시간 영업체계를 통한 고객의 시공간적인 접근향상
업무범위	금융과 관련한 대부분 업무 취급	지급결제,소액대출,신용카드 등 업무 특화(Niche Marketing)

또한 최근 해외 주요국에서 인터넷전문은행(Internet Primary Bank)이 꾸준하게 성장하고 있어 국내에서도 인터넷전문은행 설립에 대한 논의가 본격화될 전망이다. 그러나 금산분리 원칙이나 지분을 제한 등 규제 문제와 보안 문제는 여전히 풀어야 할 숙제이다.

인터넷전문은행은 지점망 없이 운영되는 저비용 구조로, 기존 은행에 비해서 각종 수수료를 최소화 하면서도 수익을 낼 수 있는 구조로 은행 이용자에게 보다 높은 예금금리, 낮은 대출금리, 저렴한 수수료 제공이

가능하다는 장점이 있다. 문제는 ICT 기반의 인터넷은행은 대부분 온라인으로 이루어지기 때문에 비대면에 따른 보안상 문제점을 어떻게 풀어 내느냐가 관건이다. 금융위원회에 따르면 국내 인터넷전문은행 설립을 위한 중요한 요건으로 네트워크, 백업체계 및 차별화된 보안체계를 요구하고 있다. 인터넷전문은행의 성공 여부는 모든 업무가 인터넷으로 이루어지기 때문에 강력한 사이버 보안기술과 정책이 필수적으로 수반되어야 하며 튼튼한 고객 기반과 고객의 니즈, ICT 기반 기술에서 경쟁력에 좌우된다.

### 제 3 절 해외 핀테크 동향

#### 1. 글로벌 핀테크 투자 현황

컨설팅회사 액센츄어의 발표한 ‘The Boom in Global Fintech Investment’ 보고서에 의하면, 핀테크 기업에 대한 글로벌 투자 규모는 2008년 9억2000만 달러였는데, 2013년 29억7000만 달러로 5년새 3배 이상 늘어난 것으로 나타난 것을 [표 2-2]에서 볼 수 있다.



(\* 주 : CB Insight, 현대증권 재인용)

(그림 2-2) 글로벌 핀테크 사업영역별 투자 비중(%)

이같은 추세는 당분간 계속 이어질 것으로 해외 핀테크 전문기관들은 예측하고 있다. 액센츄어는 글로벌 핀테크 투자 규모가 오는 2018년에 60억~80억달러로 늘어날 것으로 전망하고 있다. 2013년 투자규모에 비해 최소 2배 이상 더 늘어날다는 것이다.

[표 2-6] 영미중의 핀테크 도입 현황

국 가	주요 내용
영 국	<ul style="list-style-type: none"> <li>- 글로벌 금융위기 이후 금융과 IT와 융합으로 핀테크 발전속도와 투자면 세계 최고.</li> <li>* 영국내 핀테크 산업 종사자 13만5천명 추산. 런던에만 1,800여 핀테크 기업활동중</li> <li>* 핀테크 통한 거래규모 2008년 이후 매년 74% 성장(세계 성장률 27%)</li> <li>* 핀테크 투자 규모 2008~2013 년 동안 7.8 억달러</li> <li>- 영국 내 핀테크 산업은 거대 금융사의 지원을 배경으로 성장 중</li> <li>* Barclays 의 Barclays Accelerator</li> <li>* MasterCard, Lloyds Banking, Rabobank의 제휴: pan-European accelerator</li> <li>- 급격히 성장한 핀테크기업이 기존 금융기업 사업영역과 충돌하는 양상도 발생</li> </ul>
미 국	<ul style="list-style-type: none"> <li>- 미국 핀테크 산업은 영국에 비해 발전이 느린 것으로 평가되나 최근 들어 실리콘 벨리와 뉴욕은 각 지역의 강점을 바탕으로 핀테크 산업 활성화에 노력 중</li> <li>* 2013년 기준, 세계 핀테크 스타트업 투자금 중 83%가 미국에 집중</li> <li>* 한편 미국은 SNS 와 플랫폼 등 앞선 기술과 페이팔(Paypal)로 대표되는 결제 시스템 운용 경험을 토대로 영향력 높은 서비스 전세계에 보급</li> <li>- 가장 주목받고 있는 핀테크 서비스로 애플페이(Applepay)가 있음</li> <li>* 애플에서 출시한 지급결제서비스인 애플페이는 NFC(근거리 무선통신 방식)과 지문인식 결합하여 편리성과 보안성을 동시에 충족</li> <li>* 보안성이 높은 것은 결제시 단 한번 생성되는 보안 코드를 사용하기 때문임</li> <li>* 다만 애플페이의 결제시장 장악을 우려한 대형 유통사에서 애플페이 결제 거</li> </ul>
중 국	<ul style="list-style-type: none"> <li>- 중국의 핀테크 산업은 시장성 증가와 우호적인 정부정책을 배경으로 ICT 플랫폼 사업자들이 점차 핀테크 사업자로 진화하면서 발전</li> <li>* 중국의 모바일 인터넷 인구 5억명, 전체 인터넷이용인구 81%가 모바일인터넷 접속</li> <li>* 2013 년 모바일 인터넷의 총 수익 1,060 억 위안(19 조 원)으로 81.2%YoY증가</li> <li>* 중국정부는 플랫폼 사업자에게 금융업 권한을 부여, 핀테크 육성정책 확대 추세</li> <li>- 중국 핀테크의 대표 주자로 꼽히는 업체는 알리바바</li> <li>* 2014. 9. 19 일, 미국 뉴욕증권거래소 상장, 시가총액 242 조원 기록. 모바일 사용자 1.88 억명기반 다양한 핀테크 서비스 출시</li> <li>* 온라인 결제서비스 알리페이의 2013 년 거래액은 5.4 조억 위안(888 조 원)으로 중국 온라인 결제시장의 50%</li> <li>* MMF 등 개인 투자 부문으로도 사업 영역을 넓히고 있음</li> </ul>

전세계 벤처캐피탈의 핀테크 투자규모는 지난 3년간 벤처캐피탈의 전반적인 투자규모보다 무려 4배 이상 더 빠른 속도로 증가할 것으로 전망된다. 보고서에 따르면 2014년 1분기에만 무려 167건의 투자, 17억달러의 투자금이 핀테크 스타트업에 투자됐다.

벤처캐피탈의 핀테크 사업영역별 투자비중은 지난 5년간 큰 폭으로 변화한 것으로 나타났다. CB인사이트 조사에 따르면, 핀테크 초창기인 2008년에는 지급결제 부분에 70%, 금융데이터 분석에 16%가 투자됐고, 금융소프트웨어(10%)와 플랫폼(5%)이 그 뒤를 이었다.

하지만 이후 금융소프트웨어와 금융데이터 분석 영역에 대한 투자가 큰 폭으로 늘어나면서 [한국은행그림 2-2]에서 보이는 것처럼 상대적으로 지급결제 부분의 투자 비중은 2013년에 28%로 줄어들었다. 오히려 2013년에는 금융소프트웨어와 금융데이터 분석 영역이 각각 29%를 기록하며 처음으로 지급결제 영역의 투자규모를 뛰어넘기 시작했다.

플랫폼 서비스에 대한 투자도 빠른 속도로 늘고 있다. 클라우드펀딩 등 플랫폼 서비스인 킥스타터, 인디고고의 성공에 자극을 받은 유사 서비스가 잇달아 등장하면서 빠른 속도의 투자규모 확대에 힘입어 2008년 플랫폼 투자영역의 비중은 지급결제 투자규모의 14분의 1 수준에 불과했지만 2013년에는 절반 수준까지 올라섰다.

## 2. 업종별 핀테크 해외사례

### 가. 은행업에서의 핀테크

IT기술 발전에 따른 환경변화로 인해 기회와 위협을 동시에 인지하고 해외은행들은 1) 온라인 및 모바일 강화를 위한 인터넷전문은행 설립 내지는 인수, 2) SNS 활용을 통한 고객확대 전략을 추구해 왔다. 특히 개인금융부문에서는 비금융회사의 진출이 더 위협적일 수 있기 때문에 적극적인 대응에 나서고 있다. 또한 3) 핀테크가 본격적으로 도입되기 시



작한 2014년부터 해외 은행들은 핀테크 관련 기업을 직접 육성하기 위한 투자에도 적극적이다. 해외 주요 은행들은 핀테크에 대한 중요성을 이미 인지하고 관련기업에 대한 투자와 지원을 확대해가는 추세다.

[표 2-7] 해외은행들의 온라인, 모바일 경쟁력 강화 사례

구분	내용
모바일.SNS 채널 활용	- (커먼웰스, 호주) 페이스북 뱅킹서비스(조회, 이체) 개시(* 13.3) - (RBC, 캐나다) 페이스북메신저 기반 송금서비스 개시(* 13.12)
온라인 경쟁력 강화 위한 M&A 추진	- (캐피탈원, 미국) 인터넷 전문은행 ING Direct(네덜란드) 인수(* 12) - (BBVA, 스페인) 인터넷 전문은행 Simple(미국) 인수(* 14.2) - (스베르, 러시아) 페이스북 뱅킹 도입한 데니즈은행(터키) 인수(* 12)

(\* 주 : 산업은행경제연구소, 교보증권 리서치센터)

혁신은 기존 사업의 점진적 개선을 추구하는 존속적 혁신(Sustaining innovation)과 기존 사업의 패러다임을 바꾸는 파괴적 혁신(Disruptive innovation)으로 구분할 수 있다(Clay Christensen, Harvard University). 핀테크도 이처럼 혁신의 관점에서 두 가지로 분류할 수 있다. 기존 금융회사가 존속하기 위해 IT기술을 접목하는 ‘존속적 핀테크’와 새로운 회사가 IT기술을 통해 기존 금융회사의 영역에 도전하는 ‘파괴적 핀테크’이다.

금융영역에 있어 핀테크란 존속적 혁신의 영역으로 설명될 수 있다. 따라서 본 장에서 살펴볼 핀테크란 그 뿌리가 증권, 보험산업에서 시작되어 IT와 융합돼 새롭게 파생된 분야와 이를 국내에서 도입했을 때 잠재적 성장성이 가장 큰 기업이다.

[표 2-8] 설립 주체별 해외 인터넷전문은행 현황

설립주체	설립형태	인터넷전문은행
은행	사업부	HelloBank(프랑스), Zuno Bank AG(오스트리아) First Direct(영국), Cahoot(영국), Smile Bank(영국), Icesave(아이슬란드), Kaupthing Edge(아이슬란드)
	독립 법인	WeBank(이탈리아)
	별도 법인연계	ComDirect(독일), Boursorama(프랑스), BforBank(프랑스), Fortuneo(프랑스)
은행과 타업종 합자	통신업체 제휴	Jibun Bank(일본)
	포털업체 제휴	The Japan Nitet Bank(일본)
비은행 금융회사	증권: 브로커리지 서비스 확장	Charles Schwab Bank(미국), Daiwa Next Bank(일본)
	보험: 저축예금 공략	EGG Bank(영국), ING Direct(네덜란드), Sony Bank(일본)
	카드: 지급결제 서비스 확장	American Express Bank(미국)
산업자본	유통: 기존 고객기반 활용	Tesco Bank(영국), Seven Bank(일본), AEON Bank(일본), Rakuten Bank(일본)
	자동차: 자동차금융 특화	BMW Bank(독일), VM Bank(독일), Mercedes-Benz Bank(독일)
모험자본	특화 영업모델	Fidor Bank AG(독일), AlderMore, CC Bank(영국), Holvi(핀란드)

(\* 주 : 우리금융경영연구소, 교보증권 리서치센터)

[표 2-9] 해외 은행들의 핀테크 육성방안

국가	은행명	육성방안
스페인	Santander	2014년 7월 런던을 중심으로 핀테크 기업에 투자하는 1 억달러 규모의 펀드 조성
	BBVA	2013년 1월 美 실리콘밸리 중심으로 핀테크 기업에 투자하는 1억달러 규모의 펀드 조성
영국	HSBC	2014년 5월 리테일뱅킹 부문 핀테크 기업에 투자하는 2 억달러 규모의 펀드 조성
	Barclays	2014년 5월부터 유망 핀테크 기업에 대해 업체당 최고 5만 달러까지 투자하고 창업지원서비스를 제공해주는 'Barclays, Accelerator'라는 핀테크 기업 육성 프로그램을 운영 중
스위스	UBS	2014년 5월부터 유망 핀테크 기업을 선정하여 투자와 창업지원서비스를 제공하는 'Innovation Spaces'라는 Working Group을 운영 중
미국	Wells Fargo	2014년 8월부터 유망 핀테크 기업에 대해 업체당 최저 5만 달러에서 최고 50만 달러까지 투자하고 창업지원서비스를 제공해주는 핀테크 기업 육성 프로그램을 운영 중
	Citi	2014년 한 해 동안 Citi Ventures를 통해 유망 핀테크 기업에 총 7천만 달러를 투자

## 나. 증권산업에서의 핀테크

국내 금융투자업계는 타 금융권역과 비교해 2000년대 초반부터 IT기술을 빠르게 접목시켜왔다. 2000년 1월, 3월 이트레이드, 키움증권이 각각 온라인 전용 증권회사를 설립하는데 성공하여 온라인 증권거래비중을 큰 폭으로 끌어올렸다. 또한 2013년 온라인 전용 펀드판매회사인 펀드온라인코리아가 출범되어 온라인 자산관리 서비스를 제공하기 시작했다. 증권산업에서는 10여년 전부터 비교적 신속하게 IT와의 융합을 추진해 왔기 때문에 정부의 지원이 보장된다면 가장 빠르게 발전할 수 있는 영역이다. 그리고 기업으로써는 키움증권과 미래에셋증권이 이에 가장 근접해 있다. 인터넷전문은행-온라인 자산관리의 형태로 추구하는 방향은 조금 다르지만 궁극적으로 지향하는 비즈니스모델은 다양한 금융상품 제공을 바탕으로 하는 자산관리다.

다. 인터넷전문은행 비즈니스모델: Charles Schwab Bank, E\*Trade Bank

인터넷전문은행은 미국에서 설립된 Charles Schwab Bank와 E\*Trade Bank가 가장 성공적인 모델이다. 각 은행은 온라인전용 증권회사에 의해 탄생한, 비 은행 금융회사가 설립을 주도한 것이 특징적이다. 양 사는 증시 부진으로 인터넷 주식거래가 더 이상 새로운 수요를 창출하지 못한다는 판단에 증권부문의 고객 감소에 따른 매출 감소를 만회하기 위해 은행서비스를 제공하기 시작했다. 주로 주택담보대출이나 전통적인 소매은행 업무위주로 시작하였으며 궁극적인 목표는 자산관리 중심 사업구조이다. 국내에서는 키움증권이 이러한 모델에 가장 근접해있다. 2014년 6월 기준 Charles Schwab Bank의 자산은 1,037억달러로 미국 내 인터넷전문은행 중 가장 많은 자산을 보유하고 있으며 E\*Trade Bank는 총자산 445억달러 수준이다.

라. 온라인자산관리 비즈니스모델: Merrill Edge, Motif Investing

인터넷전문은행이 금융상품 중 하나로 전통적인 은행상품을 제공하기 위해 시작했다면 처음부터 ‘자산관리’를 목표로 핀테크를 접목한 비즈니스모델도 존재한다. 알고리즘을 이용하여 투자자의 성향을 파악하고 이에 맞게 자산배분, 자동 리밸런싱, 주기적 보고, 단순자문 등을 제공한다. 24시간자문 서비스를 통해 접근성을 높였고 검증되고 정형화된 채테크 모델을 사용해 저비용 자산관리를 가능케 했다. 대표적인 기업은 Bank of America Merrill Lynch가 2010년 6월 개시한 Merrill Edge와 Motif Investing이다. Merrill Edge는 5만~25만 달러를 보유한 고객층을 주요 타겟으로 자기 주도적 투자성향이 높은 고객군을 대상으로 다양한 금융상품을 판매한다. 개인별 투자성향에 맞춘 일임서비스를 제공하며 고객 요청에 따라 24시간 자문서비스를 제공하고 있다.

Motif Investing은 위탁매매에 핀테크를 접목시킨 회사다. 투자자들은 최대 30개 종목의 주식 또는 채권으로 이루어진 테마형 바스켓에 투자할 수 있고 개별종목의 가중치를 조정할 수 있다. 국내에서는 미래에셋증권이 이러한 비즈니스모델에 가장 근접해 있다.

마. 보험산업에서의 핀테크

보험산업에서 핀테크란 주로 빅데이터를 활용한 Underwriting시간의 단축 및 간편화의 방향으로 발전하는 추세이다. 보험연구원에 따르면 핀테크, 특히 빅데이터를 활용한 보험산업에 기대되는 변화는 1) 다양한 기초데이터를 확보하여 위험률 조정 등을 통해 적정보험료 산출, 2) 스마트기기를 활용한 청약 등 온라인, 모바일 채널 등 다양한 플랫폼을 통한 보험판매 활성화, 3) 보험금 지급심사 및 보험사고 조사 시 핀테크를 이용한 금융소프트웨어, 금융데이터 수집 및 분석 등을 통해 보험금 지

급 관련 프로세스 개선이다. 즉, 방대한 데이터를 활용하여 보험심사 시간을 줄이고 적정한 보험료 산출을 통한 손해율 개선이 가장 기대되는 영역이다. 해외에서는 빅데이터를 활용하여 운전자의 습관을 파악해 정교한 자동차보험료 산정에 이용하거나 손목밴드를 활용하여 고객의 건강 정보를 수집, 생명보험료 산정에 이용하는 등 프로세스 개선에 활발히 이용하고 있는 추세다. 국내에도 유사한 사례로 온라인보험을 들 수 있으며 성공적인 사례는 삼성화재의 In-bound 온라인 자동차보험 ‘애니카다이렉트’와 교보생명의 ‘교보라이프 플래닛’이다. 이 보험들은 모두가 가입부터 유지, 보험금 지급 등 모든 절차를 인터넷에서 할 수 있어 설계사 수수료나 영업점 운영비를 줄일 수 있기 때문에 기존 Off-line보험사보다 보험료를 15~30% 정도 낮게 책정할 수 있다. 웹페이지를 들어가 보면 상품구성이 단순하고 보험료 계산이 빠른 장점이 있다.

#### 바. IT/인터넷 서비스 업에서의 핀테크

최근 글로벌 IT 서비스 업체들의 금융업 진출이 활발히 이루어지고 있다. 최대 IT 업체인 애플, 글로벌 SNS 업체 페이스북 등 세계 굴지의 기업들이 지급결제서비스부터 시작해 민영은행에 까지 진출을 시도하고 있다.

일반적으로 IT/인터넷 서비스 업체의 경우 본업이 금융업과 다소 거리가 있어 불리하다 생각할 수 있지만, 사용자 기반 확보 부분에 있어 타 업종 대비 훨씬 유리한 위치에 서 있다. 실제로 페이스북의 가입자가 2015년 1월 기준 12억명으로 어느 업종의 어느 업체보다도 넓은 유저 베이스를 보유하고 있다. 국내에서도 마찬가지로 다음카카오가 3,700만에 육박하는 가입자를 보유하고 있는 카카오톡을 축으로 핀테크 및 인터넷 뱅킹 사업에 진출하고 있다.

지금까지 IT/인터넷 서비스 업체들의 핀테크 산업 진출의 모습을 살펴 보면 핀테크 산업을 통한 직접적인 수익창출보다는 본업과의 시너지 받

생에 초점을 두고 있는 것으로 판단된다. 자사의 제품판매 증진을 위해 서 혹은 기존고객들을 각인시켜 지속적인 서비스 사용을 유도하기 위해 핀테크 산업에 진출하고 있는 모습을 보이고 있다. 이러한 이유로 대다수의 업체들이 저렴한 수수료로 혹은 무료로 핀테크 관련 서비스를 제공한다. 애플의 경우 애플페이의 수수료로 카드사로부터 0.15% 수준에 해당하는 수수료만을 받고 있으며 NAVER, 알리페이 등 대형 인터넷 업체들의 경우 무료로도 관련 서비스를 제공하고 있다. 세계 각지의 업체들 모두 관련 서비스 선점을 위해 활발히 진출하고 있으며 이러한 모습은 앞으로도 지속된다.

모바일 트래픽이 급증함과 동시에 모바일 채널을 통한 금융거래가 급격히 증대되어 관련 산업이 발전할 수 있는 여건이 형성되고 있다. 해외 글로벌 ICT(Information & Communication Technology) 기업들은 자사 사이트 결제 수요 또는 모바일 네트워크 기반으로 다양한 형태의 송금·결제서비스를 제공하고 있다.

[표 2-10] 혁신적인 해외 핀테크 기업 사례

기업명	사업내용
스트라이프 (Stripe.com)	<ul style="list-style-type: none"> <li>- 자사의 앱 프로그래밍 인터페이스를 앱에 삽입한 회원에게 글로벌 고객을 대상으로 한 지급결제와 7일 안에 대금을 지급해주는 서비스 제공</li> <li>- 전세계 139개국 통화와 비트코인, 알리페이 등으로도 결제 가능</li> </ul>
어firm (Affirm.com)	<ul style="list-style-type: none"> <li>- 회원이 온라인 쇼핑몰에서 물건을 구매 할 때, 신용카드가 아닌 본인의 신용으로 할부 구매 할 수 있도록 해주는 결제서비스 제공</li> <li>- 회원의 공개된 데이터를 분석해 단 몇 초 만에 신용도를 평가한 후, 회원의 적정 할부 수수료를 산정하여 부과</li> </ul>
빌가드 (Billguard.co)	<ul style="list-style-type: none"> <li>- 자사가 개발한 예측 알고리즘을 활용하여 신용카드 청구서 상호청구 또는 수수료 과다 인출 등의 징후를 포착하여 회원</li> </ul>

m)	에게 알려주는 서비스 제공 - 모바일앱으로 회원의 신용카드와 은행계좌를 통합 관리 가능
온덱 (OnDeck.com)	- 100% 온라인 기반으로 대출 신청서 제출에 10분, 신청 일에 지정 계좌로 자금을 입금해주는 대출 서비스 제공 - 자체 개발한 신용평가 알고리즘이 대출 신청자의 금융기관 거래내용, 현금 흐름, SNS 상 평판 등을 고려해 몇분 만에 신용평가 및 대출 여부 심사

(\* 주 : 우리금융경영연구소)

페이팔(Paypal)은 1998년 설립된 전자결제 전문업체로 2002년 e-bay에 인수되었으며, 14년말까지 약 1.57억개의 유효계좌를 보유하고 있다. 이는 약 200개국에 26개 화폐를 통한 결제서비스를 제공하고 모바일 시장 규모가 확대됨에 따라 꾸준한 상승세를 기록하고 있다. 중국의 인터넷 보급률 확대와 스마트 디바이스의 확산과 더불어 전자상거래 시장이 폭발적으로 성장함에 따라 알리바바의 성장세도 상당한 수준으로 올라 왔다. ‘알리페이’를 앞세워 송금·결제서비스 시장에서 무서운 상승세를 보이고 있으며 ‘위어바오’란 상품을 통해 실질적으로 인터넷은행의 수신기능을 수행하면서 은행서비스 시장을 위협하고 있다. 그리고 최근에는 혁신적인 아이디어와 기술력을 바탕으로 핀테크 스타트업 기업들이 차별화된 비즈니스모델을 통해 핀테크 산업으로 활발하게 진출하고 있다. 해외 핀테크 산업에 대한 투자는 2008년 9억 달러에서 꾸준한 성장을 보이고 있으며 특히 금융데이터분석과 소프트웨어 부문의 투자비중이 증가하고 있다. 이와 같이 핀테크의 여러 분야가 활발하게 발전하고 있는데, 금융 관련 정책, 서비스 개발, IT 기술 지원의 3박자가 잘 맞아가는 국가와 기업은 무서운 속도로 세계 핀테크 시장을 선점하고 있다. 그리고, 투자는 그 속도에 가속을 붙이고 있는데, 우리나라 통계청 자료에 의하면 2013년 1분기 1조 1,270억원이었던 모바일 결제시장 규모는 2014년 2분기 3조 1,930억 원으로 집계되어 전년 1분기 대비 283% 성장한 것으로 나타났다. 정부는 2015년 올해 중점 금융산업으로 핀테크를 지정한 바 있다.

시장조사업체 가트너(Gartner)의 모바일 결제시장에 관한 전망에 따르면, 2015년에 4,311억 달러를, 그리고 2017년에는 4억 5,000만 명이 7,213억 달러 규모의 시장을 만들어 낼 것으로 전망하고 있다.

[표 2-11] 주요 국가의 핀테크 특징과 투자현황

국가	특징	주요내용
미국	기술혁신 통한 세계 최대의 핀테크 시장형성	<ul style="list-style-type: none"> <li>· 글로벌 핀테크 기술과 시장확대 선도</li> <li>· 애플과 구글이 탄생된 실리콘밸리에서 핀테크 분야 투자집중</li> <li>· 세계 최대 금융가인 뉴욕도 핀테크 혁신과 투자 확대</li> <li>· 전세계 글로벌 핀테크 투자의 83% 차지하고, 이중 실리콘밸리가 32%를 차지한다.</li> </ul>
영국	핀테크에 대한 적극적 정부정책	<ul style="list-style-type: none"> <li>· 런던 동쪽 테크시티 조성(핀테크메카)</li> <li>· 글로벌 금융센터의 위상 강화</li> <li>· 대형은행 중심의 핀테크 산업 육성(투자, 제휴)</li> </ul>
중국	거대한 모바일 시장 핀테크 수요급증	<ul style="list-style-type: none"> <li>· 모바일과 관련 애플리케이션 시장의 급성장</li> <li>· 온라인 소비정책으로 모바일 소비 급속 확대</li> <li>· 알리바바 등 글로벌 IT 출현(이커머스와 금융의 결합)</li> </ul>

특히, 중국은 모바일 인터넷 이용자수가 2013년 7억명에서 2016년 9억명을 돌파할 것으로 전망되고 있으며, 그에 따른 모바일 시장규모는 2013년 2,295억위안(39.8조원)에서 2016년 8,621억위안(149.6조원)에 달할 것으로 보인다. 투자 확대 만큼 해당 분야 핀테크 관련 기술 또한 날로 발전하고 있다. 기술은 글로벌 IT 기업과 신생기업의 도전으로 참신하고 흥미로운 발전을 거듭하는 양상이다. 한편, 2015년 11월 3일에 구글, 애플, 아마존, 페이스북 등 핀테크 선진 기술 보유 기업들이 핀테크 사업 활성화를 위해 새로운 IT 금융연합 FIN(Financial Innovation Now)를 설립했다. FIN은 금융 중심보다는 기술로 핀테크 사업을 활성화 하겠다는 IT기



업의 의지를 담고 있다. 기술이 산업을 리드하는 시대이다.

“혁신적인 금융서비스가 오고 있다. 이제 미국은 더욱 접근성과 저렴하고 안전한 금융시스템을 활성화할 때가 왔다. 미국 정부는 이제 묶어 놓은 금융규제 정책들을 풀어야 한다. ”

- 브라이언 피터스(Brian Peters), FIN 전무이사

FIN은 새로운 기술로 금융 소비자와 중소기업 대출에 대한 온라인 시장을 확장하며, 나아가서는 금융혁신을 위해 새로운 정책을 추진하겠다고 나섰다. 지금 미국은 자국의 안전과 경제 번영을 위해 경쟁보다는 시장 활성화를 위해 하나로 뭉치고 있다.

또한, 국가간 협력도 커지고 있다. 미국, 일본, 유럽연합(EU)의 대형 금융기관들이 핀테크 패권을 잡기 위해 서로 손을 잡았다. 22개 은행 연합이 가상화폐 비트코인에서 이용된 '블록체인(block chain)' 기술을 응용하고 송금과 결제를 저렴하게 처리할 수 있는 공통 시스템을 구축하기로 했다. 이것은 IT기업의 금융시장 진출에 대한 경계이다. 핀테크 기술과 서비스, 그리고 투자는 이제 기업과 국가 사이의 협업을 통해서 그리고 IT와 금융의 융합과 경쟁을 통해서 급속도로 성장하고 있다. 우리나라 핀테크 생태계 발전을 위해 정부, 금융기관, IT 기업, 스타트업, 투자기관 등의 협력이 시급한 시점이다.

## 제 4 절 국내 핀테크 지원 정책

### 1. 금융위원회 핀테크 정책

정부의 핀테크 활성화 정책 이후 금융기업과 핀테크 기업간의 연결창구가 마련되고, 불필요한 규제가 완화·폐지돼 실질적인 효과를 준비하고 있다.

핀테크를 국내에 국한시키지 말고 해외진출 등 해외 업체와 경쟁할 수

있는 분위기를 조성해주는 정책 지원을 준비하고 있다.

가. 혁신적 금융서비스로 국민 편의 증대

경쟁과 혁신을 기반으로 금융개혁을 추진해 창조경제를 뒷받침하는 혁신적 자금중개 기능을 강화하는 한편, 핀테크 등 금융산업을 새로운 먹거리산업으로 육성하고 새로운 금융상품과 서비스를 지속적으로 공급해 나가야 한다. 이를 위해 '창조경제를 뒷받침하는 혁신적 자금중개 기능 강화', '핀테크·금융산업을 새로운 먹거리산업으로 육성', '혁신적 금융서비스 혜택 확산' 등 세 가지를 중점 추진 과제로 제시하고 이를 실현하기 위한 구체적 방안을 제시하고 있다.

금융위는 정보통신기술(ICT)과 문화콘텐츠 등 핵심 성장 분야에 정책 자금 80조 원을 공급한다. ICT, 바이오·헬스 등 미래 신성장동력산업과 유망 서비스산업(72조4000억 원), 소프트웨어·게임·캐릭터·방송·공연·출판 등 문화콘텐츠산업(7조2000억 원)을 육성하고, 문화콘텐츠 금융센터를 설립하는 등 인프라를 강화한다. 또한 금융권의 변화와 혁신을 촉진하기 위해 1월 4일부터 시행된 '금융규제 운영 규정'을 통해 금융규제의 투명성과 합리성, 책임성을 확보한다. 금융회사의 보수·인사·평가·교육 시스템 전반에 성과주의 문화가 확산되도록 유도하고, 이를 바탕으로 금융권의 혁신과 경쟁을 촉진한다.



(그림 2-3) 금융위의 글로벌 핀테크 육성정책

## 나. 핀테크 기업의 해외 진출 다각적 지원

금융위는 금융산업을 글로벌 수준으로 강화하고 발전시킬 방침이다. 먼저, 핀테크산업의 글로벌 경쟁력을 강화한다. 이를 위해 핀테크 지원 센터-대한무역투자진흥공사(코트라), 한국특허정보원, 법무법인 사이에 해외진출 원스톱 지원체계를 운영하는 등 핀테크 기업의 해외진출을 다각적으로 지원한다. 또한 세계 최초로 핀테크 서비스 개발에 필요한 표준화된 개발도구(API)를 제공해 쉽고 빠르게 핀테크 서비스를 출시할 수 있도록 지원한다.

아울러 빅데이터 활용 제약 요인을 제거해 다양한 빅데이터 서비스를 제공한다. 미국과 유럽연합(EU) 등의 경우 비식별 정보(개인을 식별할 수 없는 정보)는 개인정보에서 제외해 상대적으로 활용이 자유롭다. 이에 비해 우리나라는 신용정보법에 의거해 비식별 정보를 활용할 수 있는지 여부가 명확하지 않아 빅데이터 활용에 제약 요인으로 작용해왔다. 이에 앞으로는 외국처럼 비식별 정보는 개인 신용정보에서 제외해 빅데이터 활용에 대한 기반을 마련할 예정이다. 금융위는 금융산업을 글로벌 수준으로 발전시키기 위해 2016년 하반기부터 점포 방문 없이 스마트폰만으로 모든 은행 서비스를 이용할 수 있는 인터넷 전문은행을 출범시킬 계획이다. 금융투자업자가 고부가가치 영역에 진출하고 창의적 서비스로 경쟁할 수 있도록 '글로벌 투자은행(IB)' 도입도 적극 추진한다. 더불어 다양한 보험상품이 경쟁하는 환경을 조성해 세계 5대 보험 강국을 이룰 방침이다.

## 다. 혁신적 금융서비스로 국민 혜택 확산

금융위는 금융서비스가 국민에게 확산될 수 있도록 노력하고, 국민의 재산을 늘리겠다는 목표도 세웠다. 일단, 혁신적 금융상품과 금융서비스

로 국민 편익을 증대한다. 이로써 은행권 외 제2금융권에서 얼굴을 직접 보지 않고도 실명 확인이 가능해져 금융거래시 시간과 공간의 제약을 해소할 수 있게 된다. 금융상품의 자문 사업을 활성화해 국민 자산을 효율적으로 운용할 수 있도록 지원한다. 특히 로보어드바이저(Robo advisor)를 활성화하기 위한 여건을 조성할 방침이다.

‘로보어드바이저’는 온라인상으로 고객이 자신의 투자 조건을 입력하면 컴퓨터 프로그램이 빅데이터 분석 등을 통해 고객별 맞춤형 포트폴리오를 구성해주고 리밸런싱(자산 배분비율 재구성)을 실행하는 것이다. 금융상품의 판매 채널을 확대해 금융상품 구입에 대한 편의성도 높인다. 이를 위해 서민금융기관 등에 단계적으로 펀드 판매를 허용하고, IT기업 등이 온라인 펀드 판매업의 대주주가 될 수 있도록 허용한다. 이와 함께 국민의 수요에 맞는 다양한 상품을 제공한다. 이를 위해 정확한 신용위험평가를 기반으로 중위험·중수익 상품 등 다양한 구조의 상품을 출시하고, 연금 자산의 효율적인 관리를 위해 개인연금 계좌를 비롯한 다양한 자산 운용방식을 도입해 퇴직연금과 개인연금의 종합적 자산 운용도 추진할 방침이다.

## 2. 금융보안원 정책

금융보안원에서는 블록체인 등 신기술 활용하여 핀테크 확산하도록 한다고 정책 방향으로 추진하고 있다. ‘블록체인 등 신기술을 활용한 핀테크 서비스 확산할 전망이어서, 금융보안원에서는 ‘금융 IT·보안 10대 이슈 전망’을 발표했다.

스마트폰 등 IT기기 발전으로 바이오 인증기술을 활용한 금융서비스가 산업 전반에 확대된다. 정맥인증을 통한 셀프뱅킹서비스, ATM기에 홍채 인증 시범 적용된다. 보험사는 목소리 인식 방식을 활용한 콜센터 상담을 시작한다. 카드사는 지문인식을 활용해 결제한다. 보안성과 투명성, 비용절감 요구가 증가해 블록체인 등 신기술을 활용한 금융서비스가 본

격 등장할 전망이다.

금융서비스를 노린 분산서비스거부(DDoS) 공격은 지속된다. 표적형 랜섬웨어 증가와 금융과 IT 융합의 가속화에 따른 신종 보안위협도 등장한다. 금융회사 책임과 역할이 강화돼 전사 관점에서 ‘금융보안 거버넌스’ 확립과 확산도



(\* 주 : 금융보안원 제공)

(그림 2-4) 금융보안원 IT,보안 10대이슈 전망

이슈다. 금융보안원은 금융권 공동 대응으로 사고를 예방하고 피해 확산을 방지한다. 이상거래탐지시스템(FDS) 등 위협정보를 공유를 확대한다. 금융보안원은 금융회사 전반 보안수준과 신뢰성 향상을 위해 정책과 기술 연구 등을 추진하며, 금융보안 뿌리를 다지는 노력을 지속한다.

## 제 3 장 핀테크 기술 동향 분석

### 제 1 절 핀테크 기술동향

#### 1. 핀테크 기술핵심

핀테크에서 사용되는 ICT기술은 금융서비스에 따라 다양한 형태로 구성된다. 최근에는 오프라인보다는 모바일로 급속히 이동하고 있다. 인터넷 은행 도입이 확정되면서 시공간의 제약이 없어진다. 핀테크에서 사용되는 ICT기술 중 새롭게 만들어진 기술은 거의 없다. 기존의 기술을 적용하고 보완하여 사용되는 기술들이 대부분이며, 신기술보다는 기존 제도의 변경, 새로운 금융서비스의 시작 등이 핀테크의 핵심이다.

핀테크 기술을 기존 금융시스템에 적용하기 위해서는 몇 가지 고려 사항이 있다. 기존 서비스에서 사용 중인 ICT기술과 어떻게 연계하고 무선 통신으로 인한 보안과 사용자 인증 문제에 대해서도 검토가 필요하다. 그리고, 무한 신뢰가 필요한 금융 소프트웨어의 품질관리에 대한 대비가 있어야 한다. 여기에서 서비스 관점에서 필요한 ICT 기술요소를 논하고, 세부적인 ICT 기술에 대해서는 아키텍처, 보안, 인증기술, 품질관리, 기술개발론으로 구분한다.

핀테크는 금융 관련 서비스이기 때문에 규제가 많다. 금융 기반의 핀테크 서비스로 해석될 경우 국가의 금융규제로 인해 많은 제약 사항이 있다. 핀테크 기반의 금융서비스가 된다고 하더라도 금융 규제를 받는 금융 기업과 ICT 기술 간의 협업도 쉽지가 않을 것이다. 이러한 관계로 금융서비스와 ICT기술 간 법규에 관한 지식과 특허에 대해서 준비가 필요하다.

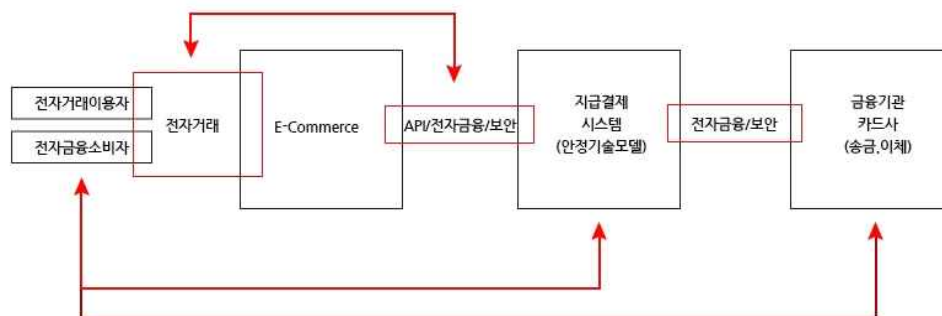


(그림 3-1) : 금융서비스와 핀테크 간의 관계

### 1) 핀테크에 필요한 ICT기술

그동안 금융 ICT서비스는 금융서비스를 도와주는 조력자(Facilitator)였다. ICT시스템을 활용한 금융서비스, 금융 솔루션 등이 있었다. 현재 핀테크의 경우도 기존 금융 ICT 서비스의 조력자 역할을 넘어 소규모 혁신기업 형태로 확대되고 있다.

인터넷 전문은행, 클라우드 펀딩, 자산관리, 송금서비스가 이에 해당된다. 핀테크의 ICT기술은 크게 2개 분야로 구분한다. 첫 번째는 전자거래 등에 필요한 요소기술 분야이고, 두 번째는 보안기술 분야이다.



(\* 주 : NIPA SW공학센터 웹진)

(그림 3-2) 핀테크의 ICT기술 분야(예)

## 1) 전자거래에 필요한 요소기술

최근에 제공되고 있는 핀테크에 필요한 요소기술은 크게 모바일 결제, 온라인 결제 및 인터넷뱅킹, 그리고 빅데이터를 활용한 신용관리 등 3분야로 구분한다. 모바일 결제는 모바일 디바이스의 확산으로 결제 프로세스를 간소화하려고 노력하고 있다. 다중 인증을 활용하거나 단순한 ID/PW를 도입하고 보안정책, 결제대행 시스템, 이상행위탐지 등을 복합적으로 적용하고 있다. 각 모바일 결제서비스는 본인 인증에 대한 기술을 필수적으로 요구하고 있고, 보유한 디바이스에 따라 본인 인증 방법을 달리하고 있다.

[표 3-1] 모바일 결제 기술

구분	구동내용
NFC + TouchID	<ul style="list-style-type: none"> <li>- 10cm내의 근거리에서 단말기 간에 데이터 전송이 가능한 NFC(근거리이동통신)기술과 지문인식으로 결제하는 방식</li> <li>- 대표적으로 애플(Apple Inc.)에서 개발한 Apple Pay에 도입</li> </ul>
ID/PW + Escrow + FDS	<ul style="list-style-type: none"> <li>- 신용카드와 스마트폰 등 결제 수단을 등록해 PC나 모바일에서 ID/PW만을 입력하여 결제하는 방식</li> <li>- ID/PW의 약화된 보안을 위해 부정행위를 탐지하는 Fraud Detection System(FDS)를 도입하거나 가상계좌를 활용하는 에스크로(Escrow)방식을 적용</li> </ul>
Barcode / QR 코드	<ul style="list-style-type: none"> <li>- 카드정보를 등록하고 결제 시 바코드나 QR코드를 읽어 결제가 진행되는 방식</li> <li>- 최근 우리나라에서 많이 늘어나고 있는 형태</li> </ul>
Beacon	<ul style="list-style-type: none"> <li>- 비콘을 통해 확보된 사용자의 위치를 이용하여 핸드폰을 꺼내지 않고 구입 의사를 표현</li> <li>- 페이팔은 비콘을 이용해 고객이 매장을 방문했을 때 자동으로 고객정보를 확인하고 비용을 청구하도록 서비스</li> </ul>



모 바 일 신용카드	<ul style="list-style-type: none"> <li>- 모바일기기에 저장되거나 카드사에 접속하여 결제서비스</li> <li>- USIM형 방식과 APP형 방식이 존재</li> </ul>
---------------	---

온라인 결제 및 인터넷뱅킹 서비스는 우리나라에서 매우 활발히 서비스되고 있다. 두 서비스는 모바일 결제처럼 본인 인증이 중요한 사항이다. 본인 인증을 위해 ActiveX와 같은 보안모듈을 설치하고 있다. 최근에는 보안모듈 설치의 불편함을 막고자 본인 인증 방법을 많이 도입하고 있지만, 일반 사용자의 만족도는 그리 높지 않은 편이다.

## 2) 빅데이터의 활용 현황

최근 빅데이터를 활용한 신용관리가 집중 조명을 받고 있다.

[표 3-2] 대출을 위한 빅데이터 분석 활용

구분	내용
빅데이터 수집	<ul style="list-style-type: none"> <li>- 정형데이터: 전자상거래 사이트내 거래량, 재구매율, 만족도수집</li> <li>- 비정형 데이터: 판매자와 구매자 간 이력, 후기 등 수집</li> <li>- 외부데이터: SNS, 포털 등의 데이터수집 및 내부 데이터와 연동</li> </ul>
빅데이터 분석/활 용	<ul style="list-style-type: none"> <li>- 빅데이터 분석 전문가의 데이터분석과 빅데이터 알고리즘 적용</li> <li>- 신청자의 대출 상환 능력과 의지를 정량적으로 도출</li> </ul>

금융권에서 가장 중요시하는 것 중의 하나가 신용관리이지만 일반적인 체크리스트로는 신용을 파악하기가 매우 어려웠다. 빅데이터 분석은 앞에서 살펴본 결제 중심의 서비스보다는 빅데이터 분석을 통한 개인 맞춤형 서비스 개발에 중점을 두고 있다. 빅데이터 분석을 적용해 새로운 금융서비스를 창출하고 있고, 금융 대출을 위해 빅데이터 분석한 결과를 기준으로 사용자에게 대출을 해주는 서비스도 나타나고 있다.

[표 3-3] 빅데이터 활용 사례

구분	금융사	내용
은행	IBK은행	- 고객감성분석을 통해 기업 이미지 재고 등 평판관리에 활용
	스탠다드차타드	- 개인 소셜미디어(SNS)를 이용한 타겟 마케팅 활용
	KB국민은행	- 지도와 고객의 데이터를 결합해 지도 위에서 고객의 거래내용으로 실시간으로 볼 수 있는 시스템을 개발해 마케팅에 활용할 계획
	하나은행	- 로그보안에 대한 빅데이터 분석을 시행, 보안성 향상
	신한은행	- 빅데이터 정의와 활용방안 등에 대해 논의 진행
	우리은행	- IT 지원부서 중심으로 빅데이터 업무 준비 중
카드	신한카드	- 2200만 고객 데이터 기반, 고객 마케팅 및 신상품 개발 등에 적용
	현대카드	- 빅데이터 기반으로 카드이용 편의성을 재고하는 마이메튜서비스 제공
	삼성카드	- 회원별로 차별화된 혜택을 제공하는 '삼성카드 링크(LINK)' 서비스
	KB국민카드	- 빅데이터 분석 기반으로 카드 이용 서비스 및 편의성 재고
보험	현대해상	- 사기범죄 적발 및 예방을 위한 빅데이터 기반의 분석 솔루션(FDS)을 도입
	삼성화재	- 빅데이터 분석 솔루션을 활용해 모럴해저드 사고 및 고위험군 사고를 분석하는 시스템인 IDFS를 개발

### 3) 핀테크 아키텍처

핀테크는 기존의 금융서비스에 ICT 기술을 접목하여 새로운 서비스를 하는 것이다. 기존의 금융서비스를 어떻게 활용할 것 인지가 핀테크 아키텍처를 결정하는 중요한 요소이다. 핀테크의 시작은 금융 아키텍처에 핀테크를 적용하여 최적의 아키텍처를 구성하는 것이다. 돈을 다루는 금융 아키텍처는 다른 업종에 비해 매우 광범위하고 복잡하기 때문에 가급

적 기존 아키텍처에 손대지 않고 핀테크를 적용하는 것이 중요하다.

#### (1) 기존의 금융서비스 아키텍처

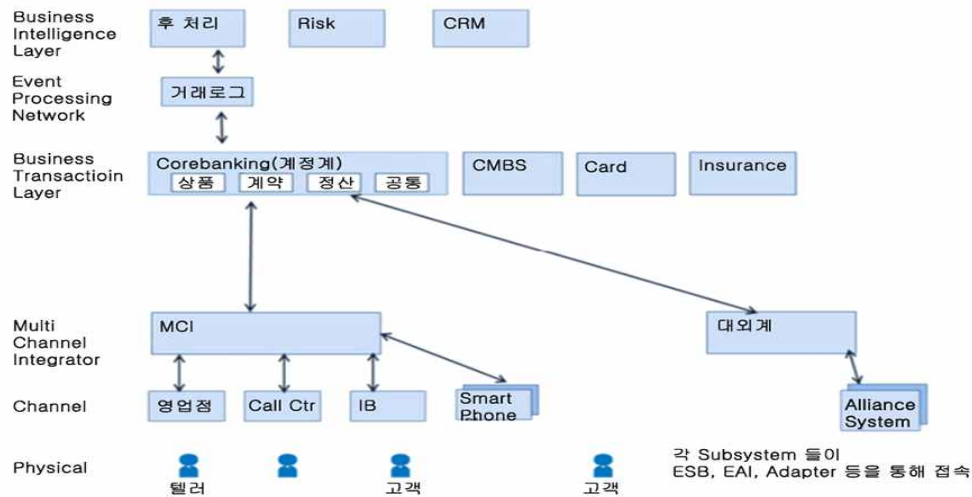
현재의 금융서비스는 고객이 직접 은행에 방문하는 서비스와 PC, 모바일을 이용한 유저 인터페이스와 채널이 추가되어 인터넷/폰뱅킹 서비스가 추가되었다.



(\* 주 : NIPA SW공학센터 웹진)

(그림 3-3) 현행 금융서비스 모델

현재 우리나라의 대표적인 금융시스템은 차세대 시스템으로 불리고 있으며, 우리나라 금융시스템의 3세대에 해당한다. 차세대 시스템은 '90년대 후반기부터 시작했으나 금융위기, 금융권 구조조정으로 '04년 IBK를 시작으로 적용되었다. 차세대 시스템 적용 전(2세대, 종합 온라인 시스템)에는 금융 아키텍처를 크게 입출금 등과 같이 거래를 처리하는 계정계(BTL; Business Transaction Layer), 금융 정보를 분석하는 정보계(BIL; Business Intelligence Layer)로 구분하였다. 우리나라의 금융시스템은 2000년 이후 괄목한 성장을 보이고 있다. 한국은행의 '금융권 차세대시스템 구축 이후 금융 IT발전 전략' 보고서에 따르면, 95년도부터 진행된 금융 차세대 시스템 구축 이후 현재는 포스트 차세대에 들어섰으며, 계정계 시스템의 경우 세계적인 수준이라고 평가되고 있다.



(\* 주 : 한국은행의 '금융권 차세대시스템 구축 이후 금융 IT 발전 전략)

(그림 3-4) 현행 차세대 시스템 아키텍처

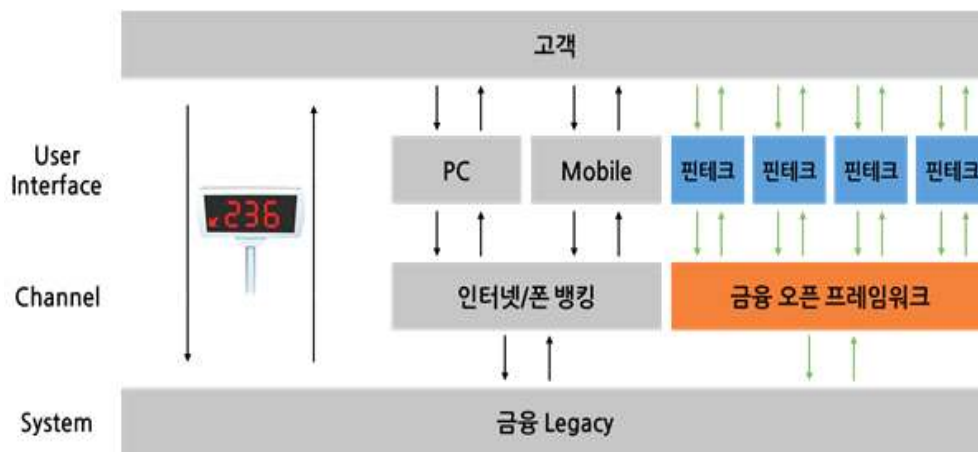
차세대 시스템을 통해 실시간 온라인 처리가 가능해졌지만 아래와 같은 이유로 지속적인 금융서비스의 변화를 요구하고 있고, 핀테크라는 용어로 이를 해결하려는 노력(4세대, 포스트 차세대 시스템)이 나타나고 있다.

- o 다양한 융복합 금융상품 서비스에 대한 비즈니스 모델 요구
- o 현재 운영 중인 시스템에 신규 서비스 적용의 어려움
- o 새로운 ICT 기술로 인해 기존에 불가능 했던 문제들의 해결\

## 2. 핀테크 아키텍처

금융서비스뿐만 아니고 대부분의 아키텍처 설계에는 강건성(모델에 여러 가지 변화를 가해도 모델이 계속 비슷한 결과를 산출하는지 나타내는 정도)이 강조된다. 강건성이 낮은 아키텍처의 수정은 오류가 없던 시스템에 회귀 결함을 발생시킬 수 있기 때문에 외부 요인으로 인한 변경에

도 기존에 구성된 아키텍처에는 영향이 없도록 설계해야 한다. 테크는 내부 뿐만 아니라 외부에서 만들어지는 다양한 금융서비스를 수시로 추가할 수 있도록 설계하는 것이 중요하다. 높은 강건성을 위해 기존 금융 시스템에 영향이 없는 독립적이고 확장성이 좋은 핀테크 아키텍처 구성이 필요하다.



(\* 주 : NIPA SW공학센터 웹진)

(그림 3-5) 핀테크 아키텍처 구성

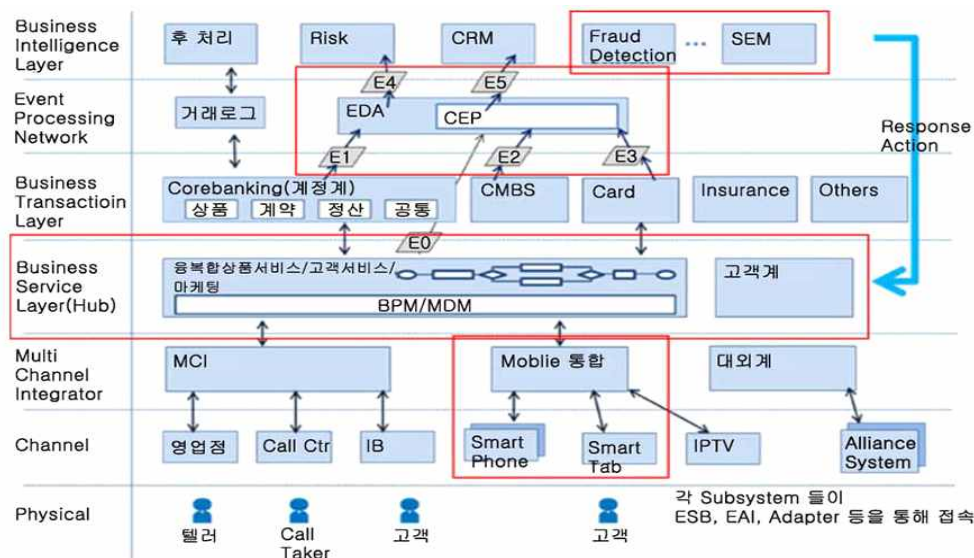
핀테크 아키텍처 구성을 비교해 보면, 핀테크 서비스를 위한 UI와 기존 금융시스템과 핀테크 사이에 프레임워크가 추가된 것을 볼 수 있다. 중요 포인트는 아래와 같다.

- o 외부 핀테크 서비스를 받아들여야 한다.
- o 오픈 프레임워크가 필요하다.

핀테크 서비스는 다양한 외부업체의 서비스를 활용해야 하기 때문에 이 부분이 아키텍처에 반드시 포함되어야 하고, 기존 금융시스템에 영향을 줘서는 안되기 때문에 핀테크 서비스와 기존 금융시스템을 이어주는 프레임워크가 필요하다. 프레임워크는 외부 핀테크 업체도 구성을 알아

야 하기 때문에 오픈 프레임워크의 연결자(Broker)역할을 한다.

한국은행에서 제시하는 포스트 금융시스템의 아키텍처를 살펴보면, 외부 비즈니스까지 받아들여 처리되도록 설계되어 있다. 포스트 금융시스템 모델의 핵심은 핀테크와 마찬가지로 ICT 기술 기반의 비즈니스 융합이다. 기존 시스템의 변경을 최소화하면서 다양한 금융상품을 만들어 내고 금융 데이터 분석을 통해 새로운 가치 서비스를 창출하는 것이다.



(\* 주 : 한국은행의 '금융권 차세대시스템 구축 이후 금융 IT 발전 전략)

(그림 3-6) 포스트 금융시스템의 아키텍처 구성

핀테크는 은행과 같은 금융기관 주도로 운용되는 것이 사실이다. 기존 금융시스템은 대부분 B2C 대상이었지만 핀테크 업체까지 대상이 확대되기 때문에 핀테크 금융시스템은 B2C와 B2B를 모두 고려해야 한다. B2B가 추가되면서 부당인출 등 금융 사고에 대한 위험이 존재하고 고객정보가 외부에서 관리되는 등의 정보 보호 이슈 발생 할 수 있다. 이러한 이슈들은 핀테크 관련 규제가 많아지는 가장 큰 요인이 되고 있다.

### 3. 핀테크 보안기술의 원칙

핀테크는 오픈 플랫폼 활용을 위한 아키텍처 정의와 함께 보안이 필수 요소다. 특히, 시스템 간의 연계 보안과 개인정보 확인을 위한 인증보안이 중요한 부분이다. 핀테크에서는 다양한 보안 기능을 추가하고 있지만 대부분은 새로 만드는 것이 아니라 기존의 보안기술을 활용하고 있다. 이러한 기술의 특징과 장단점을 잘 파악하여 핀테크에 연동되어야 한다. 핀테크는 다른 서비스에 비해 정책적인 제약이 많기 때문에, 보안에 대해 기술적인 접근과 함께 비즈니스적인 접근을 병행해야 기술과 정책을 조화롭게 구성할 수 있다. 핀테크 보안기술은 하드웨어적인 요소가 많기 때문에 이를 소프트웨어적으로 변환할 수 있는 방안이 필요하다.

#### 1) 핀테크에서 요구되는 세가지 보안요소

완벽한 보안은 없다. 다만, “정보의 가치“보다 “정보를 해킹하는 비용“이 더 발생하도록 보안을 구축하는 것이 보안의 최종 목적이다. 금융보안의 3요소는 기밀성, 가용성, 무결성이다. 철저한 보안을 위해서는 기밀성과 무결성을 높이면 되지만, 이로 인해 가용성은 떨어지게 된다. 보안요소에 중요도를 적절히 배분하는 것이 적정 보안을 유지하는 방법이다.

[표 3-4] 금융 보안의 3요소

구분	내용
기밀성	- 정보가 노출되는 것 방지 - 기밀성을 높이기 위해서 정보를 암호화
가용성	- 권한이 있는 사람은 언제, 어디서든 정보접근 - 가용성을 높이기 위해서 권한을 세분화
무결성	- 정보의 변조나 파괴를 방지 - 무결성을 높이기 위해 권한 부여 강화

핀테크 보안은 효율성, 편의성, 안전성 등 3가지 요소이다. 불과 몇 년

전만해도 금융은 우리나라만 생각하면 되었지만 금융서비스가 온라인으로 옮겨가면서 글로벌 표준에 대한 인식이 확대되었다.

기존의 금융서비스는 일관된 서비스만 제공하였지만 다양한 디바이스, 시스템과 연계해야 하는 핀테크는 비즈니스 흐름에 따라 소프트웨어를 구성해야 한다. 보안도 비즈니스 관점으로 접근하여 시스템의 효율성을 높일 필요가 있다. 핀테크는 이용자가 다양해지기 때문에 인증에 대한 보안이 강화되어야 한다. 하지만, 최종사용자(End User)의 디바이스는 모바일처럼 이동성이 강할 수도 있어 편의성도 고려해야 한다. 마지막으로, 핀테크의 보안은 우리나라뿐만 아니라 다양한 나라에서 사용될 수 있도록 글로벌 표준에 따라야 한다. 우리나라에서 거의 유일하게 사용되는 ActiveX나 공인인증서에 대하여 검토해야 하는 것도 이 때문이다. 핀테크는 ICT기술을 기반으로 하기 때문에 ICT기술에서 정의하는 보안 내에서 정의되어야 하고, 금융서비스 기반이기 때문에 금융서비스 보안 내에서 정의되어야 한다.

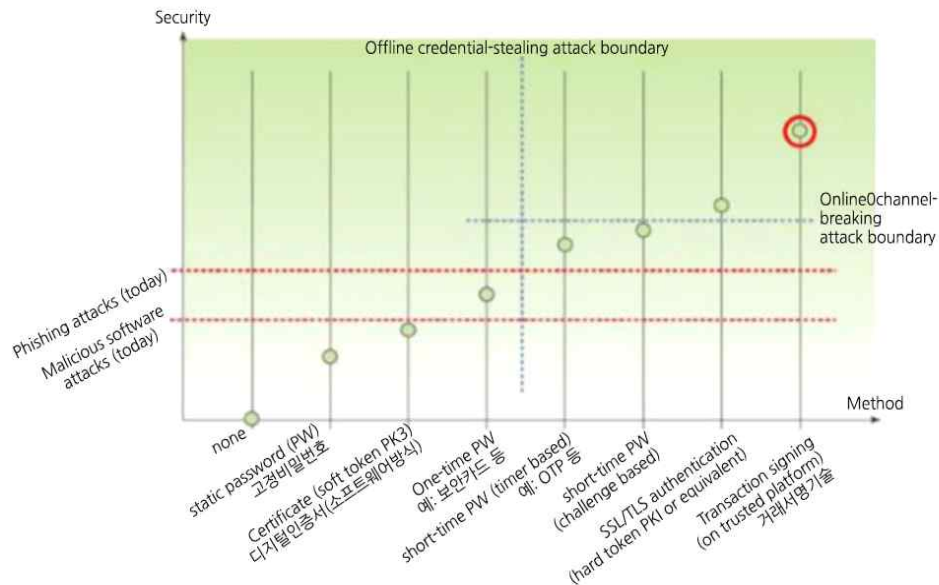
핀테크에서 사용되는 보안기술은 사용자 인증, 온라인 피싱 방지, FDS(부정거래탐지), 빅데이터 프라이버시 등이 있다. 핀테크에서는 사용자 편의성 제공과 동시에 안전한 결제를 위한 기술이 필요하다. 결제서비스는 각각의 사용자 인증 방식과 그에 따른 결제 프로토콜이 있다. 일반적으로 많이 사용되는 ID/PW 방식은 별도의 하드웨어가 필요하지 않지만 사용자들이 ID/PW를 항상 기억해야 하는 문제점이 있다. 그래서 사용자가 가진 신체나 행동의 생체 기반 인증 방식이 주목 받고 있다. 사용자가 인증에 필요한 토큰을 소유하거나 기억할 필요가 없기 때문에 사용자 편의성을 제공하고 사용자의 고유한 정보를 사용하기 때문에 보안성도 강하다. 보안에 관한 자세한 내용은 4장, 5장에서 설명하였다.

#### 4. 핀테크 인증기술

다양한 보안 위협에 대응하고 올바른 정보 제공을 위해 본인 인증이



절대적으로 필요하다. 가장 많이 사용되는 인증 방식은 계정 (ID/Password) 방식이지만 인증정보 유출 위험이 매우 높고 해킹 위험에도 많은 위험이 노출되어 있다. 최근에는 본인 확인과 해킹, 권한 탈취 방지를 포함한 새로운 인증 방식이 도입되고 있다.



(\* 주 : NIPA SW공학센터 웹진)

(그림 3-7) 본인 인증 방법 별 안정성 비교(자료:IEEE)

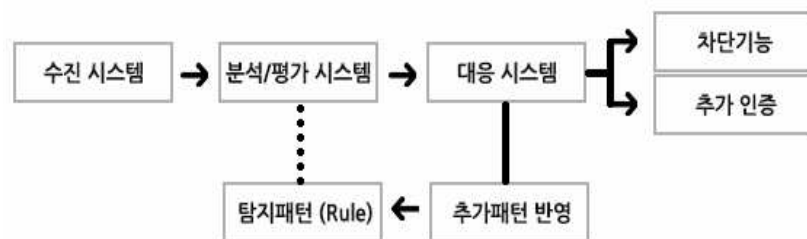
본인 인증 방안을 살펴보면, 고정 비밀번호, 디지털 인증서, 보안카드와 같이 최근까지 우리나라에서 많이 사용되던 본인 인증 방식은 보안성이 다소 낮은 것으로 나타나있다. SSL이나 거래서명기술은 보안성이 다소 높은 것으로 나타나 있으나 완전히 안전하다고 장담할 수는 없다. 핀테크를 위해서는 보안 수준이 매우 높은 인증 방식을 적용해야 한다.

## (2) 데이터 보호

금융서비스에서 사용되는 데이터들은 가급적 본인도 볼 수 없는 형태로 감춰두어야 한다. 입출력되는 결제 비밀번호, 계좌번호 등과 거래내역에 대한 무결성, 인증기술과의 연동시에 발생하는 데이터들은 모두 보호되어야 한다. 최근에는 모바일 AP를 일반 영역과 보안 영역으로 구분하는 TEE(Trust Execution Environment)나 토큰화(Tokenization)등이 데이터 보호 역할을 해준다. 토큰화는 결제 시 가상의 카드번호를 부여하여 서비스하는 방식이다. 매 거래 시마다 1회용 검증 값으로 거래를 검증하기 때문에 해킹의 위협을 낮출 수 있다. 삼성페이, 애플페이 등의 서비스가 토큰화 방식에 해당한다. TEE방식은 제4장 보안에서 자세히 설명하고자 한다.

### (3) 모니터링

기존 금융서비스는 거래내역이 완료되면 보안검증은 중단된다. 핀테크의 경우 수많은 거래내역들이 쌓이기 때문에, 이를 분석하여 이상금융거래를 판별할 수 있다. 모니터링은 정보 수집, 분석/탐지, 대응, 관리/운영의 4가지로 구분된다. 금융서비스를 위한 보안이 아니라 금융거래 운영을 위한 보안이라고 할 수 있다.



(그림 3-8) 금융거래 내역 모니터링 프로세스

거래내역을 수집한 후 이상 거래에 대한 패턴이 있는지 확인하고 이상이 감지된 경우 대응 시스템에 알리게 된다. 이 때, 사용되는 탐지 패턴

의 정확도와 범위에 따라 모니터링의 효율성이 나타나게 된다. IC Tagging, 생체 인식 등을 활용하면서 사용자 편의성은 지속적으로 개선되고, TEE, 토큰화 등과 같은 데이터 보호 기술의 향상으로 안정성은 더 높아지고 있다. 이러한 데이터를 관리, 운영하면서 금융서비스의 효율성은 높아지는 추세라고 보인다. 기존 금융서비스의 ICT기술은 인증 중심이었지만 핀테크에서는 돈이 거래되는 분야에 많이 몰려있다. 핀테크의 발달로 인해 인증 분야는 점점 간소화되고 데이터를 보호하거나 관리, 운영하는 분야로 트렌드가 변하고 있다.

## 5. 핀테크 서비스 품질관리

핀테크는 여러 가지의 금융서비스를 미리 등록한 핀테크 서비스로 통합하여 사용하는 것을 기본이다. 이러한 이유로 핀테크는 다양한 금융서비스를 연결하는 정보기술과 이에 따른 높은 품질의 아키텍처, 보안 등도 함께 요구하고 있다. 이러한 기술들 중에 이번 회에서는 핀테크 시장에서 요구하는 품질을 확보하기 위해 아키텍처와 보안 관점의 품질확보 방안에 대하여 설명하였다.

### (1) FinTech Architecture

핀테크는 새롭게 만들어진 서비스가 아니라 기존의 금융서비스에 정보기술을 접목한 금융서비스의 변형된 형태라고 할 수 있다. 따라서 비즈니스 아키텍처를 수립할 때, 기존 금융서비스에 대한 이해가 절대적으로 필요하다. 인터넷 전문은행의 비즈니스 아키텍처를 수립하기 전에 기존 서비스가 어떠한 형태로 변화가 있을 것인가를 보고자 한다.



(\* 주 : NIPA SW공학센터 웹진)

(그림 3-9) 인터넷 전문은행의 변화 형태

전통적인 은행은 물론 인터넷뱅킹도 있지만 전통적으로 콜센터나 영업점 단위로 서비스를 제공하고 저축, 대출 등과 같은 상품을 취급한다. 그리고 다양한 사람들을 대상으로 마케팅을 해야 한다. 이에 반해 인터넷 전문은행은 온라인으로 다양한 지급결제를 취급하고 빅데이터 분석을 통한 개인들에게 마케팅을 하게 된다. 여기서 중요한 점은 서비스가 어떤 것이 있다는 것을 알고자 하는 것이 아니라 어떠한 차이가 있는 지를 살펴보는 것이다. 온라인을 통해 서비스를 하도록 하는 것, 지급결제에 대한 상품이 필요하다는 것, 그리고 개인들을 대상으로 마케팅을 할 수 있도록 준비해야 한다는 것이다. 금융서비스는 가장 안정적으로 운영되는 서비스 중 하나이다. 핀테크 서비스를 도입하여 달라지는 부분에 대해서 안정적인 품질이 확보될 수 있어야 한다. 이렇게 변화된 비즈니스를 바탕으로 애플리케이션 아키텍처를 수립하는 원칙을 나타내었다.

고객채널	Real Time Event Processing Service		Data Warehouse	
	Web	마케팅규칙 FDS규칙	DW	Data Mart
플랫폼채널	Customer Data Service		Data Analytics	
	Online	고객정보 상품팩토리 마케팅서비스 로그관리	고객평점분석	고객분석
대외채널	Customer Account Service		신용평점분석	상품분석
	Offline	자산관리 가계부 뉴스레터	고객평판분석	FDS분석
한국은행 금융결제원 신용카드 ...	Core Banking		Compliance	
	계약	여신심사	AML	FDS
	정산	계약심사	VOC	감사
	회계	지급대행	보안	
			Data Detection & Visualization	
			데이터크롤링	데이터시각화

(\* 주 : SK C&C의 인터넷 전문은행 설명회)

(그림 3-10) 인터넷 전문은행의 Application Architecture 수립 원칙(예)

기존 금융서비스에 일반적으로 나타나지 않았던 실시간 이벤트 프로세싱 서비스, 데이터 비주얼라이제이션 등이 포함된 것을 확인할 수 있다. 이처럼 기존의 금융서비스가 변하지 않는 것은 이전 수준으로 품질을 확보하고, 새롭게 추가된 것들에 대해서는 항목에 따라 체계적인 품질 확보 방안을 수립해야 한다. 이렇게 변화된 부분을 단계적으로 수립하면 품질 확보에 어려움이 없을 것이다.

## 6. 핀테크와 클라우드

핀테크 플랫폼은 클라우드 컴퓨팅을 기반으로 형성되어 있다. 핀테크 산업 및 응용 ICT 서비스에 필요한 기술에는 클라우드 컴퓨팅 기술에서 출발하여 클라우드 서비스 브로커리지(클라우드 브로커), 빅데이터 기술, 정보보안/프라이버시 보호기술, 데이터 분석 및 분산처리 운영기술, 안정적인 서비스 운영 아키텍처, 블록체인에서 출발한 비트코인, 그리고 전

자화폐를 이용한 플랫폼 서비스 등의 기술이 있어야 한다. 미래의 화폐가 없는 사회를 구현하기 위하여서는 클라우드 기반 핀테크 플랫폼의 다양한 단말 환경에서 표준화된 클라우드를 통해 안전하게 금융거래를 할 수 있어야 한다.

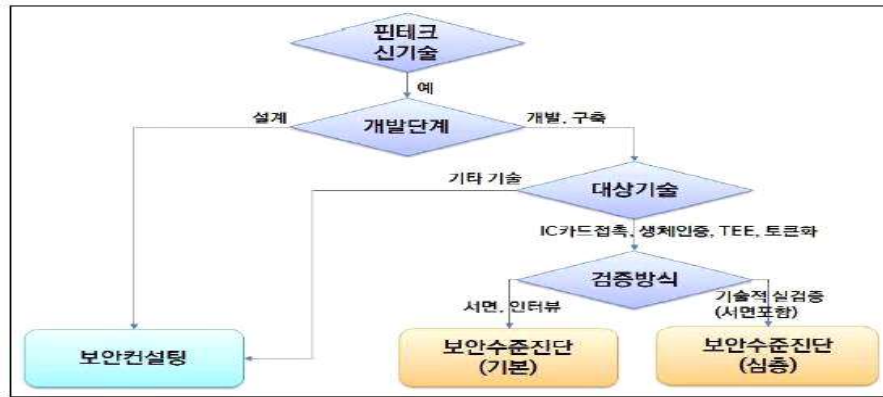


(그림 3-11) 클라우드 기반 플랫폼

핀테크 산업 또한 클라우드 기반으로 구성된 플랫폼을 중심으로 서비스가 제공되어야 한다. 사용자들의 금융거래정보, 행동 및 취미 관련 정보, 그 외 위치기반 정보, 생활정보들이 모두 클라우드 기반에서 만들어져 사용자 동의하에 공유되어야 클라우드 사용을 극대화할 수 있다. 해외의 글로벌 금융기업들은 이미 클라우드 기반 핀테크 플랫폼을 만들어 외부 IT업체의 서비스가 연동될 수 있도록 API를 제공하고 있다. 이런 방법을 통해 은행내 금융거래 기반의 정보플랫폼이 외부 IT업체들의 플랫폼과 연결돼 사용자들이 원하는 최적화된 서비스를 받을 수 있도록 하고 있다.

핀테크 서비스기술은 현재는 특별한 SW기술이 아니라, 기존 IT서비스들의 조합이다. 미래에는 인공지능과 결합하여 개인 행동패턴에 따른 위치기반 O2O 핀테크 기술의 핵심 Big Analytics Big Fast 개인화행위 개인화추천 위치기반 선호도기반 송금 결제 대출 외상 Hadoop, Spark, Storm

CEP 통계, 머신러닝, 딥러닝, 복잡계등 다양한 알고리즘으로 분석하여 실시간으로 온/ 오프라인 서비스를 제공할 수 있는 시스템간의 연계가 있어야 한다.



( \*: 금융보안원)

(그림 3-12) 핀테크 보안기술 개념도

금융정보의 보안·인증은 핀테크 기술의 전부라고 해도 과언이 아니다. 데이터양과 정보사회의 복잡성이 증가하면서, 어떤 보안기술도 100% 안전을 보증할 수 없다. 보안·인증 기술은 날로 발전해 가고 있으며 바이오메트릭스(음성, 지문, 생체, 얼굴 인식) 인증 방식 등 여러 기술이 발전되고 있다. 최근에는 인공지능을 이용한 빅데이터 분석 및 예측 기반의 보안 기술로 진화하고 있다.

국내외 핀테크 기술 전반에 관한 연구를 통하여 디지털 화폐 기반의 핀테크 플랫폼 구축에 관한 원천기술, 보안 및 빅데이터 기술들을 확보하고 핀테크 플랫폼을 제공하여 실제 현장에 적용함으로써 핀테크산업의 저변을 확대하고 금융산업 전반의 효율성 및 글로벌 경쟁력을 높일 것으로 기대된다.

다음 절부터는 핀테크 관련 기술 중에서 클라우드 컴퓨팅 서비스 기술, 클라우드 서비스 브로커리지(CSB), 블록체인과 비트코인기술 등 주요 기술들에 대하여 설명하였다.

## 제 2 절 클라우드 컴퓨팅 서비스 기술

### 1. 클라우드 컴퓨팅 서비스 개념

클라우드 컴퓨팅은 어느 날 갑자기 나타난 개념은 아니며, 이미 전부터 클라우드 컴퓨팅 개념은 IT 업계에 보편화 되어 있었던 것이다. 이 클라우드 컴퓨팅은 이전부터 있었던 그리드 컴퓨팅이나 유틸리티 컴퓨팅 등에서 유사한 기술 개념이다. 먼저 그리드 컴퓨팅은 인터넷에 흩어져 있는 컴퓨팅 자원을 연결해 가상의 슈퍼컴퓨터와 함께 활용하는 모델이다. 주로 수학, 과학, 물리 등 학술 분야에서 쓰이고 있다. 그리드 컴퓨팅은 분산된 IT자원을 통합해 사용한다는 점에서 클라우드 컴퓨팅의 분산 컴퓨팅 환경과 비슷하다. 그러나 그리드 컴퓨팅은 인터넷으로 서버와 컴퓨터 등 남은 컴퓨팅 자원을 활용하는 개념인데 비해, 클라우드 컴퓨팅은 개별 서비스 사업자의 가상화된 서버 네트워크를 이용한다는 점에서 차이가 난다. 곧 그리드가 인터넷의 모든 IT자원을 연결하는 그물망을 의미한다면, 클라우드는 사업 주체인 서비스 제공자가 제공하는 사유화된 컴퓨팅(서버) 네트워크를 가리킨다고 볼 수 있다.



[표 3-5] 클라우드 컴퓨팅과 다른 컴퓨팅 방식의 비교

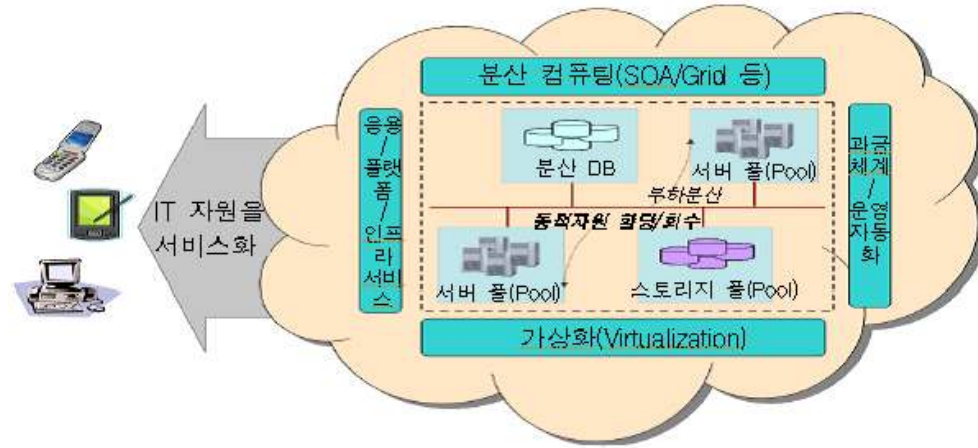
구 분	주요 개념	클라우드 컴퓨팅과의 관계
그리드 컴퓨팅 (Grid Computing)	많은 IT자원을 필요로 하는 작업을 위해 인터넷 상의 분산된 다양한 자원들을 공유하여 가상의 슈퍼컴퓨터처럼 활용하는 방식	그리드 컴퓨팅이 인터넷 상의 모든 컴퓨팅 자원을 통합해 쓰는데 반해, 클라우드 컴퓨팅은 서비스 제공 사업자의 사유 서버 네트워크를 빌려서 활용
유틸리티 컴퓨팅 (Utility Computing)	서버·스토리지 등 컴퓨팅 자원을 보유하지 않은 채 가스나 전기처럼 사용량에 따라 과금되는 방식	클라우드 컴퓨팅의 과금 방식은 유틸리티 컴퓨팅과 동일
서버기반 컴퓨팅 (Server Base Computing)	서버에 응용 소프트웨어와 데이터를 저장해 두고 필요할 때마다 접속해서 쓰는 방식. 모든 작업을 서버가 처리	클라우드 컴퓨팅은 서비스 제공자의 가상화된 서버를 이용하고, 서버기반 컴퓨팅은 특정 기업내 서버를 이용한다는 차원에서 구분되는 개념이었지만, 서버기반 컴퓨팅이 발전하면서 구분이 모호해짐
네트워크 컴퓨팅 (Network Computing)	서버기반 컴퓨팅처럼 응용 소프트웨어를 서버에 두지만, 작동은 이용자 컴퓨터의 자원을 이용해 수행하는 방식	클라우드 컴퓨팅은 이용자 컴퓨터가 아니라 클라우드 상의 IT자원을 사용

유틸리티 컴퓨팅은 사용자가 컴퓨팅 자원을 전기나 수도처럼 필요할 때마다 연결해 사용하고, 사용량에 따라 대가를 지급하는 과금 모형이다. 클라우드 컴퓨팅 역시 사용량을 기준으로 비용을 지불한다는 측면에서 유틸리티 컴퓨팅의 요소를 담고 있다.

하지만 유틸리티 컴퓨팅이 단순히 컴퓨팅 지원 과금방식을 담고 있는데 비해, 클라우드 컴퓨팅은 그 과금 방식을 포함해 좀더 다양한 특징을 지닌다. 따라서 클라우드 컴퓨팅은 그리드의 분산 컴퓨팅 모형과 유틸리티 컴퓨팅의 과금 모형을 채택하는 컴퓨팅 개념으로 볼 수 있다.

이와 함께 서버기반 컴퓨팅은 모든 처리가 100% 서버에서 이루어지고, 사용자의 단말기는 단순히 입출력만을 처리하는 썬 클라이언트(Thin Client)<sup>2)</sup> 역할을 한

다. 클라우드 컴퓨팅은 사양이 낮은 단말기로도 서버에서 처리되는 높은 수준의 서비스를 이용할 수 있다는 점에서 서버기반 컴퓨팅이 가지는 특성을 포함하고 있다.



(그림 3-13) 클라우드 컴퓨팅 개념도

그러나 서버기반 컴퓨팅은 사용자를 위한 물리적인 서버를 제공하고, 이것에 대한 활용 권한도 사용자가 가지고 있지만, 클라우드 컴퓨팅에서 사용자는 가상화된 서버 네트워크로 서비스를 받을 뿐 물적인 서버에 대한 정보나 권한을 가지지 못한다. 따라서 컴퓨팅 용량이 더 필요할 경우 서버기반 컴퓨팅에서는 물리적인 서버를 추가해야 하지만, 클라우드 컴퓨팅에서 더 많은 사용량에 대한 대가를 서비스 사업자에게 지불하면 된다.

서버에 응용 소프트웨어를 저장해 두고 사용하는 네트워크 컴퓨팅 역시 클라우드 컴퓨팅과 개념이 비슷하다. 하지만 네트워크 컴퓨팅은 서버에 있는 응용 소프트웨어를 다운로드해 사용자의 단말기에서 실행하기 때문에 개별 컴퓨팅 자원을 상당부분 사용한다는 점에서 차이가 난다. 또 네트워크 컴퓨팅에서 응용 소프트웨어

- 2) 쉘 클라이언트(Thin Client) : 기존 컴퓨터가 각종 응용 소프트웨어를 내장하고 데이터 처리가치 했던 것과 반대로 중앙 서버에 있는 여러 소프트웨어 및 자원들을 사용자에게 보여주는 인터페이스로 기능을 한정시킨 단말기를 의미한다. 단말기 자체에는 연산을 위한 중앙 처리장치나 저장을 위한 하드디스크 등이 거의 탑재되지 않거나 최소화 되어

어나 문서는 단일 기업의 서버에 존재하기 때문에 기업 네트워크에서 한정적으로 접근할 수 있지만, 클라우드 컴퓨팅은 그보다 훨씬 큰 개념이다. 여러 기업, 여러 서버, 여러 네트워크를 포괄한다. 또 네트워크 컴퓨팅과 달리 클라우드 서비스와 스토리지는 인터넷으로 연결되어 있으면 세계 어디서나 접근이 가능하다. 일각에서는 서비스로서의 소프트웨어(SaaS : Software As a Service)를 클라우드 컴퓨팅의 전부로 오해하기도 하지만, 클라우드 컴퓨팅은 SaaS를 가능하게 하는 기반 컴퓨팅 환경이자, SaaS를 포함한 광범위한 IT자원에 대한 아웃소싱 모형이다. SaaS는 클라우드 컴퓨팅이 태생하기 이전부터 서비스되고 있었지만, 현재는 클라우드 컴퓨팅 서비스 중 하나로 분류된다.

최근 기업들이 비용절감을 위한 전략적 방안 중 하나로 클라우드 컴퓨팅에 관심을 보이기 시작하면서 시장의 이슈로 부각되었으며, 클라우드 컴퓨팅은 넓은 의미로 빌려 쓰는 비즈니스의 한 형태로 볼 수 있다. 즉, 하드웨어, 소프트웨어, 네트워크 등 각종 IT 자원을 인터넷을 통해 전기나 수도처럼 빌려 쓰는 기술 및 서비스를 의미한다.

## 2. 클라우드 컴퓨팅의 정의

클라우드 컴퓨팅이란 인터넷 기술을 활용하여 “가상화된 IT 자원을 서비스”로 제공하는 컴퓨팅으로 사용자는 IT 자원(소프트웨어, 스토리지, 서버, 네트워크)을 필요한 만큼 빌려서 사용하고, 서비스 부하에 따라서 지원을 받으며, 사용한 만큼 비용을 지불하는 방식이다.

세계적인 IT 리서치 그룹인 가트너는 클라우드 컴퓨팅을 ‘인터넷 기술을 활용하여 다수의 고객들에게 높은 수준의 확장성을 가진 IT자원들을 서비스로 제공하는 컴퓨팅’으로 설명하고 있다. 또 시장조사기관 포레스터 리서치(Forrester Research)는 “표준화된 IT기반 기능들이 인터넷 프로토콜(IP, 네트워크 간 데이터 전송을 가능하게 하는 규약)로 제공되고, 언제나 접근이 허용되며, 수요가 변함에 따라 가변적이고, 사용량이나 광고에 따라 과금 모형을 달리하고 있다”며 클라우드 컴퓨팅을 소개하고 있다.

[표 3-6] 다양한 클라우드 컴퓨팅의 정의

기관명	정 의
가트너 <sup>3)</sup>	인터넷 기술을 활용해 많은 고객에게 수준 높은 확장성을 가진 자원들을 서비스로 제공하는 컴퓨팅의 한 형태
포레스터 리서치 <sup>4)</sup>	표준화된 IT기반 기능들이 IP로 제공되고, 언제나 접근이 허용되며, 수요변화에 따라 가변적이다. 사용량이나 광고를 기반으로 비용을 지불하고, 웹 또는 프로그램적인 인터페이스를 제공하는 형태
위키피디아 <sup>5)</sup>	인터넷에 기반을 두고 개발하는 것으로 컴퓨터 기술의 활용을 의미한다. 인터넷으로 자원들이 제공되는 형태
IBM	웹 기반 응용 소프트웨어를 활용해 대용량 데이터베이스를 인터넷 가상공간에서 분산 처리하고, 이 데이터를 컴퓨터나 휴대전화, PDA 등 다양한 단말기에서 불러오거나 가공할 수 있게 하는 환경

다음 표에서 보여 주는 사례는 다양한 기업에서 클라우드 컴퓨팅 기술을 바탕으로 다양한 서비스를 제공하는 CSB로 발전해나가는 것이 산업적으로 얼마나 중요한 일인가를 보여준다.

클라우드(CLOUD)라는 명칭은 작업에 필요한 컴퓨팅 서비스를 구름 저편으로부터 받아와서 작업한 문서를 S/W와 함께 다시 구름 저편으로 보내어 저장한다는 의미에서 지어졌다. 사실 이러한 개념은 새로운 것이 아니다. 이미 1990년대 중반 오라클, IBM, 애플을 포함한 5개 IT산업 거대기업들이 사업화하려고 했던 NC(네

3) 가트너 : 가트너(Gartner, Inc.)는 IT분야의 리서치 및 자문 기업이다. 본사는 미국 코네티컷 주 스탠퍼드에 위치해 있다. 2001년까지 가트너 그룹(The Gartner Group)으로 불렸다. 가트너의 고객은 대기업 및 정부 기관, IT기업, 투자 기업 등 다양하다. 1979년에 설립되어 세계 80개국에 4,400명 이상의 종업원을 거느리고 있으며, 이 중 1,200명이 연구 개발직 인원이다.

4) 포레스터리서치(Forester research) : 세계적인 미국의 IT시장조사 기관으로 마케팅 및 전략, 기술 산업, 비즈니스데이터를 중심으로 기획연구를 하고 있다.

5) 위키피디아 : 위키란 공동으로 문서를 작성하고 사용자들이 내용을 추구할 수 있는 웹페이지의 모음을 가리킨다. 이런 위키의 특성을 활용한 백과사전이 바로 위키피디아이다. 위키피디아는 온라인 참여형 백과사전으로 누구나 참여하고 편집할 수 있는 것이 특징이다.

트위크 컴퓨팅) 개념과 대동소이하다. 그러나 당시에는 초고속인터넷 망은 고사하고 전화선을 통한 네트워크가 일반적이었던 점, 넷북, 스마트폰을 비롯한 다양한 단말기 보급이 보편화되지 않았다는 점, 주요 IT업체들이 관련 OS(운영체제) 및 애플리케이션의 보급에 미온적이었던 점 등으로 그야말로 ‘뜬 구름 잡는 이야기’로 여겨졌었다.

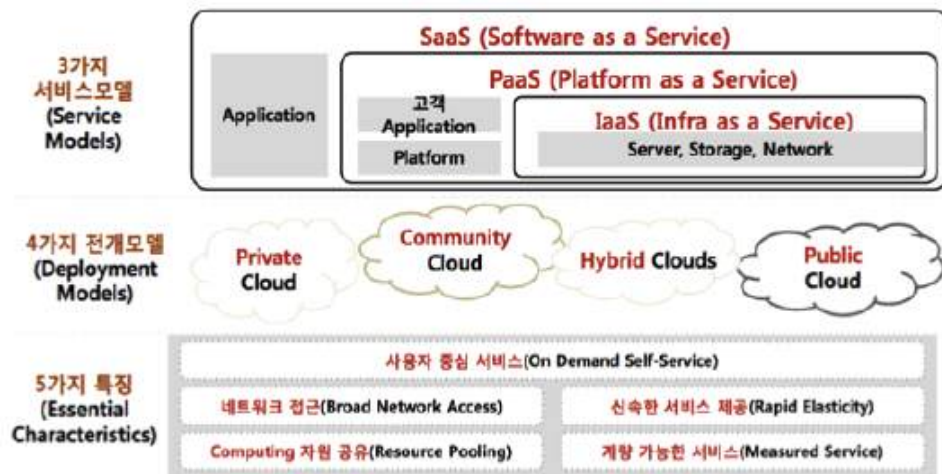
[표 3-7] 클라우드 컴퓨팅 전세계 시장 규모(단위 : 백만달러)

년도	클라우드 솔루션 시장	CSB 시장
2012	1,142	9,944
2013	1,501	12,897
2014	1,899	15,895
2015	2,402	19,966
2016	2,905	22,362
2017	3,689	25,046
성장률	<b>26.8%</b>	<b>18%</b>

이에 따라 NC는 참여 기업들의 노력에도 불구하고 상용화되지 못하고 사람들의 관심사에서 멀어졌다. 그러나 최근 들어 유무선 통신 네트워크의 확산 및 고속화, 세트 기기의 다양화, 무료 S/W의 보급 확대 등 IT인프라가 급속히 발전되면서 클라우드 컴퓨팅의 실현이 현실로 다가오고 있다.

### 3. 클라우드 컴퓨팅의 특성

클라우드 컴퓨팅의 특성은 NIST(National Institute of Standards and Technology)의 구분에 따라 다음과 같이 3가지 서비스 전달모델, 4가지 전개모델, 5가지 특징으로 나눌 수 있다.



Source : NIST(National Institute of Standards and Technology, 미국 국립표준기술원)의 Working Definition of Cloud Computing, Draft ver

Source : NIST

(그림 3-14) 클라우드 컴퓨팅의 특성(NIST의 구분)

NIST 정의에서는 클라우드 컴퓨팅의 5가지 본질적 특징을 기술하고 있다.

[표 3-8] 클라우드 컴퓨팅의 5가지 본질적 특징

특 성	내 용
신속한 서비스 제공 (Rapid Elasticity)	<ul style="list-style-type: none"> <li>- 필요에 따라 자원의 양을 증가 또는 감소시킬 수 있는 능력</li> <li>- 사용자에게 클라우드는 무한하게 보이고, 사용자는 그들의 필요에 따라 적거나 많은 컴퓨팅 파워를 구매 가능</li> </ul>
계량 가능한 서비스 (Measured Service)	<ul style="list-style-type: none"> <li>- 클라우드 서비스의 여러 요소들이 클라우드 제공자에 의해 모니터 되고 관리됨</li> <li>- 이것은 과금 정책, 접근 제어, 자원 최적화, 사용량 예측 등을 위해 필수</li> </ul>
사용자 중심 서비스 (On-Demand Self-Service)	<ul style="list-style-type: none"> <li>- 소비자가 클라우드 제공자와의 어떤 인간적인 상호작용(Human Interaction)없이 클라우드 서비스를 필요한 만큼 이용할 수 있다는 것을 의미</li> </ul>
네트워크 접속 (Broad Network Access)	<ul style="list-style-type: none"> <li>- 클라우드 제공자의 서비스가 클라이언트의 성능에 관계없이 표준절차에 의해 접근이 가능하며, 네트워크 상에서 언제든지 이용할 수 있다는 것을 의미</li> </ul>
컴퓨팅 자원 공유 (Resource Pooling)	<ul style="list-style-type: none"> <li>- 다중 소유모델(Multi-Tenant Model) 서비스를 의미</li> <li>- 클라우드 자원들은 소비자의 요청에 따라 할당되고 또 다른 소비자들에게 재 할당 됨</li> </ul>

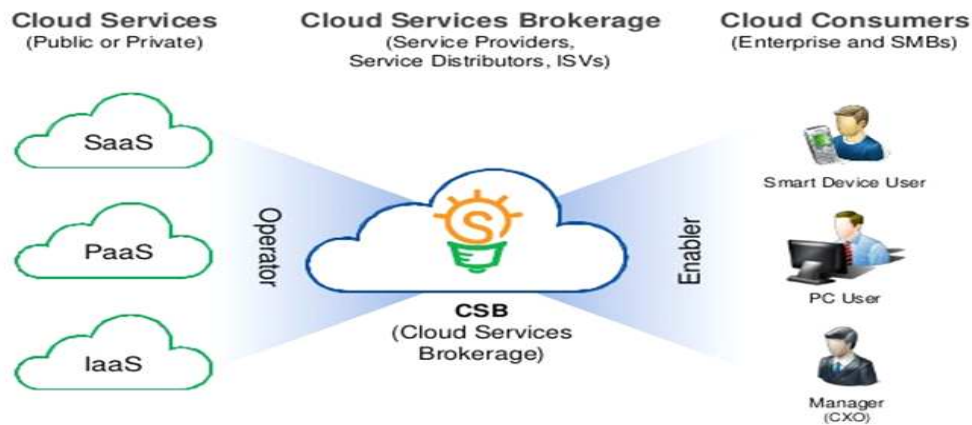
### 제 3 절 클라우드 서비스 브로커리지(CSB)

#### 1. 클라우드 서비스 브로커리지의 정의

클라우드 서비스 브로커리지(CSB : Cloud Service Brokerage)는 ‘09년 7월 가트너에서 처음 사용한 용어이며, 이후 NIST(미국 국가기술표준원)에서 이를 줄여서 Cloud Broker라고 부른다.

Cloud Broker는 클라우드 서비스 소비자와 제공자 사이에서 클라우드 서비스의 ‘부가가치’ 창출을 위해 소비자를 대신해 일하는 중개자를 말하며, 이는 소비자와 제공자간 관계 조율 및 소비자의 요구에 맞춰 최적의 클라우드 서비스를 제안하고 다양한 클라우드 서비스의 활용, 성능 관리, 전달 등을 담당한다.

예를 들면, 구글·아마존과 세일즈포스닷컴 그리고 KT, LG유플러스, SK텔레콤을 비롯해 삼성 SDS, LG CNS, SK C&C 등 기업이 ‘클라우드 서비스’를 제공한다면 이들 클라우드 서비스 제공기업과 사용 기업 사이에 CSB가 존재하면서 조율사 역할을 맡는 것이다.



(그림 3-15) 클라우드 서비스 브로커리지 개념도

## 2. 클라우드 서비스 브로커리지의 분류

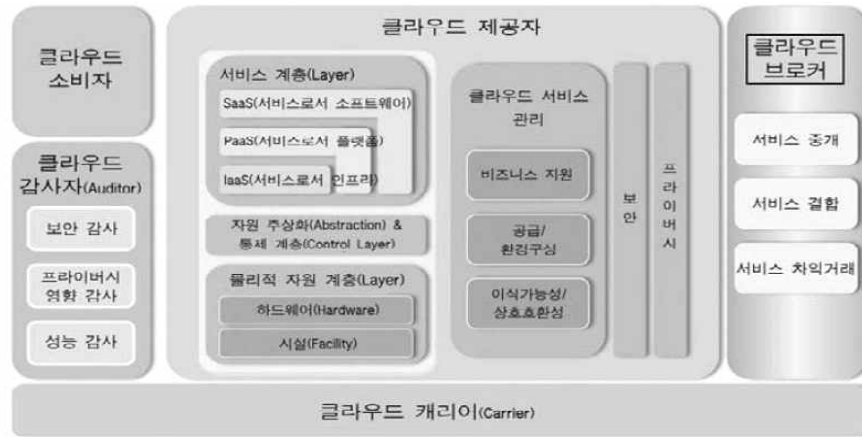
미국의 리서치 컨설팅 회사인 Gartner 사는 2009년 7월 가트너 보도자료에 클라우드 서비스 브로커리지를 다음 그림에서 보는 바와 같이 서비스 제공 측면에서 ①서비스 중개 ②서비스 결합 ③서비스 차이거래 등 세 가지 유형으로 분류하였다.

### 가. 서비스 중개 브로커(Service Intermediation Broker)

주요 클라우드 공급업체의 서비스에 서비스 부가가치를 붙여 서비스를 제공하는 형태로서 주로 특정 기능 개선을 통한 서비스 향상 및 클라우드 서비스 소비자를 위한 부가서비스를 제공한다.



AT&T, 버라이어존, 텔스트라, 버진 미디어 등의 클라우드 서비스 중개 브로커가 이 클라우드 서비스 판매 후 ID 접근 관리 도구와 같은 부가서비스를 판매하고 있다.



서비스 중개 브로커 (Service Intermediation Broker)	특정 기능 개선을 통한 서비스 향상 및 소비자를 위한 부가 서비스 제공 ※ 클라우드 서비스 판매 후 ID 접근관리 툴과 같은 부가서비스를 판매하는 사업자로, AT&T, 버라이어존, 텔스트라, 버진 미디어 등이 해당
서비스 결합 브로커 (Service Aggregation Broker)	다양한 서비스를 한 개 이상의 새로운 서비스로 통합해 제공 ※ 데이터 통합, 클라우드 소비자과 다수의 제공자간 데이터 이동 안전성 보장 등 제공
서비스 차이거래 브로커 (Service Arbitrage Broker)	서비스 결합 브로커와 유사하나, 결합되는 서비스가 고정되어 있지 않다는 차이점으로 인해 브로커에게 유연성 제공

(그림 3-16) 클라우드 서비스 브로커리지의 분류

국내의 경우 서비스 중개 브로커의 예를 들어보면, 소프트웨어 인 라이프가 “www.SiLApps.com”에서 GoogleApps를 기반으로 Google Data와 Google AppEngine 등의 핵심 기술을 활용하여 실시간 협업을 위한 최적의 환경과 시스템을 제공하는 Smart Working 솔루션을 제공하는 것과 Google Apps기반의 협업 솔루션인 DocosFlow를 서비스를 판매하고 있다.

나. 서비스 결합 브로커(Service Aggreation Broker)

여러 클라우드 서비스간의 데이터나 서비스 통합을 서비스 결합 브로커가 수행하는 것을 의미한다. 국내의 경우 2012년 1월 미래유키 컨설팅(대표 장동인)이 미국의 데이터 통합업체인 퍼베이시브 소프트웨어와 한국총판 계약을 체결하여 국내에서 처음으로 클라우드 데이터 통합 서비스를 제공하고 있다.

기업들이 클라우드 컴퓨팅을 도입할 때 가장 어려움을 많이 겪는 부분 중 하나가 바로 기존 사내 시스템과 클라우드 시스템 간 데이터 통합인데, 퍼베이시브는 퍼블릭·개인 클라우드 환경에서 기존 시스템과 데이터 통합을 전문적으로 하는 클라우드 데이터 통합의 선두 주자이다.

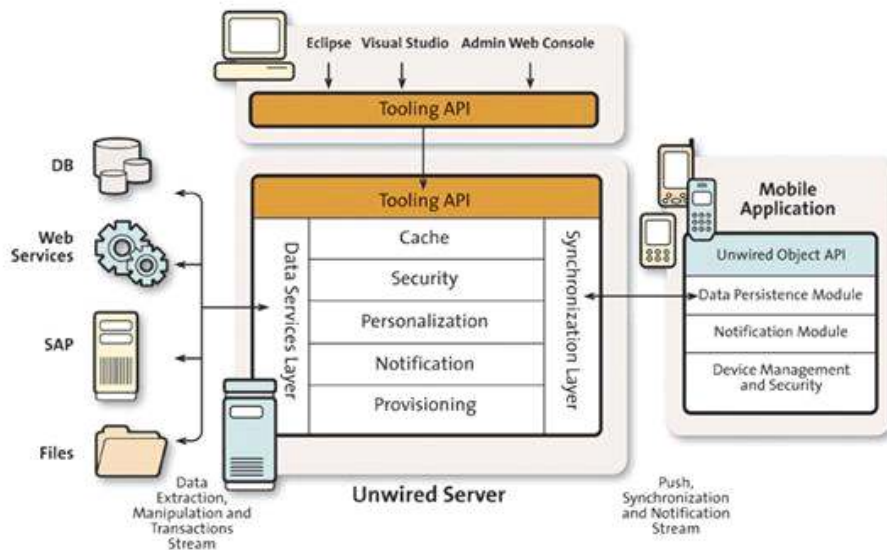
#### 다. 서비스 차익 거래 브로커(Service Arbitrage Broker)

여러 클라우드 서비스 공급자의 서비스 상품을 이들과 계약을 맺은 클라우드 서비스 브로커가 소비자에게 이들 상품을 제공하는 형식을 의미한다. 초기 클라우드 서비스 공급자가 클라우드 서비스 소비자에게 직접 하던 업무를 이들 중간에 서비스 차익 거래 브로커가 매개하는 형태이다. 이 경우 소비자는 클라우드 브로커가 지정하는 특정 클라우드 서비스의 이용을 전제로 하며, 소비자는 자사에 맞는 클라우드 서비스를 선택하는 것이다.

### 3. 클라우드 서비스 브로커리지 기술 전망

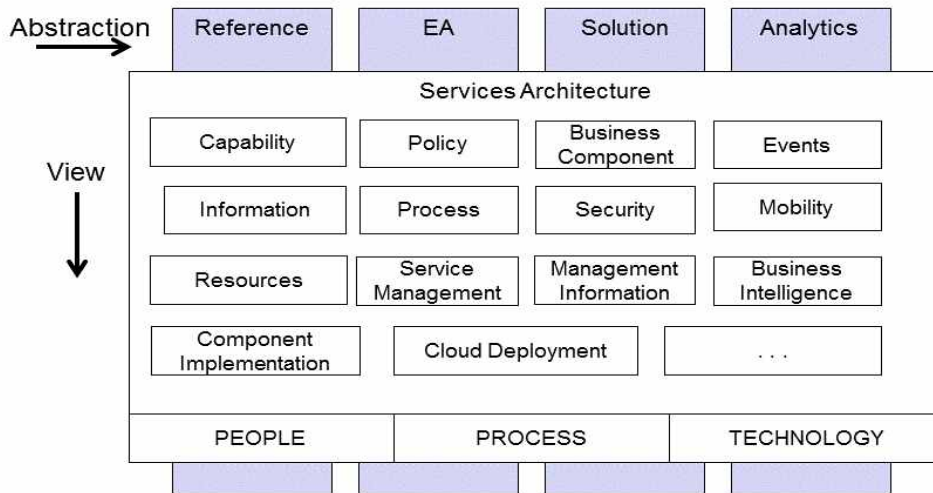
#### 가. 새로운 서비스 분야의 기술 개발

전세계적으로 많은 기업에서 클라우드 서비스를 활용하여 기업 및 조직의 경쟁력을 높이려는 노력이 많이 일어나고 있다.



(그림 3-17) 클라우드 서비스 활용 기업 경쟁력 제고

특히 클라우드 기반의 배포 및 관리와 인적 자원 관리 및 기술 관리, 프로세스 관리, 보안 및 모빌리티의 증가에 따른 데이터 보안 등을 확인할 필요가 있다. Gartner에서는 전 세계적으로 전문 인력 부족 및 전문 서비스 부족으로 CSB(Cloud Service Brokerage)가 더 중요해 지고 있으며, 클라우드 서비스의 20%가 CSB에 의하여 소비될 것으로 예측하고 있다.



(그림 3-18) 클라우드 서비스 아키텍처

CSB는 집적(Aggregation), 통합(Integration), 맞춤화(Customization)라는 3가지 역할을 하며, 집적(Aggregation)이란 최종 고객에게 여러 클라우드 서비스를 집적해 제공하는 것을 의미한다. 즉 재판매자(Reseller)의 역할이다. 또한, 통합(Integration)이란 중개자로 클라우드 서비스와 내부 시스템을 연결하는 역할이며, 맞춤화(Customization)란 고객의 필요에 맞게 클라우드 서비스를 조정하거나 클라우드에서 운용할 애플리케이션을 개발하는 것을 의미한다. CSB의 핵심 기술 개발을 통하여 클라우드 서비스의 활성화를 통하여 경제적, 산업적으로 클라우드 산업을 활성화 할 수 있다.

#### 나. 클라우드 서비스 브로커리지 기술의 기대효과

기업의 요구사항에 적합한 서비스 평가 기준이 미흡하고, 법규제 지원, 보안 및 호환성 문제, 클라우드 서비스 마다 다른 용어에 대한 이해와 기업의 비즈니스의 이해 등이 클라우드 서비스의 도입 장벽으로 작용하고 있다.

이러한 클라우드 서비스가 다양화·복잡화 되고 클라우드 위험에 대한 우려가 지속됨에 따라, 클라우드 서비스에 전문성을 보유한 CSB는 다음과 같은 기대효과를 가져올 수 있다.

- o 다양한 클라우드 서비스의 운영·통합·소비·확장 시 더 저렴하고 쉽고, 안전하고, 생산적인 서비스 제공을 통해 실질적인 사용자의 이익을 창출한다.

- o CSB는 전통적인 서비스뿐만 아니라, 다양한 클라우드 서비스 도입에 따라 발생하는 솔루션 자산관리, SLA 상호 의존성 관리, 컴플라이언스 관리, 보안 위험관리 등 복잡한 이슈의 해결 방안을 제시한다.

- o 특정 클라우드 서비스 공급업자에 대한 의존성을 예방한다.

- o 시스템 장애 시 데이터의 손실 위험을 예방한다.

- o 복수 클라우드 서비스 공급업자에 탑재되어 있는 자사의 데이터 통합, 관리, 활용의 극대화를 한다.

## 제 4 절 블록체인(분산장부)과 비트코인 기술

### 1. 블록체인(Block Chain)

비트코인의 기술적 핵심은 블록체인이라는 분산장부(Public Distributed Ledger) 기술을 기반으로 한다. 블록체인은 일종의 금융장부로서, 비트코인 프로그램을 이용하는 모든 개개인의 P2P거래내역이 모두 이곳에 기재된다. 블록체인은 인류가 최초로 갖게 된 글로벌 클라우드 분산장부이다.

세계 경제사학자들에 의하면, 인류는 기원전부터 화폐에 앞서 장부를 거래에 이용하였다. 하지만 이는 만나서 거래할 수 있는 개인 간에서만 유효한 것이었고, 그나마 매우 불편한 것으로 많은 한계를 들어 낼

수밖에 없었다. 그래서 화폐를 고안하고, 장부에 기입하고 거래시점에 물건과 화폐를 교환함으로써 채권-채무 관계를 청산하는 방식으로 금융거래를 발전시켜 왔다.

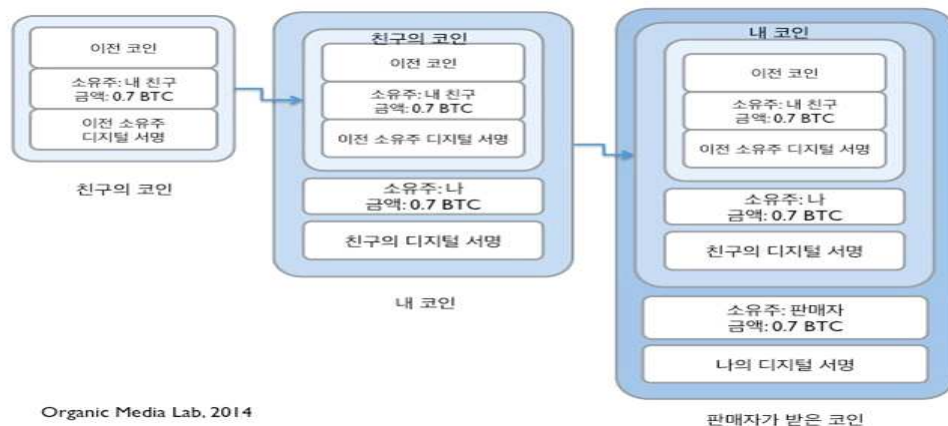
그래서 은행이 등장하면서 장부의 기입은 은행의 몫이 되었고 개인은 주로 현금을 주고받으며 거래 해왔는데, 인터넷 시대가 열리면서 대부분 금융거래가 온라인 장부로 대체되었다. 이제는 예전처럼 개인간 현금을 주고받는 것도 드문 일이 되었다. 대부분 신용카드를 쓰거나 인터넷뱅킹을 통한 금전거래, 즉, 개인간 직접거래가 아니라 은행(또는 신용카드사)을 통한 장부상의 숫자 변화가 주금융거래의 형태가 되었다.

“금융은 숫자와 정보에 불과하다”는 정보/금융 전문가들의 예견이 현실화 되고 있다. 이러한 금융기관의 거래를 중앙집중적인 장부(데이터베이스)에 기반 해 관리하다 보면 비용이 올라가게 된다. 제 3자의 중개를 필수로 하는 거래는 높은 거래 비용을 수반한다. 화폐의 단위도 국가마다 다르고 금융회사들의 네트워크(장부)도 각기 다르다. 그러므로 거래마다 연동하는 비용이 오르게 된다. 블록체인은 바로 이런 비효율적인 구조를 혁신하려는 기술적 시도이다. 누구나 비트코인이라는 P2P 프로그램을 이용해 돈을 주고받으면, 제3자 없이 글로벌 단일 장부에 그 거래 내역이 불변의 기록으로 기입되는 식으로 거래가 확정된다. 따라서 거의 비용이 들지 않으며 아울러 마치 오프라인에서 현금을 주고받듯이 개인간 거래가 가능해진다. 비트코인의 창시자 사토시 나카모토는 “비트코인은 코인 소유주의 디지털 서명의 연결(chain of digital signature)할 비트코인과 블록체인(분산장부기술)이 바꿀 인터넷의 미래다” 이라고 정의하였다[Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008].

블록체인은 분산데이터베이스의 하나로 P2P(Peer to Peer) 네트워크를 활용한다. 블록체인이 비트코인 사용자 모두의 컴퓨터에 저장할 수 있다. 분산 데이터베이스란 데이터를 물리적으로 분산시켜 다수의

이용자가 대규모의 데이터베이스를 공유하게 만드는 기술이다. 데이터를 분산 배치하므로 비용이 적게 들고 장애에 강하다. P2P는 서버나 클라이언트없이 개인컴퓨터 사이를 연결하는 통신망이다. 연결된 각각의 컴퓨터가 서버이자 클라이언트 역할을 하며 정보를 공유하면 된다.

그중 사용자 과반수의 데이터와 일치하는 거래내역은 정상 장부로 확인되어 블록으로 묶여 보관한다. 비트코인의 경우 10분 정도마다 사용자들의 거래장부를 검사해 해당 시간의 거래내역을 한 블록으로 묶는다. 만일 특정 사용자의 장부에서 누락 등의 오류가 발견된다면, 정상 장부를 복제해 대체하는 방식으로 수정한다.



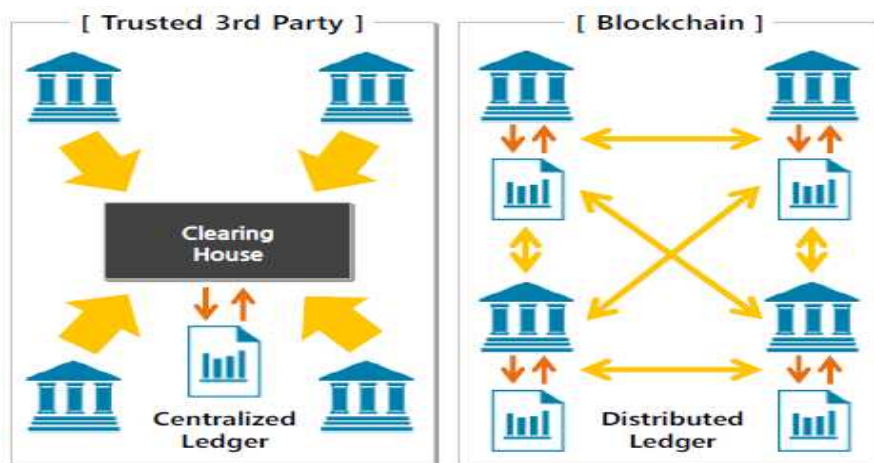
(\* 주 : ‘The Fintech 2.0 Paper’ (Santander, 2015))

(그림 3-19) 비트코인의 네트워크 프로세스

새로운 거래내역을 담은 블록이 만들어지면 앞의 블록 뒤에 덧붙이는 과정이 반복된다. 블록체인(Blockchain)이란 이름도 거래내역(블록, Block)을 연결(Chain)했다는 뜻이다. 거래할 때는 각 사용자가 가진 거래내역을 대조한다. 이를 통해 거래내역의 진위를 파악할 수 있어 데이터 위조가 방지된다. 블록체인의 보안 안정성은 데이터를 공유하는 이용자가 많을수록 커진다.

블록체인은 비트코인 이외에도 클라우드 컴퓨팅 서비스 등 다양한 온라인 서비스에 활용되고 있다. 디지털 서명이란 공개키 암호화를 기반으로 문서의 송신자(그리고 문서의 진위 여부)를 확인하는 방법으로서, 비트코인을 보낸 사람(from)을 확인하는 방법이다. 그러므로 비트코인 거래란, 보내는 사람(from)이 자신의 코인에 받는 사람의 주소(to)와 발행금액을 더하고, 여기에 보내는 사람이 디지털 서명함으로써 만들어진다. 받은 사람은 디지털 서명을 확인하여 코인의 진위 여부를 판단한다. 다음 그림은 이러한 과정이 반복되는 상황을 보여준다(이해를 돕기 위해 1개의 코인으로 1개의 새로운 코인을 생성하는 경우를 나타냈다. 실제로는 2개 이상의 코인으로 2개의 새로운 코인을 생성하는 경우도 많다).

골드만삭스와 제이피모건을 비롯한 9개의 글로벌 은행들은 2015년 9월 블록체인 이니셔티브를 결성한다고 발표하였다. 비트코인의 핵심 기술인 블록체인을 은행 간 거래 장부로 활용하고, 기술표준까지 만들겠다는 계획이라고 한다. 2016년 현재는 약 30여 개에 이른다고 한다. 일본에는 두 개 은행이 참여하고 있고 한국엔 아직 참여 은행이 없다.

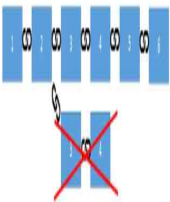


(그림 3-20) 공인된 제3자 공인기술 vs 블록체인 기술

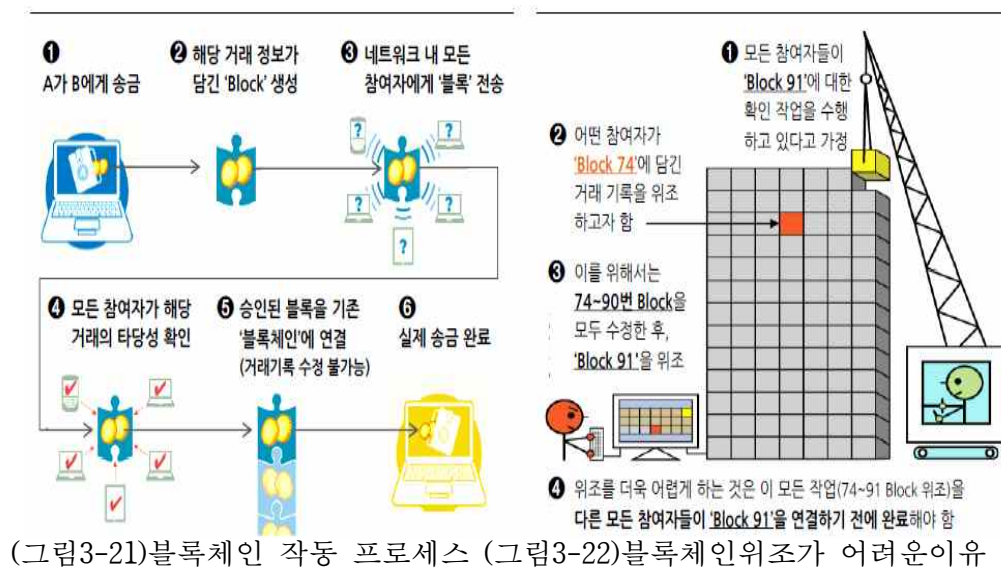


미국의 2대 증권거래소인 나스닥도 블록체인 기술을 전격 도입하겠다고 발표했다. 계획만 발표한 게 아니라 실제 개발 중인 프로토타입 화면까지 공개하며 과감한 행보를 보이고 있다. 나스닥이 지난 10월 말 라스베이거스에서 열린 ‘머니 20/20’ 컨퍼런스에서 발표한 링크(Linq)는 블록체인 기반 주식등록 및 거래 시스템이다. 비상장 회사의 주식을 디지털 에셋의 형태로 블록체인 장부에 등재하고 주주들이 자신들의 지분만큼 보관, 전송할 수 있게 한다는 계획이다. 계약서도, 변호사도 필요 없이 비트코인을 주고받듯 간편하게 주식거래를 할 수 있게 한다.

이렇게 되면 증권거래소도 사실상 필요 없어지게 된다. 블록체인 상의 오더북만으로 P2P 거래가 가능해진다. 나스닥은 거래소 운영자가 아니라 블록체인 운영자로서 다양한 수수료 모델을 갖는다.

	<p>작업증명(Proof-of-Work) 메커니즘 (비트코인 기반 블록체인의 거래 검증 방식)작업증명(PoW)은 거래승인 과정에 많은 컴퓨팅 파워가 필요한 어려운작업(반복 연산 문제 풀기 등)을 포함시키고, 이 과정을 통해 가장 많은 구성원들이 가지고 있는 블록체인을 진짜로 인식해 다른 기록은 폐기하는 것이다. 결국 블록체인을 조작하기 위해서는 전체 참여자의 과반수보다 많은 컴퓨팅 파워를 보유해야 한다 (51% attack)</p>
--	---

블록체인은 기업 영역에만 국한되고 있지 않다. 유럽의 IT강소국인 에스토니아는 전세계인을 대상으로 디지털 영주권 제도(e-Residency)를 운영 중이다. 몇 가지 조건만 갖추면 에스토니아 영주민으로서 금융기관 계좌를 만들 수 있고, 온라인상에서 사업자등록도 할 수 있다. 에스토니아는 이 제도를 이용하는 외국인들의 공공기록을 블록체인에 담아 관리할 계획이라고 한다.



블록체인의 특징은 첫째로 역사상 최초로 등장한, 분산-공공-클라우드 장부인 비트코인 블록체인은 다음과 같은 본질적인 특질을 내포한다. 둘째로 누구나 기입할 수 있으며, 비트코인 프로토콜을 준수하는 지갑 인터페이스를 사용하는 개인끼리 이메일을 보내는 것처럼 비트코인을 주고 받으면 그 트랜잭션이 장부에 자동으로 기입된다. 셋째는 누구나 모든 거래 기록을 볼 수 있다. 블록체인상에 기록되는 모든 거래이력은 브로드 캐스팅되어 참가하는 누구나 볼 수 있고, 참여자들에 의해 집합적으로 검증할 수 있다.

넷째는 누구도 거래기록을 변경하거나 지울 수 없다. 많은 참여자들의 검증과 이중 삼중의 암호화(이전 블록에 이어서 블록을 만들고 체인화) 과정을 거치기 때문에 거래기록 변경이나 삭제가 사실상 불가능하다.

비트코인은 블록체인으로 구현되고 실용화된 최초의 응용사례(application)기술의 핵심은 분산공개 장부기술이다. 비트코인 같은 화폐 말고도 블록체인으로 구현/혁신 할 수 있다.

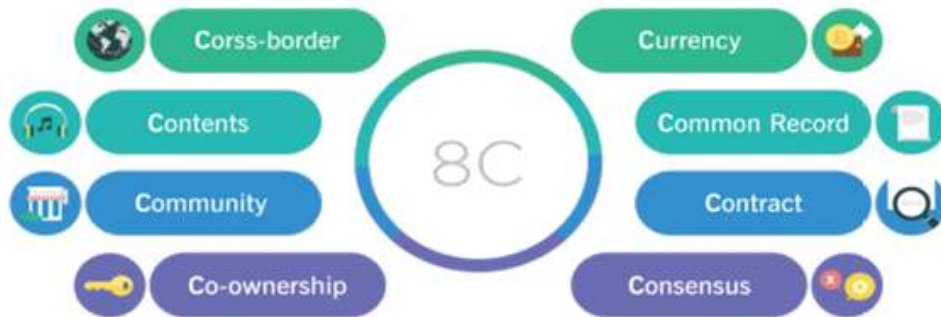
[표 3-9] Gmail과 비트코인 구조 비교

Application Layer	Gmail	Bitcoin(BTC)
Application protocol Layer	SMTP Simple Mail Transfer Protocol	Bitcoin Protocol Protocol for transferring crypto-currency
general protocol Layer	TCP/IP Internet Protocol	Block Chain

Gmail과 같은 많은 웹애플리케이션들이 SMTP와 TCP/IP 같은 프로토콜 위에 구동되고 있는 것처럼, 블록체인 프로토콜 위에서도 비트코인 뿐만 아니라 다양한 응용서비스들이 발생된다. 블록체인의 이 같은 투명성과 무결성, 가역성이라는 특성은 이중지불(double spending)이라는 전자화폐의 치명적 한계가 극복된다. 무한 복제가 가능한 디지털 경제의 장점은 금융거래에 있어서는 오히려 치명적인 결림돌로 작용하지만, 장부관리가 매우 어렵고 번거로운 것으로 만들었는데 비트코인은 블록체인에 기반해 이 같은 문제를 간단하게 뛰어 넘었다. 그러면, 단지 화폐와 금융거래 영역뿐만이 아니라 무결성, 투명성, 비가역성을 필요로 하는 다른 많은 영역에서도 혁신이 있을 것이다.

## 2. 금융 비즈니스 영역 : 8C

비즈니스가 블록체인을 기반으로 생겨날 수 있을지, 과거 인터넷 비즈니스의 4C(Communication, Contents, Community, Commerce)처럼 블록체인을 기반으로 전개될 수 있는 비즈니스 영역을 8C로 정리하였다.



(그림 3-23) 금융 8C

#### (1) Currency

가장 대표적 분야로서 지구 전체로 형성되고 임계점을 넘은 비트코인 생태계과 경제시스템에 기반해 다양한 목적을 지닌 파생화폐, 지능형 화폐들이 등장할 수 있다. 비트코인 보안성에 핵심이 되는 해시 기반 작업 증명(Proof of Work) 기능을 고안한 바 있는 암호학전문가 애덤 백(Adam Back)을 주축으로 개발된 사이드 체인은 비트코인 분위제를 가능케 할 전망이다. 특정 금액의 비트코인을 블록체인에 유보(reserve)해 놓고 그것을 기반 가치로 하는 새로운 병행체인을 만들어 운영하는 방식이다. 이런 사이드체인이 활성화되면 다양한 목적과 기능, 특정 커뮤니티를 겨냥한 실험적인 화폐시스템이 대거 등장할 수 있다. 이런 상황이 오면 비트코인은 과거 금분위제 시절의 금처럼, 디지털 화폐사이에서 기축통화 역할을 하게 될 것으로 전망된다.

#### (2) Common record

중앙아메리카의 저개발국가 온두라스는 국가 차원의 전자화된 토지대

장을 갖고 있지 않다. 온두라스는 새로 토지대장 DB를 구축하는데 블록체인 장부 기술을 이용하고 있다고 한다. 미국의 블록체인 기술 스타트업 Factom이 이 프로젝트에 참여하였다. 이처럼 블록체인은 공공적인 기록을 관리하기에 적합하고 효율적인 기술로 활용될 전망이다. 예컨대 많은 나라에서 자동차는 전산적으로 등록 관리가 되고 있으나 자전거 등록제를 전국적으로 시행하는 나라는 일본과 네덜란드 정도이다. 한국의 자전거 이용자들은 도난, 분실 등에 대비하기 위해 인터넷 게시판을 활용하고 있는데 블록체인을 이용해 자전거를 등록하고 이력 관리하는 시스템을 만들면 비용도 적게 들고 중고 자전거 마켓플레이스로도 발전이 가능하다. 블록체인을 이용하면 이 같은 시스템을 더 저렴하게 구축 운영할 수 있다.

### (3) Contract

블록체인 상에서는 모든 개별 거래는 프로그래밍(조건문 삽입)이 가능하다. 개별거래에 계약조건을 스크립트로 넣고 그게 충족이 되는 시점에서 바로 결제가 이뤄지게 된다. 지금처럼 계약 조건의 이행과 대금 결제가 분리되는 게 아니라 통합되는 것이다. 이런 스마트계약 기능을 활용하면, 주식시장에서 체결과 정산 사이에 2일 정도의 시차가 발생한다거나, 금융기관 간 거래에서도 정산까지 오랜 시간과 서류작업 등이 필요한 상황이 크게 개선될 수 있다. 분산된 시장에서 개인간 주식 및 옵션 거래가 이뤄지는 새로운 시장구조를 만드는 것도 가능하다. 특히 정부에서 추진 중인 전자증권 제도가 시행되고 이것이 블록체인과 결합되면 전혀 새로운 시장과 수요가 창출될 전망이다. 스마트계약 기능은 향후 대부분의 공증과 신탁업무를 자동화하거나 대체할 수 있다.

### (4) Consensus(Crowd-sourcing)

블록체인 상에서 발행된 토큰(token, 비트코인도 일종의 토큰)을 유권자들에게 나눠주고 맘에 드는 정책이나 후보에 토큰을 다시 보내는 방식으로 투표가 가능하다. 현재 중앙집중적인 온라인/모바일 투표는 보안상 안전하지 않으며, 무엇보다 중앙관리자가 존재하므로 비밀투표의 원칙이 철저히 지켜진다고 확신하기 어렵다. 반면 블록체인 기반의 투표시스템은 누가 투표했는지 알 수 없는 한편, 투표집계 전 과정을 참여자들이 실시간으로 모니터링 할 수 있어 투명하다. 또한 표를 여러 개로 쪼개어 여러 선택지에 투표할 수도 있어, 단순한 투표가 아니라 시장예측 컨센서스를 만든다든지 집단지성을 활용하는 다양한 방법을 개발할 수 있다.

#### (5) Cross-border

국제 송금이 비싸고 오래 걸리는 이유는 금융기관간 네트워크가 국경을 넘어서까지 원활하게 작동하지 않기 때문이다. 비트코인 같은 매개체를 이용한 서비스들은 이를 획기적으로 개선하고 있지만, 이 역시 중간에 두 차례 이상의 트레이딩 과정을 거쳐야 한다. 각 금융기관이 블록체인 상에 은행권을 발행 등록해 놓고 취급과 정산이 실시간 자동으로 이뤄지게 되면 지금보다 훨씬 빠르고 효율적인 국제 금융거래가 가능하다. 마찬가지로 이동통신사의 로밍서비스 역시 개선될 여지가 많다. 여러 나라의 이동통신사 간 정산에 30여 일이 소요되고 복잡한 유희와 환율 계산 등으로 비효율이 발생하는데 블록체인을 통해 사용량을 기록하고 정산을 자동화한다면 개선효과가 있다.

#### (6) Contents

디지털 희소성이라는 특질은 음악, 전자책 등의 비즈니스를 크게 바꾸

게 된다. 아울러 블록체인 상에 디지털아트, 웹툰 등의 저작물을 등록해 저작권을 증명하는 것도 가능해 새로운 콘텐츠 시장의 등장도 기대할 수 있다. 실제로 유럽에선 디지털 아트워크를 등록 관리하는 블록체인 프로젝트가 가동 중이다. 세계적인 디자인 기업 IDEO는 얼마 전 블록체인 기술 기반의 뮤직서비스 시나리오 작업을 진행했다. 이 작업을 보면, 음악밴드가 팬들을 앨범 제작에 투자자로 참여시킬 수도 있고, 열성 팬들의 기여도를 측정해 수익배분에 반영할 수도 있다. 음악 비즈니스의 양상이 크게 진전되었다.

#### (7) Community

비트코인의 OPA(Open Asset Protocol)을 이용하면 기존의 상품권, 로열티 포인트, 지역화폐 등을 비트코인의 블록체인 상에 기입하고 관리할 수 있다. 각 지역은 경제활성화를 위해 지역화폐, 지역 상품권 등의 다양한 수단을 강구하고 있지만, 관리비용이 많이 들고 사용성이 떨어져 활성화가 요원한 실정이다. 비트코인 블록체인에 기반 한 모바일 상품권, 지역화폐는 관리 비용을 크게 줄여주고 쉽게 모바일 이용 경험을 증진시키는 효율적 솔루션이 될 수 있다. 대형 유통회사의 포인트 시스템에 피해를 보는 지역의 중소가게(동네 빵집, 커피숍)들이 독립적으로 로열티 포인트를 만들어 관리 할 수 있다.

#### (8) Co-ownership, Sharing

우버, 에어비앤비로 대표되는 공유경제는 큰 성장 가능성을 보여주었다. 하지만 여전히 더 공유되고 효율화 될 영역은 많다. 블록체인상에 집, 사무실, 자동차 등의 소유권을 등록해놓고 매우 세부적인 수준으로 공유할 수 있다. 블록체인은 예약, 이용시간과 범위 등을 아주 세세하게

기록 관리할 수 있는 방법을 제공할 수 있다. 이에 따라 현재는 기술적인 한계로 공유할 수 없다고 생각하는 많은 자원, 서비스, 디지털 자산 등이 공유되고 효율적으로 이용되는 환경을 제공할 것이라 기대를 모으고 있다.

‘신뢰기계’가 확산되는 미래, 어떻게 대응해야 할 것인가? 세계적으로 테크놀로지 담론을 주도해 온 전기전자공학자협회(IEEE)는 2015년 7월 기관지 스펙트럼을 통해 “웹의 미래는 비트코인과 닮았을 것(The Future of the Web Looks a Lot Like Bitcoin)”이라는 전망을 제시했다. 망중립성 논의에서 드러나고 있듯이, 인터넷 구조가 지나치게 중앙집중적이라는 전문가들의 인식이 비등한 가운데 블록체인이라는 암호화-수학 기반의 분산구조 자체가 미래지향적이기 때문이다. 현재와 같이 중앙(서버)에서 이용자의 모든 정보와 데이터를 통제하는 구조 하에서 개인은 이중 삼중의 위협에 놓여져 있다. 즉 관리자 또는 관리회사가 유능하며 도덕적일 것을 믿어야 하고, 해커들에게 당하지 않을 것을 믿어야 하고, 국가권력의 부당한 요구에 굴하지 않고 이용자들의 정보를 지켜줄 것을 믿어야 한다. 이 믿음이 깨지는 순간 이용자는 위협에 처해 진다.

인터넷 서비스 및 금융회사들이 고객들의 개인정보를 내부자 소행으로 유출하거나 해킹으로 유출시킨 사례를 술하게 겪었다. 예컨대 대부분의 웹서비스/앱의 로그인에 쓰이고 있는 페이스북이나 구글이나 또는 내가 쓰는 서비스를 차단한다면 어떻게 될 것인가? 반면 블록체인은 개인의 정보 통제권을 그 자신에게 부여하고 누구도 믿을 필요가 없는 네트워크 환경을 제공한다.

블록체인을 정의하면 신뢰기계(Trust Machine)라고 한다. 서로를 믿을 수 없는 사람들이, 누군가에게 신뢰를 아웃소싱하지 않고도, 금융거래 등 신뢰가 필요한 거래기록을 관리할 수 있기 때문에 블록체인을 활용하게 된다.



[표 3-10] 블록체인 기술의 장점

1. 탈중앙성 (P2P-based)	공인된 제3자의 공증 없이 개인간 거래 가능 → 불필요한 수수료 절감
2. 보안성 (Secure)	정보를 다수가 공동으로 소유하여 해킹 불가능 → 보안관련 비용절감
3. 신속성 (Instantaneous)	거래의 승인·기록은 다수의 참여에 의해 자동 실행 → 신속성 극대화
4. 확장성 (Scalable)	공개된 소스에 의해 쉽게 구축·연결·확장 가능 → IT 구축비용절감
5. 투명성 (Transparent)	모든 거래기록에 공개적 접근 가능 → 거래 양성화 및 규제비용절감

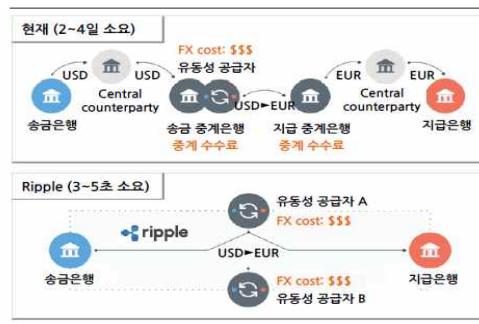
(\* 주 : ‘The Fintech 2.0 Paper’(Santander, 2015) 및 연구자 재구성)

블록체인이 확산되면, 지금까지 신뢰를 담보해줌으로써 존재가치를 인정받아 왔던 모든 주체들, 즉 정부, 금융기관, 법률기관 등이 모두 대체되거나 정체성 위기를 겪게 된다. 인터넷이라는 정보기계(Information Machine)가 현기증 나게 바꾸어 온 지난 20여 년의 시간은 많은 산업의 구조 변동을 이끌어 냈다. 이제 신뢰기계가 바뀌게 될 세상에서 금융업은 어떤 혁신을 가져오는가에 대한 대응이 필요하다.

현황	자산	사례
현재 거래 중	이체	(MeXBT) 송금/인출 가능
	해외송금	(Ripple) 은행간 송금시스템
	금	(RealAsset) 소유기록 등재
	다이아몬드	(Everledger) 등재 및 거래
준비 단계	부동산	(Factom) 소유기록 인증
	주식	(Nasdaq) 개인 주식거래
	채권	(DigitalAsset) 미 국채 거래
	로열티	(Chain) 항공 마일리지

자료: ‘Blockchain’ (Bloomberg, 2015. 9. 1)

[표 3-11]블록체인을 활용한  
자산거래사례



자료: Ripple

(그림 3-24) Ripple의  
해외송금서비스개요

### 3. 비트코인

비트코인은 2009년에 태어난 글로벌 전자지불네트워크이자 그것을 기반으로 통용되는 디지털 화폐단위의 명칭이다. 화폐이면서도 중앙 통제적인 금융기관의 개입이 전혀 없다. 그리고 글로벌 단일 단위를 사용하고 있다는 것이 가장 차별화된 특징이다. 비트코인은 수학적 알고리즘을 바탕으로 참여자 모두를 관리와 운영이 이루어질 수 있도록 설계되어 있다. 중앙관리기관 없이 사람들의 컴퓨터와 컴퓨터를 이어 직접 거래하도록 하는 ‘P2P’ (peer-to-peer) 방식의 수평적 네트워크에서 거래를 포함한 모든 활동이 이루어진다. 비트코인은 발행부터 네트워크의 관리에 이르기까지 철저하게 미리 정해진 알고리즘을 통해 이뤄진다. 사람의 손길 또는 정치 따위가 이 규칙에 개입할 여지는 없다. 비트코인은 발행될 총량이 정해져 있고 130여년 뒤면 발행이 끝난다. 발행은 알고리즘상에서 ‘채굴’ (mining)에 따라 이뤄진다. 자신의 컴퓨팅 자원을 동원해 비트코인 네트워크의 보안과 거래기록 관리 작업에 참여하는 사용자들이, 마치 금을 캐는 것처럼

컴퓨터 알고리즘을 통해 ‘채굴’ 한다. 현재 약 1,200만 비트코인(BTC)이 전세계에 유통 중이고, 2145년까지 총 2,100만 단위(BTC)까지만 발행된다. 비트코인 거래는 이메일을 주고받는 것과 비슷하다. 금융기관을 거치지 않고 개인 사이에 돈이 오가는 P2P 방식이다. 디지털 신호에 불과한 숫자가 금값이 된 상황이 난센스처럼 느껴지거나 일종의 사기극처럼 여겨질 수도 있다.

이런 혼란은 비트코인이 화폐이면서 동시에 글로벌 전자지불 네트워크이기도 하다는 사실을 깨닫지 못한 데서 나온다. 더 나아가 실리콘밸리의 기술산업전문가들과 유력 벤처투자자들은 비트코인을 새로운 금융혁신의 플랫폼이자 프로토콜(기본이 되는 규약)이다. 이메일의 프로토콜인 SMTP, 웹의 프로토콜인 HTTP 처럼, 미래 금융의 프로토콜이 될 것이다. 이 전자 금융네트워크와 금융플랫폼이라는 물적 토대를 바탕으로 비트코인은 비로소 화폐로서의 가치와 기능성을 획득하게 된다. 역사상 가장 저렴하고 효율적인 금융거래를 전 지구적으로 가능케 하려면 혁신적 금융네트워크가 필요하다. 이는 비트코인이라는 독자적인 화폐가 있어야 한다. 그런데 이 화폐는 발행량이 정해져 있어 희소가치를 지닌다. 2145년까지 2100만개까지만 발행된다.

한국에서는 2013년 비트코인 거래소 ‘코빗(<http://www.korbit.co.kr/>)’이 생겨난 이후 본격적으로 비트코인 경제가 형성되기 시작했고, 얼마 전 대기업 최초로 CJ E&M이 비트코인을 결제수단으로 도입하는 등 더욱 확산되고 있다. 해외에서는 2015년 7월 컴퓨터 제조업체 델이 비트코인 결제를 도입한 데 이어 최근에는 온라인 결제 업체 페이팔도 비트코인을 결제시스템에 통합 했다. 미국 매사추세츠공대 (MIT)에서는 학생들에게 비트코인을 나눠 주면서 가상화폐의 사용 학습을 하고 있다. LG 경제연구원은 발간한 보고서에서는 “비트코인이 화폐를 대체할 수 없을지 몰라도 효율적인 지급결제 수단으로서 신용카드와 계좌이체 등을 대체·보완할 가능성이 있다”고 설명하고 있다.

#### 4. 블록체인 기술의 핵심

블록체인 기술의 응용기술인 비트코인은 단순히 세계인이 함께 쓰는 새로운 단일화폐는 아니다. 오히려 중개자 없이 전세계 누구나 사용이 가능한 결제네트워크이며 그것을 가능케 하는 블록체인이라는 분산장부 기술이 핵심이다. 이 블록체인 기술을 이용하면, 비트코인과 같은 형태를 뛰어넘는 많은 일들을 응용 할 수 있다. 물론 금융에만 국한되지도 않는다. 이것이 가능한 것은 블록체인에 기록되는 모든 개별 거래내역을 특정한 조건문 내지는 프로그램으로 입력할 수 있다.

##### (1) 스마트 금융

조건에 따라 지불이 이뤄지거나 자동으로 유보되는 스마트 거래가 가능해진다. 예컨대 에스프로 서비스 같은 것이 별도의 시스템 없이 금융 거래에 내재될 수 있다. 이를 확장하면 개인 간의 옵션 거래도 가능해진다. 내일 날씨, 금 시세 등에 연동한 금융거래가 중개인 없이도 가능해진다. 자식에게 유산을 물려줄 때, 나이가 스무 살 이상이 돼야 자녀의 지갑에 돈이 들어가는 등의 공증/유언을 대체할 수 있다. 현재의 온라인 금융거래는 금융기관이 장부를 기록하고 관리하는 게 기술적 본질이기 때문에 거기에 아무런 프로그램을 입힐 수 없지만, 비트코인의 경우 위에서 설명한 블록체인 구조상에서 자동으로 장부가 기록되므로 거래에 프로그램을 입힐 수가 있다.

##### (2) 디지털 자산관리

비트코인 거래에는 소유권을 담을 수 있다. 예컨대 특정 비트코인 주

소에 BMW자동차의 소유권을 담고, 프로그램으로 자동차 키의 이모빌라이저로 연동시킨다. 이 차를 빌려 쓰는 사람은 차량 소유권을 가진 주소로 매달 얼마의 비트코인을 보내야 한다는 계약까지 입력한다. 만약 차를 빌려 쓰는 이가 렌트 비용을 내지 않으면 비트코인 주소에서 이모빌라이저로 신호를 보내 차량 시동이 걸리지 않게 만든다. 이런 시나리오가 가능해 진다.

### (3) 소프트웨어 비즈니스 모델의 진화

메이드세이프(MaidSafe)라는 스토리지 서비스는 비트코인의 운영체제와 마찬가지로 분산저장방식으로 서비스를 제공하는 소프트웨어다. 기존에 많이 사용되던 구글드라이브나 드롭박스 등에 비해 보안적으로 안전하며, 대용량 시스템을 필요로 하지 않아 훨씬 효율적인 이용환경을 제공한다는 것을 강점으로 내세우고 있다. 웹 2.0의 등장으로 공급자 중심에서 사용자 중심으로 패러다임이 이동했으며, 그에 따라 대용량 스토리지 공간을 저비용으로 구축할 필요성은 매우 커지고 있다. 메이드세이프는 이 같은 서비스를 제공하면서 이용료를 받는 대신, 비트코인과 유사한 세이프코인이라는 자체 코인을 발행하였다. 이용자들은 메이드세이프 이용료로 세이프코인을 지불해야 하는데, 일부는 회사에서 나눠주기도 하고 일부는 거래를 통해 구하면서 세이프코인에 시세가 형성되기 시작했다. 현재 세이프코인의 전체 가치는 90억원에 이른다. 회사는 일부 코인을 주식처럼 보유하면서 시장에 형성된 가격에 따라 코인을 내다 팔면서 자금을 마련할 수 있다. 아울러 나중에 서비스가 더 성공을 거두고 이용자가 많아질수록 세이프코인의 가치는 올라갈 것이고, 그에 따라 회사가 보유하고 있는 코인의 자산가치도 상승하게 된다. 기존의 소프트웨어 비즈니스모델과는 전혀 다른 구조로 사업이 가능해진 것이다. 비트코인 같은 금융기술의 등장으로 향후 오픈소스 소프트웨어 개발을 통한 비

즈니스가 더욱 활성화 될 것으로 전망하고 있다.

#### (4) 새로운 마켓플레이스 등장

비트코인의 핵심인 블록체인의 분산장부 기술은 앞으로 금융을 넘어 마켓플레이스 분야에도 큰 변화를 가져올 것이다. 지금의 마켓플레이스는 모두 중앙집중적이다. 마켓을 운영하는 회사, 즉 이베이나 아마존 같은 운영주체들은 금융기관 같은 중개자, 장부관리자 역할을 수행한다. 금융에서 중개자 없는, 또는 중개자들의 역할이 대폭 제한된 혁신이 가능하다면, 마켓플레이스에도 마찬가지로 일이 벌어질 수 있다. 상품에 대한 데이터베이스와 결제 등 모든 통제권을 마켓플레이스의 소유회사가 갖는 방식이 아니라, 블록체인 같은 공공장부에 상품을 등록하고 이용자들이 자유롭게 상품을 찾고 선택하며 거래하고 결제는 비트코인 같은 블록체인상의 지불수단으로 직접(P2P로) 이뤄진다. 이럴 경우 기존 이베이나 아마존은 상품의 빠르고 안전한 배송, 혹시 모를 분쟁 등의 중재자 정도로 역할이 제한되거나 브랜드로서만 기능하게 된다. 오픈바자는 이 같은 가설을 바탕으로 블록체인 방식의 마켓플레이스 실험을 전개하는 회사다.

[표 3-12] 이베이와 오픈바자의 비교

<div>   </div>		
결제	국가화폐	비트코인/분산화폐
데이터저장	회사 서버	Distributed Hash Table (비트토렌트)
계약/보증	회사, 결제사, 보험	Ricardian Contracts, Multi-signature Escrow

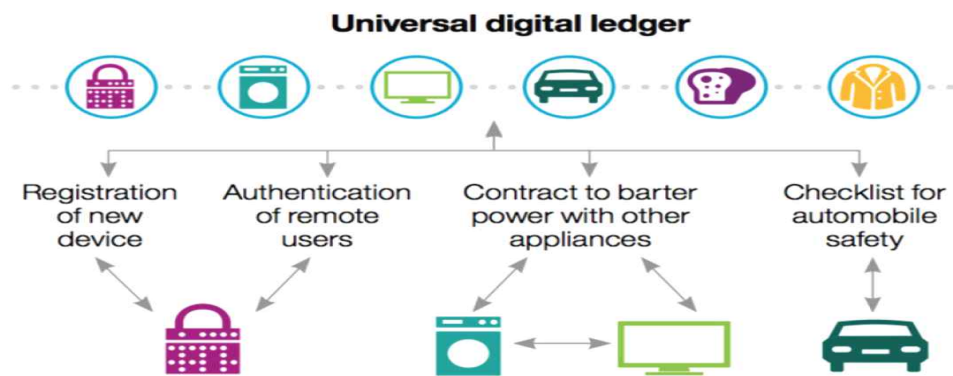
#### (5) 분산자율조직의 등장과 비즈니스의 변화

금융과 마켓플레이스가 변화한다면 비즈니스의 근간이 뒤바뀔 수도 있다. 회사라는 조직형태가 변화에 오를 것이다. 자본주의적 근대화 속에서 상법상의 주식회사는 가장 활성화된 조직형태였다. 어떤 목적을 이루기 위해 가져갈 수 있는 조직형태 중 가장 효율적인 조직이 주식회사였다. 하지만 문제점 역시 적지 않았다. 비효율성, 비대화에 따른 관료주의 등등. 이제는 기술의 발전으로 어떤 목적을 이루기 위해 굳이 회사를 설립하지 않아도 되는 세상이 오고 있다. 비트코인에는 기업처럼 운영주체가 존재하지 않는다. 알고리즘이 작동할 뿐이고 참여자만 있을 뿐이다. 비트코인의 거래를 확정하는 역할과 보안장벽의 역할까지 수행하는 마이너(채굴자)들은 비트코인에 고용돼 있지 않은 자발적 참여자들이다. 그런데 그들이 알고리즘이 요구하는 어떤 행위를 수행하면, 그에 대한 보상으로 바로 네트워크상의 화폐가 주어진다. 오픈소스 소프트웨어 비즈니스는 회사를 만들지 않아도 가능하다. 사람들이 매력을 느끼고 애용할 소프트웨어를 개발한 개인 또는 집단은 그것을 네트워크상에 올려놓고 사람들이 사용하면서 지불할 수단을 함께 제공하면 된다. 알고리즘에 따라 화폐의 발행과 소프트웨어의 사용 그리고 과금까지 이뤄지며 개발자

들은 자신들이 보유한 코인을 형성된 시장을 통해 현금화할 수 있다. 주식의 발행, 이용료, 소프트웨어 구매 등이 블록체인이라는 구조상에서 작동하기 때문에 가능하다. 알고리즘이 구동되는 블록체인 구조는 사람들이 일하는 방식도 바뀌어진다.

#### (6) 사물인터넷

사람과 조직뿐만 아니라 기계, 사물들까지 연결시켜 그야말로 중단 없는 네트워크상의 워크 플로우를 가능케 한다. IBM 비즈니스 밸류연구소(IBM)에서 제시한 어덱트(Adept)라는 사물인터넷 플랫폼은 비트코인의 블록체인 아키텍처를 차용해 만들었다. 이 연구를 주도한 폴 브로디 부사장이 밝힌, 블록체인 구조를 차용한 이유는 경제성과 보안성 때문이다. 이들이 구상한 블록체인 중심의 사물인터넷 구조가 더 기술적/경제적으로 뛰어난 것이라면, 디바이스 간 소통뿐만 아니라 디바이스 간 금융거래에 결제수단으로 이용된다.



(\* 주: NIPA SW공학센터 웹진)

(그림 3-25) IoT에 의한 블록체인의 다양한 구성 방법



## 제 4 장 핀테크(FinTech) 서비스 보안

### 제 1 절 핀테크 보안 개요

#### 1. 핀테크와 보안

미국 IT리서치 전문기업 가트너가 전망한 2017년 모바일 결제시장의 규모는 730조원으로 이처럼 시장이 폭발적으로 성장할 것으로 예상됨에 따라 모바일 결제시장 선점을 위한 각축전이 세계적으로 전개되고 있다. 세계는 금융과 ICT기술이 융합된 핀테크시대에 금융서비스 혁신과 함께 보안 패러다임의 새로운 변화에 직면하고 있다. 글로벌 핀테크 시장은 빠른 성장을 지속하고 있으며 IT 강국이라 자부하는 우리나라도 최근 모바일 지급결제 서비스 중심으로 핀테크 열풍이 거세게 불고 있다.

우리나라는 2013년 카드 3사 개인정보유출사고, POS시스템 해킹 등 전자적 침해사고 등으로 ICT기술을 활용한 금융서비스의 안전성에 대한 우려가 높은 상황에서 핀테크 시대를 맞고 있다. 핀테크의 목적은 사용자들이 좀 더 편리하게 금융서비스에 접근하여 안전하게 결제, 송금, 거래 서비스를 이용하도록 하는 것이다. 편리하고 안전한 금융서비스를 제공해야하는 환경에서는 ICT 기술들이 접목되면서 상대적으로 더욱 증가된 보안위협이 발생한다. 그러나 핀테크에 대한 관심과 기대감이 크게 증가하고 있으나, 본질적인 카드사 정보유출 사고 및 해킹 등으로 ICT 기술을 활용한 금융서비스의 안전성 확보에 있어서 우려의 목소리가 높다. 핀테크 산업의 발전과 진화는 정보보호와 동반 성장하지 않고는 불가능하다. 보안이 강구 되지 않은 불안정한 서비스로 보안사고가 발생할 경우 핀테크 산업 발전에 악영향 뿐 아니라 금융서비스 근간인 신뢰가 무너지고 만다. 핀테크의 보안은 금융서비스와 기업의 생존을 결정하는

핵심가치이다. 핀테크는 보안이 강구되지 않으면 어떤 유형의 위협이 발생할지 모른다. 핀테크는 사용자의 접근성은 간편하게 보안은 강화되어야 하는 양날의 칼과 같다. 그래서 편의성과 보안의 조화가 필요하다. 또한, 피해를 최소화할 수 있도록 법적 책임을 명확하게 하되 이해당사자간 합의가 필요하다. 이렇게 핀테크 산업이 바람직하게 성장하고 금융혁신을 이루려면 무엇보다 핀테크 보안성 대책이 필수이다.

## 2. 핀테크 보안의 3요소

핀테크에서는 다양한 보안기능을 추가하고 있지만 대부분은 새로 만드는 것이 아니라 기존의 보안기술을 활용하는 것이 많다. 이러한 기술의 특징과 장단점을 잘 파악하여 핀테크와 무리 없이 연동되도록 해야 한다. 핀테크는 다른 서비스에 비해 정책적인 제약이 많기 때문에, 보안에 대해 기술적인 접근과 함께 비즈니스적인 접근을 병행해야 기술과 정책을 조화롭게 구성할 수 있다. 핀테크 보안기술은 하드웨어적인 요소가 많기 때문에 이를 소프트웨어적으로 변환할 수 있는 방안도 필요하다. 핀테크 보안의 3요소는 일반적 보안원칙과는 조금 다르게 정의된다. 효율성, 편의성, 안전성 등 3가지 요소이다. 불과 몇 년 전만해도 금융은 우리나라만 생각하면 되었지만 금융서비스가 온라인으로 옮겨가면서 글로벌 표준에 대한 인식이 확대되었다. 핀테크는 이용자가 다양해지기 때문에 인증에 대한 보안이 강화되어야 한다. 하지만, 최종사용자(End User)의 디바이스는 모바일처럼 이동성이 강할 수도 있어 편의성도 고려해야 한다. 핀테크 보안은 우리나라 뿐만아니라 국제적으로 사용될 수 있도록 글로벌 표준에 따라야 한다. 우리나라에서 거의 유일하게 사용되는 ActiveX나 공인인증서에 대한 보완이 필요한 것도 이 때문이다.

[표 4-1] 핀테크 보안의 3요소

구분	내용
효율성	- 비즈니스 관점의 접근 필요 - 기술과 정책의 조화를 통해 피해 최소화, 이익 극대화 필요
편의성	- 이용자 편의 증대 필요 - 간편 결제 환경, 온라인 플랫폼 필요
안정성	- 글로벌 표준으로 지향 필요 - Active X, 공인 인증서 대체방안 필요

(\* 주: 한국정보통신기술협회)

핀테크는 ICT기술을 기반으로 하기 때문에 ICT기술에서 정의하는 보안에서 정의되어야 한다. 또한 금융서비스 기반이기 때문에 금융서비스 보안내에서 정의되어야 한다. 기존의 금융서비스는 일관된 서비스만 제공하였지만 다양한 디바이스, 시스템과 연계되는 핀테크는 비즈니스 흐름에 따라 소프트웨어를 구성해야 하며 보안도 비즈니스 관점으로 접근하여야 효율성을 높일 수 있다.

## 제 2 절 FDS시스템 기본 구조

### 1. FDS 시스템 구성과 기능

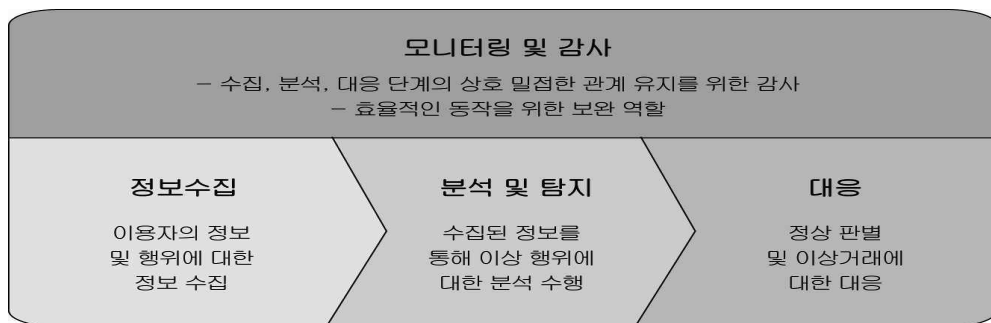
FDS(Fraud Detection System)는 전자금융거래 접속정보, 거래내역 등을 종합적으로 분석하여 이상금융거래를 탐지 및 차단하는 시스템이다. FDS는 전자금융거래에 활용되는 단말접속정보(시스템 정보, 네트워크 정보, IP정보, 거래내역)에 대한 로그를 수집한 뒤 분석을 통해 정상적인 거래가 맞는지 여부를 판단한다. FDS는 실시간으로 수많은 금융정보를

수집, 저장, 분석, 처리한다는 점에서 빅데이터 기술과 보안과 깊은 관련을 가진다. 금융정책 당국은 카드사, 보험사에 구축돼 있는 FDS를 증권 및 은행 등 전 금융권으로 확대하도록 한 바 있다. FDS를 전 금융권으로 확대함으로써 금융거래 정보 등을 분석해 이상금융거래를 탐지하고 발생 가능한 금융사고를 사전에 방지하기 위한 목적이다. 그러나 FDS 구축이 금융사기를 모두 해결한다는 것은 아니므로 사이버거래 보안대책은 다각적으로 종합적으로 시행되어야 한다. FDS 기능을 파악해 보면 다음과 같은 기능적 요구사항을 구현하고 있다. 「이상금융거래 탐지시스템」은 다양하게 수집된 정보를 종합적으로 분석하여 이상금융거래 유무를 판별하는 복합적인 시스템으로 크게 4가지 기능으로 이루어져야 하며, 각 기능은 상호 호환 또는 연동되도록 구성되어야 한다.

○ 분석 및 탐지 기능 : 수집된 금융정보를 이용자 유형별, 거래 유형별 다양한 상관관계 분석 및 규칙 검사 등을 통해 이상행위를 탐지하는 기능

○ 대응 기능 : 분석된 이상금융거래 행위에 대해 거래 차단 등의 대응하는 기능.

○ 모니터링 및 감사 기능 : 수집·분석·대응 등의 종합적인 절차를 통합하여 관리하는 모니터링 기능과 해당 탐지시스템을 침해하는 다양한 유형에 대한 감사기능



(\* 주 : 금융보안원, 이상금융거래탐지시스템 기술 가이드, 2014. 8)

(그림 4-1) 금융업무 사고 탐지 프로세스

[표 4-2] FDS 기능 요건

〈표 1〉 이상금융거래탐지시스템 요건 및 기능

기 능	요 건	
정보수집	정보수집은 다양한 채널의 거래로그를 수집	기존 시스템의 변경 최소화로 데이터 수집 가능
	DB원장의 정보 수집 기능(거래 원장 등)	수집정보는 개인정보 수집이용 관련 법규 준수
분석 및 탐지	이용자 별 과거거래 패턴을 분석하여 프로파일 생성 기능	스코어 모델 기반의 위험도 평가 기능
	기존 마트를 활용한 정형/비정형 데이터 분석 기능	금융거래의 특성을 반영하여 거래 실시간 탐지 가능
	데이터 분석 시 속도 보장 및 다양한 대쉬 보드 제공	추가된 탐지패턴에 대한 시뮬레이션 기능과 패턴 비교 분석 기능
	과거 사고유형에 대한 패턴 탐지 기능	금융보안연구원의 이상거래탐지시스템 기술가이드의 대표적인 탐지패턴 반영
대응	탐지된 거래의 경중에 차등적(추가인증, 거래 차단 등) 대응	확실한 이상거래로 판명된 경우 해당 패턴에 대한 자동탐지패턴 반영
	콜센터 및 관리자 통지(SMS, mail, 시스템 알람 등) 기능	추가 인증을 통해 정상거래 판명 시 해당 로그를 이용자 패턴에 반영
모니터링 및 감시	수집, 분석, 탐지 및 대응 기능을 시각화하여 관리 가능한 대쉬 보드	이용자 별 거래 현황 및 탐지현황 등 전반적인 업무 현황 조회 및 보고서 기능
	탐지된 데이터의 이상거래를 판단 할 수 있는 정보 및 사후 관리	이상금융거래탐지시스템 이용자의 접속 기록, 이용 기록 등 감사를 대비한 기능
기존 시스템과의 연계	기 운영시스템과 연동되어야 함에 따라 안정성 확보	타 금융기관 또는 외부기관으로부터 사고 유형 정보 수집

자료: <http://www.bispro.co.kr/FDS>

## 2. 정보 수집 및 분석

### o 정보수집 방법

매체환경 정보를 수집하기 위한 방법은 크게 플러그인(Plug-in) 기반 또는 별도 수집프로그램을 통해 정보를 수집하는 방법과 순수 웹 애플리케이션(HTML, Javascript 등)에서 제공하는 기본 기능을 이용하여 정보를 수집하는 2가지 방식으로 구분될 수 있다.

### o 정보의 분석

이상금융거래 유무 판단 위해 사용되는 탐지패턴(Rule)은 다양하게 수집된 정보를 분석한 결과를 바탕으로 한다. 무엇보다 중요한 점은 필요에 의해 수집된 이용자 매체환경 정보와 이용자의 금융거래 유형 정보가 복합적으로 활용 분석되어야 한다.

#### ○ 탐지 패턴 갱신

분석된 결과가 탐지패턴에 반영되는 등의 대응절차 및 기능이 동시에 고려되어야 한다. 이러한 활동은 이상금융거래의 탐지 정확성과 운영 안전성을 갖는 효과를 가져 올 수 있다. 탐지패턴을 개발하기 위한 통상적인 방법은 이용자 매체 환경 정보와 금융거래 유형 정보가 이용되며 과거의 정보와 현재 발생하는 정보를 비교하여 탐지패턴을 유지한다.



(\*주 : 국내 금융권의 이상금융거래탐지시스템 도입 현황 및 한국우정의 대응)

(그림 4-2) 이상금융거래탐지시스템 업무 흐름도

### 3. FDS시스템의 성능 목표

FDS시스템에서는 FDS를 통해서 탐지된 이상금융거래 중에서 실제 금융사고 발생 여부에 따라 정탐/오탐으로 나뉜다.

- 정탐 : 이상거래로 탐지한 거래가 실제 금융사고인 경우이다.
- 오탐 : 이상거래로 탐지했으나, 정상거래인 경우를 의미한다. 오탐률은 낮아야 하는 것이 목표이다.
- 미탐 : 탐지를 하지 못한 금융사고이다. 미탐이 발생하지 않도록 하

는 것이 업무목표이자 사기방지 업무의 목표이다.

FDS에서 미탐(탐지하지 못한 금융사고)도 이상금융거래의 범주로 포함되므로, 정탐률을 높이고 미탐률을 0%에 가깝게 하는 것이 목표이다.

### 제 3 절 데이터 수집 플랫폼

데이터 수집 플랫폼은 사기탐지 시스템에서 머신 데이터(machine data)를 활용 할 경우 필요한 기술이며, 본 보고서의 다음 영역에서 사용될 수 있다

- o 금융시스템 동작과정에서 발생하는 머신 데이터(machine data)는 설정, API의 데이터, 메시지 대기열, 변경 이벤트, 진단 명령어 출력, CDR(call detail record), 산업시스템의 센서 데이터 등이 포함된다

- o 핀테크 거버넌스 보안 전략과제 (B)

- 분야명 : 국·내외 핀테크 공격기술 및 사건 동향조사 추세분석에 데이터 수집 플랫폼 활용 가능함

#### 1. 머신 데이터(machine data)

금융시스템이 동작과정에서 발생하는 머신 데이터(machine data)는 설정, API의 데이터, 메시지 대기열, 변경 이벤트, 진단 명령어 출력, CDR(call detail record), 산업 시스템의 센서 데이터 등이 포함된다. 머신 데이터에는 고객, 사용자, 트랜잭션, 애플리케이션, 서버, 네트워크, 모바일 장치의 모든 작업과 행동에 대한 정확한 기록이 포함되어 있다. 머신 데이터는 예측할 수 없는 다양한 형식으로 제공되며, 기존의 모니터링 및 분석 도구로는 이 데이터의 다양성, 속도, 볼륨 또는 변동성을 파악할 수 없다. 머신 데이터는 단순한 로그 이상의 의미를 가지며 서비스 문제를 신속하게 진단하고 복잡한 보안 위협을 탐지, 원격 장비의 상태와 성능을 파악하게 한다.

[표 4-3] 머신 데이터위치와 정보속성

데이터 형식	데이터 위치	데이터 정보
애플리케이션 로그	로컬 로그 파일, log4j, log4net, Weblogic, WebSphere, JBoss, .NET, PHP	사용자 작업, 부정행위 탐지, 애플리케이션 성능
비즈니스 프로세스 로그	비즈니스 프로세스 관리 로그	채널, 구매, 계정 변경, 문제 보고서에 걸친 고객 활동
CDR	통신 및 네트워크 스위치를 통해 기록된 CDR(call detail record), 요금 데이터 레코드, 이벤트 데이터 레코드	청구, 수익 보장, 고객 상담, 파트너 계약, 마케팅 인텔리전스
클릭스트림 데이터	웹 서버, 라우터, 프록시 서버, 광고 서버	가용성 분석, 디지털 마케팅 및 일반 조사
데이터베이스 감사(audit) 로그	데이터베이스 로그 파일, 감사(audit) 테이블	장기간 데이터베이스가 수정된 방식 및 변경한 사람
파일 시스템 감사(audit) 로그	공유 파일시스템에 저장된 중요한 데이터	중요한 데이터에 대한 읽기 액세스 권한 모니터링 및 감사(audit)
관리 및 로깅 API	OPSEC Log Export API(OPSEC LEA) 및 기타 VMware 및 Citrix의 공급업체별 API를 통한 Checkpoint 방화벽 로그	관리 데이터 및 로그 이벤트
메시지 대기열	JMS, RabbitMQ 및 AquaLogic	복잡한 애플리케이션 및 애플리케이션에 대한 로깅 아키텍처의 백본에서 발생하는 디버깅 문제
SCADA 데이터	SCADA(Supervisory Control and Data Acquisition)	SCADA 인프라에서 동향, 패턴 및 특이점을 파악하고 고객 가치를 증대하는 데 사용됨
센서 데이터	온도, 소리, 압력, 전원, 수위 등과 같은 환경 조건 모니터링을 기준으로 데이터를 생성하는 센서 장치	수위 모니터링, 기계 상태 모니터링 및 스마트 홈 모니터링

(\* 주 : [http://www.splunk.com/content/splunkcom/ko\\_kr/resources/machine-data.html](http://www.splunk.com/content/splunkcom/ko_kr/resources/machine-data.html))

## 2. 비정형데이터 수집 플랫폼

비정형 데이터의 수집은 상용 프로그램인 Splunk와 오픈 소스로 Apache의 flume, chukwa, sqoop 그리고 Facebook의 scribe와 같은 SW가



널리 사용된다. 금융시스템 환경에서 이러한 플랫폼이 수집하는 머신 데이터(machine-generated data)에는 사용자 행동, 보안 위험, 용량 사용, 서비스 레벨, 부정행위, 고객만족도 등에 대한 핵심 정보가 담겨 있다. 빅데이터 중에서 가장 빠르게 성장하고 가장 복잡하면서 가치 있는 분야인 이유는 바로 이러한 정보 때문이다.

#### 가. Splunk

Splunk는 상용 데이터 분석, 보고 엔진이다. 원래는 로그를 수집, 처리하기 위해 만들어진 프로그램이지만 빅데이터 분석을 위해 많이 사용된다. 조직화 되지 않은 비정형 데이터들에 대해 빠른 시간에 색인을 생성하고 저장하는 데에 최적화되어 있다. Splunk에서 데이터를 불러오면 호스트, 소스, 소스종류, 그리고 호스트 데이터 등에 대한 색인을 자동으로 생성한다. Splunk는 유닉스나 윈도우 계열 시스템의 로그파일, 네트워크 장비의 데이터, 각종 프로그램의 로그 파일이나 통계자료 등 다양한 플랫폼의 로그들을 조회 할 수 있고 유지보수가 비교적 간단한 것이 특징이다. Splunk의 기능은 Before After Splunk에 의한 가시성과 일괄 관리, 역할 기반 액세스 관리를 통해 데이터 보관, 고객 서비스 및 बैंकिंग 고객 팀은 자체 검색, 짧은 시간에 부정행위에 대한 판단, 사후 대응에서 실시간 모니터링으로 변화 등으로 소개되고 있으며 다음과 같은 구조로 구성되어 있다.

#### 나. 아파치의 flume

Flume은 ‘인공수’라는 사전적 의미로, 여러 서비스에 산재해 있는 로그들을 하나의 수집 저장소로 저장하는 수집 도구이다. Flume은 데이터 스트림 위주의 데이터들을 지정된 모든 서버로부터 로그를 수집한 후 HDFS와 같은 분산 저장소에 적재하여 분석하는 시스템에 적용할 수

있다. 각 서버에서 로그를 수집하기 위해서 HDFS에서 직접 연결도 가능하고 별도의 에이전트(agent) 프로그램이 수집을 대행하는 방식도 가능하다. 수집 권한을 에이전트가 가지게 되면 빠르고 효율적으로 로그관리가 가능하고, 에이전트를 복수개로 운영하면 더 나은 성능과 장애 대비를 할 수 있기 때문에 flume은 복수 에이전트 운영이 일반적이다. 또한 수십 또는 수백 단위의 서버로부터 대량의 데이터를 받아오는 경우는 에이전트를 여러 단계의 계층구조(N-Tier)를 구성하여 로그를 수집하는 방식도 가능하다.

### 3. 오픈 소스 수집기

이중에서 두 가지 오픈 소스는 Apache Sqoop과 Apache Flume이다. 수집할 데이터를 저장할 Data Store는 분산 파일 시스템인 HDFS, 즉, Apache Hadoop FileSystem을 사용한다. 이 오픈 소스들은 대용량 실시간 분석 솔루션인 DAISY(Data Intelligence System)의 수집 시스템의 일부로서 실제 서비스에도 현재 적용되어 안정적으로 운용되어지고 있다. 물론, 대부분의 플랫폼에서 선택한 오픈 소스이기도 하다. 새롭게 만드는 서비스, 시스템이라면 로그 포맷과 생성 위치 등을 정하겠지만, 대부분 기존 서비스에서는 이미 어떤 형식으로든 분석의 대상이 될 로그가 생성되어 있을 것이다. 어떤 시스템은 RDBMS에 로그 테이블을 만들어 파티션하고 저장하는 경우도 있을 것이고, 어떤 시스템은 웹서버, WAS의 Access Log 형태로 파일을 Disk에 롤링해가며 저장하는 경우도 있다.

#### 가. RDBMS로 부터 수집 : Apache Sqoop

RDBMS에 저장되어 있는 경우라면 쉽고 유용한 오픈 소스가 Apache Sqoop이다. Sqoop은 Sql to Hadoop의 약자로, 간단한 CLi(Command

Line Interface)로 Oracle, MySQL 등의 RDBMS의 특정 테이블 또는 특정 조건에 맞는 데이터를 HDFS로 쉽게 옮길 수 있으며, Hive, Pig, HBase 등으로 바로 옮겨 확인 할 수 있다. 반대로 HDFS에 저장되어 있는 데이터를 RDBMS로 옮길 수도 있다. 로그 뿐 아니라 분석할 때 필요한 메타성 데이터를 가져올 때도 유용하다.

(\* 주 : [DBGuide.net] 연재글 - [데이터 수집 #1 오픈 소스 수집기 비교](#))

나. 로그 파일 수집 : Apache Flume, Facebook Scribe, Apache Chukwa

로그 파일이 서비스의 특정 서버의 특정 위치에 파일을 생성하고 있는 경우나 RPC로 로그를 전달할 경우 적용 가능한 여러가지 오픈 소스들이 있다. 그러나, 먼저 명확히 해야 할 것은 로그를 실시간으로 수집, 분석해야 할 사항이 있는가? 아니면, 배치성의 분석만 필요한 것인가? 그리고, 수집과 동시에 실시간 분석을 할 것인가? 아니면 우선 저장하고 이후에 분석할 것인가이다. 가장 많이 알려져 있는 수집기 오픈소스는 Apache Flume, Facebook Scribe, Apache Chukwa이며 최근에 Netflix에서 공개한 suro 등이 있다. 수집기 오픈소스에 대해 알아보기 전에, 대용량의 고속의 이벤트 데이터(로그)를 수집하는 시스템에 필요한 요건은 아래와 같다.

- o 확장성 : 수집대상 서버는 무한대로 확장된다. 수집에서 수천, 수만대로 수집대상 서버는 늘어 날 것이다.
- o 안정성 : 수집되는 데이터가 유실되지 않고 안정적으로 저장되어야 한다.
- o 유연성 : 다양한 포맷의 데이터, 다양한 프로토콜을 지원해야 한다.
- o 실시간성 : 수집된 데이터를 실시간으로 반영해야 한다.

다. Apache의 chukwa

Apache의 chukwa는 여러 서버에 분산되어있는 로그정보를 포함한 데이터를 수집하고, 수집된 데이터를 처리 및 분석하기 위해 만들어진 수집도구이다. Chukwa에는 분산 저장 환경인 하둡(Hadoop)의 클러스터 로그, 서버 상태 등을 관리할 수 있는 기능도 포함되어 있다. Chukwa는 수집할 대상 서버에서 로그 파일이나 서버의 정보를 전송해 주는 역할을 하는 ‘에이전트(agent)’, 에이전트로부터 수집한 정보를 Hadoop 파일 시스템에 저장하는 ‘컬렉터(collector)’, 컬렉터가 수집한 정보를 아카이빙과 디덱스 등의 처리를 하는 ‘데이터 프로세싱(data processing)’ 그리고 Hadoop 클러스터의 로그 파일과 시스템 정보를 수집하여 정보를 분석하고 사용자에게 정보를 보여주는 ‘HICC(Hadoop Infrastructure Care Center)’로 나뉘어서 운영된다. 최근의 빅데이터 플랫폼에서 수집 부분에 사용되는 오픈소스 중 대표적 오픈소스가 있다. 그러나 서비스, 시스템 상황에 맞게 다양한 오픈 소스를 검토해서 각 업무에 적합한 것을 사용해야 한다. 빅데이터 분석 플랫폼의 가장 첫 관문인 수집부분은 서비스 특성에 따라 수집기 이외에도 메시징 큐 등의 여타 Layer도 필요할 수 있으므로 다양한 검토가 필요하다.

(\* 주 : [http://hochul.net/blog/datacollector\\_sqoop\\_flume\\_scribe\\_chukwa/](http://hochul.net/blog/datacollector_sqoop_flume_scribe_chukwa/))

#### 라. Facebook - Scribe, 실시간 로그 수집

Scribe는 페이스북이 자사의 내부 로그 데이터를 수집하기 위해 만든 분산 로그 수집기이다. Facebook의 scribe는 페이스북이 개발하고 오픈소스로 제공하는 로그 수집 도구이다. 비교적 큰 규모의 서버들로부터 실시간으로 로그 수집을 위해 제작되었으며 클라이언트와 서버의 타입에 상관 없이 다양한 방식으로 로그 정보를 수집할 수 있다. Scribe는 일종의 Message Queue를 사용하는데, 수집한 정보를 저장을 실패하는 경우

에는 local disk에 임시로 메시지를 저장했다가 DB가 다시 정상화 되면 임시 저장 메시지를 다시 전송하는 형태로 운영된다. 일반적으로 scribe는 다른 수집 도구에 비해서 속도가 빠르고 실제 Facebook에 이용될 만큼 안정성과 신뢰성이 보장이 되어 있다. Scribe를 설치하기 위해서는 라이브러리가 필요하다.

마. Apache의 sqoop

앞에서 설명한 세 가지의 툴이 비정형 데이터를 다루는 수집도구라면 Apache의 sqoop은 정형 데이터를 처리하는 수집도구이다. Apache sqoop은 ‘SQL to Hadoop’의 의미로 관계형 데이터베이스(RDBMS)에서 데이터 수집을 위한 오픈소스 도구이다. 별도의 데이터 저장소가 없이 RDBMS에 로그를 저장하는 경우나, 메타성 데이터가 RDBMS에 저장되어 있는 경우 RDBMS에 누적되어 있는 데이터를 분석하기에는 비용과 시간이 많이 소모되기 때문에 Hadoop과 같은 분산 환경 저장소로 옮겨 분석할 때 유용하게 사용할 수 있는 도구이다. 이와는 반대로 Hadoop에서 분석된 결과를 원격의 RDBMS로 옮길 경우에도 활용이 가능하다. Sqoop은 Sqoop1과 Sqoop2 두 가지 버전이 사용되고 있는데, Sqoop1은 클라이언트 방식, Sqoop2는 기존의 sqoop1에 server side방식<sup>37)</sup>이 추가된 버전이다.

## 제 4 절 데이터 분석기술

데이터 분석기술은 사기탐지 시스템에서 필요한 기술이며, 본 보고서의 다음 영역에서 데이터 분석기술이 사용될 수 있다

o 사기탐지 시스템의 방법론으로 사용된다. 이는 콘텐츠 마이닝, 기계학습, 딥러닝, 빅데이터등에서 사용할 필수요소이다. 대규모 데이터의 실

시간 처리를 위한 클라우드 컴퓨팅 기술은 기본이며, 자연언어 처리, 텍스트 마이닝, 기계학습, 시맨틱 기술과 같은 인공지능 기술이 활용된다.

o. 핀테크 거버넌스 보안 전략분야(B)

- 분야 명: 머신러닝 기반의 지능형 탐지 엔진(fraud detection engine) 소프트웨어 아키텍처 설계방법

- 분야 명: 핀테크 보안 공격 시나리오 모델 연구

o. FDS 알고리즘과 기술개발 분야(D 그룹2)

## 1. 분석기술 유형

데이터 분석은 첨단 기술들이 통합 적용되어야 하는 매우 복잡하고, 섬세한 작업이다. 대규모 데이터의 실시간 처리를 위한 클라우드 컴퓨팅 기술은 기본이며 자연언어 처리, 텍스트마이닝, 기계학습, 시맨틱 기술과 같은 인공지능 기술이 활용된다. 자연어 처리(NLP)는 인간 언어를 컴퓨터를 통해 처리하기 위한 기술이다. 형태소 분석, 구문 분석, 개체명 인식 등의 기술을 포함한다. 정보 검색(IR)은 빅데이터 처리를 위해서는 정보 검색이 필수이다. 대규모 데이터를 색인하고 이 중에서 주제와 관련된 데이터를 빠르게 찾아 분석한다. 기존 검색은 인간을 위한 정보 검색이라면, 빅데이터 분석에서의 정보 검색은 컴퓨터가 검색 시스템을 사용하는 수요자라는 것이다. 빅데이터 분석 결과를 표현하고 활용하기 위한 유형에는 다음과 같은 기술이 사용된다.

o 분석된 데이터의 의미와 가치를 시각적으로 표현하기 위한 시각화 기술

o 분석결과와 기존 데이터 저장소의 정형 데이터와의 통합 기술

o 애드혹 리포팅, 정보, 운영 프로세스와의 연계 기술

## 2. 데이터 결합과 활용 기술

한편 사물인터넷 데이터 처리 관점에서 보면 기존 처리 방식이 DB 중심의 기간계, 정보계, 분석계 영역으로 구분된 정보시스템 간의 데이터

추출, 변환, 적재 기술이라고 한다면 진화 방식은 하둡 기반의 빅데이터 영역에서의 데이터 적재 기술과 이원화되었던 것이 기존 DB 영역과 하둡 기반의 데이터허브 영역이 결합되고 있다. 전사적 관점에서 데이터의 통합과 활용을 위하여 기존 DB 영역과 하둡 영역에서의 빅데이터에 대한 통합 저장과 분석이 요구된다. 또한 기존 DB 중심의 리포팅, OLAP, BI 분석과 하둡 기반의 빅데이터 분석, 특히 고급 분석으로 이원화된 것이 하나의 분석 틀의 관점에서 통합되고, 데이터 분석도 대용량·실시간 분석으로 진화되고 있다. 최근에는 센서 및 로그 데이터 그리고 소셜 데이터가 가지는 스트림 데이터를 실시간으로 처리하기 위한 데이터 표현, 저장, 가공, 처리 기술이 데이터 플랫폼 기술로 발전되고 있다.

### 3. 데이터 의미 분석 시맨틱기술

심층 분석을 위해서는 데이터에 대한 의미적 분석이 매우 중요하다. 시맨틱기술은 시맨틱 메타데이터 자동추출, 시맨틱 네트워크 생성, 지식 베이스 구축, 온톨로지의 활용, 논리 및 통계적 추론 등을 포함한다. 시맨틱기술은 비정형 데이터와 정형 데이터를 의미적으로 연결하고, 분석하기 위한 핵심이며, 왓슨 컴퓨터, 애플의 시리, 울프람 알파 등이 이런 사실을 증명하고 있다. 통계 기술은 빅데이터의 통계적 의미를 찾고 그 패턴을 분석하기 위해서 강력한 통계 기능을 필요로 한다. 통계 패키지인 R은 이런 의미에서 매우 활용도가 높다. 하둡 상에서 R을 사용함으로써 과거에 생각하기 힘든 규모의 데이터에 대한 통계처리가 가능하게 되었다.

(\* 주 : <http://blog.saltlux.com/bigdata-analysis-overview/198> >>> Data Industry White Paper)

### 4. 대량의 데이터 분석 가공 기술

## 가. 빅데이터 기술

빅데이터를 활용한 금융보안 위협분석은 해결하기 힘들었던 다양한 공격 패턴에 대한 분석을 가능하게 한다. 빅데이터의 패턴 탐색 및 분석기법을 활용하여 보험사기나 신용카드 도용방지, 부정행위 예방에 활용할 수 있다. 실제로 미국의 지온스은행(Zions Bank)은 빅데이터 분석을 통해 잠재적 금융 사기사건을 적발한 바 있고, 라보뱅크(Rabobank)는 ATM 기기에서의 범행 가능성을 높이는 요인들을 포착한 바 있다. 빅데이터 기술을 보안영역에 적용하기 위해서는 빅데이터 수집기술을 통한 데이터의 수집과 실시간 모니터링, 비정상 행위들을 미리 설정하여 이상 징후를 확인인하는 탐지분석, 빅데이터의 분석기법을 이용한 데이터 및 네트워크 분석 등이 이용된다. 이를 위해 splunk나 flume 등의 수집 플랫폼을 활용하여 금융회사의 보안 모니터링과 모니터링한 데이터를 SIEM55) 등의 통합보안관제 제품과의 통합을 통해 높은 수준의 지능적인 모니터링과 연관 분석이 가능하다.

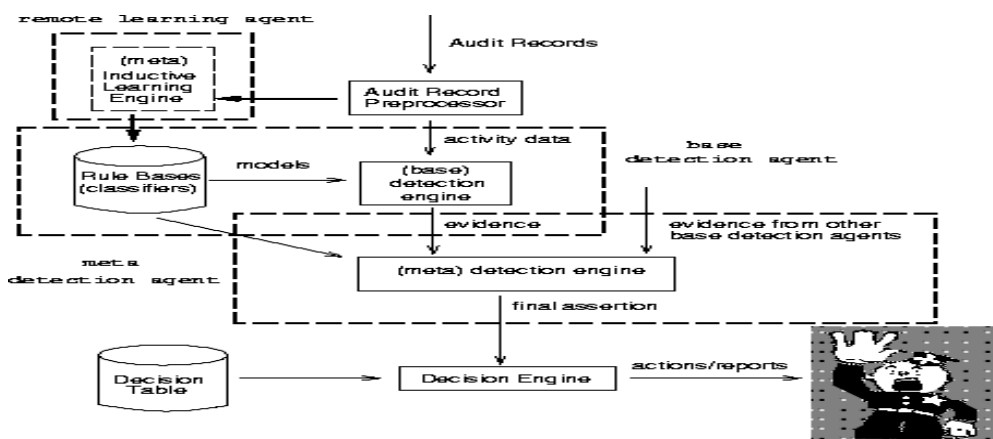
(\* 주 :2015 데이터산업 백서. [www.softwareplatform.net](http://www.softwareplatform.net)5 지급결제와 정보기술 제60호 (2015. 4), <http://techpageone.dell.com> : Big data use case summary )

## 나. 사기탐지 데이터마이닝(Data Mining Approaches for Intrusion Detection)

데이터마이닝은 방대한 양의 데이터로부터 유용한 정보를 추출하는 작업이다. 기업 활동 과정에서 축적된 대량의 데이터를 분석해 경영 활동에 필요한 다양한 의사결정에 활용하기 위해 사용한다. 의미와 가치가 없는 데이터로부터 유용한 패턴을 찾아내 전략적, 전술적으로 유용한 마케팅 정보와 지식으로 전환시키는데 활용한다. 다양한 형태로 생성되는 방대한 양의 빅데이터를 보다 더 정확하고 효율적으로 분석하기 위해 많은 기술들이 사용되고 있으며 이렇게 많은 양의 데이터를 가공해서 사람



들이 유용하게 사용할 수 있는 정보나 지식으로 만들어 주는 기술을 데이터마이닝이라 한다. 통계소프트웨어 회사인 SAS는 부정적발을 위한 데이터마이닝 역할로 예측(prediction), 분류(Classification), 탐색(exploration), 친밀관계(Affinity)를 제시하고 있다. 그리고 IT감사연수기관인 MIS Training은 비정상적인 패턴(pattern), 우회경로(Circumvention), 추세(trend), 불법행위(Illogical), 오류(Mistakes), 고난도 부정(High degree of sophistication)으로 정의하고 있다. 불법행위, 오류, 고난도 부정은 부정의 일반적 특징이며 패턴, 우회경로, 탐색은 비정상적인 행위를 탐지하는 점에서 동일한 목적수행으로 판단된다.



(\* 주 : Wenke Lee and Salvatore J. Stolfo Computer Science Department  
Columbia University 500 West 120th Street, New York, NY 10027  
{wenke,sal}@cs.columbia.edu)

(그림 4-3) Data Mining Approaches for Intrusion Detection

따라서 부정위험 탐지에 있어서의 데이터마이닝은 부정위험을 탐지하기 위해 데이터의 빈발패턴을 찾거나, 부정의 특성을 분석하여 예측하거나, 행위가 보편적인 특성을 벗어난 이상치를 찾아주는 데 활용된다.

다. 정형화되어 있지 않은 텍스트 분석(Text Mining)

정형화되어 있지 않은 텍스트는 데이터마이닝이 아닌 텍스트마이닝을 통해 분석 가능하다. 텍스트마이닝은 텍스트 덩어리 안에서 단어들을 분해해 단어의 출현 빈도나 단어들 간의 관계성을 파악하여 의미있는 정보를 추출해내는 기술이다. 뉴스나 예능 프로그램에서도 특정 주제나 인물을 다룰 때 트위터와 같은 소셜 미디어에서 언급된 단어들을 분석하여 보여주는 경우가 있다. 화면에 나왔던 그 분석 자료들이 바로 텍스트마이닝 기술을 이용해서 만들어진 자료이다. 이와 같이 텍스트마이닝은 낯선 이름과 달리 실생활에서 흔히 사용되고 있다. 대규모 텍스트로부터 의미있는 정보를 추출·분석한다. 기계학습 기반의 통계적 방법과 규칙 기반의 방법이 있으며, 최근에는 이들이 하이브리드 형태로 결합되어 사용된다. 기존의 분류, 군집 기능 외에 감성 분석과 같은 기능 구현에는 텍스트마이닝은 필수적이다. 텍스트 데이터를 활용하여 분석을 하는 기법으로 빅데이터 분석에서 가장 많은 관심을 가지는 기법이다.

- o Text 수집 및 처리: 온라인고객리뷰/학술지초록/정치 및 금융 분야 웹문서
- o Sentimental Analysis를 이용한 Text Analysis
- o Supervised Learning과 Unsupervised Learning을 이용한 Text Analysis

텍스트마이닝은 Big Data 분석의 주요 기술 중 하나이다. 대용량의 데이터에서 사용자가 관심을 가지는 정보를 찾아내며 비정형 데이터를 자연어 처리와 문서처리 기술을 적용하여 유용한 정보를 추출, 가공하는 기법이다. 데이터(문서)로부터 새로운 정보를 발견 할 수 있도록 관련 방법을 제공하며 대용량 비정형 데이터를 텍스트화하여 유용정보를 찾아가공하는 기술이다. 일반 데이터와 달리 텍스트는 각 언어별로 어휘적, 문법적 독특성이 있고 그 표현 형태가 다양하고 복잡하여 일괄된 규칙으로 규정하기 힘들다. 또한 언어가 사용되는 환경에 따라 끊임없이 변화

는 언어가 가진 복잡성 때문에 아직도 연구 소재가 많다. 정리되어 있거나 수치화된 데이터가 아닌 사람의 예측불가의 상황에서 언어가 담겨 있기 때문에 텍스트마이닝은 데이터마이닝보다 더 많은 통계적, 규칙적 알고리즘을 프로그램에 지원해야한다.

[표 4-4] 부정위험 탐지를 위한 데이터 분석방법

목적	역할	분석방법
사용자 행동	빈발패턴 (탐색적모델링)	-연관성 분석(Association/Sequence) -링크분석(Link Analysis) -요인분석(Factor Analysis) 등
사용자 특성 및 행동	분류 (예측적모델링)	-의사결정나무(Decision Tree) -군집분석(Clustering Analysis) -신경망분석(Neural Network Analysis) 등
	이상치 (탐색적모델링)	-군집분석(Clustering Analysis) -시계열분석(Time Series Analysis) 등

(\* 주 :부정위험 탐지를 위한 데이터마이닝 적용방안 연구, 감사연구원)

## 5. 대용량 데이터의 저장과 관리기술

대용량 데이터의 저장과 관리, 운영을 위해서는 클라우드 컴퓨팅 기술이 기본이며, 특히 하둡, HBase, Cassandra, MongoDB와 같은 NoSQL 기술이 활용된다. 데이터 플랫폼 기술은 최근 오픈소스 소프트웨어 기술과 맞물려 발전하고 있다. 즉, 데이터 플랫폼 시장에서의 오픈소스 소프트웨어는 기존 상용 제품 및 솔루션 중심의 데이터 관리 시장에 다양한 기술과 응용서비스를 제시하고 있다. 이 기조는 클라우드 컴퓨팅 기술과 결합하여 기존 제품 중심의 라이선스 비즈니스 모델을 서비스 중심으로 전이시키고 있다.

#### 가. HBase

HBase는 Google이 2006년에 발표한 BigTable이라는 NoSQL 데이터베이스의 아키텍처를 따르고 있다. HBase는 뛰어난 Horizontal Scalability를 가지는 Distributed DB로써, Column-oriented store model을 가지고 있다. 사용량이 늘어남에 따라서 Regionserver만 추가해주면 자연스럽게 Scale-out이 되는 구조이다. 또한, Hadoop 특유의 Sequential read/write를 최대한 활용해서 Random access를 줄임으로 Disk를 효율적으로 사용한다. 이 때문에 HBase는 보통의 RDBMS와는 다르게 Disk IO가 병목이 되기보다 CPU나 RAM 용량이 병목되는 경우가 많다. HBase는 많은 회사가 데이터 분석을 하는데 활용하고 있으며, NHN Line과 Facebook messenger 등의 메신저 서비스에서 Storage로 사용하고 있다.

#### 나. Cassandra

공개SW 역량프라자에서 분산 데이터베이스(NoSQL) 기반 기술로서 카산드라(Cassandra)는 분산 데이터 스토리지 시스템이다. 아파치 재단에서 오픈소스로 만들어 배포하고 있고, 자바기반으로 제작되었다. peer to peer 프로토콜을 이용한고가용성이 구현되어 있다. 카산드라는 리눅스의 슈퍼유저인 root 로 실행할 필요가 없다. 카산드라를 운영하기 위한 시스템 계정을 만들고 그 시스템 계정으로 운영하면 된다.

#### 다. MongoDB

최근에는 기존의 관계형 모델과는 다른 데이터베이스 관리시스템에 대한 관심이 증가하고 있다. 이 중심에는 NoSQL이라는 개념이 있는데, 이

는 데이터베이스 상호 작용에 SQL을 사용하지 않는 데이터베이스 소프트웨어를 총괄하는 용어이다. 주목할 만한 NoSQL 프로젝트 중 하나는 JSON 형태의 문서 컬렉션으로 데이터를 저장하는 오픈 소스 문서 지향 데이터베이스인 MongoDB이다. MongoDB가 다른 NoSQL 데이터베이스와 다른 점은 쿼리가 쉽게 변환되기 때문에 관계형 데이터베이스를 MongoDB로 쉽게 변환할 수 있는 강력한 문서 지향 쿼리 언어에 있다. MongoDB는 C++로 작성되어 있다. MongoDB는 JSON의 2진 버전인 BSON을 사용하여, 키/값 쌍으로 데이터를 유지하는 JSON 형태의 문서에 데이터를 저장한다. MongoDB가 다른 문서 데이터베이스와 구별되는 한 가지 기능은 SQL문을 MongoDB 쿼리 함수 호출로 매우 간단하게 변환하는 기능이다.

## 제 5 절 금융사기 방지에 활용되는 기반기술

사기방지에 활용되는 기반기술은 사기탐지시스템 구축에서 필요한 기술이며 국내에 도입이 아직 미진한 분야이나 앞으로 연구개발을 통해 선별적으로 도입 활용해야 할 기술이다. Heuristics 방법론, 빅데이터 기반 기계학습(machine learning), 데이터마이닝 분석 기법, 빅데이터 분석 등이 주목받고 있다. 세부적인 기반기술 영역은 데이터 마이닝, 콘텐츠 마이닝, 기계학습, 딥러닝, 빅데이터 등이며 대규모 데이터의 실시간 처리를 위한 클라우드 컴퓨팅 기술, 자연언어 처리, 텍스트 마이닝, 기계학습, 시맨틱 기술과 같은 인공지능 기술도 활용된다.

본 보고서에서 다음 분야는 사기방지에 활용되는 기반기술을 사용하여 연구가 진행되어야 할 대표적 소재이다.

- 핀테크 거버넌스 보안 전략분야
  - 핀테크 보안 공격 시나리오 모델 연구
  - 머신러닝 기반의 지능형 탐지 엔진(fraud detection engine) 소프트

## 웨어 아키텍처 설계방법

- 핀테크 보안 포렌식 업무 모델 발굴
- o 핀테크 보안기술 연구개발 분야(D 그룹1) 5개분야
- o FDS 알고리즘과 기술개발 분야(D 그룹1) 4개분야
  - 분야 명: Big Data 검색엔진 기반
  - 분야 명: 사기탐지 인공지능 (AI) 질의응답 전문가시스템 기술개발

### 1. Heuristics 방법론

o 대표성 휴리스틱(representativeness heuristic)은 어떤 개별적인 대상 A가 B라는 부류(class)의 특성들을 ‘대표(represent)’ 하는 것으로 보일 때 곧바로 ‘A는 B에 속한다’고 판단한다. 즉 한 사물이 다른 사물과 같은 기능을 갖는 사실을 추론하기 위하여 그 사물이 다른 사물과 가지는 대표적인 유사성에 초점을 맞춘다.

o 가용성 휴리스틱(availability heuristic)은 어떤 것에 대하여 판단을 할 때 구체적이고 생생한 예를 얼마나 쉽게 마음에 떠올릴 수 있는가에 기초하여 결론을 내리는 것을 말한다. 많은 경우에 이 판단법은 정확하고 유용하지만 문제는 가장 쉽게 떠오르는 것이 전체적으로 볼 때 전형적인 사례가 아닐 수 있다. 즉 개인경험이나 매스컴 정보의 영향으로 어떤 사건이 실제보다 과장되어 빈번하게 발생하는 것으로 판단한다.

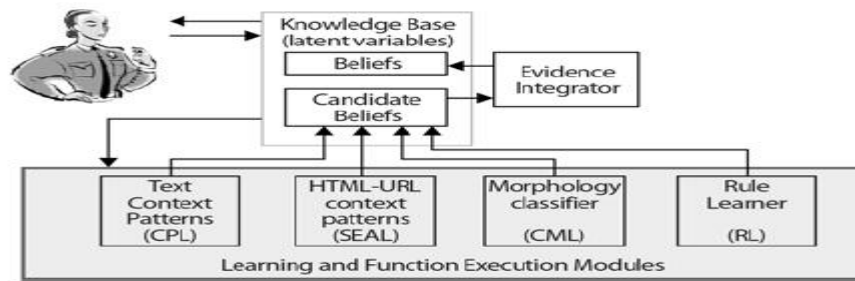
o 태도 휴리스틱(attitude heuristic)은 어떤 사건이나 상황을 평가할 때 사물들을 좋아하는 부류와 싫어하는 부류로 나누어 판단을 하는 성향이다. 어떤 사람을 좋아하면 그 사람의 성적도 좋았을 것으로 판단하고, 어떤 사람을 싫어하면 그 사람이 과거에 품행이 나빴을 것으로 판단하는 편향이 높다. 태도 휴리스틱(attitude heuristic)은 논리와 추론에 영향을 크게 미치며 다른 차원은 후광효과(halo effect)이다. 후광효과(halo effect)는 사람에 대한 호의적 비호의적 일반적 인상이 그 사람에 대한 추론과 미래의 기대에 영향을 미치는 편향이다.

## 2. 빅데이터 기반 기계 학습(machine learning)

머신러닝(machine learning) 또는 기계 학습(機械 學習)은 인공지능의 한 분야로, 컴퓨터가 학습할 수 있도록 하는 알고리즘과 기술을 개발하는 분야를 말한다. 가령, 기계 학습을 통해서 수신한 이메일이 스팸인지 아닌지를 구분할 수 있도록 훈련할 수 있다. 기계 학습의 핵심은 표현(representation)과 일반화(generalization)에 있다. 표현이란 데이터의 평가이며, 일반화란 아직 알 수 없는 데이터에 대한 처리이다. 기계 학습은 충분한 학습 데이터로부터 모델을 생성하고, 해당 모델을 통해 대용량 데이터를 자동 분석, 귀납 추론하는 시스템을 의미한다. 통상 SVM과 같은 통계 이론에 기반하며, 자동 분류, 자동 군집, 베이지안 네트워크 기반 추론 등 강력한 데이터 분석 기능을 제공한다. 빅데이터에 기반한 프로젝트는 주로 대용량 색인/검색과 같이 현재 처리하기 힘든 대용량의 빅데이터를 효율적으로 처리하는 것에 대한 것이 많기 때문에, 기계학습 기법에 기반한 프로젝트는 상대적으로 많이 진행되고 있지는 못하고 있다. NELL(Never Ending Language Learner) 프로젝트에 대해 소개한다.

### 가. 기계학습 기법에 기반한 NELL Project

CMU의 Tom Mitchell이 주관하는 NELL 프로젝트는 영속적인(never-ending) 기계학습 시스템을 구축하는 것을 목표 비구조 웹페이지로부터 구조화된 정보를 추출할 수 있는 능력을 갖추고 있다.



(\* 주 : 전자통신동향분석 제27권 제5호 2012년 10월)

(그림 4-4) NELL 시스템의 구조

이 능력은 시스템 구축 초기에 주어지는 person, sportsTeam, fruit, emotion과 같은 범주(category)를 정의한 ontology와 이에 대한 관계들을 정의한 seed로부터 시작하여 스스로 검증과정을 통해 구조화된 정보를 추출할 수 있는 belief를 자가 학습한다.

## 나. 데이터마이닝 분석 기법

### (1) 예측분석과 실시간분석

빅데이터 분석에는 여러 가지 기법들이 사용되지만 일반화된 분류 방법이나 기술체계는 존재하지 않는다. 사용되는 서비스의 종류나 성격에 따라서 적용되어야 할 기법이 달라지며, 이러한 이유로 금융서비스에서 빅데이터를 분석하기 위해서는 빅데이터 분석전문가의 역할이 필요하다. 빅데이터에서 예측분석(Predictive Analytics)기법은 고객의 신용카드 사용액 대비 연체율 등으로 신용도를 예측하거나, 새로운 금융상품에 대한 매출을 예상하는 등 기존의 데이터로 미래를 예측하여 의사결정을 지원하는 방법이다. 기존 데이터 분석이 데이터들의 연관성이나 통계적 규칙성을 찾아 현황을 분석하는 것이라면, 예측분석은 과거의 데이터로 미래의 상황을 예측하여 선제적인 의사결정을 지원하는 것이 목적이다. 소셜



네트워크(SNS)분석 등이 향상된 예측 분석 기법 중 하나로, 사용자들 사이의 관계와 특정 서비스에 대한 평판 등 여러 가지 상황을 분석하여 미래를 예측하는 기법이다.

## (2) 예측분석

미래 발생 가능한 사건의 확률이나 경향에 대한 분석으로 데이터마이닝의 한 가지 분야이다. 결과에 영향을 미치는 여러 변수들을 분석하기 위해 클러스터링, 의사결정나무(Decision Tree), 회귀분석(Regression), 신경망(Neural Network), 유전자 알고리즘(Genetic Algorithm)등 다양한 기법들이 사용된다. 예측분석은 예측모델에 적합한 데이터 결정을 위한 ‘데이터 탐색’ 단계, 분석 대상에 적합한 모델을 생성하고 검증하는 ‘모델 개발’ 단계, 그리고 생성된 모델을 실제 서비스 환경에 적용하고 필요한 지식을 추출하는 ‘모델 적용’ 단계, 그리고 개발한 모델의 성능을 개선하고 불필요한 요소를 제거하는 ‘모델 관리’ 단계로 나누어진다. 데이터마이닝 기법으로 기존의 데이터들의 특성 및 상관관계를 분석하여 앞으로의 활동이나 결과를 예측하는 분석방법으로 시계열 분석을 포함한 예측분석의 실전을 학습하게 된다

## (3) 실시간 분석

다른 분석 기법들과는 달리 환율변동이나 주식시황 분석 등 정확성 보다는 즉시성을 요하는 서비스에 필요한 기법이다. 실시간 분석을 위한 기법으로는 데이터베이스 빠른 처리를 위해 메모리를 활용하는 인 메모리 분석, 다중 프로세스를 활용하여 대량의 데이터의 병렬처리를 지원하는 MPP(Massively Parallel Programming) 등이 활용된다. 구글 분산시스템의 특징은 스케일 out방식을 사용한다는 것인데, 여러 시스템을 분산 운영하기 위해서는 특정시스템에 대한 장애가 발생할 수 있다는 사실을

전제로 처리가 되어야 한다. 분산시스템에서는 한 시스템의 장애가 특수한 상황이 아니라 일반적인 상황이 될 수 있으므로 이러한 장애 발생에서 유연하게 대처할 수 있는 장애투명성을 지원하는 기술이 필수이다. 빅데이터 처리에 있어 맵리듀스를 이용한 플랫폼을 구축하는데 있어서 가장 많이 사용되는 오픈소스는 하둡(Hadoop)이다. Hadoop은 2005년 처음 개발되어 현재 Apache로 넘어가 오픈소스로 개발되고 있다.

#### (4) HDFS(Hadoop Distributed File System)

Hadoop을 이용한 분산 저장소를 HDFS(Hadoop Distributed File System)이라 한다. Hadoop은 현재 아파치에서 운영되고 있으며 구축 대상 데이터는 Hadoop 분산 파일 시스템(HDFS)에 로딩 되어야한다. 위키본의 보고서에 따르면 현재 IT비용에 대한 문제점을 지적하며 대안으로 Hadoop을 제안하고 있다. 보고서는 현재 빅데이터를 운용하는 대부분의 기업들이 Hadoop에서 실행하고 있으며, 2014년 6억 2천 1백만 달러에서 2017년이면 16억 달러의 시장을 형성할 것이라는 전망을 내놓았다. 결국 Hadoop의 이용은 기존 RDBMS보다 비용적인 측면과 확장성, 유연성 등 기능적인 측면으로도 장점이 크기 때문에 빅데이터를 활용하려는 다양한 기관에서 많은 사용이 예상된다.

다. 빅데이터 분석에 활용되는 R프로그래밍

데이터분석 패키지로 SPSS, SAS, R프로그래밍 등이 활용되고 있다. 최근 비 정형화된 데이터를 분석하는 플랫폼(하둡 등) 기술이 나오면서 이와 연동할 수 있는 분석 패키지의 요구 역시 늘어나게 되었다. 무료 오픈소스 + 빅데이터 하둡 플랫폼과의 연동 등으로 통계패키지 R프로그래밍의 활용도가 늘어나고 있다.

o 통계 및 분석가를 위한 데이터마이닝

통계 및 분석가는 분석 데이터를 기준으로 회귀분석, 다중분석, 시계열 분석등의 기법을 활용하여 목적에 맞게 분석을 하는데, 보다 편리하게 구현하기 위해 통계프로그램을 활용한다.

o R프로그래밍을 활용한 데이터마이닝

데이터 분석은 파이썬을 포함한 프로그래밍 언어로도 가능하다. R 역시 프로그래밍 언어이지만, 문법자체가 타 언어에 비해 간결하기 때문에 기본 명령어 정도만 학습해도 패키지 안에서 기본적인 분석이 가능하다.

### 3. 인텔리전스(intelligence) 정보 변환

#### 가. 데이터 정제 기술

빅데이터는 말 그대로 기존의 일반적인 방법으로는 처리하기 힘든 방대한 규모의 데이터이다. 이러한 데이터들을 처리하기 위해서 구글은 맵리듀스를 만들어 냈으며 이 기술은 대용량의 데이터를 분산컴퓨팅 환경에서 처리하기 위해 개발되었고 빅데이터 정제 기술의 근간이 되는 기술이다. 사실상 맵리듀스는 빅데이터 처리의 실제적인 표준이라고 할 만큼 널리 사용되고 있다. 맵리듀스 기술이 사용되면서 스토리지(Storage), 맵리듀스(MapReduce), 쿼리(Query)의 세 단계 층으로 이루어진 빅데이터 시스템 스택 개념이 소개되었다. SMAQ(Storage, Mapreduce and Query)로 불리는 이 시스템 스택은 오픈소스로 Hadoop 기반의 아키텍처와 함께 빅데이터 정제 기술로 다양한 시스템에 널리 사용되고 있다.

#### 나. 맵리듀스 동작 과정

맵리듀스 기술의 핵심은 대량의 데이터 집합에 대해 쿼리를 입력받아 분할 후 병렬로 처리하여 필요한 정보만 추출하는 기술이다. 머신 데이터(machine-generated data)는 빅데이터 중에서도 가장 성장 속도가 빠

르고 복잡한 분야이다. 또한 모든 사용자 트랜잭션, 소비자 행동, 기계 동작, 보안 위협, 부정행위 등에 대한 정확한 기록이 포함된 가장 가치 있는 데이터이다. 금융보안에는 창의적인 보안 대응 방법이 필요하며 이를 위해서는 빅데이터 분석을 중심으로 한 지능형 보안시스템 구축이 필요하다. 가트너 그룹에서는 빅데이터 분석을 활용한 보안 분석을 통하여 예전에 보이지 않았던 사고패턴을 발견하고, 정보 보안을 포함한 기업경영에 대한 선명한 통찰력을 제공함으로써 기업의 비즈니스 가치를 높일 수 있다고 예측 하고 있다. 맵리듀스는 Map 과정과 Reduce 과정으로 이루어진다. ‘Map 과정’은 ‘Split input’ 단계, ‘fork processes’ 단계와 ‘Map’ 단계로 구성되고 ‘Reduce’ 과정은 ‘Partition,’ ‘Sorting’, ‘Sorting’ 으로 수행된다.

- o ‘Map 과정’,

수많은 데이터들로부터 데이터를 읽어 ‘Map 과정’ 특정 주제인 키와 그 키에 해당하는 데이터의 형태로 분류하는 과정이다

- ‘Split input’ 단계는 대규모의 데이터를 분할 처리하기 위해서 입력 데이터를 작은 크기로 분할하는 단계이다.
- ‘fork processes’ 단계는 분할된 입력 데이터들을 여러 작업자에게 분배하고 진행을 추적하는 단계이다.
- ‘Map’ 단계는 데이터를 읽고 파싱하여 실제 키 값과 데이터 쌍을 생성하는 ‘Map’ 단계를 거치게 된다.

- o ‘Reduce’ 과정

중복되는 값은 병합하여 노드를 줄이는 과정이다

- ‘Partition’ 단계는 Reduce 과정’의 Map 과정에서 생성된 키와 값의 쌍을 메모리와 분할된 디스크 영역에 저장하는 단계이다.
- ‘Sorting’ 는 데이터를 키 값에 의해 정렬하는 단계이다.
- ‘Reduce’ 과정은 동일한 키와 값을 병합하는 과정을 거치게 된다.

## 제 6 절 사기방지 대응 환경 진단

### 1. 개 관

국내의 경우 이상행위 정보 공유를 위한 시스템을 구축을 진행하고 있으며, 반면 해외에서는 국가적 차원에서 정보 공유를 위한 체계를 구축하여 운영하고 있다.

금융위원회, 금융감독원은 FDS 구축을 사실상 의무화했으며 금융보안원은 미국 연방금융기관검사협의회(FFIEC)지침을 벤치마킹해 기술가이드 라인을 마련하였다. 고객정보나 공인인증서 유출 등 금융 보안에 대한 금융사고가 끊이지 않자 금융당국은 카드사, 보험사에 구축된 FDS를 은행, 증권을 비롯한 전 금융권으로 확대하도록 권고한 바 있다. 특히 은행서비스 관련 FDS의 경우 이미 알려진 패턴에 대한 금융사기를 막는 수준으로는 앞서 나가는 금융사기 피해의 방지나 관제 기능이 충분하다고 볼 수 없다. 은행 서비스별로 특성을 반영해 이상 징후를 분석하는 기술 수준까지는 구현되지 않는 실정으로 이에 대한 대안이 시급하다. 특히 2014년 하반기에 발생한 ‘농협 1억2천만 원 인출사고’가 대대적으로 언론에 보도되면서, 일반인들의 금융사고에 대한 관심이 폭증하였고 이에 2014년 12월, 금융감독원은 FDS로드맵을 발표하고 구체적인 구축가이드 라인을 제시하여 금융사의 FDS 조기구축을 권장하였다.

### 2. 정책동향

#### 가. FDS 업무추진계획

- ① 금융감독원 FDS 로드맵 (14~16년)
  - 1단계: 블랙 IP/MAC 기준 차단(14년)
  - 2단계: 금융거래분석 후 차단(15년)
  - 3단계: 전 금융권 공동대응체계 구축 (16년)
- ② FDS 구축완료 인정 범위 - 블랙 IP/MAC차단까지는 FDS 완료가 아  
님
  - 지속적인 이상금융거래유형 분석/적용/ 차단 체계가 구축되어야 완  
료
- ③ 그 외 금감원 입장
  - 기본적으로 전자금융사기는 금융회사 책임
  - FDS Rule의 공개를 가용할 수 없음
  - 15년 상반기에 구축시작 권고

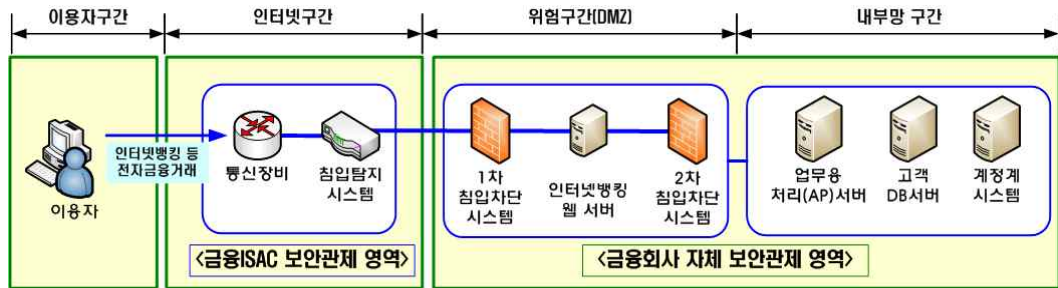
#### 나. FDS 로드맵

- 1단계 : FDS 도입, 전자적 장치의 접속정보 수집.이상금융거래 분석  
및 차단
- 2단계 : FDS 확대(2015년), 금융거래정보까지 확대.이상금융거래 분  
석 및 차단 .FDS 분석 및 상담전문인력 보유
- 3단계 : 금융권 공동대응(' 16년), FDS 전문인력 확대.금융권 공동대  
응체계 구축.관련법규 개정

#### 다. 「침해사고 대응 전담반」

인터넷뱅킹, 사이버트레이딩 등 IT기반의 금융거래 환경하에서는 크고  
작은 사이버위협이 지속적으로 발생한다. 그러나, 금융회사 침해사고 발

생시 체계적인 초동 조치·신속한 사고원인 분석·대응을 위한 상시 전담조직이 부재상태이다. 침해사고 발생시 사고조사·원인분석 등 긴급조치를 수행할 수 있도록 금융ISAC에 전문 보안인력을 확보한 전담조직을 운영한다. 침해사고는 발생 현장 출동, 사고조사·원인 분석, 긴급 대응 조치 등 고도의 전문성이 요구되는 업무이다.



(그림 4-5) 금융권 침해대응 모니터링 체계

라. 금융권 FDS 추진 협의체

2014년 12월부터 금융감독원을 주축으로 이상금융거래 탐지시스템 구축 및 고도화를 위해 ‘FDS 추진 협의체’를 구성하고 금융권 FDS 고도화 로드맵 1.0을 발표하였다. 금융회사간 FDS 구축·운영 관련 노하우 공유 및 FDS 공통기준을 마련하고, 금융회사의 신속한 전자금융사고 탐지 및 대응체계를 조속히 갖추도록 유도한다.

**[금융권 FDS 추진 협의체 구성]**

- 금감원(IT감독실) : 금융권 FDS 로드맵 추진 총괄
- 금융회사\* : FDS 구축 문제점 및 운영사례 공유 등

\* 초기 회원사는 은행(국민, 우리, 신한, 하나, 기업) 및 증권(대우, 대신, 삼성, 우리, 미래) 10개사로 구성하고, 향후 참가를 원하는 금융회사는 자율적 참여 가능

\* 업무 조정과 조직 개편

금융위원회는 카드사 정보유출 사태 이후인 2014년 2월 20일 금융보안원에 금융ISAC을 통합해 금융전산보안 전담기구로 지정했다. 금융전산보안 전담기구는 상시 모니터링을 통해 해킹 등 침해사고에 대한 예방·경보·분석·대응의 일관적 체계를 구축하고 모니터링 범위를 전 금융사로 확대해 시행하는 금융전산 보안관계 역할을 비롯해, 보안인증제 운영, 보안정책 연구·교육, 보안전문인력 양성 등을 제공한다.

마. 2015년 금융 IT 감독 정책

규제 패러다임에서 자율과 책임중심으로 전환, 오프라인 위주의 금융제도 개편, 핀테크 산업 성장 지원 등을 추진하고 이를 위해 전자금융거래에 대한 보안강화를 위해 금융권 이상금융거래탐지시스템 구축 및 고도화 등을 중요한과제로 인식하고 있다. 정책방향은 규제패러다임에서 자율과 책임중심으로 전환, 오프라인 위주의 금융제도 개편, 핀테크 산업 성장 지원 등이며 주요내용은 신규 전자금융거래에 대한 보안성 심의 전면 폐지, 사후 점검강화로 보안성 심의 대체, 특정 기술 사용의무 폐지, 액티브 X 퇴출 등 기술 중립성 원칙 구현, 전자금융서비스에 대한 보안강화(금융권 FDS 구축 및 고도화, 시장 자율적 금융보안 인증체계 도입 등), 금융업계와 소통 활성화, 비상사태시 관련 유관기관과 공동 대응 체계 강화, 핀테크 생태계조성 지원(금융회사 및 전문가의 기술진단), 처리절차 간소화 등 정보처리 및 전산설비 위탁규정 개정 등 이다. 금융전산 보안강화 종합대책'을 통해 금융회사의 망분리 가이드라인을 발표하고 2015년까지 금융회사의 전산시스템 망분리를 의무화했다. 이에 따라 금융회사 전산센터는 의무적으로 물리적 망분리를 완료해야 하고 각



은행 본점 및 영업점은 2015년 말, 제2금융권은 2016년 말까지 망분리 방식을 선택 이행해야한다. 지속되는 금융사기 방지를 위해 2014년도 말까지 은행권에 이상금융거래 탐지시스템(FDS)를 구축하도록 권고했다.

#### 바. 2016년 금융 IT·보안 10대 이슈 전망

금융보안원은 연간 금융 IT·보안 주요 트렌드 분석을 기반으로 2016년도 10대이슈 도출을 통해 금융 IT·보안의 정책 방향 및 전략 수립 지원한다. ‘선정기준 개선’, ‘객관성 및 신뢰성 확보’, ‘주요이슈 전망도출’을 통해 보안담당자는 물론, 최고경영 층(CxO)도 관심가질 수 있도록 추진한다. 주제선정에 있어서 보안기술은 물론 정책적 이슈도 적극적으로 고려하며, 흐름 파악은 물론 의사결정에 도움이 될 수 있는 구체적인 이슈를 선정한다. 빅데이터 분석, 전문가 패널 검토를 통해 결과의 신뢰성을 확보한다. 2016년 금융 IT·보안 10대 이슈 전망에 의한 이슈는 다음과 같다.

- (1) 핀테크 서비스 확대와 보안성 요구 증가
- (2) 금융거래 정보를 이용한 빅데이터 활성화
- (3) 바이오인증(FIDO 등) 기술을 활용한 금융서비스 확대
- (4) 실명확인 방식 전환에 따른 비대면 금융거래 확산
- (5) 금융권 자율보안체계 확립과 금융 보안거버넌스 강화
- (6) 블록체인을 활용한 금융서비스 본격 등장
- (7) 클라우드 서비스 활성화를 위한 보안 투명성 요구 증대
- (8) 모바일 및 표적형 랜섬웨어 증가
- (9) 진화된 기법을 활용한 DDoS 공격의 지속 시도
- (10) FDS 구축 확산과 위협정보 공유 확대

#### 3. 사기방지 인프라 구축 상황

#### 가. 금융보안원의 FDS 정보공유 시스템

금융보안원에서는 FDS 정보공유 시스템을 구축하였으며, 구축 완료시 각 금융회사에서 탐지된 이상행위 정보 혹은 의심되는 정보를 금융회사 간 공유한다. 또한, 유관기관 및 관련 기업으로부터 사이버 위협 정보를 수집·공유함으로써, 효율적이고 선제적인 대응이 가능하도록 한다. 이를 위해서는 이상행위의 탐지 정보의 표현 규격 및 전송 규격을 만듦으로써, 효율적인 정보공유가 이루어 질 수 있도록 한다.

#### 나. 한국인터넷진흥원의 사이버위협정보 분석 공유시스템(C-TAS)

2014년 8월, 한국인터넷진흥원(KISA)에서 사이버 침해 사고에 대한 신속한 대응을 위해 각종 사이버위협 정보의 수집·분석·공유체계를 고도화한 사이버위협 정보 분석·공유 시스템인 ‘C-TAS(Cyber Threats Analysis System)’를 본격적으로 운영하였다. C-TAS는 사이버위협 정보(악성코드 정보, 명령제어 서버 정보, 취약점 및 침해사고 분석정보 등)를 체계적으로 수집하고, 종합적으로 연관 분석해 관계기관 간 자동화한 정보공유를 목적으로 한다. 공유 정보는 5개 그룹(위협 도메인·IP, 사이버사기 도메인·IP, 악성 파일, 취약점, 보고서) 36종 정보(악성코드 유포지, 경유지, C&C, 공격 IP, 피싱, 파밍, CVE, PoC, 기술문서, 분석보고서 등)를 공유하고 있으며, 점차 수집·공유 항목을 확대 추진하고 있다. 외부로 제공되는 정보는 업종별로 상이하다.

#### 다. 사이버 위협 정보 표현 규격 CTEX(Cyber Threat Expression)

각종 침해정보는 사이버 위협 정보 표현 규격 CTEX(Cyber Threat Expression)으로 표시되어 통일된 형태로 자동 작성될 수 있도록 하며, 외부 기관으로 자동으로 전파될 수 있도록 한다. C-TAS와 C-TEXT는 유

기적으로 연결된 침해사고 전반을 바라볼 수 있는 눈을 가지게 된 것으로써, 사고 발생 전 사이버테러 이상 징후를 파악하여 선제적으로 대응하여 피해를 최소화하기 위해 노력하고 있다. 현재 국내 금융권에서는 이상행위 탐지 정보 공유 시스템을 구축함으로써 체계적인 대응을 위한 첫 걸음을 나아가고 있다. 금융권에서 이 기술을 활용하여 이상금융거래 탐지시스템, 보험사기 예방시스템, 카드부정 적발시스템, 내부자 부정행위 적발, 개인정보 부정 사용방지 등 보안 전반적인 분야에서도 널리 사용되고 있다. 국내 금융권의 경우 공동으로 이상행위를 대응하기 위한 공유 시스템 마련이 미흡하다. 비금융권의 경우 한국인터넷진흥원에서 사이버 위협 정보를 공유하기 위해 시스템을 구축함으로써, 효율적으로 사이버 위협을 대응하기 위해 노력하고 있다.

#### 라. 표준화 동향-이상 금융거래의 탐지 및 대응 방법

이상 금융거래의 탐지 정책 및 방법은 이용 환경, 거래 패턴, 거래 사전 행위에 의해 종합적으로 결정이 되어야 하며, 각각의 허용 범위에 따라 이상금융거래 여부를 판별하는 탐지 방법이 결정되어야 한다.

##### (1) 이상 금융거래 탐지·대응 시스템

이상 금융거래 탐지·대응 시스템은 타 도메인 정보 공유 시스템과 이상금융거래 탐지 관련 정보를 교환하는 탐지정보 공유 모듈과, 금융거래 차단 정보관리 모듈, 탐지 정책 관리 모듈, 이상 금융거래 탐지 모듈, 금융거래 분석 모듈, 이용정보 수집모듈, 이용자 추가인증 모듈, 통계 분석 모듈 및 금융거래 패턴 정보 저장소, 금융거래 이용정보 저장소, 금융거래 차단 정보 저장소로 구성되어 있다. 만약 공격자에 의한 금융거래 시도가 이상금융거래 탐지 정책을 기반으로 하여 각각의 저장소에 저장된 정보와 비교분석을 통해 이상금융거래에 대한 징후로 판단이 되고, 이용

자의 추가인증을 통하여 이상금융거래로 탐지가 된다면, 이러한 탐지 정보는 타 도메인 정보 공유 시스템과 연계하여, 공격자가 타 도메인의 금융거래에 대한 공격 시 이를 사전에 차단할 수 있게 된다. 이러한 이상금융거래 탐지·대응 시스템의 자세한 기능은 아래와 같다.

- 금융거래의 공격자에 의한 금융거래 시도 시 이상금융거래 탐지·대응 시스템은 이용자의 금융거래 이용 환경, 거래 패턴, 거래 사전 행위 정보를 추출하여 저장한다.

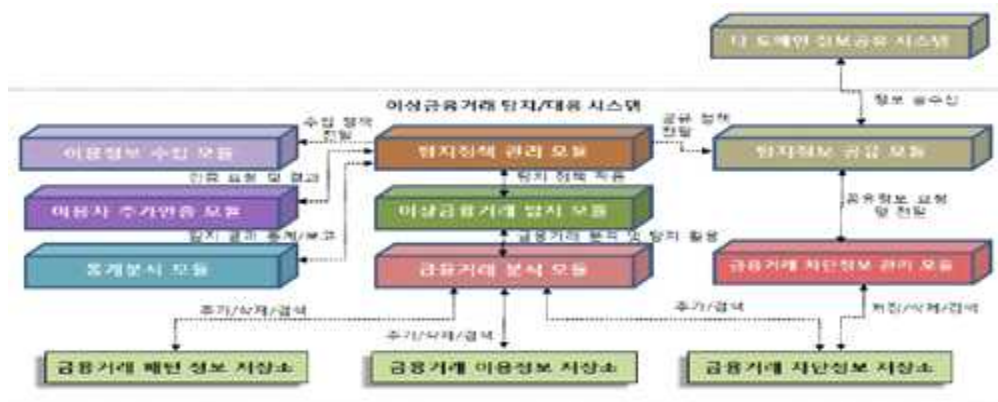
- 탐지 시스템은 사전에 저장되거나 정의된 금융거래 차단정보, 사전 행위 분석, 이용자의 거래 패턴 정보를 이용하여 이상금융거래 여부를 검사한다.

- 이상금융거래의 징후로 판단 될 시 금융거래에 이용하지 않은 이용자의 추가 인증방법을 이용하여 금융거래 이용자의 인증을 요청한다.

- 추가인증 결과가 정상 금융거래로 판단될 시 수집된 이용 정보를 정보 저장소에 보관하고, 거래 패턴을 재설정한다. 추가인증 결과가 이상금융거래로 탐지된다면 해당 금융거래를 즉시 차단하고, 해당 이용정보는 금융거래 차단정보에 저장한다.

- 저장된 금융거래 차단 정보는 정보 공유 정책에 따라 타 도메인의 정보 공유 시스템에 전송한다.

- 만약 금융거래 공격자가 같은 이용 정보를 이용하여 타 도메인을 공격한다면 공유된 정보를 이용하여 별도의 추가인증 없이 즉시 금융거래를 차단한다.



(\*주 : 정보통신단체표준(국문표준) TTA.KO-12.0178)

(그림 4-6) 이상금융거래 탐지·대응 시스템의 세부 구조

#### 4. 금융권 FDS 구축동향 (2015년 기준)

##### 가. 금융권 FDS 구축

금융권을 중심으로 이상금융거래탐지시스템 도입이 잇따르고 있는데, 특히 카드사에 비해 이상금융거래탐지시스템 구축 경험이 적은 증권사들은 지난해와 올해 초에 잇따라 이상금융거래탐지시스템 도입을 추진하고 있다. 2015년 3월말 기준으로 27개의 금융회사가 이상금융거래탐지시스템을 구축하였고 국내은행의 경우 17개사 중 10개사(국민, 농협, 부산, 신한, 외환, 하나, 경남, 전북 등)는 시스템을 구축하였으며, 나머지 7개사도 시스템 구축 중이다.

[표 4-5] 금융권 FDS 구축 현황(' 15. 3월말 기준)

권역	구축완료		구축중		계	
은행	10	(58.8)	7	(41.2)	17	(100)
증권	9	(21.8)	23	(71.9)	32	(100)
카드	8	(100.0)	0	(0.0)	8	(100)
기타*	0	(0.0)	2	(100.0)	2	(100)
계	27	(45.8)	32	(54.2)	59**	(100)

\* 신흥중앙회, 저축은행중앙회

\*\* 전자금융이체 비중이 낮은 보험사, 외국은행 지점, 선물회사 등은 조사대상에서 제외

자료: 금융감독원, 표 편집: 오마이뉴스 24

[표 4-6] 금융권의 이상금융거래 탐지시스템(FDS) 고도화 로드맵

단계	1단계 (2014년): FDS 도입단계	2단계 (2015년): FDS 확대단계	3단계 (2016년): 금융권 공동대응단계
수집 시스템	단말기 접속정보 수집	단말기 접속정보 및 금융거래정 보 수집, 과거패턴정보 구축	단말기 접속정보 및 금융거래 정보 수집, 과거패턴정보 구축
분석/평가 시스템	오용 탐지(black list)	오용거래 및 이상거래 탐지	오용거래 및 이상거래 탐지(고 도화), 금융회사간 정보 공유
대응 시스템	차단조치, 추가 인증수단 마련	차단/지연 조치, 추가 인증 조 치, 실시간 처리	차단/지연 조치, 추가 인증 조 치, 실시간 처리
모니터링 및 감사		모니터링 및 상담전문인력 확보	모니터링 및 상담전문인력 확 대, 탐사 결과 감사기능 구현, 관련법규 개정

(\* 주 : 금융감독원)

#### 나. 해외의 정책과 기반 사례

해외의 경우, 범정부적 차원에서 국가기관, 민간기관 등이 상호 협력하여 효율적으로 대응할 수 있도록 정보 공유 시스템을 구축하여 운영하고 있다.

##### (1) 미국 : 사이버 위협 정보 표현/전송 규격

국토안보부(DHS)는 사이버 위협에 효율적으로 대응하기 위해 안전한 정보공유 체계 구축의 필요성을 인지하고, 산하 MITRE를 통해 2013년 4월 사이버 위협 정보 전송 규격인 TAXII(Trusted Automated eXchange of Indicator Information)를 발표하고, 10월에는 사이버 위협 표현 규격인

STIX(The Structured Threat Information eXpression)를 발표했다. STIX/TAXII는 ISAC(Information Sharing Analysis Center) 및 CSIRT(Computer Security Incident Response Team), 정보보호 산업군 등 누구나 사용 할 수 있도록 개발하였다. STIX는 8가지 구성요소로 사이버 위협정보를 구조화하고, TAXII는 실시간으로 공유하기 위한 자동 전송 규격을 지원하기 위해 4가지 서비스 규격을 정의하고 있다. 또한, 참여 조직간 형태를 고려하여 3가지 모델(P2P, 중앙분배형, P2P-중앙 분배 결합형)을 지원한다. 미국의 금융 ISAC에서는 사이버 위협 정보공유 체계를 구축하고 있으며, 이를 금융기업, 지자체, FBI, US-CERT 등이 활용하고 있다.

## (2) 일본 : 사이버 정보 공유 이니셔티브(J-CSIP)

IPA(Information-technology Promotion Agency)<sup>18)</sup> 기관의 J-CSIP(Initiative for Cyber Security Information sharing Partnership of Japan)를 중심으로 정보공유가 이루어지고 있다. IPA는 사이버 공격을 대응하기 위해 5대 산업, 45개 참여기업('13.12월 기준) 정보공유 체계를 발족·운영한다. 정보공유에 대한 정책 및 운영은 IPA와 참여기업 SIG(Special Interest Group)간 NDA를 체결한 것으로 시작되고, 참여기업은 정보 제공처에 대한 정보와 민감한 정보를 익명화하여 탐지된 사이버 공격 정보를 IPA에 제공하면, 분석정보를 추가하여 정보제공자의 승인을 얻어 공유 가능한 정보를 공유한다. 정보공유 체계를 확립한 후 단순히 정보가 공유되는 것이 아니라 공격동향 및 공격의 상관관계에 대해 파악이 가능해졌다. IPA는 통합거점으로 역할을 수행함에 따라 분석정보의 생산 및 향후 예상되는 고격에 대한 대책검토가 가능해졌다.

## (3) 영국 : 다양한 범죄를 예방하기 위해 통합전략을 수립

영국의 사례와 같이 다양한 범죄를 예방하기 위해 통합전략을 수립하고, 개인과 기업을 보호하기 위한 의무로서 적극적으로 개입하였다. 영국정부는 이상행위를 심각한 사회문제로 인식, ‘2005년 Fraud Review’를 시작으로 방지 대책 마련에 본격적으로 돌입하였다. 이후 법 제정(Serious Crime Act 2007)19), 기구 설립, 정보 공유 등을 제안하였으며, 2008년 10월 NFA(National Fraud Authority)가 설치되면서 국가차원에서의 전략 수립, 공·사협조체계 강화, 공·사·민관간 정보공유, 정보공유 시 중복 또는 충돌 문제 해결, 교육 및 홍보 등의 업무를 수행하고 있다.

## 제 7 절 사기탐지 적용 모델과 시스템 사례 진단

### 1. 국내 사례

#### 사례1) 카드사, 부정사용방지시스템

신용카드 사용자의 일반적인 사용 패턴을 인식하고 패턴에서 벗어난 거래가 발생 시 경고를 발생하여 혹시 있을 수 있는 카드 부정사용을 미연에 방지하는 방법이다. 비대면 거래의 문제점을 완화하기 위해 모니터링 요원의 분석과 연계 기관이 유기적으로 연결되고 정보와 데이터가 연결되는 시스템이다. 부정사용방지 룰(Rule)은 misuse detection 기반의 사고 패턴 룰로서 다음과 같은 기능이 중심이다. 카드 승인시 의심되는 거래패턴에 해당될 경우 경보를 발생시키고 논리적으로 발생 불가 패턴, 예를 들어 국내 카드거래 후 1시간 후 원격지 해외 카드거래 시도 등 특이 거래 발생 시 사전 통제 그리고 발생은 가능하나 과거의 패턴을 분석할 때 사고 개연성이 높은 경우 등 이다.



## 사례2) 사고 가능성 스코어링(Scoring) 모형

스코어링 모형(Scoring Model)은 프로젝트를 선택할 때 고려하는 기준을 일컫는 사업 용어이다. 이는 시스템의 다양한 특징에 비중을 부여하고 가중합계를 계산한다. 모든 객관적인 기법들처럼 스코어링 모형의 사용과 관련된 많은 질적인 판단들이 있다. 이 모형을 사용하려면, 쟁점과 기술을 이해하는 전문가가 필요하다. 결과가 얼마나 기준의 합리적인 변화에 민감한지 살펴보려면 기준과 비중을 변화시키면서 스코어링 모형을 몇 번 순환시키는 게 좋다. 스코어링 모형은 시스템 선택의 마지막 중재자라기보다 결정의 확인, 합리화, 지원하는 데 가장 일반적으로 사용한다. 스코어링모형은 데이터분석에 기반하여 구축한 지능형 시스템에 의한 상시 모니터링을 통해 업무 효율성 및 효과성을 극대화시킨 대표적인 사례에 해당하며 일정 기준에서 경고(Alert)를 발생시키는 기능으로 구성된다. 부정사용방지 룰(Rule)은 부정사용으로 예상되는 카드 사용 거래를 사전에 모니터링하여 예방함으로써 카드 사용자, 또는 발급 기관의 재정 손실 리스크를 축소시키도록 하는 기능을 수행한다.

## 사례3) 지식베이스를 활용한 자금세탁방지시스템

국내 및 국제적으로 이루어지는 불법자금 세탁을 적발·예방하기 위한 시스템 도입의 필요성 증대. 특정금융거래정보의 보고 및 이용 등에 관한 법률, 범죄수익은닉의 규제 및 처벌에 관한 법률 제정. 자금세탁방지 시스템은 금융기관이 자금세탁방지제도를 잘 이행하도록 하기 위해 구축하는 지식기반 정보시스템으로 금융기관들은 국제기준에 맞는 체계 및 시스템을 갖출 필요가 대두되었다. 혐의 거래를 적출하여 신속·정확하게 검사하고, 적절하게 보고할 수 있는 지식기반 자금세탁방지시스템을 구축하고 있다. 이 시스템은 KYC(Know your customer)모듈, STR보고를 위

한 TMS(Transaction Monitoring Systems) 모듈, CTR(Currency Transaction Report) 모듈 등으로 구성된다. 룰(Rule)과 스코어링(Scoring) 모형은 이 시스템은 혐의거래를 추출해내기 위한 룰을 생성하고, 룰을 통해 특정 고위험군을 필터링한 후 위험도 점수를 산출하는 모형 구축한다. 모형 모니터링 모듈을 도입하여 상시적인 모형 검증체계를 수립한다.

#### 사례4) 지능형 감사정보시스템

금융환경의 대형화, 겸업화, 글로벌화가 진행되고, 전자금융 등 영업형태가 변화함에 따라 국경 없는 은행 간 경쟁으로 인한 영업점의 공격적 경영이 진행되고 있다.

내부적으로 검사 인력 충원에 한계가 있기 때문에 영업점 감사준비 시 효율성 증진에 대한 요구가 발생하고 있고 횡령/유용 등 사고의 발생 개연성, 부실여신에 대한 우려에 대비한다. 이 같은 필요성에 의해 감사정보시스템 구축을 통한 직접적 기대효과로 사고예방 및 조기 적출, 불건전여신 및 금융사고의 최소화, 감사조직의 운영 효율성 증대, 감사대상 영업점 선정의 합리성, 감사 DB구축으로 검사업무의 효율성 제고, 영업점 업무 경감 등이 있다. 간접효과는 감사업무의 선진화 및 효율화이며 전산화를 통해 사고예방기능을 강화한다. 부정방지 룰은 데이터 분석 룰 베이스(Rule base)를 활용한다. 직원위험요소, 위험거래, 영업점 위험요소 등 위험요소 결합에 의한 필터 룰 베이스를 구축한다. 스코어링(Scoring) 모형은 영업점 모형과 직원모형으로 모형을 구분하여 구축한다. 영업점 모형은 영업점의 직원, 점장, 환경에 대한 고유 위험과 수신, 여신, 외환 등 거래 위험을 결합하여 위험수준을 도출한다. 직원 모형은 인구통계정보, 직무특성 등을 고려하여 직원의 부정위험을 중심으로 위험수준을 도출한다.

## 사례5) 리스크 관리 시스템

고객 및 직원의 사기 또는 부정을 탐지하기 위한 시스템 개발

o 금융지주사인 BB&T는 자금세탁 추적을 위해 분산거래, 송금, 현금 거래 등 다양한 거래내역을 분석한 자금세탁 적발을 통해 수개월이 소요되던 작업을 하루 단위로 단축 - JP모건은 미승인거래 등 직원 비리에 따른 손실 방지를 위해 직원 인터넷 사용 데이터, 이메일 및 전화 기록을 분석하는 등 사내감찰 업무에 빅데이터를 활용한다. 비정형 데이터를 활용해 신용평가모형 개선한다.

(\* 주: 각종 기사와 자료를 분석하여 작성)

## 2. 해외 사례

### 가. 주요 미국은행의 이상금융거래 탐지시스템(FDS)

미국에서는 이미 2003년에 제정된 ‘공정·정확 신용거래법(FACTA)’에 따라 금융사들이 2008년 11월부터 FDS를 필수적용하고 운영 중이다. US Bank와 Net Bank는 룰 기반의 비정상적 금융거래행위를 찾아내는 탐지모형을 도입, 크로스 채널 탐지는 물론 위치정보와 디바이스 정보까지 활용하고 있다. 크로스 채널 탐지는 인터넷 연결뿐만 아니라 자동화기기(ATM 등 사용자 거래 트랜잭션이 발생하는 모든 채널에 대해 탐지하는 방법이다. 위치정보를 이용하여 물리적 및 논리적인 위치 정보에 대한 이상 유무를 탐지하고 디바이스정보를 이용하여 디바이스 쿠키, 브라우저 언어 및 버전, 운영체제(OS) 버전 등의 정보를 통해 사용자 디바이스 프로파일로 활용한다. 금융보안원에서 조사한 주요 미국은행의 이상금융거래 탐지시스템(FDS) 사례를 보면 아래표와 같다.

[표 4-7] 주요 미국은행의 이상금융거래 탐지시스템(FDS) 특성 비교

구분	탐지방법	탐지모델	크로스 채널탐지	위치 정보이용	디바이스 정보이용
Wells Fargo	트랜잭션분석 및 사용자 프로파일 분석 혼용	룰기반 퍼지로지	O	-	-
Bank of America	트랜잭션분석 및 사용자 프로파일 분석 혼용	-	-	O	O
US Bank	트랜잭션분석 및 사용자 프로파일 분석 혼용	룰기반 비정상행위탐지	O	O	O
NetBank	사용자 프로파일 및 트랜 잭션 모니터링	룰기반 비정상행위탐지	O	O	O

(\* 주 : 금융보안원(FSA))

#### 나. 연구보고서를 통해 소개되는 다양한 제안들

사례1) 데이터를 제시하는 온톨로지 그래프(DOI : 10.5121 /ijsptm. 2012.1501 1 CREDIT CARD FRAUD DETECTION BASED ON ONTOLOGY GRAPH)

온톨로지는 주로 다음 세 개의 에이전트, 즉 클래스 사이의 관계를 묘사, 인스턴스 사이의 관계를 묘사, 클래스, 속성과 인스턴스 사이의 관계 묘사에 의해 제공된다. 온톨로지 그래프는 데이터를 표시하는 데 필요한 그래프가 작성되어 특정한 이벤트에 대해 트랜잭션이 발생되고 사용자 데이터가 작성 완료되면, 사기 검출 프로세스는 사기 검출에 필요한 온톨로지 그래프를 저장하고 모델링한다. 데이터간 연관성이 성립되어야 그래프에서 모델링이 가능하다. 사기탐지 시스템에 의해 제안된 프레임워크를 정의하는데 예를 들면, 신용카드 소유자는 신용의 기간 동안 자신의 필요에 따라 자신이 좋아하는 행위를 하고 그 결과는 이벤트 트랜잭션이 발생한다. 특정 계정번호에 대한 카드 사용, 사용자가 수행한 모든 이벤트 트랜잭션이 채집되고 데이터화 된다. 그래프 형태로 트랜잭션이 저장되며 이 결과는 행동 레지스터를 생성시킨다. 이것이 사건 프레

임 워크이다. 신용카드 사용과 관련된 거래에서 사기탐지가 표시된다.

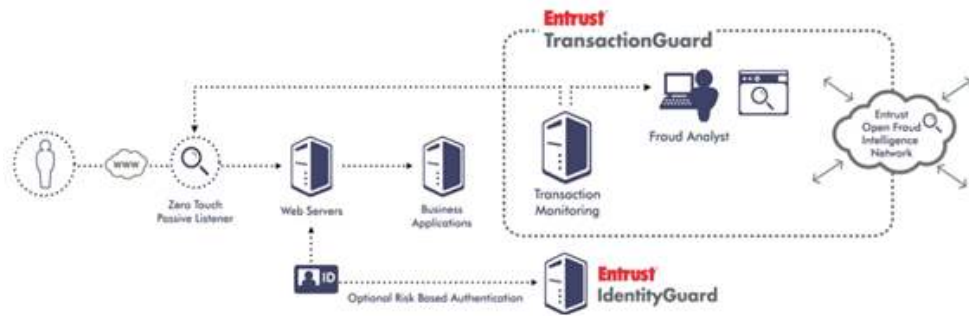
(\* 주 : International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 5, October 2012)

사례2) 제로 터치 사기탐지(Addressing Online eCrime: Layered security for addressing fraud today ... and adapting to tomorrow)

온라인 범죄자는 반복적으로, 피싱을 포함한 정교한 공격을 통해 기존의 인증 안전장치를 우회한다. 사기전술이 빠르게 발전하기 때문에, 사기탐지 솔루션은 행동의 패턴보다는 개별 트랜잭션을 분석해야 한다. 특정 고위험군 트랜잭션은 미리 정의된 업무 절차에 따라 식별되고 더 가까운 평가 플래그가 되어야 하지만, 고급 사기 검출 뿐만 아니라 거래의 패턴을 평가하고, 간섭 없이 동작 할 수 있을 것이다. 사기행위 탐지 솔루션은 트랜잭션을 평가하는 실시간 또는 배치 모드에서 작동 할 수 있어야 하고, 완전한 트랜잭션 패턴 흐름의 작은 서브 세트를 분석 할 수 있는 능력을 가져야 한다. 사기탐지 솔루션은 침입자의 액세스 패턴을 평가하고 사기행위의 잠재적인 새로운 패턴을 연구하는 모니터링 및 포렌식 도구를 제공한다. 따라서 사기탐지 솔루션은 빠르게 온라인으로 생성된 대규모 트랜잭션 볼륨을 처리 할 수 있는 강력한 분석 엔진을 동반해야 한다. 효과적인 사기탐지 방법은 현재 시도되고 있는 사기행위를 차단하고 앞으로의, 사기 행동 패턴을 예견하는 정보를 공유한다.

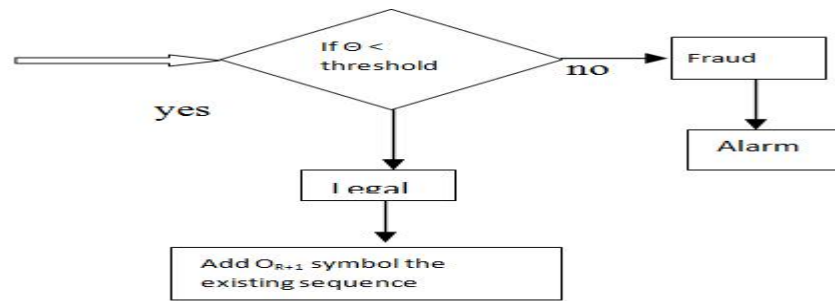
(\* 주 : [www.entrust.com](http://www.entrust.com))

사례3) 온라인 거래의 확률 신용카드 사기탐지 시스템(Probabilistic Credit Card Fraud Detection System in Online Transactions)



(그림 4-7) Zero Touch Fraud Detection & Analysis

오늘날 전자사회 환경에서 인터넷을 활용한 전자상거래의 급속한 발전으로 구매를 위한 신용카드의 사용이 편리하고 필요하게 되었다. 그것은 신용카드와 직불카드, 영국, 스페인, 프랑스에서 순환 카드가 있다는 것을 보여주고 있다. 신용카드 기반 구매는 물리적 카드와 가상 카드 두 가지 유형으로 분류 될 수 있다. 사기 거래를 수행하기 위해 공격자는 신용카드 정보를 도용한다. 신용카드 사용자의 수는 전세계적으로 증가함에 따라 다양한 비즈니스 활동에 사용된다. 사기행위는 연속적으로 신용카드의 사용을 통해 사기를 수행한다. 신용카드 거래의 증가는 사기자의 신용카드번호 도용을 위해 더 많은 기회를 제공한다. 개인과 기업에서 사용하는 온라인 데이터베이스는 컴퓨터 침입에 의해 저장된 신용카드번호가 유출 되고 손상되어 보안의 취약점이 될 수 있다. 신용카드사 기검출시스템(CCFDS)은 가능한 신속히 활용되어 부정이나 비정상 트랜잭션을 식별함으로써 부정 검출을 수행 하도록 시도하는 컴퓨터 프로그램이다.



(\* 주 : International Journal of Software Engineering and Its Applications Vol. 6, No. 4, October, 2012)

(그림 4-8) The Architecture of Detection Phase

사례4) 그래프 기반의 사용자 행동분석방법 모델(Graph-Based User Behavior Modeling:From Prediction to Fraud Detection )

어떻게 이상, 사기, 스팸 이메일을 탐지하는가? 어떻게 사용자의 환경을 모델링 할 수 있는가? 어떻게 사기 행동을 탐지하기 위한 모델을 수정할 수 있는가? 본 연구는 이상 및 사기를 탐지하기 위한 모델링을 사용자 행동에 대한 그래프 분석 도구로 연결하여 수행하는 방법론이다. 특히 정적으로 서브 그래프 분석 응용프로그램, 라벨 전파 및 잠재 요인 모델에 초점을 맞춘다. 본 연구에서는 제안되는 각각의 방법론에 대해 간략한 알고리즘을 설명한다. 이어서 모델을 이해하고 예측하는 기술을 위해 사용하는 최근 연구의 사례를 제공한다. 사기를 탐지하기 위해 사용되어 왔던 관점은 이상행동 이해와 사기탐지이다. 이같은 논리의 진행에는 일반 사용자 행동 모델링, 데이터마이닝과 기계 학습, 현장 환경, 사용자 동작 이해 방법이 사용된다. 정상적인 동작을 일반적 사용모델로 제시할 것이다.

(\* 주 : [http://www.cs.cmu.edu/~abeutel/kdd2015\\_tutorial/tutorial.pdf](http://www.cs.cmu.edu/~abeutel/kdd2015_tutorial/tutorial.pdf)

Christos Faloutsos Carnegie Mellon University, [christos@cs.cmu.edu](mailto:christos@cs.cmu.edu) March 2015 Ab)

사례5) 전문가의 Heuristics을 모델화 할 수 있는 지식공학 능력

기능 솔루션의 핵심 원칙에 대한 주요 고려 사항 (Key considerations for the functional solution Core Principles)은 다음과 같이 정리된다. 오용과 사기의 차이를 이해한다(Understand the difference between abuse and fraud). 사기는 직접 금융 이익을 위한 의도적, 고의적, 지속적 행위(Fraud: knowingly, intentionally, willfully, ongoing for direct financial gain)이다. 오용은 과도한, 부당한, 잠재적이지만 당장 필요하지 않은 행위(Abuse: excessive, unwarranted, potentially not needed)이다. 업계의 벤치마크, 포트폴리오 분석 및 비교를 통해 보험 회사에 실제적인 통찰력을 제공한다(Provide practical insights to insurers, through portfolio analysis and comparison to industry benchmarks). 유통/보험/클레임 처리, 브로커/에이전트/보험/TPA/조절기 및 기능에서 모든 수준에서 배포할 수 있는 도구를 제공(Deliver tools that can be deployed at all levels, ie: broker / agent / insurer / TPA / regulator and across functions - distribution / underwriting / claims processing)한다..

(\* 주 : Cognizant Fraud Control - IT Interventions and Solutions 2011)

## 제 8 절 사기탐지 알고리즘과 기술 진단

### 1. 개 요

알고리즘이란 작업을 수행하기 위한 과정으로서 Software를 개발하기 위해서는 알고리즘들에 대한 총체적 관리가 필요하다. Software의 바른 동작을 위해서는 알고리즘 작성이 중요하며 복잡하고 어려운 작업일수록 높은 수준의 알고리즘 아키텍처가 필요하다. Software의 개발은 부가가



치가 높은 창조적인 활동으로서 보안, 게임, 교육 등분야별 Software의 전문성의 차이는 매우 크다. 사기탐지 알고리즘과 기술 적용방법 도출은 이 분야에 대한 다양한 기술에 대한 깊은 이해가 바탕이 되어야 하며 각 방법론에 대한 분석에서부터 출발한다. 따라서 알고리즘과 방법론의 대안을 도출하기가 결코 용이하지 않은 분야이다. 방법론 분석은 대상 업무의 현황을 파악하는 것부터 시작되므로 위험을 탐지하기 위한 전체 업무 프로세스를 이해해야 한다. 금융업무의 경우 부정 거래 탐지 외에도 전자금융 사기에 대응하기 위해 보험 가입 등 리스크 관리 방안을 마련해 소비자를 보호하고 보안 사고에 따른 대책을 구축해 두는 것이 필요하다. 적용방법론 진단은 학문적인 이론보다는 분석방법이 추구하는 목적이 무엇인지, 활용사례는 무엇이며 어떠한 성과를 거두는지가 중요하므로 목적에 따라 장단점과 수행방법론을 도출하였다.

## 2. 사기탐지에서의 지식공학(Knowledge Engineering)

### 가. 인공지능 기술

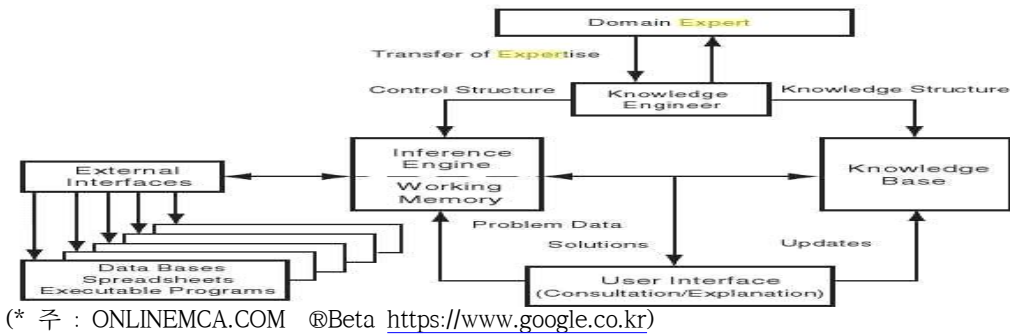
인공지능 기술 AI는 인간의 학습능력과 추론능력, 지각능력, 이해능력 등을 실현하는 기술로서 모든 사물간 통신이 가능한 무선 네트워크를 기반으로, ‘Smart Information’을 활용한 ‘Actuator’와 ‘Context’로 구성된다. ‘Smart Data’는 정보 스스로가 의미를 갖는 것으로, AI의 기본적인 단위이며, ‘Context’란 서비스가 제공되는 상황이나 맥락을 이해하고 해석하는 것이다. ‘Actuator’란 ‘Smart Information’과 ‘Context’정보를 이용해 실질적으로 현실세계(물질, 생물 등)에 영향을 미쳐 변화를 초래하는 것으로 통제 및 행동과 관련된다. ‘Actuator’는 ‘로봇틱스’와 밀접한 관계를 가지며 AI의 궁극적인 목표이다.

#### (1) 전문가시스템(Expert systems)

인공지능 기술 분야 중 가장 일찍 단위 기술분야로 시작된 영역이다. 사기탐지업무에서 그 중요성이 다시 부각되고 있다. 금융분야의 경우 전통적인 데이터 분석만으로는 사기탐지 기능을 완전히 해결하기 어렵다. 데이터 분석에 기반하지만 Data Driven만으로 할 수 있는 분야는 매우 제한적이며 전문가 Heuristics을 모델화 할 수 있는 지식공학 능력이 필수이다. 지능형 금융정보시스템의 핵심 성공 요인은 지식베이스(Knowledge-base)를 어떻게 잘 만드느냐, 어떻게 잘 관리하는가에 있다. 지식베이스는 반드시 Rule base를 지칭하지 않으며, Rules & Scenarios, Scoring Models 등 해당 도메인의 문제해결이 가능한 구조화된 지식을 의미한다. 지식의 원천은 전문가/조직 지식, 또는 데이터 크게 이 두 가지로 나누어 볼 수 있으며 문제해결을 위한 지식 원천을 찾아 적절한 방법으로 지식베이스화 한다. 구축된 지식베이스의 적절성은 시스템 성과에 지대한 영향을 미친다. 지식 공학, 관련 전문가를 지식공학자라 하며 전문가시스템(Expert systems)은 일반적으로 다음과 같은 요소로 구성된다.

- o 지식베이스획득인터페이스(Knowledge-Acquisition Interface)
- o 사용자인터페이스(User Interface)
- o 지식베이스(Knowledge Base)

## ■ 인터페이스엔진(Inference Engine)



(그림 4-9) expert system에서의 Knowledge-base 구조

### (2) 지식베이스(knowledge base)

전문가시스템의 구성 요소의 하나로서, 인공지능 에이전트가 사용될 분야와 관련된 지적 활동과 경험을 통해서 축적한 전문 지식 그리고 문제 해결에 필요한 사실과 규칙 등이 저장되어 있는 데이터베이스이다. 전문 지식의 표현 방법으로 IF-THEN 형식의 생성규칙이 사용되며, 사실의 표현을 위해서는 프레임 표현이 사용된다. 생성규칙과 프레임 표현을 사용함으로써 지식의 모듈화구조화가 가능하고 그 결과 지식의 추가와 변경이 가능하게 되어 상황의 변화에 따라 성장하는 시스템을 구축할 수도 있다. 지능형 금융정보시스템의 지식베이스(Knowledge base) 구축은 기업의 핵심지식을 시스템화, 구조화하여 인코딩 가능한 형태로 변환시켜주는 전문영역이다. 시스템 개발자가 아닌 지식공학전문가, Business Analytic 전문가 등 해당 분야 전문가가 필요하다.

### (3) 추론 엔진

추론 엔진은 지식베이스를 검색하여 문제해결에 이용되는 추론방법을 담고 있는 소프트웨어이다. 지식베이스를 이용하여 문제해결 지식을 포함하고 프로그램을 제어하는 인터프리터에 해당된다. 전통 시스템과 달

리 전문가시스템은 추론엔진이 있으므로 불확실성을 다룰 수 있다. 주요 추론방법으로는 전방추론, 후방추론, 이들을 혼합한 혼합형 추론이 있다. 지식베이스와 추론기관을 분리하는 이유는 지식베이스는 바뀔 수 있는 동적인 성격, 즉 융통성이 존재하며 추론 기관은 정적인 면을 담고 있다. 게임의 승리나 정리 증명 같은 어떤 목표 달성을 위해, step-by-step 방식을 사용했다. 미로를 찾아갈 때 계속 나아가면서 막힌 길이 있으면 다른 길이 있는 곳까지 되돌아 왔다 가는 식이다. 이 패러다임은 “탐색 추리”이다. 주요한 문제는, 간단한 미로에 있어서도 경로로 사용할 수 있는 수가 대단히 많다.

#### (4) 인공신경망(Artificial Neuron Network):

인공신경망은 기계학습 분야에서 연구되는 학습 알고리즘들 중 하나이다. 패턴인식에 쓰이며 인간의 뇌의 뉴런과 시냅스의 연결을 프로그램으로 재현한다. '가상의 뉴런'을 '시뮬레이션'한다고 볼 수 있는 것이다. 신경망 구조를 만든 다음 '학습'시키는 방법으로 적절한 기능을 부여한다. 지성을 가진 시스템 중 인간의 뇌가 가장 훌륭한 성능을 가지고 있기 때문에 뇌 모방 인공신경망은 궁극적 목표를 가지고 발달된 학문이다. 신경망은 학습데이터에 있는 예러에 민감하지 않기 때문에 학습 예제로부터 함수를 학습하는 일반적이고 실용적인 방법이다. 신경망은 문자 인식, 음성인식과 합성 등 비교적 하위 수준의 자연언어처리 문제에 적용되어왔으며, 품사 태깅 문제에도 활용되었다. 신경망은 다른 기호학습 방법과 결합되어 보다 복잡한 문제에 적용되기도 하는데, 구절 경계 찾기(identification of clause boundaries), 구문 분석, 문법 추론(grammar induction), 전치사 접속 결정, 의미 중의성 해소, 문서 분류, 철자 교정 등이 있다.

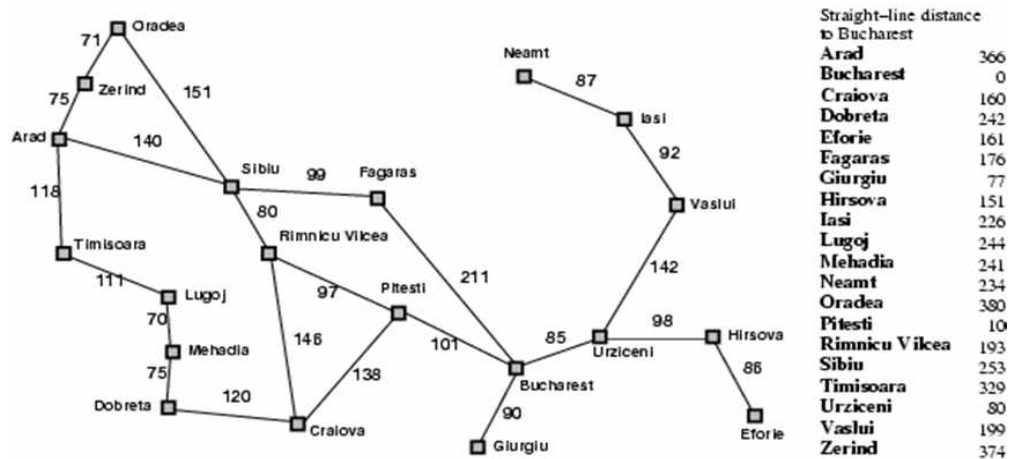
#### (5) 지능형 에이전트

지능형 에이전트 시스템은 환경을 인식하고 성공을 가장 극대화 할 수 있는 행동을 취한다. 이러한 정의에 의하면 인간과 인간들의 조직처럼, 예를 들어 회사처럼 특정 문제를 해결하는 간단한 프로그램들을 지능형 에이전트라고 한다. 지능형 에이전트는 AI 연구자들을 “the study of intelligent agents”로 정의한다. 이것은 AI의 정의의 일부를 일반화 한 것이다. 이것은 인간의 지능을 넘어 모든 종류의 지능의 연구를 추구한다. 지식의 추가와 변경 작업에 대한 방식이 인공지능 에이전트의 사용분야에 따라 다르며, 에이전트의 사용자들의 기준에 따라 달라지기 때문에 이러한 작업은 상황에 맞게 개별적으로 작성되어야 한다. 인공지능 대상의 관련 지식을 지식베이스에 반영하는 작업을 지식 획득(knowledge acquisition)이라고 한다. 지식 획득에는 확립된 방법이 없으며 이것이 전문가시스템 구축에 큰 장애가 되고 있다. 자금세탁관련 혐의거래는 날로 지능화 추세이며, 국제적으로 자금의 투명성에 대한 요구가 발생하고 있다. 위험고객 및 위험거래를 자동으로 분류하고, 측정된 리스크에 따라 제한된 검사자원을 고위험군에 집중함으로써 효율성과 효과성을 제고할 수 있다.

#### 나. 휴리스틱 방법론

어떤 특정 애플리케이션에 관련되어 있는 사실들이나 데이터를 담고 있다. 추론엔진은 이 정보를 이용해서 문제를 풀어나간다. 즉 프로그램이 지능적으로 실행될 수 있도록 해주기 위해서는 정보를 지식베이스에 저장할 필요가 있다. 지식베이스에서 지식을 표현하는 방법으로는 생성 규칙(Production Rule), 의미론적 네트워크, 프레임, 블랙보드, 사례중심 추론, 퍼지논리, 신경망 등이 있다. 특히 알고리즘과 휴리스틱 대부분의 전문가시스템의 규칙은 휴리스틱하다. 즉, 경험적인 규칙 또는 제한된 조건하에서만 적용할 수 있는 단순화된 규칙이다. 알고리즘 방법을 통해

서는 문제의 뜻에 맞는 정확한 답 또는 최상의 답을 얻을 수 있지만, 휴리스틱방법은 대부분 최상의 답은 아니지만 사용자가 받아들일 수 있는 정도의 답을 제공한다.



(\* 주 : Informed search algorithm )

(그림 4-10) 최적해를 찾아가는 휴리스틱경로(Romania with step costs in km)

## 다. 지식공학(Knowledge Engineering)에 대한 소견

### (1) Knowledge-base

지능형 금융정보시스템의 지식베이스(Knowledge base) 구축은 기업의 핵심지식을 시스템화, 구조화하여 인코딩 가능한 형태로 변환시켜주는 전문영역이다. 이 과제를 성공시키기 위해서는 비즈니스 컨설턴트나 시스템 개발자가 아닌 지식공학전문가, Business Analytic 전문가 등 해당 분야 전문가가 필요하다. 학습을 통해 웹상의 모든 콘텐츠를 반영한 지식베이스(Knowledge Base: KB)를 구축한다. 전문지식의 표현 방법으로 IF-THEN 형식의 생성규칙이 사용되며, 사실의 표현을 위해서는 프레임

표현이 사용된다. 생성규칙과 프레임 표현을 사용함으로써 지식의 모듈화, 구조화가 가능하다. 그 결과 지식의 추가와 변경이 가능하게 되어 상황의 변화에 따라 성장하는 시스템을 구축할 수도 있지만, 지식의 추가와 변경 작업에 대한 방식이 인공지능 에이전트의 사용분야에 따라 다르며, 에이전트의 사용자들의 기준에 따라 달라진다. 인공지능 대상의 관련 지식을 지식베이스에 반영하는 작업을 지식 획득(knowledge acquisition)이라고 한다.

(2) 기계학습(Machine Learning)과 베이저안 확률(Bayesian Probability)  
<http://aistory.egloos.com/4493798>

기계학습에서 확률추론이 차지하는 비중은 매우 크다. 확률추론에서 관심을 갖게 하는 부분이 베이저안 확률이다. 베이저안 확률이란 확률의 개념을 좀 더 확장하는 이론인데 예를들면 어떤 사건의 발생을 가정할 경우, 사건발생을 반복시행을 할 수 없는 명제나 상황이라 해도, 이것의 “불확실한 정도“ 혹은 “믿음의 정도“를 확률로 할당하는 것이다. 즉, 확률을 불확실한 상황에서의(Boolean) 진리값의(이산 변수에서 연속 변수으로의) 확장으로 간주한다는 이론이다. 즉, ‘어떤 명제가 얼마나 진리에 가까운 것인지 - 객관적이지 않아 보이는 양을 어떻게 계산할 수 있을까’에 대한 관점을 취함으로써 전통적이며 고전적인 확률개념을 확장하고자한다. 베이저안 관점에서는 확률을 다루는 데 있어서 사전 지식(Prior knowledge)을 자연스럽게 고려하고 확률을 좀더 신중하게 적용하는 방법을 사용한다.

### 3. 사기탐지 시스템과 빅데이터(Big Data)

가. 빅데이터 사용 조건

빅데이터 시장에는 과대광고와 혼란이 기술 선정을 어렵게 할 수 있다. 표면상으로 Hadoop 배포 벤더, SQL-on-Hadoop 데이터베이스 벤더, 기존 데이터 웨어하우스 벤더 등이 시장을 주도하는 것처럼 보인다. 하지만 이러한 솔루션의 장점과 약점을 파악하고 어떤 솔루션이 자신의 분석에 적합한지를 판단하기란 매우 어렵다. 금융정보 환경에서 정보시스템 상에는 정형, 비정형 및 반정형 데이터가 끊임없이 증가한다. 볼륨, 속도 및 다양성이 복잡도를 유발한다. 금융정보시스템의 규모가 지속적으로 증가하는 가운데 어느 기업이나 마찬가지로 소셜 미디어 콘텐츠, 오디오 및 비디오 파일, 이메일, 문자 메시지, 이미지 파일, 문서, 거래 정보 등으로 스토리지가 채워지고 있다. 빅데이터의 가능성은 새롭고 다양한 대량의 데이터를 수집할 수 있을 뿐만 아니라 보다 광범위한 대상에게 분석을 제공할 수 있다는 것이다. 다수 조직의 경우 이 중요한 비즈니스 분석에 대한 개인화된 액세스는 새로운 워크로드 문제를 초래하고 있다. 대형 금융시스템의 경우 통신 네트워크 및 그 관련 스위치, 과금 시스템과 서비스 부서는 각기 매일 수억 건에 달하는 CDR(Call Details Record)을 생성하고 있다. 이 동적 고객 데이터는 통신사가 새로운 서비스를 추가하고 IP기반 트래픽이 증가하면서 앞으로도 기하급수적으로 증가할 것이다.

(\* 주 : 한국휴렛팩커드 Technical white paper : A Heterogeneous Approach to Big Data Analytics, 빅데이터 분석에 대한 이중 접근방식)

## 나. 빅데이터 활용 사기탐지 방법론

### (1) 지능형 의사결정지원시스템

FDS는 이상금융거래의 실시간 차단(Real-time Transfer Block)을 생명으로 한다. FDS 시스템이 도입 후, 즉시 성과를 내기 위해서는 이상금융거래 탐지에 대한 노하우가 확보되어야 하며 그 핵심은 FDS Rule이다.



FDS Rule를 설계하기 위해 이상금융거래탐지 경험 지식이 필요하다. FDS Response System 도입을 위한 금융사고 대응체계 구축에는 축적된 FDS Knowhow가 필요하다. 만약 구축 즉시 성과를 내는 시스템을 도입하려면 금융사고 대응 경험에 기반 한 FDS Rule 적용이 필수이다. 또한, 탐지 즉시 사전차단이 가능한 초고속 Infra가 구성되어야 하며, 사건 발생 후 이에 대응할 수 있는 사고 대응체계 구비가 필요하다. 이상금융거래탐지 시 이체 전에 차단이 되어야 금융 사고가 예방되며 이를 해결할 수 있다. 지능형 의사결정지원시스템은 ‘사람의 뇌’에 해당하는 ‘지식베이스’ 또는 ‘Intelligence Module’을 탑재하고 있다. 지능형 의사결정지원시스템 적용 대상은 신용평가시스템, 조기정보시스템, 분석적발시스템, 상시감사시스템, 영업점감사시스템, 위험징후탐지시스템, 자금세탁 방지시스템, 외환거래위험방지시스템, 카드부정사용방지시스템, 보험사기적발시스템 등 이다.

## (2) 알고리즘 방식과 빅데이터 방식의 비교

데이터로부터 의미를 가지는 데이터를 추출하고 결과를 분석하여 가치를 창출할 수 있도록 하는 기술 전반을 의미한다. 빅데이터 기술은 다양한 경로로 수집된 정형, 비정형 데이터를 지정된 공간에 수집하는 기술과 수집된 데이터를 정제하여 분석하는 일련의 과정에 사용되는 기술이다. 빅데이터와 관련 기술은 데이터의 수집을 포함한 처리 기술과 데이터의 분석 기술로 나뉘어진다. 전통적인 알고리즘 방식과 빅데이터 방식의 비교해보면 5가지 측면에서 차이점이 나타난다. 알고리즘 방식과 빅데이터 방식은 근본적인 개념, 사용목적, 새로운 사기 패턴 발생 시 알고리즘 개발, 처리 방식 기본, 등장시기에서 차이를 보이고 있다. 알고리즘 방식은 문제해결의 절차와 방법의 개념을 가지고 출발하며 사용목적은 사기탐지 기능 전문 용도로 개발되어야 한다. 반면 빅데이터 방식은 빅데이터 처리 방식을 다양한 업무에 공동활용이 가능하다. 새로운 사

기 패턴 발생 시 알고리즘 개발 필요성을 보면 새로운 유형의 사기패턴 발생 시탐지에 필요한 알고리즘을 별도 개발해야하고 새로운 사기유형에 새로운 방법론이 필요하다. 빅데이터 방식은 새로운 유형의 사기패턴 발생 시 필요한 알고리즘을 별도 개발하지 않으며 빅데이터처리 기능을 사기탐지에 활용할 수 있다. 처리 방식의 기본은 알고리즘 방식은 데이터(속성)와 처리기능(method)이 일종의 분리 형태이지만 빅데이터 방식은 데이터(속성)와 처리기능(method)이 결합된 형태이며 데이터 자체가 로직의 성격을 가지고 있기 때문이다.

[표 4-8] 알고리즘 방식과 빅데이터 방식의 비교

구분	알고리즘 방식	빅데이터 방식
개념	문제해결의 절차와 방법	Volume 측면의 비정형 데이터 집합 전통적 데이터처리 알고리즘으로 처리한계
사용목적	사기탐지 기능 전문 용도	빅데이터 처리 방식을 다양한 업무에 공동활용
새로운 사기 패턴 발생 시 알고리즘 개발	새로운 유형의 사기패턴 발생 시탐지에 필요한 알고리즘을 별도 개발 새로운 사기유형에 새로운 방법론 필요	새로운 유형의 사기패턴 발생 시 필요한 알고리즘을 별도 개발하지 않음 빅데이터처리 기능을 사기탐지에 활용
처리 방식 기본	데이터(속성)와 처리기능(method) 분리형태	데이터(속성)와 처리기능(method) 이 결합된 형태 데이터자체가 로직의 성격

### (3) 빅데이터 적용단계

#### o 저장 - 로딩 및 준비

데이터를 분석하려면 먼저 데이터를 입수해야 한다. 따라서 데이터를 저장할 공간이 필요하며 종종 구문 분석이나 여타 형태의 보강을 통해 최초 사용을 위한 준비를 해야 한다. 이를 흔히 ETL(Extract(추출), Load(로딩), Transform(변환) 또는 ELT(Extract, Load, Transform)라 한다. 여기서는 배치 성능이 중요하며, 확장에는 비용이 수반되기 때문이다. 특히 데이터가 문서와 유사한 형식(예: JSON)일 경우 로딩 작업은 사용자 쿼리에 비해 느린 속도로 변하는 경향이 있기 때문에 사용 편의성은 다소 덜 중요하다.

#### o 탐색 - 다크 데이터(Dark Data) 파악

분석 라이프사이클의 이 단계는 단일 선형 흐름일 경우가 드물다. 흔히 이 단계는 분석 모델이 어떨지를 규명하기 위해 데이터 관련 질문을 하는 분석가의 엄청난 상호작용을 요한다. 그 적절한 예가 다음 단계의 예측 모델 개발에 필요한 정보를 제공할 수 있는 예비 상관관계를 검토하는 일련의 데이터 변수 조사이다. 하지만 데이터의 질이 아직 확정되지 않았을 수 있기 때문에 그 특성 등이 잘 파악되지 않으며 분석가들이 종종 모델링 단계에 착수하기 전에 광범위한 임시 조회를 수행해야 한다. 데이터 과학 용어에서는 이를 흔히 “탐색적 데이터 분석”이라고 한다. 이는 흔히 분석의 가장 복잡한 단계로서 데이터가 아직 잘 파악되어 있지 않으며 조회에 적합한 형태가 아닐 수 있다.

#### o 적용

이 단계에서는 일반적으로 통찰력 있는 정보를 찾아내어 운영하기 위한 모델을 구축한다. 일례로, 분석가는 온라인 게임 사용자들이 진행이 막히게 되는 지점에서 게임을 포기하는 경우가 흔하며 그 지점을 지난 사용자들은 훨씬 더 높은 가치를 가진다는 점을 발견할 수 있을 것이다. 이제 분석가는 게임 사용자가 이 지점에 도달할 즈음에 장애물을 통과하는데 도움이 되는 게임 내 도움말을 제공함으로써 수익을 증대시켜는 예측 모델을 개발해야 한다. 모델이 선정되면 그 모델을 실제로 적용하거나 배치해야 한다. 경우에 따라 보고서나 대시보드의 형태를 취할 수 있

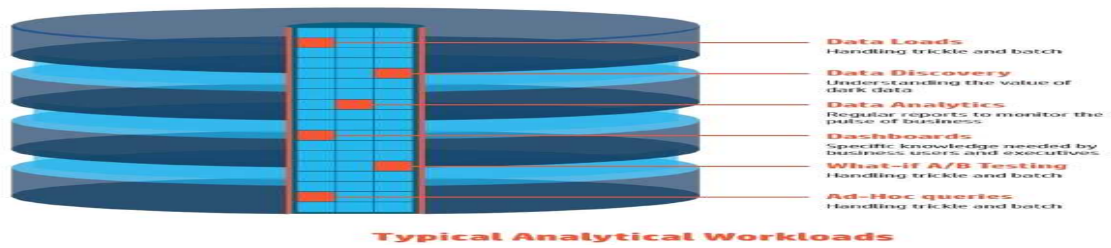
으며 때로는 애플리케이션의 형태를 취할 수도 있다.

o 실행

이 단계에서는 원하는 결과가 가시화되어야 한다. 따라서 조직은 최소한 분석이 바람직한 효과를 거둘 수 있도록 유입 데이터의 흐름을 관찰해야 한다. 아울러 이 과정에서 조직은 분석 통찰력을 증진하기 위해 더 많은 정보가 필요하다는 것을 종종 깨닫게 된다. 따라서 이 단계의 핵심은 데이터 생성 및 수집 프로세스의 적응이며 이는 분석 사이클의 새로운 반복을 의미한다

#### (4) 스토리지로서의 Hadoop(Hadoop for Storage)

한편으로는 강력한 분석 데이터베이스가 있다. 다른 한편으로 Hadoop은 대량의 데이터에 대한 효과적인 스토리지 기반이 될 수 있는 분산 파일 시스템을 갖춘 분산 처리 프레임워크이다. Hadoop은 모든 유형(정형, 비정형 또는 반정형)의 데이터에 효율적입니다. Hadoop은 또한 직접적인 대화형 분석이 요구되지 않는 일괄 처리에도 적합하다. 급부상하고 있는 Hadoop의 한 가지 분야는 “SQL-on-Hadoop” 개념으로 다수 조직들이 가치가 알려지지 않은 대규모의 데이터 호수를 생성했으며 그 데이터에서 심층 분석을 수행하는 비용을 정당화해야 할 필요성이 주된 동인이다. 각종 산업에서 100종 이상의 애플리케이션이 하둡을 활용하고 있다.



<http://ko.hortonworks.com/blog/how-big-data-is-revolutionizing-fraud-detection-in-financial-services/>

(그림 4-11) 빅데이터의 전형적인 워크로드

#### 4. 사기탐지 알고리즘 적용시 참고사항

##### 가. 사기탐지 방식 진화 방향.

전통방식과 진화방향을 비교하여 보면 데이터측면에서는 데이터베이스에서 지식베이스로 다시 빅데이터로 진화하고 있다. 분석방법은 전통적 방식이 형태분석, 형상 분석, 외형 분석, 행위위주의 분석이라면 진화방향은 행태, 행동, 내면적 움직임 분석, 심리학, 감정까지 분석대상이다. 패턴인식은 패턴매칭에서 휴리스틱 방식이 필요하며 알고리즘은 단위 알고리즘, 사용목적 별 알고리즘에서 통합화 알고리즘, 통합화 분석으로 진화된다. 탐지방식 측면에서는 static 고정식에서 dynamic 유연성 방식으로 변화 되고 있다. 사용자의 룰세팅 방식은 완성된 제품의 옵션만을 선택하는 방식에서 지속적 커스터마이징을 전제로 하며 룰세팅 자체를 사용자가 수행한다.

[표 4-9] 사기탐지 알고리즘 진화방향

구분	전통적 방식	진화방향
데이터	데이터베이스	지식베이스

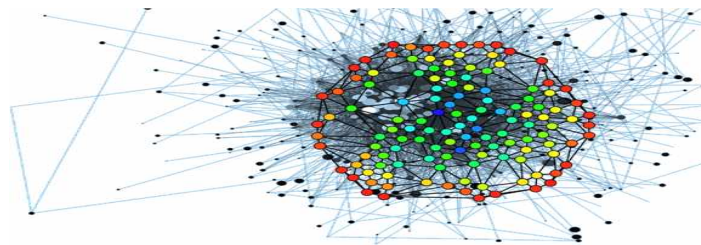
		빅데이터
분석방법	형태분석, 형상분석, 외형분석 행위위주의 분석	행태, 행동, 내면적 움직임 분석 심리학, 감정까지 분석대상
패턴인식	패턴매칭	휴리스틱
알고리즘	단위 알고리즘, 사용목적별 알고리즘	통합화 알고리즘 통합화 분석
탐지방식	static 고정식	dynamic 유연성
룰세팅	완성된 제품의 옵션만을 선택	지속적 커스터마이징을 전제로 함 룰세팅 자체를 사용자가 수행
품질관리 방법론	QoS	QoS, MoS
기능 요구분석	사용자요구사항이 의무사항이 아님	사용자요구사항 전제

#### 나. 머신러닝(Machine Learning) 방식 진단

개발자는 높은 정확성을 보유한 머신러닝 모범 사례를 이용해 모델 구축부터 배치까지 모든 것을 할 수 있다. 자동화는 애플리케이션 내 머신러닝 확산의 핵심이다. 개발자와 밀접히 협력할 수 있는 소수의 데이터 엔지니어를 확보할 수 있다 하더라도 충분한 인력을 확보할 수는 없다. 스카이트리(Skytree)의 오토모델(AutoModel)의 사례가 모델 정확성 최대화를 위한 최적의 파라미터와 알고리즘을 자동으로 결정하는 데 도움이 될 수 있다. 사용이 간편한 인터페이스를 통해 개발자는 훈련, 조율, 시험 모델의 과정을 거치면서 통계적 실수를 방지할 수 있다.

인공지능의 한 분야로, 데이터를 바탕으로 반복해서 기계가 학습할 수 있도록 하는 알고리즘과 기술을 개발하는 분야. 즉, 데이터를 분석하여 숨겨진 특성인 ‘패턴’을 발견해 학습 모델을 구축하고 추론하는 기술이자, 더 나아가 경험으로부터 습득 지식을 기반으로 스스로 성능을 향상시키는 과학이다. 인공지능이 인간과 같은 사고를 하는 컴퓨팅, 즉 인간의 뇌를 수학적으로 모델링하는 것을 의미한다면, 머신러닝은 인공지능 내부 시스템 가운데 ‘학습’ 영역을 구체화한 기술이다. 1980년대 본격적으로 머신러닝이 새로운 연구 분야로 정의되기 시작해서, 자연어 처

리, 로봇, 패턴 인식, 전문가시스템 등 인공지능의 모든 분야와 관련되어 발전되었다. 오늘날에는 훈련된 지식을 기반으로 습득한 데이터에 대해 유용한 답을 찾고자 하는 일련의 컴퓨터 알고리즘 혹은 기술을 총칭하며, 지식을 습득하는 기법을 의미한다. 머신러닝은 수많은 학문적 경계가 허물어져 합쳐진 기술로, 영상인식, 음성인식, 문자 인식, 자연어처리, 로봇틱스, 인터넷 검색 등의 다양한 분야의 핵심 기술로 자리 잡고 있다. 머신러닝은 사람의 지식을 기반으로 하는 것이 아니라, 학습시킬만한 양질의 데이터의 양에 따라 성패가 갈린다. 머신러닝을 평가할 때는 다음과 같은 요구 사항을 고려해야 한다. 속도(Speed), 가치 창출 시간(Time to value), 모델 정확도(Model accuracy), 손쉬운 통합(Easy integration), 유연한 구축(Flexible deployment), 사용 편의성(Usability), 시각화(Visualization)



(\* 주 : [https://casil.llnl.gov/technical\\_focus\\_area/machine\\_learning](https://casil.llnl.gov/technical_focus_area/machine_learning))

(그림 4-12) 머신러닝 개념도

#### o 머신러닝 프로세스 내의 자동화

머신러닝 프로세스 내의 자동화는 여러 측면에서 데이터 엔지니어나 개발자를 위해 인공지능의 원리를 통합하고, 알고리즘이 생각하고 학습하는 모델 구축 작업의 부담을 덜어 줄 수 있다. 즉, 데이터 엔지니어를 머신러닝과 분리할 수 있다는 생각이 실수이며, 특히 업무에 필수적인 모델일 경우에는 더욱 그렇다. 기초 기술의 정확함, 정교함, 확장성 등에

대한 생각 없이 적용할 수 있는 간편한 머신러닝 기능의 가능성을 인지하자. 이를 통해 높은 예측 정확성과 머신러닝이 제공해야 하는 이로 인한 높은 비즈니스적 가치를 얻을 수 있다.

o 머신러닝의 실제 사용 사례

- 구글, 페이스북과 같은 기업이 머신러닝(machine learning)을 사용해 자동차를 운전하고 음성을 인식하고 이미지를 분류한다.

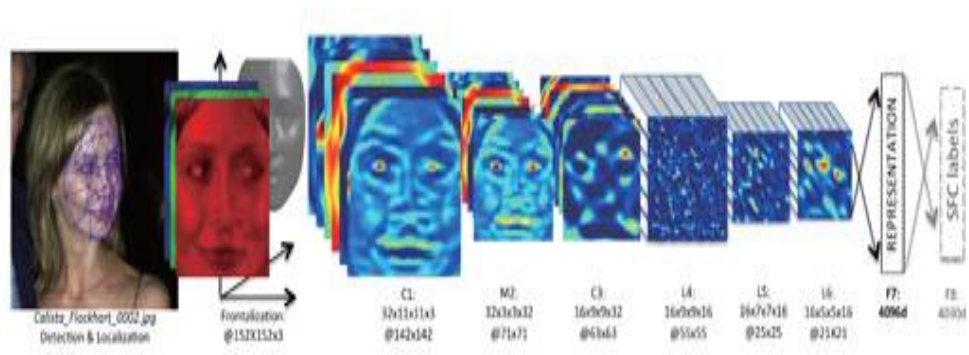
- 한 지불 결제 처리 업체는 실시간으로 10억 개 이상의 거래 중에서 숨겨진 사기를 탐지함으로써 손실 금액을 월 100만 달러가량 줄이고 있다.

- 페이스북은 최신 머신러닝 기법을 사용해 사기성 결제를 실시간으로 식별하는 모델을 구축했다.

다. 딥러닝 방식 진단

현재, 과거에는 엄두도 내지 못할 정도의 데이터가 온라인상에서 생성되고 쌓이고 있지만 이러한 데이터를 효과적으로 사용하는 것은 한계이다. 사람이 하는 일에는 한계가 있기 때문에, 무수한 정형/비정형 데이터에서 유의미한 결과를 도출하기 위해 모델링 또는 상관관계를 사람이 직접 뽑아내는 것이 아닌 머신이 스스로 배우도록 할 필요가 생겼다. 이를 위하여 대규모 데이터의 처리하고 의미있는 정보를 발굴하고 활용하는 기술들이 아래와 같이 개발되고 있다. 페이스북은 개발자 커뮤니티에 딥러닝 기술을 공개하여 자체 인공지능 프로젝트를 강화하려는 움직임을 보이기도 했다. 공개된 기술은 오픈소스 기반 유명 딥러닝 소프트웨어 프로젝트 ‘토치(Torch)’에서 쓸 수 있으며, 엔비디아 그래픽처리장치(GPU)에 최적화됐다.





(\* 주 : <http://m.technbeyond.co.kr/>)

(그림 4-13) 칼리스타 플록하트의 얼굴 인식 과정

‘머신러닝’, ‘빅데이터’, ‘데이터마이닝’은 서로 상호보완적인 역할을 담당하면서도 각자의 길을 걷는 기술이다. ‘빅데이터(Big Data)는 대규모(Big) 모든 정형 및 비정형 데이터를 처리하는 기술이다. ‘데이터마이닝(Data Mining)은 수많은 데이터 가운데 의미있는 정보를 찾아(발굴해)내는 기술이며 ‘머신러닝(Machine Learning)은 과거 데이터에서 어떤 패턴을 읽어내어 기계가 학습 후 미래예측 기술이다. 각 특성과 용도를 구분할 수 있지만 실제적으로는 인공지능의 원리를 통합하고, 알고리즘이 생각하고 학습하는 모델을 구축하는 작업이다. 여기서 머신러닝과 딥러닝의 차별성에 주목할 필요가 있다. 머신러닝은 유사성을 기반으로 원소를 구분하는 방식이다. 그런데 원소의 유사성을 기준으로 대상 원소를 그룹화 하면 예를 들어 픽셀의 유사성을 기준으로 하면 구분은 되지만 서로 다른 대상이 형태적 유사성으로 동일 집합으로 분류된다. 즉 다른 개체이지만 동일한 집단으로 분류된다. 이것은 머신러닝의 한계이다. 이 문제를 극복하기 위해 진화된 알고리즘이 딥러닝이다. 딥러닝은 유사성을 기준으로 분류된 개체를 2차적으로 다시 한번 분류한다. 이 방식은 소위 지능적 해석이 가능한 원리이다. 금융사기 패턴을 분석할 때 머신러닝 대신 딥러닝 알고리즘이 사용되어야 하는 이유이다.

[표 4-10] 인공지능의 원리를 사용하는 데이터 처리 알고리즘

방식	빅데이터 (Big Data)	데이터마이닝 (Data Mining)	머신러닝 (Machine Learning)	딥러닝 (Deep Learning)
특성	대규모(Big) 의 모든 정형 및 비정형 데이터를 처리하는 기술	수많은 데이터 가운데 의미 있는 정보를 찾아 (발굴해) 내는 기술	과거 데이터에서 어떤 패턴을 읽어내어 기계가 학습한 후 미래를 예측 하는 기술	높은 수준의 추상화를 시도 하는 기계학습 알고리즘의 집합

#### o 딥러닝 적용에서의 장벽

컴퓨팅비용 : 딥러닝의 실용적인 활용은 제한.

연구경험 : 실무적 문제에 딥러닝을 적용하기 위한 이론과 경험 부족

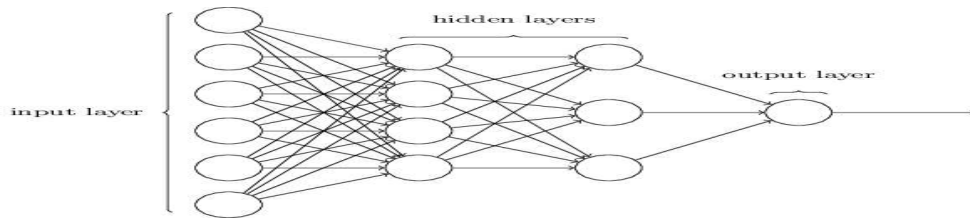
현장기술력 : 높은 진입 장벽

알고리즘 : 제한된 시간과 자원 내에서 다른 방법이 딥러닝보다 더 효과적.

무어의 법칙에 따른 발전으로 컴퓨팅 비용은 급격히 낮아졌으며 혁신적인 알고리즘으로 훨씬 더 빠르고 효율적으로 모델을 학습시킬 수 있게 됐다. 경험과 지식이 누적되면서 데이터 과학자들도 딥러닝에서 가치를 끌어내기 위한 이론과 실무적 지침을 갖췄다. 미디어에서는 미래에 가능해질 음성 및 이미지 인식 분야의 활용 사례에 초점을 맞추는 경향이 있지만, 현재 데이터 과학자들은 딥러닝을 사용해 비즈니스 각 분야에서 실무적인 문제를 해결하고 있다.

#### o 딥러닝을 사용한 사기탐지 사례

- 금융 결제 업무 : 업체는 딥러닝을 사용해 의심스러운 거래를 실시간 파악한다.



(\* 주 :<http://www.droid-sec.com/2014/03/deep-learning-in-android-malware-detection/>)

(그림 4-14) Deep Learning in Android Malware Detection, March 08 2014, by Lyq, analysis

- 사기탐지 : 대규모 데이터센터와 컴퓨터 네트워크를 운영하는 기업은 딥러닝을 사용해 로그 파일을 마이닝하고 위협을 탐지한다.

라. 다른 머신러닝과 비교한 딥러닝의 4가지 핵심 이점

#### o 4가지 장점

4가지 장점을 통해 딥러닝은 다른 방법으로는 불가능한 유용한 결과를 도출할 수 있고, 다른 방법보다 더 정확한 모델을 구축할 수 있으며 유용한 모델을 구축하는 데 필요한 시간을 단축할 수 있다. 특징 간의 복잡한 상호작용을 탐지하는 능력이다.

최소한으로 처리된 원시 데이터에서 저수준의 특징을 학습하는 능력으로서 높은 기수(high-cardinality) 클래스 멤버십을 다루는 능력, 미분류(unlabeled) 데이터를 다루는 능력 등이다.

#### o 보이지 않는 변수 간 상호작용 탐지

딥러닝은 표면적으로는 보이지 않을 수 있는 변수 간의 상호작용(interactions)을 탐지한다. 상호작용이란 상호 조합되어 움직이는 두 개 이상 변수의 효과다. 예를 들어 한 약품이 젊은 여성에게 부작용을 일으

키지만 노령의 여성에게는 부작용을 일으키지 않는다고 가정해 보자. 이 경우 성별과 연령을 조합한 효과를 수용하는 예측 모델이 성별만 기반으로 하는 모델에 비해 훨씬 더 효과적일 것이다. 기존의 예측 모델링 방법도 이런 효과를 측정할 수 있지만 많은 가설 테스트를 수작업으로 수행해야만 한다. 딥러닝은 이런 상호작용을 자동으로 탐지하며 분석가의 전문 지식이나 기존 가설에 의존하지 않는다. 특히 딥 뉴럴 네트워크(deep neural networks) 사용 시 비선형적 상호작용을 자동으로 생성하고 충분한 뉴럴로 임의 함수를 근사치로 계산할 수 있다. 일반적인 예측 분석 방법을 사용할 경우 분석의 성공 여부는 특징 가공(feature engineering)을 사용해 데이터를 준비하는 데이터 과학자의 역량에 크게 좌우된다. 이 준비단계에는 상당한 분야별 지식과 기술이 필요하며, 특징 가공에는 시간도 소요된다.

## 제 9 절 도출되는 현안사항

### 1. 금융사기 자체의 속성

#### 가. 금융사고 원인 입증 복잡성

금융업무 환경에서 트랜잭션 타입은 인터넷뱅킹, 펌뱅킹, 핀테크 뱅킹으로 혼재되며 데이터 처리환경은 OPEN 플랫폼, 통신망 인터넷(공중망), 전용선 인터넷(공중망)으로 다양하다. 통신 암호화 기술은 SSL/TLS VPN SSL /TLS 인증 클라이언트 (PC&스마트폰) 공인인증서가 복합적으로 사용된다. 모든 데이터를 이용하여 지난 30 일, 90일 전체 기간을 분석하여 새로운 부정행위 패턴을 특정 패턴이 출현 때마다 실시간 경고를 생성한다. 이상거래 부분은 365일 24시간 가동해야하는 만큼 휴일과 밤낮이 없다. 사고율을 줄이기 위해서는 내부적으로 오탐율을 줄이거나, 분

석을 통해 정확한 탐지 및 차단이 이뤄져야겠지만, 거래나 이체가 지연되더라도 이를 감수하고, 추가인증에 대한 부분도 감내할 수 있어야 한다. 이 모든 변수는 예측성과 규칙성을 초월하는 복잡계의 속성을 가지고 있다. 사기 사건 자체의 속성은 복합적 요소의 사건, 요인 간 상호작용 사건(Context matters, Interacting entities)이다. 사고원인 책임소재기관 규명 불명확성은 고객, 금융회사, 전자금융사업자 규명불명확성을 말한다. 예를들면 정보유출, 텔레뱅킹 경우 고객, 공급자간 규명 불명확성이 존재한다. 해킹, 전산오류는 금융회사 귀책으로 규정화된 바 있다. 사고원인 제공시스템 규명 불명확성이다. 네트워크, 서버, 운영체제, 데이터, 프로그램, 통신프로토콜, 단말 시스템 중 어느 시스템에서 원인이 되는지 규명이 곤란하다. 사고관련 영역의 광범위성은 기술영역, 처리영역, 데이터 영역, 사용자영역 중 어느 영역이 원인인지 규명이 곤란하다

#### 나. 금융사기 영역에 대한 인식

우리의 일반적인 인식에는 금융사기가 그 영역에서 해킹의 영역인지가 모호하다. 금융사기의 영역은 해킹영역과 사회공학(Social Engeneering) 영역이 혼합된 형태이다. 금융사기의 방지 기술은 인공지능 기술, 빅데이터, 포렌식 기술, QoS기술, 암호학 기술이 대표적이며 학문은 사회학, 심리학, 컴퓨터공학이 혼합된 영역이다. 사기방지는 다수의 기술, 학문영역이 중첩되는 융합 소재이므로 기술적 난이도가 대단히 높은 영역이며 그 대책 도출 또한 쉽지 않고 매우 특화된 분야이다. 이같이 단일 영역이 아닌 복합 소재의 영역에서는 대응책 또한 전문화된 특화된 방법이어야 한다. 금융사기의 1차적인 업무 카테고리는 정보보호업무 중 위험관리 영역에 속한다. 위험관리 영역은 자산분석, 위협분석, 취약점분석, 위험도측정, 정보보호체계 분석 체계로 구성되어 있다. 금융사기의 기술영역은 정보보안 위험관리 업무를 금융분야 업무에 적용하는 방법론으로 특성화 시킨 소재라고 분류할 수 있다. 기타 금융사기 업무를 보안측면

에서 분류하면 다음과 같은 카테고리가 가능하다.

- 정보보호업무중 정보보호 지표개발업무 추가.
- 정보보호업무중 정보보호성숙도수준평가업무 추가.
- 금융분야업무인 금융사고 모형연구업무 추가.
- 금융사고 모형별 측정연구업무 추가.
- 해킹 영역 중 사회공학 영역
- 종합적으로 정보보호분야와 금융업무 영역에서 상이한 5가지 이상 소재가 혼합된 다중화 소재 개발 프로젝트

다. 사기행위 관련 인자

수집하는 데이터의 양이 방대하고 수집과 연동되는 시스템이 수십 개에서 많게는 수천개에 해당하는 빅데이터 기반의 시스템이라면 일반적인 수집 기술로는 처리가 힘들다. 서로 다른 시스템에서 발생하는 다양한 종류의 데이터들을 실시간으로 처리되도록 하여야 하고, 장애가 발생하였을 경우 재시도 하는 등의 처리 절차가 고려되어야 하기 때문이다. 탐지결과에서 나타나는 사기행위 관련 인자들의 속성이 복합적 성격(Complexity of acting on detection results)이다. 사기행위는 정형패턴과 비정형 패턴이 혼재하며 관련되는 데이터는 FDS 서비스 사례 온라인 금융 관리 솔루션의 주요 공급 업체 1800 개 이상의 금융기관과 4백만 이상의 소비자(from 2011), 응용프로그램이 관련된다. 관련 업무는 소비자 및 기업용 인터넷뱅킹, 전자 결제, 개인용 온라인 채무 관리, 금융기관 웹사이트 호스팅 및 개발 등 이다. 입력 데이터(Input Data)의 복잡성(Complex Data Types), 데이터 간 관계(Relationship among data instances)의 복잡성, 순차성이 아닌 템퍼럴(Sequential ->Temporal) 데이터 등이 혼재된다.

2. 사기 대응 정책과 관리제도 측면

금융정책 당국의 정책은 다양한 분야에서 선도적으로 추진되고 있는 사례를 발견할 수 있다. 다만 금융사기 사건의 기술 수준이 날로 비상하고 새로운 패턴의 사기가 증가하는 현실에서 대응 태세 자체가 거버넌스 사상에 기반 한 종합 플랜(master plan)에 기초하고 있는지에 대해서는 다소 우려되고 있다. 정책은 PDS 사이클로 가동될 때 사회 전반적인 사기 발생 가능성이 낮아진다. 장단기 로드맵을 기반으로 단편적인 대책이 아닌 종합 프레임구조에서 시스템 플레이가 필요하다고 보여진다. 다음과 같은 소재는 금융사기 대비 정책에 반영되어야 할 소재로 사료된다.

- o 금융사기 보안 전문가(specialist) 영역 발굴, 전문가 양성제도, 금융사기 보안 전문가 자격 검정제도 신설

(\* 주 : “ CERT를 구성하고 운영하는 조직에서는 보안을 기술적인 부분에 한정하여 다루어서는 안되며 해당 조직 전체를 보호할 수 있도록 조직체제와 역할을 정의하여야한다” - KISA 2010.침해사고대응팀 CERT구축운영안내서, CERT의정의 및 목적)

### 3. FDS 개발 방법론 측면

#### 가. FDS 이해관계자 요구사항 분석 여부

소프트웨어 아키텍처 설계 절차에서 금융사기 방지 이해관계자의 관심을 도출한 결과를 토대로 요구사항을 분석해야 한다. 요구사항은 기능적 요구사항과 품질요구사항으로 구분된다. 금융사기 방지업무 이해관계자는 정보 사용자(User), 정보시스템인수자(Acquirer), 정보시스템 개발자(Developer), 정보 시스템 유지보수자(Maintainer)로 구분하며 이해관계자의 관심을 다음과 같이 도출할 수 있다.

[표 4-11] FDS 이해관계자 식별과 관심사항

이해 관계자	관심사항
정보사용자(User)	<ul style="list-style-type: none"> <li>• 금융사기 실시간 탐지 여부</li> <li>• 탐지결과 실시간 파악</li> <li>• 탐지시스템 사용방법</li> <li>• 탐지시스템 사용, 설치 가이드라인</li> </ul>
정보시스템인수자 (Acquirer)	<ul style="list-style-type: none"> <li>• FDS 사용, 설치 가이드라인</li> <li>• 시스템 경제성</li> </ul>
정보시스템개발자 (Developer)	<ul style="list-style-type: none"> <li>• FDS 이해관계자 식별여부</li> <li>• FDS 사용자 요구사항 조사</li> <li>• FDS 구현절차</li> <li>• FDS 사양</li> </ul>
정보시스템유지보수자 (Maintainer)	<ul style="list-style-type: none"> <li>• FDS 설치방법</li> <li>• FDS 유지보수 방법</li> <li>• FDS 정보 업데이트 방법</li> </ul>

#### 나. FDS 아키텍처 기술서 준수 여부

소프트웨어 아키텍처 설계 절차에서 이해관계자와 이해관계자들의 관심을 식별해서 아키텍처 기술서에 명시해야 한다. 아키텍처 기술서는 뷰(view)들로 이루어진다. 관점은 모델(model) 작성 방법을 정의하고 어떤 모델(Model)의 어떤 부분이 어떤 뷰를 만들 때 꼭 필요한 것인지 정의한다. 관점의 정의에 따라 모델(model)들 가운데 꼭 필요한 뷰를 작성한다. 이해관계자 관점을 논리, 프로세스, 개발 관점, 유즈케이스 물리 관점 기준으로 정리하면 아키텍처를 도출할 수 있다.

### 4. FDS 운용 측면

#### 가. FDS 기능 최적화 작업

FDS 기능에서 어려움은 데이터의 분리처리와 분석으로 인한 분석기능 취약성(Fragmented data)을 들 수 있다. 알려지지 않은 새롭게 등장하는 패턴의 증가(Previously unknown, newly emerging, schemes)로 기능 최적화 작업은 지속적으로 이뤄져야 한다. 사기거래를 정교하게 잡아내



오탐율을 최소화하는데 가장 중요한 부분이다. 오탐율을 최소화하는 근거는 얼마나 많은 패턴과 경험을 보유했느냐에 따라 달라진다. 대부분의 금융기업들은 FDS 활용패턴이 고객행태분석과 패턴 정립이후 임계치를 넘기면 바로 차단하는 과정을 진행하고 있다. 또한 오탐 방지를 위한 전담인력의 분석역량 강화를 주요 활용분야로 생각하고 있다. FDS 기능 최적화 작업은 운용현장의 핵심소재이다. FDS의 핵심은 탐지율 높이는 것이다. 그러기 위해서는 FDS 조직을 통해 분석 역량을 강화하고, 끊임 없이 고도화하는 작업이 필요하다. 현재 시장에서는 FDS를 실제로 구축하고 운영하면서, 실제 금융사고를 대응해 본 솔루션업체가 부족하다. 축적된 Know-how를 기반으로 제품이 개발되어 시스템 Open 즉시 FDS의 정상운영이 가능해야 성과를 낼 수 있다. FDS를 도입했다고 해도 오탐율은 발생하기 마련이다. 의심이 들면 일단 차단하고 확인하는 과정이 필요하다. FDS 고도화 작업을 통해 분석능력 전문성을 지속적으로 높여야 한다.

#### 나. FDS 기능 만족도 문제

2015년 FDS 구축동향 실제 운영 현황자료를 보면 실제 구축과 운영에 있어서는 FDS Know-how 부족으로 구축 및 실제 FDS운영에 어려움을 겪고 있다는 의견이 있으며 기타 다음과 같은 불편을 호소하고 있다.

- FDS 시스템은 실시간 분석이 불가능하다.
- FDS 시스템은 기초적 데이터마이닝, 통계분석만 가능하다.
- FDS 운용 Knowhow 부족으로 분석이 어렵다
- FDS는 बैं킹과는 분리된 시스템이다.
- FDS 단계별 조치 및 안내가이드가 없다.
- FDS 시스템은 실시간 정보수집이 불가능하다.
- FDS 시스템은 운용환경 별로 추가기능 개발 필요하다.
- FDS 시스템의 분석결과 구체적 이상금융거래탐지인가를 모른다.

o FDS 시스템 RULE SET이 초기 수준이다(경험 미흡).

(\* 주 : FDS 구축전략 (성공사례 분석을 통한 효과적인 인터넷뱅킹  
FDS구축전략) <http://www.slideshare.net/infinigru/fds-strategy-by-infinigru>)

다. 사기방지 전문기술 지원기능, 컨설팅 기능

이상금융거래탐지는 지금까지의 금융업무와는 전혀 다른 업무로, 진화하는 금융사기범들의 사기수법을 지속적으로 모니터링하고 이를 FDS에 반영해야 한다. 분석→운영→대응이 선순환으로 운영되어야 계속 변화하는 금융사기에 효과적 대응이 가능하다. 사기방지 기술과 알고리즘은 원칙적으로 대외비 사항임. 사기공격자와 방어기관 간, 또는 금융기관 간 사기방지 알고리즘 정보를 공유할 수 없는 특수한 성격임. 만약 금융사기 방지 기술을 처음 도입 적용해야 하는 금융기관의 경우 국내 어느 기관, 어떤 전문가로부터 교육, 자문을 받아야 하는지 대안이 없다. 이를 해결하는 방법은 전문적인 기술지원과 업무 컨설팅 기능을 국가 주도로 도입하고 국내의 지도자급 인력풀을 총 가동 할 수 있는 인적자원 확보가 우선적으로 필요하다.

라. 사기사건 사례 수집 실적 빈곤

사기 발생 사례 수집정보가 절대 부족(Lack of historical examples of fraud)하다. 그 원인은 사기사건 자체를 외부에 공개할 때 발생하는 금융기관에 대한 외부의 신용도 등 이익 보다는 피해가 많다는 현실에 기인한다고 보여진다. 또한 전통적인 전자금융사고, 인터넷뱅킹 사고에 비해 사기 발생사례에 대한 자료 채집 자체가 기술적으로 어렵고 방법이 체계적이지 않다. 패턴 공유로 탐지율을 높이고, 시스템 공동 구매체계, FDS 활성화가 필요하다. 또한 오탐에 대한 고객들의 불만을 고려해 불편할 수 있는 거래상황을 이해하는 사회적인 문화가 형성돼야 한다.

#### 마. 금융기관 간 사기탐지 정보 공유 문제

패턴 공유에 대해 의문을 제기하는 부분도 있지만 사기탐지에 관한 전문기술정보, 사고 정보를 공유할수록 탐지 효율에 도움을 줄 수 있다. 코스콤과 같은 제3의 기관을 통해 통합 콜센터를 운영하는 것도 방법이다. FDS와 연계해 보이스피싱과 같은 위협요소를 관리한다면 증권사의 경우, 개별적으로 관리해야하는 보안사고 방지 수고를 덜 수 있으며, 시스템을 보다 안정적으로 운영할 수 있을 것이다. 금융당국에서도 FDS 효과를 위해 기업 간 패턴을 공유할 수 있는 환경을 조성할 필요가 있다는 입장을 밝힌 바 있다. 업계에서는 FDS가 활성화되기 위해서는 패턴 공유를 통해 서로간의 시너지를 높이고, 오탐율을 최소화 할 수 있는 분석능력을 강화하는 것이 필요하다고 강조하고 있다.

#### 바. 탐지 룰 시나리오 공개 문제

룰 시나리오 공개 시 사기범이 쉽게 파악할 수 있고 이미 공유된 패턴으로 범죄행위를 하지는 않을 것이다. 개별적으로 운영되고 있는 은행과 증권사들의 패턴(룰)을 최적화하기는 어렵다. 룰 시나리오를 공유하자는 의견도 있지만, 금융결제원 및 코스콤 또는 다른 제3의 기관에서 나선다고 해도 중재하기가 어렵다. 패턴에 대한 기밀성 확보가 전제돼야 한다. 그러나 룰 시나리오를 공유 하더라도 서로간의 공정성 부분도 요구되고 있다. 기업 간에 이해관계가 있는 만큼 서로 공유를 공정하게 해야 할 필요가 있다. 업계에서는 패턴 공유에 대해 필요성은 인식하고 있다. 은행이 개별적으로 운영하는 것은 일정부분 한계가 있고, 비용에 대한 부담이 클 수 밖에 없다. 증권사간 패턴 공유를 통해 다양한 변수들을 활용하면서 오탐율을 줄일 필요가 있다. 이렇게 되면 비용과 노력을 최소화하면서 서로 시너지를 확보하는 효과를 볼 수 있다.

## 5. 사기탐지 알고리즘 자체의 특성

### 가. 인공지능

초기 인공지능 기술은 확정된 환경에서 유한 개의 솔루션을 탐색하는 일이었다. 현실 환경은 매우 불확정적이고, 솔루션도 미리 유한개로 정해져 있지 않은 경우가 많았다. 가변적 환경에 대처할 알고리즘이 정형적 패턴의 환경에 맞춰져 있다는 것은 인공지능 기술 자체의 효용성에 문제가 되었다.

### 나. 휴리스틱

금융사기 탐지에서 태도 휴리스틱을 적용한다면 주의해야 할 하나의 차원은 허위-합의 효과(false-consensus effect)이다. 대부분이 자신과 같은 의견을 가진 사람의 비율을 과대평가하는 경향을 말한다. 즉 다른 사람들도 대부분 내가 믿는 바와 같은 신념을 가지고 있을 것이라고 비약하는 경향이다. 주의해야 할 점은 이성을 사용해야 할 경우까지 직관이나 휴리스틱에 의존할 경우 실수가능성이 높아진다.

### 다. 빅데이터 분석기술

기존의 방식으로는 관리 및 분석이 어려울 정도로 규모가 크고 그 형식 또한 다양한 데이터의 처리를 위하여 빅데이터 분석기술이 활용되고 있으며 매년 빠른 속도로 관련 시장이 성장하고 있다. 빅데이터의 활용도가 높아짐에 따라 분석에 활용되는 데이터에 대한 관리의 중요성도 높아지고 있으나 다양한 형태의 데이터에 대한 일관된 정책 적용의 한계, 중요 데이터 암호화의 어려움 등으로 인하여 빅데이터 정보에 대한 보안

위협이 증가하고 있는 상황이다. 따라서 빅데이터를 활용하여 분석하고 결과를 도출하는 각 단계에서 현실적으로 적용할 수 있는 수집 데이터에 대한 접근통제, 데이터의 안전한 저장·관리, 데이터의 필터링·등급 분류, 익명화된 데이터 처리·분석 등의 보안 조치에 대한 연구가 필요하다

#### 라. 기계학습

기계학습에서 확률추론이 차지하는 비중은 매우 크다. 반복시행 자체를 할 수 없는 경우에도 우리는 일상적으로 확률의 개념을 사용하는데 이를 Frequentist interpretation에서 다룰 수 없다. 조건이 완벽히 같은 독립적인 반복 시행은 원칙적으로 존재하지 않는다. 각각의 시행이 같은 조건에 이루어지며 서로 독립적이라는 가정이 보통의 상황에서는 성립하기 때문이다. 하지만, 엄밀히 말해서 각각의 시행은 시간 순서대로 일어나고 나중의 시행의 결과는 전 시행의 결과를 안 이후의 조건부 결과이기 때문에 원칙적으로 조건이 완벽히 같은 독립적 반복 시행이 아니다. 기계학습 알고리즘에는 한계가 노출된다.

## 제 5 장 핀테크 기술개발 분야

### 제 1 절 국내외 핀테크 서비스 보안기술 분석

#### 1. 국내외 핀테크서비스 관련 보안위협 및 사고 사례분석(결제사기 등)

##### 가. 핀테크 서비스 관련 보안위협

한국은행이 최근 국내 지급수단 이용형태를 조사한 결과 인터넷 결제를 사용하지 않는 사람 72.3%가 정보유출 가능성과 보안문제를 우려하고 있다. 특히 모바일 결제에서는 정보유출 및 보안에 대한 우려를 미사용 이유로 꼽은 비율이 78.3%나 됐다. 통계청 조사에 따르면 2014년도 온라인 결제 이용자들의 모바일 결제 미사용 이유로 정보유출 및 보안우려를 가장 중요시하고 있다. 최근 금융권 및 주요 기관에 대한 보안 위협은 장기간에 걸쳐 조직적으로 이루어지고 있으며, 다양한 공격방법을 동원하기 때문에 피해 규모가 크고, 사전 탐지가 어려운 특성을 지닌다. 이상 징후를 사전에 포착해 선제적으로 대처할 수 있게 해주는 FDS 기술은 전자금융거래 안전성을 확보하고 이용자들을 보호하기 위한 대책이 필요하다. 금융사기의 급증 및 지능화와 금융사기단의 조직화 및 대규모화, 외국인이 포함된 금융사기는 증가하고 있다. 또한 날로 발전하는 금융사기 패턴 거래채널 다양화, 개인정보유출증가, 금융시장환경 및 감독기관 요구사항 금융사기 증가 등 사례가 나타나고 있다.

##### 나. 금융사고 분류 방식

금융사고 유형은 사고발생 형태를 기준으로 분류할 수 있으며 다른 방

법으로 업무방식 기준으로 분류할 수 있다.

#### (1) 사고발생 형태 기준

금융감독원의 분류기준이 있는데 금융감독원이 발표하는 통계자료에서는 금융사고의 유형을 횡령·유용, 사기, 도난·피탈, 기타로 구분하고 있다. 사고 발생 형태별 금융사고의 유형을 설명해보면 먼저 횡령·유용은 금융기관 직원에 의한 사고가 대부분을 차지하는 사고로 금융기관의 공금을 불법적으로 가로채거나 일정한 용도 이외에 다른 곳으로 전용하는 행위, 또는 일정한 기간 동안 타인의 동의없이 임의로 사용하는 행위를 의미한다. 사기라는 뜻은 타인을 속여 재산상의 이익을 취하는 행위이고, “도난·피탈”은 CD/ATM, 금융기관 영업점 등에서 현금을 빼앗는 행위를 포함한 각종 현금 도난사고를 의미한다.

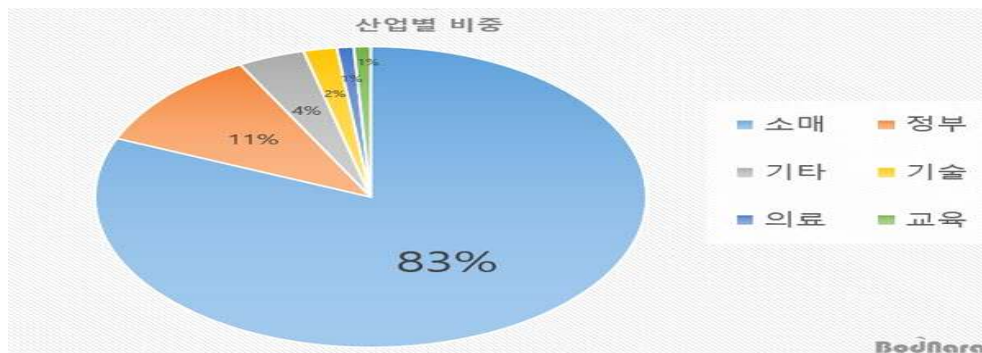
#### (2) 업무처리 방식 기준

형태별 분류가 아닌 업무처리 방식에 따라서 분류할 경우는 전통적인 일반 금융사고와 전자금융 사고로 분류 될 수 있다. 일반 금융사고는 전통적인 은행 창구업무 과정의 금융사고이며, 전자 금융사고는 폰뱅킹, 인터넷뱅킹 등 전자금융서비스와 관련된 사고와 각종 해킹에 의한 금융사고를 말한다. 금융사고의 개념이 위법한 행위에 초점을 두었기 때문에 업무 수행중 발생하는 각종 전산장애는 전자금융사고는 아니다. 전자 금융사고는 다시 전자금융서비스 처리중 발생하는 각종사고와 해킹등 의도적인 정보보호 침해 사고로 구분된다.

#### ※ 세이프넷이 발표한 2014년 2분기 BSI 결과

세이프넷이 정기적으로 발표하는 전세계 데이터 유출/침해 통계인 BLI(Breach Level Index)의 조사에 따르면 2014년 2분기 전세계 각국에서 237건의 개인정보 및 기타 민감한 비즈니스 정보가 유출 사고가 발생했

으며 이를 통해 1억 7,500만 건의 고객 기록, 개인 정보, 금융 정보 등이 외부로 세어 나간 것으로 집계되었다. 이는 1분기 3억7,500만 건에 비해 다소 줄어든 수치이지만 그 이면에는 한 가지 주목할 점이 발견되었다. 2분기 유출 사건을 업계 별로 구분해 볼 때 가장 큰 비중인 83%를 차지하는 곳이 소매 업계로 나타난 것이다. 한 가지 흥미로운 사실은 2분기에 보고된 237건의 사건을 일으킨 기업이나 기관 중 데이터 암호화와 강력한 인증 수단을 기반으로 한 접근 제어 체제를 갖춘 곳은 1%에 불과하다는 것이다. 이와 관련해 세이프넷코리아 이사는 “전세계적으로 데이터 유출/침해 사건, 사고가 끊이지 않고 주요 국가에서 관련 규제 강화에 열을 올리는 것과는 대조적으로 기업 및 기관은 정보 보호에 아직도 소극적인 면을 보이고 있다”고 설명했다.



(\* 주 : 보드나라 : [www.bodnara.co.kr](http://www.bodnara.co.kr))

(그림 5-1) 전세계 데이터 유출/침해 통계

## 2. 모바일 기반 핀테크 서비스 보안기술 분석(FDS 등)

### 가. 핀테크 서비스 보안기술 구조

핀테크는 다양한 분야에 적용되면서 금융서비스의 역할과 분야는 확대되고 있다. 그 중에서도 핀테크 보안 3요소가 고려되면서 인증, 데이터



보호, 모니터링 분야 중심으로 다양한 신기술이 적용되고 있다. 핀테크 서비스와 보안기술 구조는 다음 그림과 같이 통신, 생체인식, 데이터 분석, 인증, 데이터 보호, 모니터링 서비스로 구성되며 이에 따를 기술구조가 그려진다.

구분		결제	뱅킹	투자/대출
비보안	통신	NFC (결제정보전달) BLE(결제인증) MST(결제정보전달)	NFC (결제정보전달)	
	생체인식	지문, 정맥, 음성, 필기, 얼굴 등		
	S/W		OPEN API 금융 SI (인터넷전문은행)	
	데이터분석	빅데이터 (마케팅, 부정거래감시)		빅데이터(신용평가) 빅데이터(투자정보분석)
보안	인증	IC Tagging 생체인증 규격(FIDO 등)		
	데이터보호	TEE(단말) 토큰화(네트워크)		
	모니터링	FDS(고도화)	FDS(구축)	FDS(구축)

(\* 주 : 금융보안원)

(그림 5-2) 핀테크 서비스와 보안기술 구조

## 나. 핀테크 보안 영역 구성도

### (1) 공통 기반기술을 기준으로 분류

핀테크 보안영역에서 공통 기반기술이란 보안기술로서 핀테크에서 기본적으로 사용되어야 하는 기술이다. 인증기술, 암호기술, 악성코드 분석 기술, 보안관리 등 4개 영역으로 구성되어 있다.

## (가) 공통 기반기술 영역

### o 인증기술

핀테크에서 인증기술은 단말노드에서 종단(end to end)구간에서 사용해야 할 기술이며 단말노드의 종류에 따라 차이가 있지만 다음과 같이 방식으로 구성되며 이 방식은 일반적인 보안 인증과도 다르지 않다.

- Something You Know -> 아이디와 패스워드 등 사용자가 알고 있는 정보를 이용해 인증

- Something You Are -> 지문(Fingerprints)등 생체조직을 통해 인증하는 방식

- Something You Have -> OTP(One Time Password),공인인증서등 인증 수단으로 인증하는 방식

### o 암호화기술

핀테크에서 센서와 임베디드 단말, 그리고 백엔드 서버간 송수신 되는 데이터를 암호화하는 Encryption 기술이다. 각 주체(센서, 임베디드 단말, 백엔드 서버) 간에 서로 상대방을 식별하는 Authentication, 각 주체가 자신을 식별할 수 있는 증명 정보(예: ID)를 관리하는 Identity Management, 각 주체들에게 허용되는 권한을 관리하는 Access Control 등의 기술이 있다.

## (2) 트래픽 도메인을 기준으로 분류

### (가) 클라이언트 구간

#### o 센싱 트래픽도메인 구간

핀테크에서 센서구간은 외부 변화를 감지하는 입력장치로 시청각 정보는 물론 빛, 온도, 냄새 등 물리적, 화학적 에너지를 전기 신호로 변환

하는 기능이 수행되는 영역이다. 특정 상황이나 환경에 대한 센싱이 가능한 센서(Sensor Node)와 수집된 정보를 처리하는 프로세서, 데이터 송수신 장치(Sink Node)로 구성된다. 센서네트워크 소프트웨어는 UC 버클리와 같은 TinyOS, 데이터베이스, 스토리지 관리(TinyDB), 네트워크 프로토콜(예:802.15.4, ZigBee), TinySec 보안이 적용된다.

- 보디센싱 구간 : 인체에 부착되는 센서 장치로 인체 활동을 감지하는 다수의 작고 가벼운 장치 센서가 부착된다. 사람의 신체적, 행동적 특징을 자동화된 장치로 추출하고 분석하여 정확하게 개인의 신원을 확인하는 기술. 넓은 뜻으로는 생물 데이터를 측정, 분석하는 기술을 의미하나 정보기술에서는 지문, 눈의 망막 및 홍채, 음성, 얼굴 표정, 손 측정 등 인증 목적으로 사람의 신체특성을 측정, 분석하는 기술이다.

- 환경센싱 구간 : 집안, 공장, 사무실등 인간생활 공간 상의 가전 , 전자 기구에 장착된 센서이다. 센서 사이는 무선 또는 유선 네트워크를 연결하며 환경을 스스로 인지하고 판단하기 위한 센서와 프로세서로 구성한다. RFID에서 센서는 다양한 종류의 태그가 그 역할을 한다. 프로세서는 RFID 태그안에 포함되는 칩을 의미하며 원활한 커뮤니케이션을 위해서 RFID에 안테나를 부착하고 RFID 태그를 읽을 수 있는 리더기를 사용할 수 있다.

#### o 사용자 PC 구역

핀테크에서 센서 및 임베디드 단말(HW) 보안영역이다. 데이터 소스로부터 직접 데이터를 수집하는 센서, 수집된 데이터를 모아 1차 가공 역할을 하는 임베디드 단말 부분을 담당할 하드웨어(예: NFC 센서, 모바일 폰).전력, 네트워크, CPU 등의 리소스가 충분하지 않은 제한된 환경에서 동작해야 하기 때문에 가볍고(lilght) 단순(simple)해야 하며 환경에 맞게 쉽게 Customization이 가능해야 하기 때문에 기술이 오픈된 Open Hardware(공개 하드웨어) 형식이 적합하다. 이 구간에서 이용자가 정보를 열람하고 입력 하며 입력정보를 전송하는 단순기능이 주류이다. 그러나 PC를 대상으로 하는 많은 해킹 기법이 등장하고 해킹을 자동화 형태

로 발전시킨 웹이 증가하며 PC에 저장된 개인정보를 자동으로 유출시키는 바이러스로 인해 서버 시스템에 버금가는 위협이 등장한다.

#### (나) 종단(end to end) 구간

##### o 근거리 통신 구간

핀테크 종단(end to end) 구간에는 수 많은 센서와 거기에서 나오는 임베디드 단말 사이에 원활한 데이터 송수신을 가능케 하는 프로토콜로서, 대체로 경량이어야 하고 특히 전력 소비가 적어야 한다. (예 : Bluetooth, Zigbee, Beacon 등의 기술)이다. 원거리 통신 센서에서 수집된 데이터를 임베디드 단말에서 바로 처리하는 경우도 있지만 대부분의 경우는 백엔드에 있는 분석 및 응용 시스템으로 보내야 하며 이 때 사용되는 통신이다.

##### o 원거리 통신 구간

핀테크 구간에는 근거리 만큼은 아니어도 역시 저전력, 경량 프로토콜이 필요하며 데이터에 대한 전송 보장(QoS)도 필요하다. 핀테크 구간에서도 기본적인 통신은 TCP/UDP 레이어를 사용하고 그 위에 프로토콜로는 HTTP와 함께 MQTT가 등장된다. 정보시스템 네트워킹 도메인에서 제3구역으로 설정되는 구간은 원격 통신망 구역으로서 원격 무선통신 구간을 설정할 수 있다. 선박, 항공기, 자동차 등의 이동체와 고정 국과의 상호 무선통신. 무선국이 이동하는 장소에 따라 육상 이동무선, 해상 이동무선, 항공 이동무선 등으로 분류된다. 원거리 통신인 경우 장파, 중파, 단파가 사용된다. 통신 범위가 좁은 경우는 초단파(VHF)대나 극초단파(UHF)대가 사용되며, 60MHz, 150MHz, 400 MHz, 800 MHz대가 주로 이용된다.

#### (다) 서버 구간

핀테크 서비스 시스템 호스트 구간에는 개인정보 등 중요정보가 집중되고 다수 직원 접근으로 정보유출 문제가 가장 심각한 부분이다. 호스트 구간에서는 분석, 필터링, 로깅 구간으로서 데이터가 모아져 base로 전송되므로 다양한 상태 정보를 판독하고 분석된다. 웹브라우저와 웹서버 간 전송데이터는 128bits 이상 키값으로 암호화되어 전송되므로 공개된 네트워크라 해도 1차적 위협은 서버 시스템에 대한 것이다.

#### (라) 데이터 베이스 구간

핀테크 시스템에서 수집된 데이터에서 비즈니스적으로 의미있는 결과 정보를 뽑아내고, 그것을 시각화하여 비 IT 전문가들이 쉽게 활용할 수 있도록 하는 과정이다. 대량 데이터를 저장 하고 다룰 수 있는 BigData 솔루션과 데이터에서 패턴을 찾아내는 Data Mining, 가공하는 ETL(Extract Transformation and Load), 시각화하는 BI(Business Intelligence) 등의 분야를 모두 포함하는 BI/DW 솔루션이 있다.

#### 다. 핀테크 서비스 도메인별 보안위협 요소 분석

##### (1) 클라이언트 구간

###### o 보안위협 요소

최근의 전자금융사고는 클라이언트 구간, 즉 고객이 금융기관 시스템 또는 네트워크에 접근하는 대고객 접점 영역에서 대부분 발생한다. 이는 적극적으로 네트워크 및 시스템보안에 대한 투자를 지속해야하는 금융기관 또는 전자금융업자와는 달리, 상대적으로 보안에 민감하지 않은 불특정 다수의 일반 사용자가 개방형 환경에서 다양한 용도로 사용되는 접근 매체로 서비스에 접속하다보니 인식하지 못하는 사이에 악의적 제3자에 의한 해킹 위협에 노출될 가능성이 높기 때문이다. 주요한 사고 원인 및

형태를 분류해보면 다음과 같다.

## (2) 네트워크 구간

### ○ 개요

펀테크 시스템에서 클라이언트와 서비스 제공시스템 사이에서 각종 데이터가 송수신되는 네트워크 구간에서는 데이터 도청 및 변조 공격, 네트워크 부하초래 공격이 발생할 수 있다. 스니핑이란 네트워크에서 송수신되는 데이터 트래픽을 엿볼 수 있는 도청장치인 스니퍼를 랜포트(Lan Port)나 AP(Access Point)에 설치하여 데이터를 가로채는 기법이다. 유선 인터넷 기반의 전자금융 데이터는 대부분 암호 알고리즘에 따라 암호화되어 송수신되고 있어 스니핑으로 인한 직접 전자금융사고로 이어질 가능성은 크지 않으나, 악성코드와 결합하거나 암호화되지 않은 데이터일 경우 유출에 따른 피해는 가능하다. 무선 네트워크 이용 확대 추세는 무선 환경에서의 스니핑 위협을 현실화시키고 있다. 무선망이 유선망에 비하여 물리적 특성, 인증 및 암호화 매커니즘의 취약성 등으로 인해 보안이 상당히 취약한 것으로 알려지면서 이를 겨냥한 공격 시도가 나타나고 있다.

### ○ 보안위협 요소

#### - 스니핑(sniffing) · 세션 하이재킹(session hijacking)

네트워크에서 송수신되는 데이터 트래픽을 엿보거나 가로채어 변조하는 형태의 공격으로, 대표적인 공격 기법으로는 스니핑(sniffing) · 세션 하이재킹(session hijacking) 등이 있다. 해킹 수행을 위해 네트워크 구간에서 기본적으로 사용하는 공격기법이다.

#### - 비밀번호 탈취

비밀번호 탈취는 다양한 환경에서 다양하게 이루어진다. 특히 네트워크 구간과 시스템 구간에서 발생하며 국내에서는 2007년 7월 가짜 현금 인출기를 설치, 스키머와 몰래카메라를 장착한 후 서비스를 이용한 100

여명의 현금카드를 복사하고 비밀번호를 탈취하는 사고가 발생하여 7,000만원 이상의 금전적 피해가 발생한 바 있다.

- 카드 복제 사고

IC현금카드는 2008년 12월 기준 5,628만장 발급 및 97.1%의 CD/ATM 적용률을 보이며 IC칩 전환에 성공한 것으로 평가되나, IC신용카드는 80% 가량의 카드 전환 발급에도 불구하고 IC카드 전용 단말기 보급률이 19% 정도에 불과하여 IC칩 전환에 따른 실제적 리스크 축소 효과없이 카드 복제 사고가 지속되고 있다.

- 일명 부채널공격(side channel attack)기법

IC칩 카드 내에서 암호 알고리즘 작동시 발생하는 전기소모량 · 전자 신호량 · 열 · 소요시간 등의 부가적인 정보를 측정하여 이를 통해 암호 알고리즘 및 키 값을 분석하는 공격기법이다. 2008년 일부 현금카드가 부채널공격 위험에 노출된 것으로 알려져 감독당국이 해당 복제위험 IC칩 현금카드에 대한 단계적 교체 계획을 밝힌바 있다.

- 봇(bot)

자동화된 기능을 수행하는 프로그램을 지칭한다. 악성코드에 감염된 경우 훼손된 시스템에서 자동으로 악의적 공격을 수행하는 종속 프로세스로 작동한다. 일명 좀비(zombie)라고도 불리며, 사용자가 인식하지 못한 상태로 설치 · 작동할 가능성이 높다. 봇(bot)들과 조종자(명령제어 서버, 봇마스터)로 구성된 네트워크를 지칭하며, 이를 통해 DDoS 공격 뿐만 아니라 애드웨어, 스파이웨어, 스팸발송, 불법 정보수집 등 다양한 형태의 공격이 가능하다.

- DDoS 공격

전자금융시스템 등 특정 정보처리시스템에 동시다발적으로 막대한 양의 트래픽을 발생시켜 병목 현상을 야기함으로써 정상적인 사용자의 서비스 접근을 방해하는 공격 기법이다. 이를 위해 공격자는 사전에 악성 코드를 사용자 PC에 유포하여 다수의 봇(bot)으로 구성된 광범위한 봇넷(botnet)을 구성한다. 네트워크를 대상으로 하는 DDoS 공격은 중요 노드

공격, 대역폭 소비 공격형태가 대표적이다. 금융권에서는 2007년 6월 최초의 DDoS 공격을 받은 이래 금융회사가 공격을 받았으며, 금융정보 유출이나 불법이체와 같은 금전적 피해는 없었으나 인터넷뱅킹서비스의 일시중단 또는 접속지연 문제를 겪었다. 특히 2009년 7월 7일 발생했던 DDoS 사고는 일명 7.7 DDoS 대란으로 불리며 DDoS 공격에 대한 우려를 일으켰다. 공격 대상이 되었던 21개의 주요 국내 웹사이트 중 7개가 금융기관 웹사이트에 해당하였으며, 이로 인해 최소 20분, 최대 2~3시간 가량 서비스 접속이 지연되었다. 이같은 DDoS 공격은 감염된 PC가 사용자도 모르는 사이에 공격자의 명령을 수행하는 가해자가 된다. DNS, 라우터, 스위치, 집선장치 등 한정된 대역폭의 네트워크 회선 상에 막대한 공격 트래픽을 전송하여 네트워크 서비스를 마비시키는 방식이다.

### (3) 시스템 구간

#### ○ 개 요

핀테크 시스템에서 정보의 실제적 처리 및 저장이 이루어지는 시스템 구간에서는 금융기관 및 전자금융업자가 관련 당국의 감독하에 상당한 수준의 보안시스템을 구축·운영하고 있는 만큼 사고가 빈번하게 발생하지는 않으나, 사고 발생 시 불특정 다수에게 막대한 피해를 야기할 위험이 크다.

#### ○ 위협요소

##### - 랜섬웨어 등 신종 전자금융 보안사고

네트워크 레벨의 샌드박스 기반 보안 제품을 회피하기 위해서 기능이 세분화된 모듈화된 다수의 악성코드를 통해서 구성되며 이러한 과정에서 네트워크상의 보안 솔루션 탐지를 회피하기 위해 암호화 통신을 사용한다. “지능형 악성코드”와 비교해서 랜섬웨어는 불특정 다수에게 최대한 많이 유포되어 감염을 유도하는 형태로 공격이 이뤄지고 있다. 또한, 감염 이후에 가급적 ‘감염 사실’을 최대한 오랫동안 장기 잠복하는



‘지능형 악성코드’와 달리 랜섬웨어는 파일 암호화 등을 위한 최소한의 사전 작업 이후에는 스스로 자신을 노출시켜서 제한된 시간 내에 빨리 금전 결제를 유도한다. 물론 감염 과정 및 금전 결제 과정에서 랜섬웨어 제작자가 노출되는 것을 방지하기 위해서 HTTPS 암호화 트래픽 및 토르(Tor) 등의 네트워크 기술과 함께 비트코인(bitcoin)이라는 전자화폐를 사용한다.

[표 5-1] 신종 전자금융 보안사고 유형

구분	방법
랜섬웨어	PC에 악성 프로그램 이식, 내부문서나 데이터를 암호화해 사용불능상태로 만든 후, 해독 프로그램 제공을 대가로 금전 요구
스피어 피싱	특정 개인이나 기업을 대상으로 공신력 있는 기관이나 지인을 사칭한 이메일을 보내 PC에 악성코드를 심은 후, 중요 정보를 탈취하는 기법
ATM 해킹	USB 드라이브를 활용해 악성코드를 ATM에 감염시킨 뒤, 내부에 탑재된 현금과 거래 고객의 정보를 탈취
모바일 해킹	모바일 기기의 운영체제(OS)나 앱의 보안 취약점을 공격, 개인정보를 탈취하는 행위로서 공인인증서 복제 후 전자금융사기에 악용

(\* 주 : KB금융지주경영연구소)

#### - 사용자 정보 탈취 공격

금융기관 및 전자금융업자의 내부 시스템에 침입하여 고객정보를 무단 유출하는 사고유형에 해당한다. 2008년에는 7개 상호저축은행과 여타 기관의 고객 금융정보 약 970만건이 유출되는 사고가 발생한 바 있다. 동 사고에서 공격자는 추적 가능성이 낮은 공공장소에서 인증이 필요 없는 무선 공유기에 접속하여 금융기관의 네트워크 및 서버 취약점을 수집하는 방식으로 DB 및 웹하드 계정을 획득하였고 이를 통해 고객 금융정보를 대량 유출시켰다. 이같은 고객정보 유출은 추후 이를 활용한 2차적인 금융사고로 이어질 가능성이 높다는 점에서 위험성이 크다. 특히 비금융기관의 지급결제참여가 확대됨에 따라 이들이 보유한 고객의 개인·금융

정보를 탈취하려는 움직임도 지속적으로 시도될 것으로 예상된다.

- 서버 공격을 통한 시스템 마비

DDoS 공격 중 서버 시스템을 겨냥한 DDoS 공격의 형태이다. 시스템의 CPU·메모리와 같은 가용자원을 고갈시켜 서비스를 제한하거나 시스템 자체를 마비시킬 수 있다. 공격자 집단은 정치적 의도, 보복성 공격, 금전 요구 등의 목적으로 DDoS 공격을 수행한다. 네트워크 공격 같이 범위가 광범위하지 않으나 시스템의 정상적인 운영 장애를 유발시킨다.

라. 핀테크 서비스 보안기술 분석

(1) 정보시스템 보안 도메인

핀테크 서비스에서도 정보시스템 보안 도메인은 다음과 같이 5개영역으로 구분되며 각 영역에서의 위협 발생 요소도 다음표와 같이 차별화된다.

[표 5-2] 정보시스템 보안 도메인

도메인	센싱구간	클라이언트 구간	네트워크구간	서버구간	DB구간
구성자원	.센서	.임베디드 단말기	.네트워크 .통신장비	.웹서버 .응용서버	.DB서버 .계정계서버
보안위협	.노드 포획, 아나 로그신호스니핑, 라우팅 경로 공격	.데이터도용 .불법sw실행 .불법접근접근제 어관리취약	.패킷스니핑, .데이터변조	.데이터처리 오류 .불법접근,	.보안설정부실 .패치미흡 .서버취약점
측정 체크리스 트	경량암호및인증기 술, 랑키 관리 프 라이버시보호기 술.부채널공격방 지	.사용자인증능 .데이터관리해킹 시도	도청,감청 .전송정보노 출	.전송정보노출 .보안카드번호 노출 .피싱 .파밍 .패스워드관리 .암호화,복호화	.내부통제제도 .데이터관리
측정방법	.모의침투 .취약점점검 .기술보안체계점	.모의침투 .취약점점검 .기술보안체계점	.모의침투 .취약점점검 .기술보안체	.모의침투 .취약점점검 .기술보안체계	.모의침투 .취약점점검 .기술보안체계

	검	검	계점검	점검	점검
--	---	---	-----	----	----

## (2) 인증기술 동향 분석

핀테크, 간편결제, IoT, 스마트워크, 이 모든 환경에서 공통으로 요구되는 것이 ‘인증’이다. 비대면 환경에서 본인이 자유로운 의지로 해당 거래를 진행하는 것이라는 사실을 검증하기 위해서는 강력한 보안이 보장된 인증기술이 필요하다. 어떠한 환경에서도 인증을 수행할 수 있도록 표준을 준수하면서 간편하게 인증이 완료돼야 한다는 요구도 있다. 간편결제가 부상하면서 함께 주목받는 다양한 인증기술을 진단한다.

### (가) 지문인식

금융 결제서비스에서 바이오인식이 주목받고 있는 이유는 핀테크 산업의 최대 걸림돌인 보안 문제에서 비교적 자유롭고 사용이 편리하기 때문이다. 인증을 위해 별도의 도구를 구비할 필요가 없고, 분실할 위험이 없다는 게 가장 큰 장점이다. 사실 지문인식이 개인 기기의 암호를 안전하게 대체하는 방법으로 꼽힌지 오래됐지만 상용화되지는 못했다. 애플이 아이폰에 ‘터치아이디’라는 지문인식 기술을 적용하면서 비로소 대중화시대를 맞이했다. 애플이 성공한 이유는 편의성 때문이다. 국내 지문인식 시장에서 독보적인 선두를 달리고 있는 슈프리마는 스마트폰 제조사, 통신사, 금융권, 사물인터넷 관련 기업들과 다각적인 협력을 맺고 지문인식 기술의 사용처를 다각화하고자 한다.

### (나) ‘홍채인식

지문인식 다음으로 유망한 기술이 홍채인식이다. 홍채인식은 구축비용이 높기 때문에 고도의 보안을 요구하는 연구소·국방관련 시설 등에 일

부 적용됐지만, 수요가 늘어나면서 가격이 낮아지고 활용처가 높아지게 됐다. KT가 이리언스와 기술 협업으로 IBK기업은행의 인터넷전문은행에 홍채 인식 기술을 공급하기로 하면서 홍채인식을 이용한 인증 상용화이다. 홍채정보를 은행에 전송하면 대면인증없이 온라인상에서 인증절차가 완성될 수 있을 것으로 기대된다. 홍채인식 소프트웨어와 하드웨어를 개발하고 있는 아이리시스는 홍채인식 기술을 탑재한 USB와 모바일 애플리케이션을 제공해 새롭게 열리는 홍채인식 시장을 제공한다.

#### (다) IC Tagging과 생체 인증

핀테크를 위해서는 보안 수준이 매우 높은 인증 방식을 적용해야 한다. 최근에 많은 주목을 받고 있는 인증 방식은 IC Tagging과 생체 인증 방식이다. IC Tagging은 보안성이 높은 저장 매체인 IC카드에 인증 정보를 넣고 스마트폰을 통해 인증을 하는 방식이다. IC카드를 본인이 항상 소유하고 비설치 기반이기 때문에 보안성이 높다고 볼 수 있다.



(\* 주 : 한국정보통신기술협회)

(그림 5-3) IC Tagging 인증 방식

#### (라) TEE(Trust Execution Environment)

최근에는 모바일 AP를 일반 영역과 보안 영역으로 구분하는 TEE(Trust Execution Environment)나 토큰화(Tokenization)등이 데이터

보호 역할을 해준다. TEE는 스마트폰 안에 일반 영역(Normal World)과 보안 영역(Security World)를 함께 두고 각 APP들 간 인터페이스를 통해 필요한 데이터를 주고받는다. TEE는 보안성이 매우 뛰어나지만 스마트폰에서 해당 기능을 제공해줘야 하기 때문에 제조사에 매우 의존적이라 할 수 있다. 토큰화는 결제 시 가상의 카드번호를 부여하여 서비스하는 방식이다.

[표 5-3] TEE의 장점

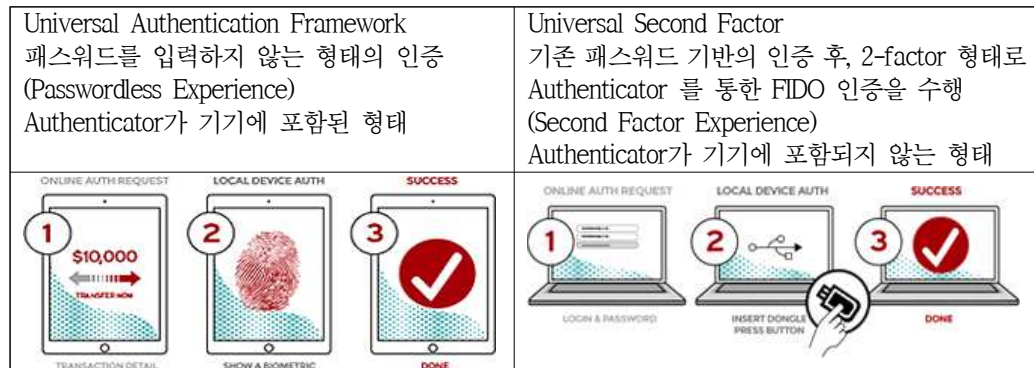
구분	장점
입출력값보호	입출력값 탈취 방지, 화면 캡처 방지
거래내역무결성제공	보안 영역의 암호화 처리로 거래 내역 무결성 제공
인증기술연동	TEE기반의 본인 인증(OTP, 인증서 등) 구현 가능

(\* 주 : 한국정보통신기술협회)

#### (마) FIDO(Fast IDentity Online) 지문인증

FIDO는 Fast IDentity Online의 약자로 아이디, 패스워드 방식보다 더 간단하면서도 안전한 인증 표준 기술이다. FIDO는 인증 데이터를 서버에 전송하는 방식이 아닌 Client의 인증장치를 통해 인증 결과 값을 생성하여 서버에 전송하고, 이를 서버에서 검증하는 간편하고 안전한 차세대 인증기술입니다. FIDO는 크게 UAF(Universal Authentication Framework)와 U2F(Universal Second Factor)로 구분한다.

UAF	U2F
-----	-----



(\* 주 : [https://www.crosscert.com/solution/03\\_7\\_01.jsp](https://www.crosscert.com/solution/03_7_01.jsp))

(그림 5-4) FIDO 구분

#### o FIDO 지문인증 기능 분석

글로벌 간편인증기술인 FIDO(Fast IDentity Online)기반의 바이오인증기술을 이용하여 별도의 패스워드 없이 공인인증서 전자서명과 본인확인이 가능한 인증으로 지문을 통해 은행, 증권 등 금융권과 간편결제 등 보안이 요구되는 서비스에서 사용가능하다.

[표 5-4] FIDO 지문인증의 특징

FIDO Authenticator + 공인인증서	FIDO Client + FIDO Sever	전자서명 + 서명검증
공인인증서 비밀번호를 바이오 정보로 대체 바이오 정보를 이용한 간편인증 스마트폰 등 모바일 단말기를 통한 인증	FIDO Client Server 바이오 인증 정보 확인 및 검증	공인전자서명을 통한 부인방지 및 서명검증

#### - FIDO(Fast IDentity Online) 국내동향

FIDO(Fast IDentity Online) 얼라이언스(Alliance)는 온라인 환경에서 생체인식기술을 활용한 인증방식인 FIDO 대한 기술표준을 정하기 위해

2012년 7월 설립된 협의회이다. 회원사로 삼성전자, 블랙베리, 크루셜텍, 구글, 레노보, 마스터카드, 마이크로소프트, 페이팔, LG전자 등이 있다. 2014년 12월 9일, 국제 인증기술 표준인 FIDO 1.0을 공개했다. FIDO는 바이오인증 서비스에 진출하여 기존 비밀번호 방식과 달리 생체 인증을 활용해 글로벌 표준으로 개발한다. 핀테크 확산과 함께 인터넷뱅킹에서 공인인증서 의무 사용이 폐지되며 차세대 인증 방법으로 FIDO 기반 바이오인증이 떠올랐다. FIDO가 각광받는 것은 생체인증 정보를 서버가 아닌 개인이 소유한 기기에서 인증하기 때문이다. 인증 거래시 스마트 기기 안전한 영역에서 인증하고 결과값을 서버에 전송한다. 이를 서버에서 검증해 본인인증을 수행한다.

#### o 한국정보인증

지문과 공개키기반(PKI) 기술을 이용해 본인을 인증한다. 한국정보인증은 FIDO 바이오인증 서비스로 해외 진출도 확대한다. 한국정보인증과 한국전자통신연구원(ETRI)는 바이오인증과 사물인터넷이 연계되는 연구과제도 수행 중이다. “현재 알리페이와 삼성페이에 적용된 FIDO 기반 바이오인증 서비스 핵심기술은 바이오인증과 PKI”이다. 한국정보인증은 15년이 넘는 공인인증 서비스 관리역량과 PKI 기술력을 결합해 서비스 하고 있다

#### o 라온시큐어

FIDO 바이오인증 솔루션을 출시했다. 간편인증·결제 솔루션 ‘터치엔원패스’는 FIDO 인증을 받았다. 터치엔원패스는 인터넷뱅킹과 카드, 간편결제, 게임, 포털 본인인증 등 다양한 서비스에 적용된다. 스마트폰·스마트카·도어락에서부터 스마트홈·사물인터넷 기기 등 본인확인과 인증이 필요한 하드웨어 전반에도 쓰인다. 인증 정보 저장이나 데이터 네트워크 전송이 필요 없는 방식을 사용한다. ETRI 웹 인증 표준 호환성 시험도구 개발 사업을 수행하며 FIDO 대체인증 핵심 기술을 확보했다. 국내 카드사에 비콘(Beacon)과 FIDO 인증기술을 결합한 간편결제 시범 서비스를 구축했다.

#### o 한국전자인증

FIDO 바이오인증 사업에 진출한다. 최근 한국인터넷진흥원(KISA)이 진행하는 PKI2.0 프로젝트인 ‘FIDO와 공인인증서 연계 기술개발’ 사업을 수주했다. 글로벌 바이오 인증솔루션 기업인 크루셜텍과 협력해 공동개발을 추진한다. 바이오정보를 공인인증서와 결합해 이용이 간편하면서도 안전한 서비스를 제공하고 있다.

#### - 비트코인2.0 '블록체인' 인증

MIT공대 연구팀은 '아이덴티티 확보를 위한 분산화된 공개키기반구조 (A Decentralized Public Key Infrastructure with Identity Retention)'이라는 논문을 통해 일명 '서트코인(Certcoin)'을 제안했다. 비트코인 생태계의 근간을 이루는 블록체인에서 아이디어를 차용해 별도 관리기관 (Certificate Authorities, CA) 없이도 분산화되고 안전한 인증체계를 만들 수 있다. 공인인증서가 은행뿐만 아니라 각종 전자정부를 활용한 민원서류 발급, 조달청 입찰 등에서 활용되고 있다는 점 때문에 비트코인 생태계에서 시작된 블록체인이 개인정보유출이나 해킹 등으로부터 보다 안전하면서 저렴한 수단으로 재조명되고 있다. 한국형 인증서 발급 시스템이 가진 맹점을 비트코인 생태계의 근간을 이루는 블록체인이 해결할 수 있을 것이다.

#### - 터치엔 원패스 인증

사용자 본인의 홍채정보가 있어야 하기 때문에 USB를 분실해도 생체 정보가 유출될 우려가 없다. 기존의 시스템에 변화를 주지 않고 적은 비용으로 적용할 수 있으며, 홍채인식 USB는 OTP 단말과 비슷한 금액으로 공급할 수 있어 비용장벽 없이 사용자를 확보할 수 있다. 홍채는 위변조가 어렵고 가장 높은 정확성을 갖고 있어 생체인식 분야 중 가장 빠르게 상용화 될 것으로 예상된다. 이 기술을 이용하면 본인인증과 전자서명을 위한 인증장치를 안전한 USB에 저장할 수 있다. 전자금융거래시 홍채인증으로 본인인증을 완료한 후 USB 키를 USB 포트에 연결하면 금융 웹사이트에서 바로 로그인, 송금, 금융결제에 가능하다. USB에 OTP를 내장



시켜 2차인증이 필요할 때 일회용 비밀번호를 제공할 수 있다. 생체정보는 USB의 안전한 하드웨어 보안영역에 암호화 돼 저장된다.

- 공인인증서

기본적으로 PKI에 대해 국제전기통신연합(ITU-T)이 정한 표준기술인 'X.509' 표준을 따른다. 공개키, 개인키를 생성하고 이를 통해 상대방과 통신이 안전하다는 사실을 확인하기 위한 일련의 절차를 따른다는 것이다. PKI 기술을 공급해 온 기업들은 공인인증서에서 벗어나 다양한 분야에 PKI를 적용하고자 한다. 인증과 전자 서명, 무결성 검증 기능을 함께 제공하는 PKI는 모든 거래에서 본인인증과 부인방지 기능을 제공하기 때문에 금융거래를 비롯해 많은 분야에 적용할 수 있다. 중요한 전직서를 보내거나 대금 청구서를 보낼 때, 기밀정보가 포함된 이메일을 전송할 때 등 위변조 방지와 부인방지가 가능한 PKI가 유용하게 사용될 수 있다. 공인인증서를 처음 발급하기 위해 은행을 활용하는 경우를 생각해 보면 다음과 같다. 먼저 사용자 PC, 스마트폰으로 인터넷뱅킹사이트/모바일뱅킹앱으로 은행 서버에 접속, 필요한 개인정보를 입력한 뒤 인증서 발급을 신청하면 은행은 해당 정보를 공인인증서 발급 기관에 보낸다.

(3) 코드 사이닝 기술 동향

코드 사이닝은 소프트웨어를 만든 사람이나 회사의 이름을 알려주는 다이얼로그이다. 즉 개발사가 개발한 결과물을 암호학적으로 사인했다는 것. 소프트웨어를 사인하는 것은 최종사용자들에게 적절한 다이얼로그를 보여줌으로써 그 사용자들이 이상한 바이러스를 설치하는 것이 아니라는 신뢰감을 갖게 한다. 디바이스 드라이버의 경우에 코드 사인은 사용하는 윈도우 버전에 따라 더 필수적이다. 핀테크 시스템에서 사용되는 소프트웨어도 보안을 위해 코드 사이닝을 통해 원 저자의 다이얼로그를 적용해야 할 필요성은 동일하게 존재한다.

#### o SHA-1과 SHA-2

이 문서는 원래 2013년 1월에 최초로 나왔고, SHA-2 해쉬 알고리즘을 사용하는 인증서를 쓰면서 겪었던 문제들을 설명한 문서이다. 처음 글을 낸 이후에, 마이크로소프트는 2016년 1월에 SHA-1을 deprecate할 것이라고 발표(Deprecation of SHA-1)했다. SHA-1은 더 이상 장기적인 방법이 될 수는 없으므로 많은 분들이 SHA-2로 바꿀 것을 고려하기 시작하였다. 2012년 후반부터 SHA-2 인증서들을 사용하려고 했을 때 겪었던 여러 문제들에 대해서 경고하는 내용을 담고 있다. 그런데 이들중 많은 부분이 해결된 상태. KB-2763674는 윈도우 비스타에서 SHA-2를 사용해서 실행 파일을 사인했을 때 발생하던 문제점을 해결했다. 윈도우 비스타 64비트 버전에서는 커널 드라이버를 SHA-2 인증서로 사인하고 로드하는 게 거의 불가능 하다. SHA-2 인증서로 변경할 때 문제점은 대부분의 윈도우 컴퓨터들의 “신뢰할 수 있는 루트 인증서 기관(Trusted Root Certification Authorities)” 리스트에 루트 인증서가 이미 포함된 인증서 제공회사를 찾는 일이다.

#### (4) RSA cryptosystem

실행파일이나 드라이버 파일을 사인하는 작업들은 1970년대에 Rivest, Shamir, and Adleman이 발명해 낸 RSA cryptosystem 시스템을 사용하게 된다. RSA가 제공하는 것은 공개키와 개인키라는 것으로 구성된 키 쌍(pair)을 생성하는 방법이다. 공개 는 우리가 이하  $f$ 라고 부를 함수를 제공한다. 메시지를 암호화(encrypting)하고 복호화(decrypting) 하는 것은 각각 함수  $f$ 와  $g$ 를 호출한다. 누구나 메시지를 받는 사람의 공개키로부터 얻은  $f$ 함수를 통과하도록 해서 암호화를 할 수 있다. 받는 사람은 암호화 된 메시지를 읽을 수 있는 유일한 사람이며,  $g$ 를 적용하여 복호화 한다. 메시지를 사인(Signing)하고 검증(verify)하는 것은 함수  $g$ 와  $f$ 를 각각 적용한다. 보내는 사람은 메시지에 대한 시그니처를 만들기 위해

그의 메시지를(또는 메시지의 해쉬) 그의 개인키로부터 얻은  $g$ 함수에 넘겨준다. 보내는 사람만이  $g$ 에 접근할 수 있기 때문에 유일하게 이 작업을 할 수 있다. 이 메시지를 받는 모든 이는 공개키로부터 얻은  $f$ 함수를 시그니처에 적용하여 모든 것이 일치하는지 검증할 수 있다.

#### (5) 카드정보 저장 토큰제이션(Tokenization)

핀테크 서비스의 형태는 다양할 수 있으나 결국 거래에 필요한 데이터를 주고 받는다는 점은 동일하다. 이 데이터를 보호하기 위해서 암호화를 적용해야 한다. PCI-DSS에서 요구하고 있는 조건이다. PCI-DSS는 국제 데이터 보안 표준 규격 중 하나이다. 이 규격은 비자, 마스터, 아메리칸익스프레스, JCB, 유니온페이 등 글로벌 신용카드사에서 정보 유출을 막기 위해 설립한 신용카드협회 보안표준위원회(PCI SSC)에서 만들었다.

##### o PCI-DSS 규격

PCI-DSS 규격의 암호화 방법인 토큰제이션(Tokenization)은 카드사 서버 방화벽 내부에 사용자의 카드정보를 저장하고, 실제로 이를 사용할 때는 무작위로 생성된 16자리의 숫자를 제공한다. PCI-DSS 구성은 ▲방화벽 ▲초기 비밀번호 ▲암호화 ▲보안통신 ▲백신 ▲시스템 업데이트 ▲액세스 제어 ▲고유 ID ▲물리적 액세스 ▲로그관리 ▲지속적인 테스트 ▲사람 등 12개의 규정 및 하부 규정으로 되어있다. 토큰제이션(Tokenization) 효과는 사용자 카드정보를 토큰제이션으로 암호화한 뒤, 복호화에는 HSM을 사용하면 사용자는 안전한 결제를, 사업자는 개인정보의 안전한 보관이 가능하다. 토큰제이션이 적용된 데이터는 유출돼도 상관이 없을 정도로 강력한 보안을 제공한다

#### (6) 데이터 안전저장과 인증HSM(Hardware Security Module)

온라인 / 인터넷 업무 환경의 확대와 데이터 보안을 위한 암호화(PKI, SSL/TLS 등)의 적용에 따라 데이터를 보호하는 암호화 키(Cryptographic Key)에 대한 안전한 저장/관리 및 고속의 암호화 처리를 수행할 수 있다. 전용 하드웨어에 대한 요구에 따라 출현하게 된 하드웨어 암호화 장비이며 PKI 기반 시스템 운영의 핵심인 서버의 개인 키를 HSM에 보관하여 관리 및 보호한다. HSM은 인증서 발급, 전자서명 및 서명 검증 등의 암호업무 수행 시 서버의 부하를 감소 및 암호화 성능 향상을 위하여 필요하다. 금융권에서 운영되어지는 키의 보호 및 관리 상황을 충분하게 이해하여 각 업무별 Key를 적절하게 HSM에 적용할 수 있도록 방안을 강구해야 한다. HSM을 이용하여 암호화 성능 향상 및 서버의 부하 감소를 위한 기능을 사용한다.

#### o HSM 사례

##### - Luna SA - 네트워크 연결형 HSM

네트워크 연결형 하드웨어 보안모듈인 SafeNet Luna SA는 사내, 가상 및 클라우드 환경에 있는 애플리케이션에서 사용되는 암호화 키 보호 기능이다.

##### - Luna PCI-E - 내장형 HSM

내장형 PCI-E HSM인 SafeNet Luna PCI-E는 암호화 키에 대해 암호화 가속과 뛰어난 보호 기능을 제공한다.

##### - Luna G5 - USB 연결형 HSM

USB 연결형 HSM인 SafeNet Luna G5는 휴대형 어플라이언스에 키 관리 기능을 제공한다.

\* 출처 : 한국전자인증 [https://www.crosscert.com/solution/03\\_2\\_06.jsp](https://www.crosscert.com/solution/03_2_06.jsp)

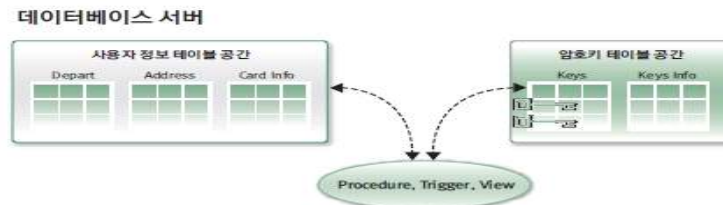
## (7) DB보안

### (가) DB 암호화 개요

핀테크시스템에서 적용하는 DB 암호화는 전통적인 암호화 방법론을 따르되 핀테크에서의 특징을 고려해야 한다. 2012년 3월 30일 개인정보 보호법이 본격 시행되면서 전체 350만 공공기관 및 기업이 개인정보 보호를 의무적으로 도입하여야 한다. 이 상황은 핀테크시스템에서 수집하는 DB 암호화 방법론과 동일하다. DB암호화솔루션은 개인정보보호법 의무화하고 있다. DB암호화 특징은 Web기반 인터페이스로서 웹기반의 인터페이스를 통한 OS중독성 제거 브라우저 중독성 제거, Dashboard를 통한 Easy status viewing, Dashboard를 통해 초기페이지에서 KMS, KS, 암호화 진행상태 및 작업내역 확인가능 등 이다. DB는 기업의 IT자산 중 가장 가치 있는 핵심으로서 고객정보, 재무 데이터, 거래 기록 등을 유지·관리하고 있다. 이러한 DB를 보호해야 하는 중요성은 점점 증가하고 있지만 이를 수행해야 하는 일은 매우 어렵고 특히 암호화를 수행하는 경우는 더욱 그렇다.

#### (나) 암호화 알고리즘 요건

일반적인 암호화 알고리즘 요건은 암호화될 데이터의 중요성에 따라 어떤 암호화 알고리즘이 사용되는가와 암호키 사이즈가 어떤가에 따라 달라지게 된다. DB 암호화를 위해 DES 알고리즘이 많이 사용되고는 있지만, 다소 보안성이 약한 것으로 여겨지기도 한다. 반면, 3DES 알고리즘은 속도 면에서 뒤떨어지기는 하나 보안성 측면에서 강한 면으로 인해 널리 사용되고 있다. 사실상 3DES 알고리즘은 보안 알고리즘 중에서 속도가 뒤떨어지는 알고리즘 중의 하나로 평가되기도 하지만 DB 암호화를 구축할 때는 산업계에서 안전하다고 평가되는 알고리즘을 사용할 것을 권고한다. 암호화 알고리즘의 성능과 보안성을 떠나 더욱 중요한 것은 암호키 관리이다. 시스템 성능에 미치는 영향은 애플리케이션 초기 설계부터 DB 암호화를 고려한다면 좋은 결과를 가져올 수 있다.



[그림 3-2-1] DB 서버 내부에서의 암호화

(\* 주 : <http://www.dbguide.net/db.db?>)

(그림 5-5) DB서버 내부의 암호화

#### (다) DB 암호화 제품 보안 요구사항

데이터 암호화 자체는 암호화 알고리즘에 따라 진행되므로 매우 간단하지만, 암호화에 사용되는 키 관리가 매우 중요하며 신중한 관리절차가 필요하게 된다. 본 절에서 다루는 암호화의 대상이 일반 파일이나 네트워크 구간이 아닌 DB이기 때문에, DB 서비스의 연속성을 위해서 DB 암호화 후 기존 DB 제약사항 유지나 서비스의 안정성이 무엇보다 중요하다. DB에는 중요한 정보들이 여러 테이블내의 컬럼들속에 존재하고 있고, 이러한 정보들은 DB 내부의 인덱스(Index), 내장 애플리케이션(Stored Application), 패키지(Package), 함수(Function) 그리고 DB 외부의 애플리케이션들과 밀접하게 상호 작용하므로 DB 암호화 후에도 이러한 시스템적 관계유지가 절대적으로 필요하다. 또한, DB 암호화를 위해 솔루션 도입 시에는 다음의 국가정보원 “DB 암호화 제품의 핵심 보안요구사항(<http://www.kecs.go.kr>)” 을 준수해야 한다. 또한, DB 암호화 시에 사용되는 모듈은 다음 국가 정보원의 검증대상 알고리즘(암호 검증 기준 - KS X ISO/IEC 19790)을 사용해야 한다.

(\* 주 : <http://www.dbguide.net/db.db?>)

#### (마) 일방향(해쉬함수) 암호화

#### o 일방향 암호화

일방향 암호화 방식은 해쉬함수를 이용하여 암호화된 값을 생성하며 복호화되지 않는 방식이다. 해쉬함수는 임의의 길이를 갖는 메시지를 입력으로 하여 고정된 길이의 해쉬값 또는 해쉬 코드라 불리는 값을 생성하며, 동일한 입력 메시지에 대해 항상 동일한 값을 생성하지만 해쉬값만으로 입력 메시지를 유추할 수 없어 전자서명 체계와 함께 데이터의 무결성을 위해 사용된다. 비밀번호와 같이 복호화가 필요 없지만 입력값의 정확성 검증이 필요한 경우에 사용하고 있다. 대표적인 해쉬함수로는 SHA-2(SHA-224/256/384/512), RIPEMD-160 등과 국내에서 개발한 HAS-160이 있다.

#### (8) E-T-E 전송 암호화

##### (가) 웹서버와 클라이언트 간 암호화

핀테크 서비스가 클라이언트 서버구간으로 운용될때는 웹서버와 클라이언트 간 암호화를 적용한다. 웹서버와 클라이언트 간 개인정보 전송 시 암호화를 위하여 공인인증기관이 발급한 서버 인증서를 설치한 보안 서버를 사용하는 방식으로 웹브라우저에 기본적으로 내장된 SSL/TLS 프로토콜로 접속하는 SSL 방식과 웹브라우저에 보안 프로그램을 설치하여 접속하는 응용프로그램 방식으로 구분할 수 있다. SSL 방식은 웹페이지 전체를 암호화(웹페이지내 이미지 포함)하며 응용프로그램 방식은 특정 데이터만을 선택적으로 암호화할 수 있지만, 보안서버와 웹브라우저에 부가적인 프로그램을 설치해야한다. 공공기관에서는 국가정보원이 안전성을 확인한 암호모듈 또는 제품을 적용해야 한다.

##### (나) S S L 방식

핀테크 서비스가 클라이언트 서버구간으로 운용될 경우 SSL 방식은 전송 계층(Transport Layer)을 기반으로 한 응용계층(Application Layer)에서 암호화를 수행한다. 암호키 교환은 비대칭키 암호알고리즘을 이용하고, 기밀성을 위한 암호화는 대칭키 암호 알고리즘을 이용하며 메시지의 무결성은 메시지 인증 코드(해쉬함수)를 이용하여 보장한다. 인터넷 쇼핑이나 인터넷뱅킹 시 계좌정보 및 주민등록번호 등과 같은 중요한 정보를 입력할 때, 거래당사자의 신원 및 거래 내용의 위·변조 여부를 확인하고 중요정보가 제3자에게 유출되는 것을 막기위해 SSL/TLS와 같은 통신 암호기술을 이용할 수 있다. 사용자가 웹서버에 처음 접속하면 인증서 및 통신 암호화에 이용할 암호키를 생성하기 위한 정보를 공유하고, 이후 공유된 정보를 통해 생성된 암호키를 이용하여 데이터를 암호화하여 전송한다.

#### (다) 응용프로그램 방식

핀테크 서비스에서 사용되는 응용프로그램 방식은 별도의 모듈을 서버와 클라이언트에 설치해야 하며 필요한 데이터만 암호화하여 전달할 수 있다. 이를 위해 웹서버 프로그램에 대한 수정작업이 필요하며, 응용프로그램 방식을 제공하는 솔루션에 따라 수정작업의 범위가 달라질 수 있다. 보안서버를 구현한 웹서버에 사용자가 접속하면 사용자 컴퓨터에 자동으로 보안 프로그램이 설치되고 이를 통해 개인정보를 암호화하여 통신이 이루어진다. 웹브라우저의 확장기능인 플러그인 형태로 구현되며 웹사이트접속 시 초기화면이나 로그인 후 윈도우 화면 오른쪽 하단 작업 표시줄 알림 영역을 확인하여 프로그램이 실행되고 있음을 알 수 있다.

#### (라) 개인정보처리시스템 간 암호화

핀테크 서비스에서 개인정보처리 시스템간에 개인정보를 전송할 때 암호



호화를 지원하기 위하여 공중망을 이용한 VPN(가상사설망)을 구축할 수 있다. VPN은 기반이 되는 보안 프로토콜의 종류에 따라 IPsec VPN 방식, SSL VPN 방식, SSH VPN 방식 등으로 구분할 수 있으며, 개인정보처리시스템 간의 통신에서 사용할 수 있는 VPN 전송 방식도 있다.

#### (마) IPsec VPN 방식

IPsec VPN 방식은 응용프로그램을 수정할 필요가 없으나 IPsec 패킷의 IP 주소를 변경해야하는 NAT와 같이 사용하기 어려운 점이 있다. 사용자 인증이 필요 없으므로 VPN 장비 간 서로 인증된 경우, 사용자는 다른 인증절차를 거치지 않아도 된다. IPsec VPN 방식의 구조는 게이트웨이 대 게이트웨이, 호스트 대 게이트웨이, 호스트 대 호스트로 구분할 수 있다. 게이트웨이 대 게이트웨이는 네트워크 간의암호화 통신, 호스트 대 게이트웨이는 개인정보처리시스템과 네트워크 간의암호화 통신, 호스트 대 호스트는 개인정보처리시스템 간의 암호화 통신을 설정할 수 있다.

#### (바) S S L VPN 방식

SSL VPN 방식은 응용프로그램 수준에서 SSL/TLS을 구현하는 것이일반적이며 NAT를 사용할 수 있다. SSL/TLS는 메모리 소비가 많으므로 동시 접속이 많은 대용량 처리에서 성능 저하가 발생할 수 있다. 하지만 개별사용자 인증이 필요한 경우 SSL VPN 방식이 좋은 선택이 될 수 있다.

#### (사) SSH VPN 방식

SSH VPN 방식은 응용계층의 VPN 기술로서 원격 단말기에서 접속하

는 경우에 주로 이용되며 SSH를 이용한 파일 전송 및 파일 복사 프로토콜(예: SFTP, SCP)을 이용할 수 있다. 오픈소스 SSH의 일종인 OpenSSH의 경우 프락시 방식의 VPN 서버로 구성할 수도 있다.

#### (아) 개인정보취급자 간 암호화

개인정보취급자 간에 개인정보를 전송할 때 주로 이메일을 이용하게 된다. 이메일은 네트워크를 통해 전송되는 과정에서 공격자에 의해 유출되거나 위조될 가능성이 있다. 이러한 위협으로부터 이메일로 전송되는 메시지를 보호하기 위해서 PGP 또는 S/MIME을 이용하는 이메일 암호화 방식과 암호화된 파일을 이메일에 첨부하여 전송 하는 이메일 첨부문서 암호화 방식이 있다. 개인정보취급자 간에 이메일을 사용하지 않고 직접 파일을 전송하고자 하는 경우는 개인정보처리시스템 간 전송시 암호화 방식의 VPN 기능을 적용할 수 있다.

#### (9) 모바일 지불결제(Payment) EMV

##### o 루프페이(LoopPay) 기술

루프페이 기술은 마그네틱 기반의 신용카드 정보를 단말에 등록하고 별도의 자기장 발생 장치를 통해 외부의 POS (Point Of Sale) 단말의 자기인식 센서 부근에 위치시킨다. 신용카드의 마그네틱을 단말에 긁는 (Stripe) 효과를 내어 신용카드를 이용할 수 있다. 이 방식의 장점은 기존 POS 단말에 별도의 장치를 설치하거나 교체하지 않고 갤럭시S6 등 단말을 이용해서 신용카드를 결제하는 것과 동일한 효과를 낼 수 있다. 삼성전자는 페이팔(PayPal)과 전략적인 제휴를 진행하면서 결제시장에 뛰어 들었다. 페이팔은 전세계에서 널리 사용되고 있는 서비스이긴 하지만 신용카드를 사용하는 사람들의 숫자에 비하자면 그 규모가 작다. 루프페이가 삼성전자에게 매력적일 수 밖에 없는 것은 많은 사용자층을 한번에

확보할 수 있는 동시에 페이팔과 같은 좀 더 진보된 솔루션을 한 서비스로 만들 수 있는 점이다. 삼성페이를 사용하면, 지갑에서 카드를 꺼내지 않고, 스마트폰을 단말기에 갖다 대는 것으로 결제가 된다. 루프페이 기술은 마그네틱 (Magnetic) 카드 정보를 읽어 칩에 저장하고, 다시 아날로그로 형태로 만들어 저장된 정보를 단말기(POS, Point of Sale)까지 자기장(Magnetic Field)으로 전송하는 기술이다.

#### (10) 근거리 센싱 및 통신 NFC(Near Field Communication)

핀테크 서비스에서 사용되는 NFC란 근거리 무선통신 기술이다. 10cm의 가까운 거리에서 스마트폰과의 데이터를 전송하는 기술이다. 현재 간편결제 뿐 아니라, 여행정보, 마켓, 교통기능, 출입통제, 잠금장치, 실행하고자 하는 APP 및 단축스티커 등 다양한 방면에서 사용이 가능하다. NFC를 활용한 결제서비스인 “NFC 간편결제“이며, 소비자 스마트폰의 NFC기능과 신용카드를 활용하여 온라인, 모바일 쇼핑결제를 하는 서비스이며 모바일 결제 시 카드정보나 개인정보등을 입력하지 않고 대중교통 요금을 지불하듯이 스마트폰 뒷면에 터치만으로 결제를 할 수 있는 간편 결제서비스다. 소비자 본인의 스마트폰이 카드단말기가 되는 것이다. 특히 결제 시 카드정보와 개인정보를 입력하지 않아도 되는 장점을 가지고 있으며 이는 휴대폰 분실 및 해킹 등의 보안문제로 부터 보다 안전하다 판단 받고 있다.

(\* 주 : <http://youtu.be/rKctE8UiXLU>)

애플에서 발표한 아이폰6에서 지원되는 애플페이는 아이폰6의 NFC기능과 카카오페이나 페이팔과 같은 간편결제 기능을 합쳐 놓은 모바일 간편 결제서비스. 즉 스마트폰의 NFC를 통해 모바일쇼핑이 가능하고 식당에서 플라스틱 카드 대신 휴대폰을 통해 결제를 할 수 있다. NFC 간편결제는 스마트폰의 NFC기능과 신용카드의 터치만으로 결제를 한다. 즉

소비자 본인의 스마트폰이 결제 단말기 역할을 하게 되고 소비자 본인이 버스나 지하철의 교통요금을 지불하듯 터치만으로 결제가 완료되는 시스템이다. 특히 결제 시 카드정보와 개인정보를 입력하지 않아도 되는 장점을 가지고 있으며 이는 휴대폰 분실 및 해킹 등의 보안문제로부터 보다 안전하다 판단받고 있다. 근거리 센싱 및 통신의 종류는 다음표와 같다. WI-FI, Bluetooth, Zigbee, Z-wave등이 핀테크에서 가장 널리 사용될 수 있는 무선통신방식이다.

#### (가) WiFi

핀테크 서비스에 와이파이가 사용될 경우 와이파이는 장소에 관계없이 액세스 포인트만 있으면 누구나 사용할 수 있다. 기존 모바일 통신에 비해 월등히 높은 속도도 자랑한다. IoT 기술이 진화될수록 와이파이 사용량은 더욱 늘어날 것으로 예상된다. 최근 상용화에 성공한 와이파이 802.11ac 계열은 초기 전송속도가 1Gbps에 이른다. 와이파이의 가장 큰 약점은 반드시 액세스 포인트가 필요하다는 점이다. 가정용 기기 간 통신할 때 적절한 위치에 AP를 설치해야 한다. 사무실에 쓰이는 기기 간 통신을 위해서는 방마다 일정 거리를 확보할 수 있는 AP가 필요하다. 또 와이파이 주파수인 2.4GHz와 5GHz는 기존 기기 채널로 많이 쓰이고 있다. 트래픽 증가로 속도가 떨어질 수 있고, 보안에 취약한 편이다.

#### (나) Bluetooth

핀테크 서비스에 블루투스가 사용될 경우는 간단한 제어신호 전달을 목적으로 고안된 통신기술이다. WiFi와 동일하게 Zigbee는 대비 높은 전력 소모와 가격, 또 페어링의 단점으로 인하여 한동안 사물인터넷에서 제외되었던 기술이다. 하지만, 전력소모와 가격을 개선한 Bluetooth 4.0 single mode(Bluetooth Low Energy)의 출시와 함께 다양한 의료기기, 생

체센서 및 스마트홈 솔루션에 적용되어 스마트폰과 함께 사용되고 있다. 그러나, 대용량 데이터를 전달하지 못해 마스터 기기에 적용하기 어려운 한계가 있다

#### (다) Zigbee

지그비는 블루투스보다 간단한 구조의 칩으로 저전력·낮은 가격을 구현한 통신기술이다. 핀테크 서비스에 지그비가 사용되면 무선 키보드·마우스·무선 조명제어·무선 센서네트워크 등에 사용된다. 현재까지 누구도 반론할 수 없을 정도로 확고히 사물인터넷의 연결 기술로 거론되고 있으며 통신거리 확장성은 수백미터까지 가능하며, 사물인터넷에서 요구되는 저전력, IPv6, Meshing 등의 다양한 기능을 지원하지만, 서로 호환이 되지 않는 다양한 프로파일의 존재와 취약한 보안 등이 단점으로 거론되고 있다. 이러한 단점을 극복하고자 CSEP(Consortium of SEP 2 Interoperability)가 결정되었다.

#### (라) Z-WAVE

Z-Wave는 현재 홈오토메이션과 같이 장치를 제어하기 위해 가장 폭넓게 사용되는 RF기술이다. 핀테크 서비스에 Z-WAVE가 사용되면 저전력, 양방향 RF, 메시 네트워킹 기술과 배터리 대 배터리 지원은 센서와 장치를 제어하는 데 아주 적합하다. 또한 Z-Wave는 주요 경쟁기술인 ZigBee와는 다르게 서로 다른 벤더의 제품들과 애플리케이션 레벨에서 상호 운용되며 더 저렴하다. 그러나, 데이터를 전송하는 bandwidth가 낮아서 극히 단순한 정보만 교환 가능하고(예를 들면 On/Off), 스마트폰이나 개인의 PC를 통하여 Z-wave 장비를 제어하고자 할때 반드시 Wi-Fi Router를 사용해야 하는 단점이 있다.

#### (마) RFID 및 NFC

RFID는 사물에 부착된 정보를 안테나를 통하여 정보를 담은 전파를 보내고 컴퓨터로 해석되어 정보가 분석·집적되는 것이다. 부연하면 특정 전파를 쏘면 태그는 자신의 정보를 담고 있는 전파 신호를 방출하고 그 신호를 재수신하여 분석하는 것이다.

NFC는 근거리 통신 방식으로써 접촉만으로 바로 데이터 교환이 가능하다. 단, NFC는 읽고 쓰기 중 하나를 선택하여 단방향(one-way) 통신만 가능하기 때문에 사용자가 개입하여 내가 데이터를 받을 것인지 줄 것인지를 선택해야 하는 문제가 있는데, 여기서는 두 장치가 서로 번갈아 가며 주고 받기를 서로 알아서 하도록 프로그래밍 했기 때문에 사용자가 할 일이 거의 없다.

#### (11) 핀테크 SIM 카드 기술

##### (가) SIM 카드

SIM 카드는 가입자 식별 모듈(Subscriber Identification Module)을 구현한 IC 카드로, GSM 단말기의 필수 요소이다. 보통 단말기 뒤에 들어가는 슬롯이 있고, 이에 끼워넣는 작은 카드를 부르는 말이다. SIM 카드는 각자의 고유한 번호가 있다. 고정된 번호인 ICCID(SIM 카드 외부에 기록된 89로 시작하는 19자리 숫자)와 가입자 회선마다 달라지는 IMSI(450으로 시작하는 15자리 숫자)가 있으며, 가입자 정보를 가지고 있어서 이 카드만 끼우면 자기 단말기처럼 쓸 수 있다. 어느 곳으로 여행을 갈때 단말기가 아닌 이 작은, 지갑 속에도 들어가는, SIM 카드만 있으면 그 나라에서 전화기를 빌려 자기 것처럼 쓸 수 있고, 보안이 뛰어나서 전자상거래 등에서도 효용성이 높다. SIM 카드가 없으면 통화와 문자메시지 등 대부분의 서비스를 사용할 수 없지만, 응급 전화번호로는 전화할 수 있

다. SIM 카드가 장착되지 않은 단말기로 응급 전화번호로 전화하면 응급 전화 상황실에는 전화번호를 알 수 없어 신고자 신원 파악을 위해 단말기 고유 번호(IMEI)가 대신 표시된다.

(나) 범용사용자 식별모듈 USIM카드(Universal Subscriber Identity Module Card )

가입자의 전화번호, 신상 등의 정보를 담은 메모리 카드로 사용자 인증과 국제 로밍, 전자상거래 등 다양한 기능을 1장의 카드에 구현한다. 은행업무, 증권, 교통카드, 각종 제휴카드 등 다양한 부가서비스로 가능케 한다. 3세대 이동통신(WCDMA) 단말기 뒷부분 건전지 부근에 장착된다. 일반적으로 가입자 정보를 탑재한 SIM(subscriber identity module) 카드와 UICC(universal IC card)가 결합된 형태를 띈다.

(\* 주 : [네이버 지식백과] USIM카드 [Universal Subscriber Identity Module Card] (한경 경제용어사전, 한국경제신문/한경닷컴 )

3세대 이동통신 단말기에서 사용하는 사용자 식별 모듈은 범용 사용자 식별 모듈 (Universal Subscriber Identity Module, USIM)이다. GSM의 SIM이 확장된 표준이다. 가입자 식별 모듈(USIM)은 WCDMA 네트워크 접속 및 가입자 인증용 애플리케이션으로 통신용 스마트카드인 UICC(Universal Integrated Circuit Card)에 탑재되어 구동된다. USIM 애플리케이션은 가입자 정보, 네트워크 정보, 인증 정보 등의 중요 정보와 텍스트 메시지, 이메일, 폰 북 등의 개인부가서비스 정보를 저장한다. USIM 애플리케이션은 WCDMA 가입자인증을 위하여 인증센터 (AuC:Authentication Center)와 비밀키(K)를 공유하여 아래와 같은 인증절차를 수행한다. 이 과정을 통하여 USIM카드와 네트워크는 세션 키(CK, IK)를 획득하고 이를 통하여 무선 네트워크 서비스의 기밀성 (confidentiality)과 무결성(integrity)을 제공하게 된다.

#### (다) UICC 서비스

UICC에는 통신 인증용 USIM 애플리케이션 외에도 자바를 이용한 banking, 증권, 신용카드, 전자화폐 등의 다양한 응용서비스 애플리케이션을 탑재할 수 있다. 이들 서비스는 나라별로 서비스 방식이 제각각이었으나 최근에는 SWP를 이용한 NFC 규격으로 통합되고 있다. SIM 카드는 GSM 통신 방식을 사용하는 국가에서 표준으로 널리 사용된다. CDMA 통신 방식을 사용하는 국가에서는 일반적으로 3세대 이동통신 서비스가 시작되면서 USIM 카드 형태로 도입된다. 대한민국에서 쓰이는 CDMA 방식에는 단말기 각자에 고유번호(IMEI와 ESD)를 가지고 있어서 단말기를 바꿀 수 없고 도입되지 않았다. 2002년 6월, SK텔레콤과 KTF가 WCDMA 시범 서비스를 실시하면서 일부 도입되었으며 2007년 3월 1일 KTF가, 2007년 3월 30일 SK텔레콤이 WCDMA HSDPA 전국망 서비스를 시작하며 본격적으로 보급되기 시작했다. 2012년 5월 이후 출시되는 단말기는 OMA-MMS를 탑재하여 사업자가 달라도 MMS를 문제없이 쓸 수 있다. USIM만 있으면 기술상 큰 문제가 없지만, 이동통신사업자의 단말기 통제시스템(EIR)을 화이트리스트방식으로 운영하여 이동통신사가 허용한 단말기에서도 이동통신사업자가 허용한 서비스만 이용이 가능하다.

#### (라) USIM의 PIN 번호

대한민국에서 유통되고 있는 USIM은 PIN 번호가 초기값으로 0000으로 되어 있으며, PIN2 번호는 대한민국의 이동통신사업자 3사가 유통하는 단말기에서는 사용하지 않는다는 이유로 해당 기능을 쓰지 못하게 해 두었을 뿐 아니라, PUK2 번호 또한 공개하지 않고 있다. 각각의 USIM에는 PUK 번호(8자리로 고정되어 있다)와 PUK2 번호(8자리로 고정되어 있다)가 할당되어 있다. PIN 번호는 사용자의 필요에 따라 4~8자리로 변경할 수 있다. PIN 번호 혹은 PIN2 번호를 3회 연속 잘못 입력하면 잠기



게 되며, PUK 번호 혹은 PUK2 번호를 입력하여 PIN 번호 혹은 PIN2 번호를 다시 설정할 수 있다. PUK 번호를 10회 연속 잘못 입력하면 폐기하고 다시 구매해야 하며, PUK2 번호를 10회 연속 잘못 입력하면 특정 번호로의 발신 제한 등 해당 기능이 잠기게 된다.

(12) PCI-DSS(Payment Card Industry Data Security Standard 지불 카드 산업 데이터 보안 표준) 보안기술

(가) PCI-DSS 개요

PCI DSS는 PCI보안표준위원회(Security Standards Council)에서 주관하는 카드회원정보 관련 글로벌 인증으로, 결제 보안성을 평가받을 수 있는 체계다. PCI DSS는 예방, 탐지 및 보안 사고에 대한 적절한 반응을 포함하는 강력한 지불 카드 데이터 보안 프로세스를 개발하기 위한 실행 가능한 프레임워크를 제공한다. PCI DSS란 PCI 보안 표준 협의회(PCI Security Standards Council)에서 만든 데이터 보안 표준 인증이다. PCI 인증은 신용카드의 부정 사용 및 정보 유출을 방지할 목적으로 신용카드 결제를 수행하는 업체에 준수하도록 요구된다. 기업들은 PCI DSS 규격의 준수를 통해 비즈니스 효율성과 서비스의 효율성을 높이고, 보안위협을 감소시킬 수 있다. PCI DSS(Payment Card Industry Data Security Standard)는 신용카드 정보를 지킬 수 있는 유일한 국제 정보보호 표준이다. 핀테크로 시대에 진입하기 위해서는 카드 소유자의 데이터(Card Holder Data) 보호가 가장 기본이 돼야하며, 카드 데이터의 저장, 처리, 전송 과정에서 유출 가능성을 검증하는 PCI DSS 인증이 핵심 역할을 하게 된다.

(나) PCI-DSS 표준에서 정의하는 사항

높은 수준에서, PCI 데이터 보안 표준을 제공하는 것을 목표로 열두 요구 사항으로 구성 “카드 소지자의 데이터를 보호 할 수 있도록 설계 기술 및 운영 요구 사항의 기준을.” 다음과 같은 요구 사항은 다음과 같다

- 어떤 종류의 암호화가 사용되어야 하는가?
- 안티 바이러스를 충분히 사용하여, 또는 HIPS 등 사전 예방 기술이 사용되어야 하는가?
- 어떤 시스템 내 패치 프로토콜에 포함되어야 하는가?

(다) PCI-DSS 보안표준 위원회



(\* 주 : PCI Security Council)

(그림 5-6) PCI Security Council

(라) PCI-DSS 3.0 버전

2014.1월 1일부터 PCI DSS 3.0 버전으로 이 버전은 전 버전에 비해 한층 복잡한 요건으로 구성되어 있어 규정 준수를 위한 세세한 노력이 요구된다. 이미 최신 버전인 3.0의 효력이 발생했지만, 기업들은 해당 표준 준수를 2015년 1월까지 보류할 수 있다. 가트너는 PCI 3.0 버전의 차이점 및 대응방안(What's Changing and How to Respond to PCI v3.0)”

이라는 보고서를 통해 PCI 3.0은 총 408가지의 요구 사항을 포함하고 있으며, 이는 2.0에 비해 27 %이상 증가된 것이라고 밝혔다. 또한 실질적으로는 2.0 버전의 규정 중 13 %만이 변경됐으며, 2.0을 준수하는데 필요한 노력에 비해 3.0을 준수하기 위해서는 188일의 추가 업무가 필요할 것으로 예상했다. 이러한 가트너의 연구는 새로운 규정에 대한 변경 사항과 최적의 대응 전략에 대한 훌륭한 통찰력을 보여주고 있다.

#### (마) 데이터(data-at-rest) 암호화를 위한 단일의 포괄적 플랫폼

기업들은 저장 데이터(data-at-rest)의 암호화를 위한 단일의 포괄적인 플랫폼을 통해 물리적 데이터 센터, 가상화, 클라우드 및 빅데이터에 이르는 모든 환경에서 보안 키 소지자에 한해 데이터 확인이 가능하도록 관리할 수 있다. 보메트릭 플랫폼은 파일 및 컬럼이라는 두 단위에서 암호화를 지원함으로써 뛰어난 유연성을 제공한다. 이 솔루션을 통해 기업들은 업무를 효율적으로 분리하고, 데이터 수명주기 전반에 걸쳐 중요한 데이터와 보안 키를 보호할 수 있다. 또한 이미 많은 레퍼런스를 통해 보메트릭의 데이터 시큐리티 플랫폼은 PCI DSS 감사를 통과할 수 있도록 지원할 뿐만 아니라 가장 중요한 권한 있는 관리자에게만 중요 정보를 공개하는 강력한 보안 성능이 입증되었다.

#### (바) 국내 기업 PCI DSS 인증

금융권에서 F-ISMS 인증 개발에 앞서 우선적으로 ISMS, PCI-DSS 등을 인정하고 있는데, 특히, PCI-DSS의 경우 400여개의 요구사항이 상세히 나와 있는 등 높은 보안성을 요구하고 있어 주목받고 있다. 일례로 PCI-DSS 요구사항에는 카드 정보의 시스템 및 시큐리티 리스크를 감소 시키기 위해 신용카드 회원정보를 보유하지 않고, 시스템 안에서의 카드 회원정보 활용을 가능한 최소화해야 하며, 카드 회원정보에 최소 인원만

이 접속하도록 요구하고 있다. 내외부에서의 취약성 스캔 실시, 침투 테스트, 무선 LAN의 접속포인트 확인, WAF(Web Application Firewall), 카드정보의 암호화, IDS·IPS, 조작로그 등 로그관리, 보안패치 관리, 물리적 입·퇴실관리 및 감시 카메라, 파일정합성 감시 등이 포함된다.

## 제 2 절 모바일 결제사기 대응기술 관련 연구 및 적용분야 도출

### 1. 모바일 기반 핀테크 보안기술 연구분야 도출

#### 가. 바이오 인증

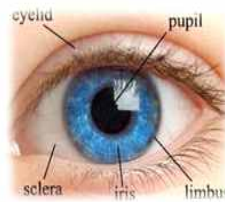
##### (1) 사 례



지문인식



정맥인식



홍채인식



얼굴인식

(그림 5-7) 생체인증 사례

o 금융서비스 보안의 수단으로 지금까지 PIN, 공인인증서, OTP 등을 사용하였으나, 몇몇 은행의 오프라인 금융서비스에서의 지문인식 보안시스템 도입을 시작으로 생체인증 시스템 도입이 제 2의 금융서비스 보안으로 각광받고 있다.

o 기존 인증기술은 효율성 측면에서 다음과 같은 한계가 존재한다.

- Something You Know는 사용자의 기억에 의존하므로 망각 가능성

## 상준

- Something You Are 인증 소요 시간 약 3초미만, 망막인증 10초~15초
- 공인인증서는 인터넷뱅킹, 온라인, 신용카드 거래에 많이 사용하나 번거로운 절차, 주기적인 갱신

## (2) 연구 분야

- 생체인증 응용기술로 개발하여서 새로운 인증메커니즘 도입
- 생체정보 인증과정에 활용할 양자컴퓨터용 공개키 기반구조 보안처리기술 개발
- BT, IT와 NFC(비접촉 근거리통신) 기술 간 융합인증기술을 개발하여 금융, 의료, 보안, 유통, 농축산, 스마트미디어, 공공복지행정 등 서비스 생산 기반에 활용

[표 5-5] 개발기술 사양

개발기술	사양
생체정보 생체인증 기반기술	생체정보 : 생체 프로파일링 분석
생체정보의 개인식별용 스마트폰 USIM 칩	USIM 칩 : 보안 USIM(메모리 1G이상)
스마트폰 USIM 칩의 NFC 기반	NFC : 주파수 2.4 GH(ISM대역) 반경 20cm
전자인증체계에 적용할 무선신호 및 저장데이터 보안	보안기술 : 전자인증 보안, 무선신호 보안 저장데이터 암호화 : 양자컴퓨터용 공개키 기반구조

## ○ 용 도

인체의 개인 식별이 필요한 제반 영역, 모든 인증기술 활용분야 금융(전자결제), 의료(유헬스케어), 보안(생체인식), 영농(농산물품질관리), 유통(품질기반물류), 축산(가축질병관리), 스마트미디어(스마트폰), 주민행정(신개념전자주민등록), 국방(요원신원확인), 치안(범죄자식별) 분야의 공공, 복지, 행정, 민간산업, 제품개발, 서비스 생산

o 기 능

① 생체 추출(sampling) ② 추출된 생체 ③ 생체 값 암호화 ④ 암호화된 value 저장(국가DB, USIM칩) ⑤ 생체정보를 개인식별용 스마트폰 USIM 칩에 탑재 ⑥스마트폰 생체 USIM 칩의 NFC 기반 연동 ⑦전자인증 체계에 적용할 무선신호 및 저장 데이터 보안 ⑧ 인증 처리 => 변환된 두 개체 데이터에 의해 ④, ⑤간 동일성 여부 확인

나. 기타 인증

(1) 스마트사인

사인행위를 분석해 본인 인증을 하는 바이오인식 방식 가운데 하나다. 스마트 사인은 사인의 시작점과 끝나는 지점·가속도·입력·방향성·소요 시간·좌표 추적 등을 분석해 본인을 인증한다. 아직 바이오인식에 필요한 주요 기술은 해외업체들이 주도하고 있다. 글로벌 간편인증기술인 FIDO(Fast IDentity Online)기반의 바이오인증기술을 이용하여 별도의 패스워드 없이 공인인증서 전자서명과 본인확인이 가능한 인증으로 지문을 통해 은행, 증권 등 금융권과 간편결제 등 보안이 요구되는 서비스에서 사용 가능하다.

(2) 2채널 지문 인식 : 이용자의 지문을 이용한 본인 인증

임의의 순서대로 2개 이상의 지문을 지문인증 패드에 입력해 본인 확인 및 지문카드를 결제하는 기술이다. 기술 도입 시 지문 복제 악용을 막고, 개인정보 유출을 차단하는 효과가 기대된다.

(3) 인증 SMS : 인증 SMS의 주요 정보 암호화

SMS의 주요 정보를 암호화해 이동통신사 폐쇄망을 통해 전송하고, 안심SMS 앱에서 복호화 후 화면에 출력해 불법 탈취·도용을 방지하는 기술이다. 도입 시 현행 2채널 인증(ARS 및 SMS 인증)의 보안성을 강화할 수 있다.

(4) QR코드 : QR코드를 이용한 2채널 사용자 인증

PC 에서 ID와 패스워드를 입력해 QR코드를 생성하고, 본인의 스마트폰으로 생성된 QR코드를 스캔해 2채널(유선과 무선채널)로 분리해 인증하는 기술이다. 도입 시 보안채널을 통한 일회용 랜덤키 활용을 통해 악의적인 명의 및 계정도용을 방지할 수 있다

(5) NFC 인증 : 본인의 IC카드를 스마트폰에 터치해 사용자 인증

NFC(Near Field Communication)란 10cm 이내의 가까운 거리에서 다양한 무선 데이터를 주고받는 근거리 통신 기술을 말한다. 전자금융거래시 IC카드를 스마트폰에 터치(NFC통신)해, 생성된 인증정보를 서버에서 검증하는 기술이다. 도입 시에는 OTP생성시 연계정보로 시간정보에 거래정보를 추가해 보안성 향상이 기대된다.

(6) 무작위 행렬판 인증 : 무작위 문자형태 암호입력 방식으로 사용자 인증

암호를 문자형태(예:두꺼비)로 지정하고 거래시 무작위로 생성된 암호 문자판에 해당하는 숫자를 입력해 인증하는 거래연동 OTP를 말한다. OTP(One-Time Password)란 사용자가 인증을 받을 때 고유한 알고리즘을 통해 매번 새로운 비밀번호를 사용하도록 하는 보안시스템이다. 거래시 사용자가 일회용 인증코드를 만들어 유출돼도 타인 도용이 불가능하

다.

(7) 2채널 분할 입력 : 2가지 매체를 통한 분할 입력 인증

전자금융거래 시 개인정보를 인터넷, 전화 등 2가지 디바이스로 분할 입력해 본인 인증하고, 생성된 정보를 서버에서 재조합하는 기술이다. 도입 시 등록된 사용자의 단말기로 전화가 걸리므로 타인의 개인정보 부정사용을 방지할 수 있다.



(\* 주 : boan3@boannews.com 김경애 기자)

(그림 5-8) 2채널 분할 입력

(8) ‘ZEP(Zero Effort Payment)’

사용자가 결제 장소에 접근하면 결제 장치를 꺼내지 않아도 결제할 수 있는 완전히 새로운 방식의 핀테크 및 보안기술. ‘카드터치인증’ 과 비콘 활용. 사용자가 결제 장소에 접근하면 결제 장치를 꺼내지 않아도 결제는 ‘ZEP(Zero Effort Payment)’ 방식. 완전히 새로운 방식 핀테크 및 보안기술

다. 종단간(P2P: Point to Point) 암호화



사물인터넷과 핀테크의 보안을 위해서는 데이터의 무결성을 확보해야 한다. 이를 위해 암호화(PKI)와 키 관리가 필수적이다. PCI-DSS 준수를 위한 맞춤형 암호화, 키 관리가 필요하다. 지불, 결제 관련 핀테크 서비스 사업자라면 PCI-DSS와 같은 최소 요구 조건을 충족시켜야 한다. 새로운 소프트웨어와 데이터를 차량(커넥티드카)이 내려받을 때는 반드시 해당 데이터의 안전성과 무결성을 확보해야 한다. 여기서 필요한 것이 암호화와 키 관리다. 서비스 제공자는 암호화를 통해 데이터를 전송하고, 이 데이터는 차량에 탑재된 하드웨어 보안모듈(HSM) 키로만 복호화돼 적용되도록 설계해야 할 것” 이라고 말했다. 이는 원본 파일의 해시값을 확인하는 것과 유사하다. 패치 매니지먼트시스템(PMS)가 파일의 MD5와 같은 해시 정보가 일치하는지의 여부를 확인한 뒤 배포하듯이, HSM은 암호화된 데이터의 유효성을 확인한 뒤 복호화하고 시스템에 적용한다.

#### 라. 코드 사이닝(code signing)

코드 사이닝(code signing) 기법은 디지털 서명을 사용해 소프트웨어 개발자 이름을 프로그램이나 인터넷 애플릿과 연결시킨다. 이 코드는 서명을 파괴하지 않는 한 변경될 수 없기 때문에 사용자들이 회사와 프로그램을 연결시킬 수 있는 길이 생긴다. 최근 MS는 오센티코드(Authenticode)라는 이름을 가진, 인터넷에서 다운로드된 액티브X 컴포넌트 및 드라이버를 확인하기 위해 몇몇 윈도우 플랫폼에 코드 사이닝을 사용하고 있다. 드라이버의 경우, MS 윈도우 하드웨어 품질 연구소가 일련의 호환성 테스트를 통과한 코드에 사인한다. 액티브X 컴포넌트의 경우 베리사인(VeriSign)같은 써드 파티가 MS의 엄격한 지침에 따라 디지털 서명을 부여할 수 있다. 두 가지 방법 모두 사용자들이 시스템에 설치된 소프트웨어가 어느 회사 제품인지 알 수 있도록 보장한다.

## 마. 사물인터넷 보안

### (1) 양자 컴퓨터 트래픽 암호화

양자암호(Quantum Cryptography) 양자의 역학적 특성을 이용한 암호화 기술. 비공개 채널로 키를 주고 받고 공개 채널로 암호문을 보내는 방법이다. 공격자가 키를 읽기 위해 펄스를 측정하는 순간 펄스가 변화되어 데이터가 무용지물이 되며, 수신자는 이러한 변화를 통해 해커의 공격 시도를 알 수 있어 데이터를 폐기하고 새로운 키를 재송신 받아 도청 없는 통신이 가능하다.

### (2) 사물인터넷 ‘게이트웨이’ 보안

수백, 수천개의 기기들이 서로 연결돼 데이터를 주고받는 사물인터넷(IoT) 시대가 도래하고 있다. 사람과 기기간의 통신과 데이터를 보호하기 위해 ‘게이트웨이’ 보안이 반드시 필요하다. 이같은 이유로 게이트웨이가 보호는 앞으로 모든 네트워크보안의 숙제가 될 것이다. 가정에서 쓰이는 사물인터넷 기기들은 대부분 인터넷공유기와 같은 게이트웨이를 통해 데이터를 주고받는다. 사이버공격자가 게이트웨이를 공격해 권한을 탈취할 경우 개인정보, 민감정보 등이 모두 탈취될 수 있다. 공격자는 자동화 도구를 통해 비밀번호가 설정돼 있지 않은 공유기에 접속, 호스트 주소(host.ics)를 변조한다. 해당 공유기에 접속한 모든 사용자들은 공격자가 의도하는 파밍 사이트로 접속하게 되고, 개인정보유출 등의 위협에 고스란히 노출된다. 특히 최근에는 공공장소에 있는 공유기의 환경설정을 변조해 파밍용 애플리케이션을 내려받도록하는 공격 유형이 나타나고 있다. 사물인터넷 기기 대부분이 무선 네트워크 통신이므로 이에 따라 무선공유기 공격을 통한 보안 위협도 증가할 것이다. 사물인터넷 통신 표준은 올조인(AllJoyn)을 채택해 각종 통신에 대한 접근 권한을 통제

하거나 REST, XMPP, MQTT 같은 개방형 표준을 사용, 암호화 적용이 가능하다.

\* 출처 : 이민형 기자 kiku@ddaily.co.kr

### (3) 사물인터넷, 프라이버시 보호

사물인터넷 산업이 성공하기 위해서는 프라이버시를 간과해서는 안된다. 아무리 좋은 서비스라도 프라이버시 보호가 안되면 사용이 어렵다. 사물인터넷은 많은 요소기술 통합으로 보안 취약성 발생 가능성이 높다. 하지만 이러한 특징으로 인해 보안이나 프라이버시 보호가 쉽지 않다. 디바이스, 네트워크, 플랫폼, 서비스 등 모든 산업군에서 프라이버시 문제는 발생할 수 있다. 사물인터넷이 성공하기 위해서는 프라이버시 보안 강화 등이 반드시 필요하다. 강력한 보안체계를 갖추기에 사물인터넷 기기는 제한적인 요소가 많다. 기기의 크기가 작기 때문에 자원 제약성이 높으며, 보안기술 자체가 아직 미미하다. 또 매시업 보안기술의 부재로 프라이버시 보호도 쉽지 않다. 사물인터넷 기기에 독자적인 보안체계를 구축할 경우 가격 측면에서 이득이 사라진다.

### (4) 사물인터넷 보안 엔드투엔드 암호화

- 사물인터넷 통신 표준 올조인(AllJoyn)은 각종 통신에 대한 접근권한을 통제하거나 REST, XMPP, MQTT 같은 개방형 표준을 사용한다면 암호화 적용하기가 쉽다.

- 사물인터넷 기기와 서버 간 통신을 보호해주는 암호 모듈은 통신 암호화를 위한 암호 알고리즘을 이미 보유하고 있고, 가상사설망(VPN) 기술 등을 사용한다.

- 보안 Protocol은 사물인터넷 기기 간 CoAP(Constrained Application Protocol)과 DTLS(Datagram Transport Layer Protocol)가 있다. 자원 한정

적인 노드와 네트워크 환경에서 DTLS 패킷의 크기를 제한해 부하를 줄이고, 추후 추가될 그룹키 관리기법을 통해 보안도 강화한다. 개인식별 정보를 삭제한 뒤 정보를 수집하더라도 다른 정보와 결합을 통해서 식별 정보를 알 수 있다. 데이터 수집 단계에서 노이즈를 추가하거나 암호화를 하는 방법 등으로 프라이버시를 보호해야 한다.

\* 출처 : 이민형 기자 [kiku@ddaily.co.kr](mailto:kiku@ddaily.co.kr)

## 바. 블록체인

거대한 거래장부인 블록체인을 공인인증서 시스템에 활용하는 기술이 개발됐다. 비트코인 거래내역을 기록하는 거래장부 역할을 하는 '블록체인'을 활용해 인증서를 발급하는데 드는 비용을 줄이면서도 사용자 PC나 스마트폰에 저장돼 유출위험성이 높은 인증서, 개인키를 안전하게 관리할 수 있다. 공인인증서는 기본적으로 PKI에 대해 국제전기통신연합(ITU-T)이 정한 표준 기술인 'X.509' 표준을 따른다. 설명하면 공개키, 개인키를 생성하고 이를 통해 상대방과 통신이 안전하다는 사실을 확인하기 위한 일련의 절차를 따른다. 공인인증서를 처음 발급하기 위해 은행을 활용하는 경우, 사용자PC, 스마트폰으로 인터넷뱅킹사이트/모바일뱅킹 앱으로 은행 서버에 접속, 필요한 개인정보를 입력한 뒤 인증서 발급을 신청하면 은행은 해당 정보를 공인인증서 발급기관에 보낸다. 발급기관은 이 정보를 확인한 뒤 공개키와 개인키를 생성해 사용자PC에 전송한다. 그동안 국내에서 공인인증서 유출로 인한 금전피해가 심각했던 이유는 공인인증서를 통한 사용자PC-인터넷뱅킹사이트 혹은 스마트폰-모바일뱅킹앱 간 서로 믿을 수 있는지 판단하기 위해 필요한 개인키가 공개된 폴더 안에 저장돼 있었다는 점이다.

\* 비트코인2.0으로 진화하는 '블록체인'

MIT공대 연구팀은 '아이덴티티 확보를 위한 분산화된 공개키기반구조

(A Decentralized Public Key Infrastructure with Identity Retention)’이라는 논문을 통해 일명 ‘서트코인(Certcoin)’을 제안했다. 비트코인 생태계의 근간을 이루는 블록체인에서 아이디어를 차용해 별도 관리기관(Certificate Authorities, CA) 없이도 분산화되고 안전한 인증체계를 만들 수 있다는 설명이다. 공인인증서가 은행뿐 아니라 각종 전자정부를 활용한 민원서류 발급, 조달청 입찰 등에서 활용되고 있다는 점 때문에 비트코인 생태계에서 시작된 블록체인이 개인정보유출이나 해킹등으로부터 보다 안전하면서 저렴한 수단으로 재조명되고 있다. 한국형 인증서 발급 시스템이 가진 맹점을 비트코인 생태계의 근간을 이루는 블록체인이 해결할 수 있을지 주목된다.

#### 사. O2O

O2O란 Online to Offline의 약자로 넓은 의미로는 오프라인과 온라인을 경계를 허무는 마케팅이다. Payment를 붙여서 좁게는 결제 분야에서 과거라면 100% 오프라인 결제였을 성격의 거래를 온라인 결제로 유도하는 현상을 의미한다. 스마트폰에 리더기를 붙인 형식이라면 무선단말기 결제 처리도 실제로는 온라인 모바일 거래일 가능성도 높다. 만약 IT기업이 예금과 같은 금융 고유의 분야까지 진출한다면 향후 카드사와 금융사가 고유하게 제공 할 수 있었던 여신도 제공 할 수가 있게 되므로 Buy Now, Pay Later가 본질인 신용카드사 역시 안심할 상황은 아니다.

#### 아. 클라우드 보안

##### (1) CSA의 클라우드 컴퓨팅 가이드نس

클라우드 보안 관련된 통제 모델과 지침으로는 FedRAMP, NIST SP800-53 R3, HIPAA/HITECH Act, ISO/IEC 27001-2005, COBIT4.1, PCI

DSS v2.0, BITS Shared Assessments SIGv6.0, BITS Shared Assessments AUPv5.0, GAPP, Jericho Forum, NERC CIP 등 다양하다. 2008년 설립된 CSA는 클라우드 보안 영역에서 국제적인 기관으로 20,000명 이상의 개인회원과 100여개의 기업회원으로 구성되어 있으며, 120여 개국의 정부, 금융, 기업을 망라하여 수천 명의 보안 전문가들이 클라우드 보안을 연구하고, 적용하기 위한 노력을 진행하고 있다. 한편, CSA가 발간한 대표적 클라우드 컴퓨팅 가이드선으로는 “클라우드 컴퓨팅 중심의 핵심영역에 대한 보안 가이드선과 클라우드 컴퓨팅의 최고 위협들, 클라우드 통제 매트릭스(CCM) 등 3가지를 들 수 있다.

## (2) 클라우드 컴퓨팅 중심의 핵심영역에 대한 보안 가이드선 V2.1

클라우드의 본질적 특성으로 인해 거버넌스가 상실에 대한 다양한 이슈와 클라우드 모델을 구현에 있어 발생하는 기술적, 업무적, 고전적 위협 등 다양한 문제가 상존한다. 이는 클라우드의 핵심문제로 클라우드 고객과 서비스 제공자 모두에게 주요한 관심이 되고있다. 따라서 클라우드 컴퓨팅의 핵심 문제를 설명하고 전략적 도메인 내에서 클라우드 컴퓨팅 고객과 공급자 모두에 대한 조언을 제공하고자 CSA는 “클라우드 컴퓨팅 중심의 핵심영역에 대한 보안 가이드선”을 발표하였다. 2009년 4월에 Ver1.0이 처음 발표되었으며, 2009년 12월에 Ver2.1이, 2011년 1월부터는 Ver3에 대한 작업을 진행되었다. Ver1.0에서는 핵심영역이 15개였으나 Ver2.1에서는 일부영역에 대한 통합과 변경을 통해 13개 영역으로 조정되었다.

[표 5-6] 클라우드 보안가이드의 핵심영역

구분	영역	
클라우드 구조	D1	클라우드컴퓨팅 구조적 프레임워크
	D2	거버넌스 및 전사적 위험관리
클라우드 통제	D3	합법 및 전자적 복구
	D4	컴플라이언스 및 감사
	D5	정보 생명주기 관리
	D6	클라우드에서의 통제
	D7	고전적인 보안, 비즈니스 연속성 및 재난복구
클라우드 운영	D8	데이터 센터 운영
	D9	사고 반응, 알림, 교정
	D10	응용 보안
	D11	암호와 및 키관리
	D12	신원 및 접근관리
	D13	가상화

(\* 주 : 나중회<sup>+</sup>이태훈<sup>+</sup> 클라우드 컴퓨팅의 보안위협과 통제모델에 대한 고찰)

## 2. 모바일 결제사기 대응기술 개발을 위한 적용분야 도출

### 가. PCI-DSS(Payment Card Industry -Data Security Standard) 인증

o 핀테크는 상대적으로 보안성이 취약하여 이를 보완하는 기준이 강화되고 있는 실정이다. 이미 일부 비트코인 거래소가 해킹으로 파산한바 있으며, 글로벌 기업들의 고객정보 유출이 증가하고 있다. 또한 신용카드의 부정사용금액도 증가 추세이다.

o 이를 보완하기 위해 보안수준을 강화하고, 기존의 인증방식을 다양화하고, 생체인식 정보를 활용하는 추세로 시장이 확대되고 있다.

o 보안 요구수준은 지불카드산업의 정보보안표준인 PCI-DSS(Payment Card Industry -Data Security Standard) 인증을 취득하게 하고, 이상금융거래탐지시스템인 FDS(Fraud Detection System) 도입을 의무화하도록 하고 있다.

o 또한 국내 공인인증서를 대체하는 ARS인증, SMS인증 등에 이어 지

문인식, 홍채인식, 안면인식 등 생체인식을 도입하는 사례가 늘고 있다.

#### 나. Big Data 검색엔진 기반 이상금융거래 탐지

최근 서버 메시지 블록 프로토콜을 이용한 파일 접근 제어 시스템 및 방법과 관련한 특허권을 취득한 시큐브는 실시간 통합 분석 모니터링으로 실시간 IT 수집된 로그 정보를 제공하며 접속자의 위협 분석을 시스템에서 자동 분석해 고객에게 제공한다.

전자금융거래의 발달로 정보유출 사고를 막기 위한 니즈가 생겼고 금융사고 이후 강화된 각종 규제로 사고 발생 시 이증고를 겪을 수 있는 금융권이 기술적, 법률적 대비를 할 수 있는 유용한 내용이 발표됐다. 과거 사이버 위협 방어 기술의 핵심기술은 알려진 공격에 대한 공격 시그니처 데이터베이스를 확보하고 고성능 패턴매칭 알고리즘을 구현하여 얼마나 빨리 비교할 수 있느냐에 달려 있었지만, 복합데이터 처리기술의 발달로 내부 망에서 발생하는 다중소스의 누적 데이터에 대한 특성인자를 정의하고 연관성 분석을 할 수 있는 보안기술로서 빅데이터를 활용한 보안 분석 기술이 부각되고 있다. 가트너 그룹은 빅데이터 분석을 활용한 보안 분석을 통하여 예전에 보이지 않았던 사고패턴을 발견하고 정보보안을 포함한 기업경영에 대한 선명한 통찰력을 제공함으로써 기업의 비즈니스 가치를 높일 수 있다고 예측하고 있다. 빅데이터를 활용한 보안 분석(big data security analytics)은 데이터 분석 기술의 고도화 측면에서 기존에 해결하지 못한 공격위협 분석을 가능하게 할 것으로 예측되고 있다.

#### 다. 핀테크 생체 인증

금융서비스 보안의 수단으로 지금까지 PIN, 공인인증서, OTP 등을 사용하였으나, 몇몇 은행의 오프라인 금융서비스에서의 지문인식 보안시스



템 도입을 시작으로 생체인증 시스템 도입이 제 2의 금융서비스 보안으로 각광받고 있다. 생체인증 시스템들 중 특히 얼굴인증 시스템은 사용자의 얼굴을 비교 인증함은 물론 사용자의 얼굴 이미지를 남김으로써 부인 방지, 사용자 동선 추적 등의 기능에 있어 크게 부각되고 있다.

#### o 모바일 서비스 얼굴인증 시장 동향

지문과 얼굴, 홍채 등 생체 정보를 인증 수단으로 활용하는 생체 인식 기술이 급물살을 타고 있다. 중국 최대 전자상거래 업체 알리바바 마윈 회장이 최근 얼굴인증을 활용한 결제시스템을 시연하면서 지문인식과 모바일위주로 관심이 집중되던 생체인식 기술 전선이 확장되는 추세이다. 또한 모바일 생체인식 시장 전망 자료에 따르면 모바일 서비스에 있어서 생체인식 수익율은 90% 이상의 연평균 성장률을 가지고 있을 만큼 기존 인증 방식의 대체 기술로 인정을 받고 있다

#### o 얼굴인증

FinTech는 모바일 시대의 혁명, 금융서비스의 혁신이라고 표현을 한다. 오프라인 대면형태의 금융서비스에서 온라인 대면형태의 금융서비스로의 변화는 금융의 대혁신이라 표현 할 수 있다. 모바일 간편 결제서비스가 본격적으로 등장하기 시작하였다. 아울러 텐센트의 텐페이, 알리바바의 알리페이, 이베이의 페이팔, 아마존의 아마존 페이먼트 등 해외 모바일 간편결제시스템도 이미 국내 시장과 제휴 형태로 서비스를 시작하였다. 규제 완화도 시장 및 기술의 개방도 중요하다. 그러나 사용자가 신뢰할 수 있고 간편한 보안기술을 개발하여 FinTech 산업에 적용해야 한다.

#### o 강력인증(Strong Authentication)

비대면 환경에서 본인이 자유로운 의지로 해당 거래를 진행하는 것이라는 사실을 검증하기 위해서는 강력한 보안이 보장된 인증기술이 필요하다. 어떠한 환경에서도 인증을 수행할 수 있도록 표준을 준수하면서 간편하게 인증이 완료돼야 한다는 요구도 있다. 간편결제가 부상하면서 함께 주목받는 다양한 인증기술을 살펴보고, IoT, 클라우드, 스마트워크

환경에서 이용할 수 있다.

#### 라. 간편결제

‘간편함’과 ‘보안’ 두 가지 소재를 위해 애플페이, 카카오페이, 네이버페이, 삼성페이 등 ‘각종 페이’들이 간편성에 초점을 맞춰 서비스를 소개하고 지문 혹은 비밀번호만으로 간단하게 결제가 가능하다는 점을 강조하고 있지만, 결제정보가 안전하게 처리되고 있는지 여부도 중요하다. 최근 모바일을 이용한 간편결제가 과열양상을 보이자 차별성을 강조하기 위해 핀테크, 간편결제, 모바일 결제가 같은 뜻인 것처럼 소개되고 있다. 다양한 핀테크 모델 중 간편한 전자거래가 필요한 서비스에 간편결제가 적용되며, 간편결제의 간편성을 높이는 수단 중 하나로 모바일 기기가 사용되는 것이다. 간편결제에서 인증 문제는 매우 논란이 많다. 현재 우리나라 전자금융거래에서 액티브X와 공인인증서, 키보드 보안·백신·방화벽 등 보안모듈 3종세트가 의무화 대상에서 제거되고, 금융사가 자율적으로 보안기술을 검토해 거래를 편리하게 하면서 안전하게 제공할 수 있는 방법을 마련하도록 하고 있다.

#### 마. 새로운 인증기술

##### o 멀티팩터(multi-factor) 인증

사용자 인증기술은 ▲지식요소: ID/비밀번호와 같이 사용자가 알고 있는 것 ▲소유기반: OTP, 보안카드, 스마트카드 등 사용자가 갖고 있는 것 ▲생체인식: 사용자 고유의 생체정보 등으로 구분한다. 멀티팩터(multi-factor) 인증은 이 세 가지 요소 중 2가지 이상을 이용해 인증하는 것을 의미한다.

##### o 멀티채널(multi-channel) 인증

멀티채널 인증은 인터넷망과 통신망 등 인증 채널을 달리해 인증받는 것을 멀티채널 인증이라고 하며, 인터넷뱅킹을 진행하면서 공인인증서로 본인확인을 하고 SMS나 ARS로 통신망을 통해 본인인증을 다시 하는 경우를 예로 들 수 있다.

○ 강력인증(Strong Authentication)

강력인증은 세가지 요소 중 한가지 요소 안에서 두 가지 이상의 수단을 사용하는 방법이다. 사용자가 갖고 있는 스마트폰과 스마트카드를 연동해서 인증하거나 사용자 소유기반 인증 수단을 두 가지 사용한 강력인증이다. 전자상거래의 인증 요건을 갖추기 위해서는 2팩터·2채널 이상 복잡성을 갖춘 인증수단을 이용하며, 강력인증으로 인증의 정확성을 높일 수 있다.

바. 웨어러블 만능 인증

○ IC칩을 스마트폰에서 인식하는 데 NFC 기술만 쓰지만 앞으로는 블루투스으로도 읽을 수 있도록 할 계획이다. 블루투스 통신은 IC칩을 통합 인증수단으로 활용한다.

○ 세이프터치 기술 + 웨어러블 기기 = 로그인 과정을 모두 생략한다. 사용자가 IC칩이 들어간 스마트워치를 차고 컴퓨터에 가까이 다가가면 알아서 로그인이 된다. 컴퓨터를 다 쓰고 자리를 뜨면 거리가 떨어진 걸 인식하고 알아서 로그아웃된다. 사용자는 아이디나 비밀번호를 입력할 필요가 없다. 세션하이재킹을 스마트워치만 차고 다니면 로그인으로 대변되는 인증절차를 손가락 하나로 원천 차단한다.

사. 핀테크 포렌식

핀테크 포렌식은 기존의 DS, Anomaly 탐지, 포렌식, 패킷캡처, Flow&SNMP 분석, VoIP 모니터링과 그밖의 다른 기능 등 포렌식을 핀테크

크에 적용하는 방법이다.

디지털데이터는 시스템에서 로그와 같이 자동적으로 생성된 정보와 사람이 입력한 정보로 구별된다. 시스템이 생성한 정보는 의도적인 조작이나 시스템의 오류가 없었고, 믿을만한 수준으로 관리되었다면 증거로 인정된다. 반면에 사람이 의도적으로 입력한 정보는 증거 제출 목적이 특정 사실을 입증하기 위한 것(전문)이면 증거로 허용될지 판사의 판단이 필요하다. 보안사고와 관련한 디지털 증거는 대부분 로그와 같이 시스템이 자동으로 생성한 정보이기 때문에 증거로 허용되며, 이에 대한 논란은 없다고 한다. 그러나 공안사건과 관련된 증거는 대부분 사람이 입력한 문서 파일이기 때문에 조작가능성에 대한 첨예한 논쟁이 있으며, 전문 증거인 경우가 많아 증거로 채택되지 않는 경우도 종종 있다. 디지털데이터가 법적 증거로 채택되기 위해서는 생성과정에서 의도적인 위변조가 없었음이 입증되어야 하고, 신뢰할 수 있는 도구를 사용하여 전문지식을 보유한 전문가가 신뢰할 수 있는 방법을 적용했음이 제시되어야 한다.

\*출처:이상진 고려대학교 사이버국방학과교수, · 디지털포렌식연구센터장

### 제 3 절 연구 분야 발굴

#### 1. 분야 발굴 전제

o 기술연구를 위해서는 업무의 전체적인 프레임워크가 구성되어져야하고 그 속에서 정책분야와 기술분야가 포함된다고 판단하였다. 전체적인 프레임워크는 프로세스 측면에서 종적으로, 업무 영역에서 횡적으로 이루어지는 큰 그림이며, 이 구조를 거버넌스로 흔히 표현하고 있다.

o 금융보안을 강화하기 위해서는 “보안 전략”을 금융보안 거버넌스

체계로 먼저 설계해야 하며, 사전 예방 차원의 라이프사이클에 기반하여야 한다. 라이프사이클은 금융보안 거버넌스 전략 체계 구축, 취약점 분석·평가 등 사전 예방 활동으로부터 알고리즘과 기술개발, 평가와 피드백 프로세스로 이루어진다.

금융위원회 발표에 의하면 보안규제의 방식을 선진형 규제 방식인 사전 규제 최소화와 사후점검 강화로 개선할 계획이다. 핀테크가 활성화되도록 보안에 대해서 시장의 자율성을 높여주되, 대신 책임은 엄격하게 묻겠다는 뜻이다. 과거에 보호대상으로 정보자산인 시스템, 네트워크, DB, 보안시스템 등 IT 분야로 한정돼 있었다면, 이제는 전사적, 서비스 전체가 대상으로 확대 되며, IT부서 직원, 보안담당자 등이 해야 하는 일에서 전부서 전 직원의 필수 업무로 바뀌고 있다.

○ IT 거버넌스를 지원하는 프레임워크는 COBIT, ITIL, ISO38500, BS25999 그리고 의사 결정 모델 등이 있으며, 이러한 프레임워크는 기업 또는 조직의 목표와 IT투자 의 목적에 따라 활용할 수 있다.

○ CERT의 성공적인 활동을 위해서는 우선 해당 조직에 대한 정보보호 정책이 구축되어야 하며, 수립된 정보보호 정책을 통해 CERT의 역할 및 범위와 정보보호 활동계획 등이 정의되어 유기적인 연관관계를 가져야 한다(2010 KISA CERT구축/운영 안내서).

○ 이상과 같은 취지에서 본 연구보고서는, ‘4절 연구분야 도출’에서와 같이, 전체 연구분야 21개 영역 중 거버넌스 보안 전략분야 9개영역을 제시하였고 거버넌스 보안 전략속에서 기술분야는 실제로 다음과 같이 12개 영역이다

- 기술분야 -> 거버넌스 보안 전략과제 12영역중 3개영역

C	시나리오	핀테크 보안 공격 시나리오 모델 연구			
E	시스템 설계	머신러닝 기반의 지능형 탐지 엔진 (fraud detection engine) 소프트웨어 아키텍처 설계방법	*	*	
H	포렌식	핀테크 보안 포렌식 업무 모델 발굴	*	*	

- 핀테크 보안기술 연구개발 과제(D 그룹1) 5개영역
  - FDS 알고리즘과 기술개발 과제(D 그룹2) 4개영역
- (계 12개 영역)

## 2. 분야 발굴 목표

### o 거버넌스 사상의 종합 프레임워크 방향 연구.

사기탐지 기능 활성화를 위한 이용환경 조성, 제도, 기술, 활성화 동기부여 등 종합적인 지원 정책을 발굴할 때 소기의 성과가 나타난다고 판단된다.

### o 현안사항과 문제점 도출

그동안 금융위원회, 금융감독원 등 관련기관에서는 금융사기 예방, 차단 제도 개선을 위한 규제 철폐, 보완 등 정책과 국내의 FDS 도입의 확산 지원을 펼치고 있으나 금융업무 현장에서의 사기탐지 기능 도입과 활성화를 위해서는 아직도 개선할 점이 많다.

### o 금융사기 예방, 차단 제도 개선안 도출

금융사기 예방, 차단은 제도적인 측면의 진단과 개선없이 기술 및 서비스 개발 위주의 FDS 활성화 대책은 성과에 한계를 나타낼 수 있다. 이 같은 환경에 적합한 금융산업 자체의 FDS 활성화 정책모델을 도출한다.

### o FDS 사기탐지 기능 확산과 기능 효율성 방향 도출

금융산업 현장에서 사기탐지 시스템 도입은 꾸준히 확산되고 있지만, 개별 금융기관단위로 독자적인 기술을 도입하는 구조로서 금융사기 예방, 차단 활성화 추진과제를 도출하고 FDS 기능 효율화를 위한 기술연구 과제를 발굴한다.

## 3. 연구분야 발굴 과정

국내의 FDS 활성화 전략에 따라 위치정보 연구분야를 발굴한다. 연구 분야는 현안사항에서 나타난 문제점을 개선하기 위해 추진전략을 도출한 후 전략 방향에 따라 분야별로 구분된 추진분야를 발굴한다.

○ 국내/외 FDS 자료의 수집 및 검토

- 국내/외 FDS 서비스에 관련하여 관련 법 조항 및 정책안 수집
- 검토 과정 중 정부부처의 보관 자료의 검토 필요
- 국내/외 FDS 자료 검토 후 차이점 비교분석
- 분석된 자료의 문제점 여부를 검토

○ 선진이론 모형조사

- 국제적 현황조사 : 선진화 모델, 발전모형
- 참조 이론모델 : 기술성숙과 시장형성 모형
- 해외 선진 사례 벤치마크
- 해외 선진 기업과 경쟁을 위해서는 해외의 동향
- 국내외 연구결과

○ 현안사항과 문제점 진단한다.

외부요인과 내부요인에 관해 수집된 정보를 통합하고 포괄적으로 분석하여 제품이나 서비스의 경쟁력 진단.

- 분석 항목 : 정책/제도, 정보기술수준
- 핵심현안 요소 도출 : 취약요소, 문제점 요소
- 핵심현안 수준 진단 : 취약수준, 문제점 요인

○ 문제점을 기반으로 원인 분석

- 사기탐지 업무 자체의 속성
- 사기 대응 정책과 관리제도 측면
- FDS 운용 측면
- 사기탐지 알고리즘 측면

○ 활성화 방안 도출

- 저해요소 개선을 위한 분야 정책방향 비교 검토
- 문제점 연구 개선방안 모색

- 금융사기 예방과 차단 방안 연구소재 도출

#### 4. 연구작업 프레임워크

##### o 연구 프로세스

진단 프로세스 결과에 따라 서비스 사기탐지 기능의 효율화, 사기탐지 업무의 활성화 전략과 분야를 도출한다.

사기 환경 조사 단계	사기 패턴 조사 단계	문제점 진단 단계	전략 단계	분야 단계
사기 발생 환경	사기발생 사고 패턴	도출된 문제점	추진전략	추진분야

##### o 연구 프레임워크

연구작업의 전체 프레임워크는 금융사기 발생 환경, 금융사기 발생 패턴, 탐지기술, 차단기술을 찾아가는 모형을 구조화 한다. 도출된 내역을 업무 및 연구작업 소재로 발굴한다.

사기발생환경	금융사기 발생 환경				
사기모형	직접입력 사기 + 다단계 입력 사기				
사기발생 디바이스	PC	스마트 디바이스	신용카드	무선 디바이스	기타 디바이스
	금융사기 발생 패턴				
	실제발생 패턴		미래발생 예측 패턴		
	탐지기술				
	실제사용기술		미래개발기술		
	차단기술				
사기패턴	실제사용기술		미래개발기술		
탐지알고리즘					
탐지엔진					
차단알고리즘					
차단엔진					



## 제 4 절 연구분야 도출

### 1. 분야 도출

#### (1) 분야 도출 프로세스

전략은 각기 다른 테마를 서로 어떻게 수행하고 연결시킬지를 연구하고 선택하고 집중한다. 각각의 업무에는 업종별 특성이 있다. 업종이 어떤 것이냐에 따라 기업경영체로서의 특성이 있게 되고, 경영관리나 연구방법, 또는 관리방법의 종류나 이용방법에 있어서도 업종 간 특색이 있다. 본 연구에서는 다음과 같은 프로세스로 여섯 가지 점에 착안하여 전략을 발굴한다.

- 중점 추진분야를 선정하여 추진방향을 총론으로 도입한다.
- 중점 추진분야 선정은 현황 및 문제점에서 도출된 테마를 문제 개선의 방향측면으로 필요한 분야를 우선 순위로 선택한다.
- 총론으로 기술된 테마에 대한 추진분야를 도출한다.
- 추진분야는 우선 순위와 실현가능성에 기반하여 별도의 현실적인 사업계획 수립의 요구사항 정의 수준에서 작성한다.
- 전체적으로는 거버넌스 사상에 기반한 연계 조직과 활동을 도모하는 방안을 추구한다.

#### (2) 도출분야의 분류

- 거버넌스 보안 전략분야 :
  - 핀테크정보시스템의 탄생에서 운영 폐기까지의 라이프사이클을 13개 단계로 설계
  - 계획 운영 진단 개선 PDS 업무 순환과정을 설계 분야로 도출한다.

○ 핀테크 보안기술 연구개발분야

블록체인 핀테크 보안 취약성 실험 및 진단 방안 연구, 근거리 무선통신 경량암호화, 랜섬웨어, 금융정보 양자암호, 사물인터넷 등 기술 현안 분야를 도출한다.

○ FDS 기술 연구개발분야 : 기존 시스템 업그레이드와 미래형 신소재 발굴

FDS 구축이후 업그레이드 방안, 빅데이터\* 분석(Science Map) 시스템 구축 방법, 빅데이터 기반 사기탐지 기능(fraud detection big data) 설계, 사기탐지 인공지능(AI) 질의응답 전문가시스템 개발분야를 도출한다.

## 2. 발굴분야 구성

가. 핀테크 거버넌스 보안 전략분야

구분	영역	거버넌스 분야	제안 분야	분야구분	
				총괄	기관
A	대응 전략	라이프사이클에 기반한 핀테크 보안 거버넌스 전략 도입	*	*	*
B	추세 분석	국·내외 핀테크 공격 기술 및 사건 동 향조사 추세 분석 방안	*	*	
C	시나 리오	핀테크 보안 공격 시나리오 모델 연구			
D	기술 연구	1)핀테크 보안기술 연구개발 분야 (5개 세부 분야)	*	*	
		2)FDS 알고리즘과 기술개발 분야 (4개 세부 분야)	*	*	
E	시스템 설계	머신러닝 기반의 지능형 탐지 엔진 (fraud detection engine) 소프트웨어 아 키텍처 설계방법	*	*	
F	제품평 가	핀테크 보안 제품 평가방법 개발	*	*	
G	프로세 스 평 가	사기탐지 프로세스 평가방법 개발	*	*	
H	포렌식	핀테크 보안 포렌식 업무 모델 발굴	*	*	
I	인 력 양성	사기탐지 전문직(스페셜리스트) 분야 발 굴과 및 역할 모델 정립	*	*	
J	가이드 라인	사기방지 업무 분야별 표준 가이드라인 제정	*	*	*
K	지원 센터	사기방지 기술지원센터 기능 도입	*	*	*
L	자 체 진단	사기방지 업무 자체 운영실태 진단 방 안 개발	*	*	*
M	성숙도 평가	조직별 사기탐지 업무성숙도 평가모델 개발	*	*	
계		13	9	12	4

나. 핀테크 보안기술 연구개발 분야(D 그룹1)

번호	영역	연구분야	제안 분야	연구분야	
				총괄	기관
1	블록 체인	블록체인 핀테크 보안 취약성 실험 및 진단 기술개발	*	*	
2	암 호 화	근거리무선통신 경량암호화 기술개발	*	*	
3	랜 섬 웨어	랜섬웨어 실시간 대응' 보안 솔루션 기술개발	*	*	
4	양 자 암호	금융정보 양자암호(Quantum Cryptography) 통신 기반 구축 기술 개발	*	*	
5	사 물 인 터 넷	사물인터넷 환경의 핀테크 네트워크 보안 프레임워크 기술개발	*	*	
계		5	5	5	

다. FDS 알고리즘과 기술개발 분야(D 그룹2)

번호	영역	연구분야	제안 분야	연구분야	
				총괄	기관
1	업그레 이드	FDS 구축이후 업그레이드 기술개발	*	*	*
2	빅 데 이 터	사기방지 빅데이터* 분석 Science Map 설계 기술개발	*	*	
3	빅 데 이 터	Big Data 검색엔진 기반 이상금융 거래 탐지 기술개발	*	*	
4	전 문 가 시스템	사기탐지 인공지능 (AI) 질의응답 전문가시스템 기술개발	*	*	
계		4		4	1

## 제 5 절 세부 연구분야

### 1. 핀테크 거버넌스 보안 전략분야(A)

(가) 분야명 : 라이프사이클에 기반한 핀테크 보안 거버넌스 전략 도입

(나) 분야 선정 사유

금융보안을 강화하기 위해 보안관리 패러다임의 전환이 필요하다. “보안 전략”을 금융보안 거버넌스 체계로 설계해야 하며 사전 예방 차원의 라이프사이클에 기반하여야 한다. 라이프사이클은 금융보안 거버넌스 전략 체계 구축, 취약점 분석·평가 등 사전 예방 활동으로부터 알고리즘과 기술개발, 평가와 피드백으로 이루어진다. 금융위원회 발표에 의하면 보안규제의 방식을 선진형 규제 방식인 사전 규제 최소화와 사후점검 강화로 개선할 계획이다. 핀테크가 활성화되도록 보안에 대해서 시장의 자율성을 높여주되, 대신 책임은 엄격하게 묻겠다는 뜻이다. 과거에 보호대상으로 정보자산인 시스템, 네트워크, DB, 보안시스템 등 IT 분야로 한정돼 있었다면, 이제는 전사적, 서비스 전체가 대상으로 확대 되며, IT부서 직원, 보안담당자 등이 해야하는 일에서 전부서 전 직원의 필수 업무로 바뀌고 있다.

(다) 사기방지 거버넌스 전략

IT 거버넌스 프레임워크는 BT(Business Area), MT(Management Area), OT(Operatoon Area)로 구분되고, 이해관계자의 의지와 목적을 이해하고 전사 또는 조직의 비전을 정렬하여 가치를 전달할 수 있도록 위험 및 자

산관리 그리고 성과 측정을 통한 효율적인 의사결정을 지원한다. IT 거버넌스를 지원하는 프레임워크는 COBIT, ITIL, ISO38500, BS25999 그리고 의사결정모델 등이 있으며, 이러한 프레임워크는 기업 또는 조직의 목표와 IT투자의 목적에 따라 활용할 수 있다.

- o 사기방지는 조직 전반에 걸친 이슈(An Enterprise-Wide Issue) : 보안은 사업적인 이슈로서 조직 전반에 걸쳐 종적 및 횡적으로 관리

- o 위험관리(Risk Based) : 보안의 중요성은 노출된 위험의 크기에 따름.

- o 역할과 책임(Role, Responsibilities, Segregation of Duties Defined) : 경영진 및 운영 조직의 역할이 명확해야 한다.

- o 정책과 절차(Addressed and Enforced in Policy) : 보안과 관련된 정책은 잘 정비되어 있어야 하고 엄격하게 지켜져야 한다.

- o 능력과 권한(Adequate Resources Committed) : 보안 조직의 인원은 적합한 능력과 권한을 가짐.

- o 교육과 훈련(Staff Aware and Trained) : 모든 직원이 보안 인식을 갖추고 보안 교육을 받음.

- o 계획, 수행 및 평가(Planned, Managed, Measurable, and Measured) : 사업의 전략 및 사업 계획 수립 등에서 보안이 고려되어야 한다.

검토 및 감사(Reviewed and Audited) : 주기적 감사 등을 통해 확인되고 개선

#### (라) 분야 발굴 방향 사기방지 업무 모델 수행 5단계

- o 평가(Assess) : 내부역량 자가평가 과정이다. 효과적인 사기방지 업무 모델 구축을 위해 현재 운영 체계를 점검하여 주요 개선사항 및 해결방안 도출하여 설계 단계에 반영한다.

- o 설계(Design) : 향후 업무 모델의 청사진을 확립하며, 이행 전략을 고려하여 모델을 설계한다.

- 구축(Construct) : 설계(Design) 단계의 청사진을 구체화하며, 업무기능별 세부 계획을 수립하여 진행한다.
- 이행(Implement) : 설계된 모델을 업무 기능별로 이행하며, 이행 중 발견된 개선사항은 지속적으로 반영한다.
- 운영/개선(Operate/Review) : 실제 사업 효율성 및 효과성 평가와 운영의 고도화,개선 동시 진행

#### (마) 연구분야

금융기관에서 도입해야 할 사기방지 업무 구성 블록은 상호 유기적으로 연결되어 있고 조직 전반에 걸쳐 종적 및 횡적으로 관리 순서로 조합되어 완성되어야 한다.

- 관리작업 전체를 프레임워크로 재설계 방안
- 사기탐지 업무 단계와 라이프사이클 재정립
- 사기탐지 관리기능 모델 구조화
- 취약점 분석·평가 등 예방 활동
- 사기탐지 이해관계자 재정의
- 사기탐지 기능적, 비 기능적 요구에 대한 재정의
- 관리작업 전체를 프레임워크로 재설계 방안

## 2. 핀테크 거버넌스 보안 전략분야(B)

(가) 분야명 : 국·내외 핀테크 공격 기술 및 사건 동향조사 추세분석방안

(나) 분야 선정 사유

핀테크 공격 기술 및 사건 추세분석(Trend analysis)이 가능하도록 객

관적, 계량화된 지표를 사용한 동향조사 실시가 필요하다. 추세분석은 시간에 따른 시계열 자료의 추세선을 유도함으로써 그 추세선상에서 미래 수요를 예측한다. 추세분석은 패턴이 비교적 안정되어 있는 단기, 중기예측에 적합한 방법을 선별해야 한다. 상세, 최신 동향 조사로 현실적 상황을 파악해야 하며 수시조사 보다 시스템화 된 정기조사로 정책 연속성과 미래예측 기반을 조성해야 한다. 단순 통계가 아닌 기술, 사건 간 매트릭스 형태의 동향정보 분석과 연관성 추이 그래프가 도출되어야 한다.

(다) 사고 모형 패턴 화(추가분야로 제안한 분야)

o 사고모형 코드설계

- 설계기준

· 국내에서 발생하였거나 향후 발생가능성이 예상되는 사고유형을 유형별로 모형화하고 각각의 코드를 부여한다

· 사고모형 코드설계는 정보시스템구축시 활용가능토록 10진 분류방식의 코드체계로 구성하되 4단계 계층구조로 설계.

· 대분류 : 금융부문별 5개 영역으로 구분하며, 영역중복 시 최초 발생부문으로 분류

· 중분류 : 금융부문별 하부구조로 사고유형을 기준으로 코드부여하되, 모형중복사고는 선행 행위를 기준

· 소분류 : 중분류 하부구조로 정보보호침해사고, 전자금융사고 유형별로 코드부여 하되 두 가지 유형 이외의 유형은 향후의 활용을 대비하여 소분류 단위 명칭

- 일련번호 : 소분류단위의 사고별 일련번호를 코드화

- 코드체계 자릿수는 총 9자릿수로 구성

대분류(3)	중분류(1)	소분류(2)	일련번호(3)
--------	--------	--------	---------

- 코드 부여기준



- 대분류 : 한국은행의 업무분류기준 4종과 예비1종
- 중분류 : 정보보호 1종, 전자금융 1종, 핀테크 1종
- 소분류 : 본 연구작업에서 설정->정보보호침해, 전자금융, 핀테크  
별로 세분류. 소분류의 양 분야에 중복되는 사고 다수 존재
- 일련번호 : 소분류사고의 일련번호

사고 제목				
모형분류	대분류	중분류	소분류	일련번호
○ 사고개요 (조사 가능한 항목의 사고발생개요를 6하원칙에 따라 기재) - 발생장소 : - 발생과정 : ○ 사고특징 (조사가 가능한 특징적상황을 기재) - 공격기법 : - 피해사항 : ○ 기타참고사항 (선택기재사항 : 자료조사가능경우 한) - 사고 방지대책 : - 사고 발생원인 :				

#### o 사고 수집방법 체계화

국내외 금융회사, 유관기관 또는 기타 단체에서 지속적으로 발생하고 있는 이상금융거래 동향 정보를 수집하고 해당 정보가 금융회사의 「이상 금융거래 탐지시스템」에 반영될 수 있도록 주기적인 동향정보 수집 필요하다.

#### o 이상금융거래 정보의 공유

사고로 판명 또는 분류된 이상금융거래가 타 금융회사로의 전이를 미연에 방지하기 위해 각 금융회사에서 적발된 이상금융거래 정보는 상호 공유되도록 해야 한다.

효율적인 대응을 위해서는 공유되어야 할 정보유형(데이터유형, 전송규격, 암호화통신, 무결성 등)과 전문규격을 사전에 정의하고, 공유 절차 및 방안에 대해 논의한다.

- 사고일시(예 : 날짜, 시간 등)

- 사고정보(예 : 공통 디바이스 형상 정보, 금융회사명, 사고계좌번호, 사고소유자명, 생년월일, 성별, 국가<지역>정보 등)

(라) 연구분야

- 동향조사 : 기술동향, 사기 사건 동향 정기조사- 특별조사 → 추세선이 최고점, 최저점 형성 원인조사
- 코드설계 : 발생하였거나 향후 발생 예상되는 사고유형을 유형별로 국내의 공통모형화하고 코드 부여
- 추세분석 : 기술과 사건 연관도 분석, 추세선 진단 후 방향 도출

3. 핀테크 거버넌스 보안 전략분야(C)

(가) 분야 명 : **핀테크 보안 공격 시나리오 모델 연구**

(나) 분야 선정 사유

이상금융거래 탐지시스템은 인터넷뱅킹 및 스마트폰 뱅킹 등과 같이 비대면으로 이루어지는 자금이체 행위에 대한 이용자 패턴분석, 사고패턴 등 종합적인 분석을 통해 이상징후 포착 시 거래중단 혹은 추가인증을 통해 사고를 예방하는 시스템이다. 최근 모바일 환경으로의 변화, SNS의 활성화, 사물인터넷의 발전 등으로 인해 발생하는 데이터가 급속도로 늘고 있어 이를 분석하기 위한 빅데이터 활용이 가속되고 있다. 단순 기술이 아닌 기능 간 종합과 연동 형태의 모니터링과 분석, 연관성 분석이 필요하며 한국의 환경에 맞는 사기탐지 알고리즘 개발을 위해서는 보안 공격 시나리오 모델 연구가 필요하다. 그동안 시행되었던 시나리오 모델 연구는 기초로 하되 변화하는 환경에서 발생가능한 다양한 패턴의 모델이 정기적으로 개발되어야 한다

(다) 배경

- 공격 방법과 횟수가 늘어나고 공격 경로도 지속적으로 증가하는 상황에서 완전한 방어란 불가능하다.
- 방어 효율을 높이기 위해서는 핀테크의 확산과 더불어 발생 가능한 다양한 패턴의 모델이 정기적으로 개발되어야 한다
- 지금까지는 실제 공격이 이뤄지는 공격 시나리오 자체는 그리 많지 않았다. 공격자들이 실행하는 공격 시나리오는 전세계적으로 500~5,000개를 넘지 않을 것으로 추정하는 보고도 있다.
- 수십 만개 이상의 공격은 이런 공격 시나리오를 반복할 뿐이다. 단 이모델에 대한 심층 분석과 정기적 진단을 통해 새로운 시나리오를 예측해야 한다.

(라) 데이터 처리 알고리즘 종류

방식	빅데이터 (Big Data)	데이터마이닝(Data Mining)	머신러닝 (Machine Learning)	딥러닝 (Deep Learning)
특성	대규모(Big)의 모든 정형 및 비정형 데이터를 처리하는 기술	수많은 데이터 가운데 의미있는 정보를 찾아 (발굴해) 내는 기술	과거 데이터에서 어떤 패턴을 읽어내어 기계가 학습한 후 미래를 예측하는 기술	패턴의 2차 유사성을 평가 이해평가

(마) 딥러닝의 핵심 이점

4가지 강점을 통해 딥러닝은 다른 방법으로는 불가능한 유용한 결과를 도출할 수 있고, 다른 방법보다 더 정확한 모델을 구축할 수 있으며 유용한 모델을 구축하는 데 필요한 시간을 단축할 수 있다. 특징 간 복잡

한 상호작용을 탐지하는 능력, 최소한으로 처리된 원시 데이터에서 저수준의 특징을 학습하는 능력, 높은 기수(high-cardinality) 클래스 멤버십을 다루는 능력, 미분류(unlabeled) 데이터를 다루는 능력 등 이다.

- 보이지 않는 변수 간 상호작용 탐지

딥러닝은 표면적으로는 보이지 않을 수 있는 변수 간의 상호작용(interactions)을 탐지 한다. 상호작용이란 상호 조합되어 움직이는 두 개 이상 변수의 효과다. 기존의 예측 모델링 방법도 이런 효과를 측정할 수 있지만 많은 가설 테스트를 수작업으로 수행해야만 한다. 딥러닝은 이런 상호작용을 자동으로 탐지하며 분석가의 전문지식이나 기존 가설에 의존하지 않는다. 특히 딥 뉴럴 네트워크(deep neural networks) 사용 시 비선형적 상호작용을 자동으로 생성하고 충분한 뉴럴 네트워크로 임의 함수를 근사치로 계산할 수 있다.

(바) 새로운 공격패턴 연구분야

- 알고리즘과 기술에 대한 최근의 흐름과 조류 진단 방안
- 다양한 보안 요구 환경에서 발생하는 새로운 공격시나리오 발굴방안
- 데이터처리 알고리즘 종류 별 새로운 공격시나리오
- 딥러닝 알고리즘 환경의 새로운 공격시나리오
- 공격동향 추세분석에 기반한 공격시나리오

4. 핀테크 거버넌스 보안 전략분야(E)

(가) 분야 명 : 머신러닝 기반의 지능형 탐지 엔진(fraud detection engine) 소프트웨어 아키텍처 설계방법

(나) 분야 선정 사유

사기탐지 소프트웨어 개발에서 분석·설계의 중요성은 아무리 강조해도 지나치지 않으며 특히 FDS 소프트웨어 개발 시 분석·설계 단계가 간과 가능성이 높다. 지능형 탐지 엔진(fraud detection engine) 소프트웨어 아키텍처는 시스템을 개발하기 위해 전체 생명주기에 걸쳐 작성하는 산출물을 정의하고 산출물의 작성 방법을 안내하는 지침서로서의 역할을 해야 한다. 기존의 방법론은 사기탐지라는 최근의 특화된 시스템의 소프트웨어 개발자들이 사용할 분석 및 설계방법론 및 산출물 가이드가 부족하고, 방법론들도 산출물간의 연관관계 및 체계가 본격적으로 연구되지 못했을 것으로 예상된다. 특화된 사기탐지 요구사항 분석, 설계에 가이드로서의 역할을 충분하고 산출물 작성 부담을 경감하는 아키텍처 설계 방법이 필요하다.

#### (다) 사기탐지 소프트웨어 아키텍처 필요성

- 이해 관계자와의 커뮤니케이션을 위하여 정의된 형상이자 표현의 수단이다. 소프트웨어 아키텍처를 통해 이해 관계자들(프로젝트 관리자, 품질 담당자, 개발자, 테스터, 고객등)은 보다 원활한 커뮤니케이션을 할 수 있다.

- 소프트웨어 아키텍처는 설계 방향의 가이드이다. 전체적 관점에서 품질 속성을 고려하여 목표 시스템의 설계 방향을 조기에 결정할 수 있도록 지원하고, 향후 발생할 수 있는 위험요소를 감소시킬 수 있다.

- 재사용 가능한 시스템의 추상화를 제공함으로써 소프트웨어 아키텍처가 시스템 구성요소와 이들간 관계를 간략하고 명확하게 나타낼 수 있다.

#### (라) 카네기멜론 대학 SEI(Software Engineering Institute) 정의

소프트웨어 아키텍처에 관한 연구를 주도하고 있는 미국 카네기멜론

대학의 SEI(Software Engineering Institute)에서는 일반적으로 다음과 같이 정의한다.

“한 시스템의 소프트웨어 아키텍처란 그 시스템의 한 구조나 구조들로 각 요소들과 외부에 보이는 특성들 그리고 그들간의 관계를 절충한다. “

“Software architecture for a system is the structure or structures of the system, which compromise elements, their externally-visible properties, and the relationship among them.“

#### (마) 머신러닝 기반 소프트웨어 아키텍처 요구사항

사기탐지 소프트웨어는 속도(Speed), 가치 창출 시간(Time to value), 모델 정확도(Model accuracy), 손쉬운 통합(Easy integration), 유연한 구축(Flexible deployment), 사용 편의성(Usability), 시각화(Visualization) 요구사항을 고려해야 한다.

- 손쉬운 통합: 머신러닝 소프트웨어는 실무 환경의 복잡한 빅데이터 소프트웨어 사양과 공존해야 한다.

- 유연한 구축: 머신러닝 소프트웨어는 하둡 또는 프리스탠딩 클러스터에서의 코로케이션을 포함한 다양한 구축 옵션을 지원해야 한다. 아키텍처에 클라우드가 포함되어 있다면 아마존 웹 서비스, 마이크로소프트 애저, 구글 클라우드 플랫폼과 같은 다양한 클라우드 플랫폼에서 실행되는 소프트웨어를 찾아야 한다.

- 사용 편의성: 데이터 과학자는 R, 파이썬(Python), 스칼라(Scala)와 같은 분석 언어를 포함한 다양한 소프트웨어 도구를 사용해 작업을 수행한다. 머신러닝 플랫폼은 데이터 과학자가 이미 사용하고 있는 도구와 손쉽게 통합되어야 한다.

(\* 주 : IDG Korea 머신러닝 입문 가이드, IDG Deep Dive | Machine learning Guide )

(바) 연구 분야

- 요구사항 다양화와 짧아지는 개발 기간에 대비한 머신러닝 기반 소프트웨어 소프트웨어 아키텍처 요구사항 정의
- 클라우드 표준 플랫폼으로 오픈소스 기반의 Open PaaS 개발
- 프레임워크는 다양한 아키텍처 지원 유연한 프레임워크 설계= 디자인 패턴 + 라이브러리 설계
- 머신러닝 기반 소프트웨어 애플리케이션 구조 결정

(\* 주: 정보통신단체표준(국문표준) 참조)

5. 핀테크 거버넌스 보안 전략분야(F)

(가) 분야 명 : **핀테크 보안 제품 평가방법 개발**

(나) 분야 선정 사유

정보보호제품 성능시험의 정의는 정보보호제품의 효율성을 평가하고 신뢰성을 개선하기 위하여 수행하는 성능 측정 및 개선 관련 모든 활동을 의미한다. 같은 유형의 정보보호제품에 대한 표준화된 시험항목을 이용하여 성능을 비교함으로써 사용자에게 최적화된 정보보호제품을 선택할 수 있게 해주는 것이 목적이다. FDS 제품 구매 시 자사의 IT 환경에 가장 적합한 기능 및 성능을 보유한 제품을 선택하기 위해서 개별적으로 BMT를 실시한다. BMT 수행은 표준화된 성능 시험 방법론 및 기준의 부재로 인하여, 성능 관련 측정정보보다 기능측정에 치중하는 경향이 있다. 그 결과, 제품 본연의 품질보다 기능에 대한 정보만 얻게 될 수 있다. 표준화된 시험방법론에 근거한 FDS제품 성능시험은 사용자들에게

제품 선택 시 고려해야할 유용한 정보를 제공해 줄 수 있다.

(다) 정보보호제품 성능시험 정의

정보보호제품이란 “정보의 수집·가공·저장·검색·송신·수신 중에 정보의 훼손·변조·유출 등을 방지하기 위한 관리적 기술적 수단”을 말하며, 대표적인 정보보호제품으로는 안티바이러스, 침입차단시스템, 침입방지시스템, DDoS 대응장비, 웹 방화벽 등이다. 성능시험이란 “다수의 클라이언트의 요청을 처리하는 서버의 효율성을 평가하고 신뢰성을 개선하기 위하여 수행하는 성능 측정 및 개선 관련 모든 활동을 의미한다. 성능시험 목적은 시스템의 애플리케이션 프로그램과 웹 서비스 인 프라(웹서버(Web Server), 웹 애플리케이션 서버(Web Application Server), 데이터베이스, 네트워크 등에 문제점 및 성능 개선 방안을 제시하여 품질 향상 및 중단 없는 서비스를 제공하기 위함이다.

(라) 기존 평가제도

o CC 평가·인증 제도

CC 평가·인증제도는 민간업체가 개발한 정보보호시스템에 구현된 보안 기능의 안전성과 신뢰성을 보증하여 사용자들이 안심하고 제품을 사용할 수 있도록 지원하는 제도로 「국가정보화기본법」에 근거하고 있다. 시험기준은 “ISO/IEC 15408 : 공통평가기준”, “ISO/IEC 18045 공통평가 방법론”에 기반으로 평가·인증을 수행한다.

o 법으로 지정한 한국인터넷진흥원(KISA)과 인증기관이 승인한 4개 평가기관(한국산업기술시험원(KTL), 한국시스템보증(KoSyAs), 한국아이티평가원(KSEL), 한국정보통신기술협회(TTA))은 정보보호제품 평가 등의 역할을 수행한다.

o TTA(한국정보통신기술협회)



전기통신 관련 표준화 활동을 위해 1988년 설립된 재단 법인으로써 1991년 8월 전기 통신 기본법에 따라 법정 법인이 되었다. 정보통신 방식, 통신 프로토콜 등의 국내 표준 작성 및 보급과 국내외 표준화 조사 및 연구, 국제 연구단의 구성 및 운영, 국제 표준화 관련 기관과의 협력, 국내 IT 제품에 대한 시험 인증 등 활동한다.

(마) 세계 동향

○ 국제적 인증 체계

- TCSEC과 ITSEC은 CC로 통합되고 1996년에 초안이 나와 1999년 국제 표준 승인

- CC는 인증을 위해서 PP(Protection Profile)는 사용자 또는 개발자의 요구사항을 정의. ST(Security Target)는 개발자가 작성하며 제품 평가를 위한 상세 기능을 정의. PP는기술적인 구현 가능성을 고려하지 않는 데 반해, ST는 기술적 구현 가능성을 고려 TOE는 획득하고자 하는 보안 수준을 의미한다.

○ 국제 공통 평가 기준 상호 인증 협정(CCRA)

보안 제품 공동평가 통계 관리 프로그램은 크게 4가지의 기능이 있다. 첫째 CCRA가입국의 각 국가별 통계 기능과 둘째 사용자가 쉽게 알아볼 수 있도록 그래프 통계 기능과 셋째 결과들을 쉽게 문서화를 시킬 수 있는 리포트 생성기능과 넷째 사용자가 데이터들을 쉽게 관리 할 수 있는 데이터 입출력 기능이 있다. 시스템 구조도는 사용자 측면에서 쉽고 편리한 기능으로 CCRA 가입국 제품들의 통계를 알아볼 수 있고, 문서화를 시킬 수 있다.

○ 시험인증기관 THE TOLLY GROUP

1987년에 설립된 이래로 전세계적으로 정보통신 장비 및 서비스 제조업체로부터 400 여건 이상의 위탁시험을 수행했으며, 제 3자 서비스를 제공하고 있는 사설 독립 시험 기관으로서 세계적으로 영향력을 보유하고 있는 네트워크 장비 시험 센터이다.

(바) 연구 소재

- FDS 제품 구매 시 자사 IT 환경에 가장 적합한 기능 및 성능 개별적 BMT 방안
- 최소한 성능 기준을 만족하는 제품 인증 제도 실시방안
- 제품 수출을 위해 CCRA의 정책 변화에 대응하여 국내외 시장에 적합한 품질 평가 방안
- FDS CC인증 평가기준은 CC 인증 모델을 참조하되 독창적 모델을 개발

6. 핀테크 거버넌스 보안 전략분야(G)

(가) 분야 명 : 사기탐지 프로세스 평가방법 개발

(나) 분야 선정 사유

카네기멜론대학의 SEI(Software Engineering Institute)는 미국국방성의 요청으로 소프트웨어 프로세스 능력을 평가하는 Capability Maturity Model Integration을 개발하였다. CMM은 각 수준별로 핵심적으로 수행해야 하는 프로세스들을 정의하고 업체에서 그 프로세스들을 모두 수행하면 해당 수준을 달성했다고 판단한다. CMM에서는 24개의 프로세스 영역을 고려하고 있으며 프로세스의 능력(process capability)을 6단계로 평가한다. 조직의 성숙도(organizational maturity)는 여러 프로세스의 능력을 종합하여 5단계로 평가한다. 이상금융거래 탐지시스템도 프로세스 성숙도 수준이 높은 조직일수록 생산성이 더 높기 때문에 프로세스 성숙도를 높이는 방향으로 사기탐지 프로세스 평가모델 개발이 필요하다.

(다) 사기탐지 프로세스 모델

사기탐지 프로세스는 정보 수집, 분석/탐지, 대응, 관리/운영의 4단계로 수행된다. 거래내역을 수집한 후 이상 거래에 대한 패턴이 있는지 확인하고 이상이 감지된 경우 대응 시스템에 알리게 된다. 이 때, 사용되는 탐지 패턴의 정확도와 범위에 따라 모니터링의 효율성이 나타나게 된다.



(라) ISO 27001의 프로세스 평가 항목

순번	구분	세부평가항목
1	A.5 보안 정책(Security Policy)	2
2	A.6 정보 보안 조직(Organization of Information Security)	11
3	A.7 자산 분류 및 통제(Asset management)	5
4	A.8 인력 자원 보안(Human Resource Security)	9
5	A.9 물리적 및 환경적 보안(Physical and Environmental Security)	13
6	A.10 통신 및 운영 관리(Communications & Operations Management)	32
7	A.11 접근 제어(Access control)	25
8	A.12 정보 시스템의 구축과 개발 및 운영(Information Systems Acquisition, Development & Maintenance)	16
9	A.13 정보 보안 사고의 관리(Information security incident management)	5
10	A.14 사업의 연속성(Business continuity management)	5
11	A.15 준거성(Regulatory compliance)	10

(마) 연구개발 사항

사기탐지 프로세스 평가방법 프로세스 모델을 새롭게 개발한다. 국내의 금융 업무 현장에서 사기탐지 업무에 적용할 수 있는 모델을 목표로

하며 SO27001, ISMS 모델을 참조하되 개선 순환구조 모델을 개발 인증제도와 연계하여 개발한다.

o 프로세스 참조모델(process reference model)

주요 내용은 프로세스 정의이다. 성숙모델과 측정모델에서 참조된다. 프로세스 및 세부 프로세스 정의 및 분류, 프로세스별 목적 결과물 세부 활동으로 구성된다.

o 프로세스 성숙모델(process maturity model)

프로세스의 성숙레벨을 정의하고 각 레벨별로 핵심 프로세스 영역(key process areas : KPA)을 정의한다. 성숙 레벨 정의, 레벨별 KPA 속성 정의로 구성된다.

o 프로세스 측정모델(process measurement model)

프로세스 성숙 레벨을 측정하는 기준과 방법을 정의한다. 프로세스 성숙도 정의, 프로세스 측정을 위한 측정 항목 정의, 항목별 측정 지표로 구성된다.

o 프로세스 개선모델(process improvement model)

조직내에서 정보 및 데이터 품질관리 프로세스 성숙도를 개선하여 데이터 품질을 향상시키기 위한 방안 또는 지침을 정의한다.

o 프로세스 표준화 평가지표 개발

최근 기업들이 프로세스 표준화의 중요성을 인지하고, 서비스 컨설팅 기업에 의뢰하여 자신의 기업에 적합한 서비스접점 매뉴얼을 개발하여 교육시키고 프로세스 표준화가 서비스품질에 긍정적인 영향을 미치고 직무만족 또한 서비스품질영향을 검증한다.

## 7. 핀테크 거버넌스 보안 전략분야(H)

(가) 분야 명 : **핀테크 보안 포렌식 업무 모델 발굴**

(나) 분야 선정 사유

CERT(Computer Emergency Resonse Team)업무 모형은 미 국방부 고등연구 계획국(DARPA:The Defense Advanced Research Projects Agency)이 컴퓨터 관련 침해 사고에 대응하고자, 피치버그의 카네기멜론 대학내의 소프트웨어공학 연구소에서 시작되었다. 이상금융거래 탐지시스템은 인터넷뱅킹 및 스마트폰뱅킹 등과 같이 비대면으로 이루어지는 자금이체 행위에 대한 이용자 패턴분석, 사고패턴 등 종합적인 분석을 통해 이상징후 포착 시 거래중단 혹은 추가인증을 통해 사고를 예방하는 시스템으로 매우 특화된 보안영역이며 CERT의 또 다른 패턴 업무이다. 이상금융거래 탐지 프로세스는 금융기관마다 상이하게 구성되어 있고 그 효율성 모델에 대해 별도의 연구개발이 이루어지지 않았다. 본 분야를 통해 한국형 금융사고 포렌식 프로세스 모델을 개발함으로써 국내 금융사기 포렌식 체계화 기초를 다진다.

(다) 일반적 CERT 모형

사전대응 - 사고 발생 - 사고 탐지 - 대응 - 제거 및 복구 - 후속조치



(라) 핀테크 포렌식 모델 개발분야

(1) 핀테크 포렌식 기능 체계화

o 핀테크 보안사고 탐지과정 정립

침해 사고 발생을 실시간으로 식별하는 과정은 주로 침입 탐지 시스템 (IDS)이나 침입 방지 시스템(IPS), 네트워크 트래픽 모니터링 장비 (MRTG:Multirouter Traffic Grapher), 네트워크 관리 시스템(NMS:Network Management System)이다. 핀테크 환경에서는 사용자 단말 노드에서부터 상황이 발생하므로 핀테크사고 탐지과정 정립도 핀테크 환경을 전제하여 개발되어야 한다.

- 핀테크 보안사고 식별 과정에서 확인 사항 정립
- 핀테크 보안사고 대응 프로세스 정립
  - 단기 대응, 백업 및 증거 확보, 시스템 복구, 후속 조치 및 보고

#### (2) 평시와 사고 시 핀테크 포렌식 수행 추가

- 평시 핀테크 보안사고 모니터링 체계 정립
- 사고 발생 후 핀테크 포렌식 수행
  - 수사 준비, 증거물 획득(증거 수집), 보관 및 이송, 분석 및 조사, 보고서 작성

#### (3) 핀테크 포렌식 증거 수집 방법

- 핀테크 보안 솔루션 이용
- 네트워크 로그 서버 이용
- 스니퍼 운용
- 시스템(PC)에서의 증거 수집

#### (4) 핀테크 포렌식 기술연구소재 발굴

- 모바일 결제사기 공격 역추적
- 피해방지를 위한 프로파일링

## 8. 핀테크 거버넌스 보안 전략분야(I)

### (가) 분야 명 : 사기탐지전문직(스페셜리스트) 분야 발굴과 및 역할 모델 정립

#### (나) 분야 선정 사유

사기탐지에 소요되는 전문기술은 사회학과 심리학 등 인간 심리분석기술이며 공학영역에서는 사기탐지 알고리즘, 인공지능, 암호화, 빅데이터, 포렌식 등 고도의 전문기술력이다. 각 기능별 사기탐지 전문가 양성은 시간이 오래 걸리고(slow), 꾸준해야 하며(persistent), 조금씩 축적되는 학습(cumulative learning) 과정이 필요하다. 글로벌 수준의 이상금융거래 탐지 인력 양성이 요구되므로 사기탐지전문직(스페셜리스트)의 역할 모델을 정립하고 핵심역량 양성과정 설계를 통해 국내 선도기업, 유관기관, 수요기관 공동 협의체의 사기탐지 전문인력 양성 프로그램 도입이 필요하다.

#### (다) 연구사항

##### (1) 사기탐지전문직은 직종 발굴

o 사기탐지전문직에 대한 분야와 수요예측이 필요하다(본 연구 예비진단).

번호	전문직종 영역	연구소재
1	사기 위험관리 체계	사기 위험관리 체계 전문직 역할
2	FDS 알고리즘	FDS 알고리즘 전문직 역할
3	핀테크 암호화	핀테크 암호화 전문직 역할
4	FDS 아키텍트	FDS 아키텍트 전문직 역할
5	데이터 사이언티스트	데이터 사이언티스트(Data Scientist) 역할

6	FDS 품질관리	FDS 품질관리 역할
7	FDS 코디네이터	FDS 코디네이터 역할
8	FDS 컨설턴트	FDS 컨설턴트 역할

## (2) 기술 육성 프로그램

- 커리큘럼 : 글로벌 추세 파악을 통한 커리큘럼 개발 (현장 교과 운영)
- 수요조사 : 산업체 대상 수요조사 기반 현장에서 바로 활용할 수 있는 Application-oriented Specialist 과정 운영 (인력 공급기반 확대), 관련 학과 연계
- 교육시설 : 교육장 인프라, 교육용 기자재(H/W, S/W 등)
- 운영계획 : 운영계획 사전수립, 교수법 및 교재 개발

## 9. 핀테크 거버넌스 보안 전략분야(J)

### (가) 분야 명 : 사기방지 업무 분야별 표준 가이드라인(Guidelines) 제정

#### (나) 분야 선정 사유

현재 기술가이드가 개발되었으나 특화된 영역으로서 분야별 업무 표준 가이드라인(Guidelines) 제정이 필요하다. 정보보안 정책서는 회사에서 보호해야 할 정보 자산을 정의로서 정보 보안을 실현하기 위한 기본 목표와 방향성을 설정한다. 정보 보안 지침서는 각 절차서의 기준이 되는 문서이다. 정보 보안 조직의 구성과 운영에 대한 내용과 각 지침절차의 기본 방향 등을 기술한다. Standards는 소프트웨어나 하드웨어 사용 등의 일반 운영에서 지켜야 할 보안 사항을 기록하는 문서로서 세부적인 기술이 아니라 일반적인 절차 표준을 담고 있음. Procedures는 가장 하위의 문서로 각각의 절차에 대한 세부 내용을 담고 있다. 업무 표준 가이드라



인(Guidelines)은 상위 지침 방향에 따라 실무적 사기방지 업무 처리요령이다.

(다) 가이드라인(Guidelines) 제정 필요 분야

o 보안성 검토 분야

- 검토부서는 정보화사업의 예산, 개인정보 규모, 정형성 유무를 판단하는 사전 검토를 수행하여 자체 보안성검토나 상위기관으로 검토 의뢰를 결정 지원
- 보안성 검토 자체 처리 시 보안성 검토 체크리스트를 활용하여 정보화사업에 대한 점검 및 평가를 수행

o 정보보안 사고조사 분야

- 정보보안사고가 발생 시 즉시 피해확산 방지 조치를 취하고 사고 원인 규명시까지 피해 시스템에 대한 증거 보존(1. 일시 및 장소 2. 사고 원인, 피해현황 등 개요 3. 사고자 및 관계자의 인적사항 4. 조치내용 등)

o 내부통제 분야

- 최소 권한(Least Privilege)은 한 사람이나 조직이 업무에 필요한 권한 이상을 부여받으면 안 된다는 개념
- 직무 분리(Segregation of Duties)는 하나의 업무 절차를 두 사람이 수행하도록 업무를 분리하는 것

o 사기탐지 처리 과정 분야

단계	모니터링	데이터 수집	데이터 가공	침입탐지	보고 및 대응
기능	평상시 감시	감사 데이터 수집	데이터 가공	침입여부 판정	침입사실 보고, 차단

10. 핀테크 거버넌스 보안 전략분야(K)

(가) 분야 명 : 사기방지 기술지원센터 기능 도입

(나) 분야 선정 사유

금융보안 영역에서 ISAC을 흡수하여 금융보안 전담 조직이 설립된 이후 많은 신기술 연구를 통한 사기방지 업무가 적용되고 있다. 금융사기는 사기 기법이 속도가 빠르게 나타나며 사기방지 업무현장에서 새로운 기술 수요는 지속적으로 발생한다. 이 필요한 기술의 금융 현장 보급은 현행 환경에서는 제도적으로 양적·질적으로 쉬운 분야가 아니다. 금융업무 현장의 기술 요구 및 흐름을 제대로 반영하여 해결하기 위해 창의적 기술인력, 현장 문제해결 지원 능력 구비가 시급하다. 금융사기 기술발전 속도를 능가할 수 있는 전문기술 인력양성을 바탕으로 현장지원 대안이 필요하다. 사기방지기술지원센터 설립을 통해 전문 기술지원, 컨설팅, 교육지원업무를 전담 지원하는 기능이 요구된다. 금융 사업자간 자율 지원센터를 설치하여 상생협력, 공동교육, 우수모델 발굴, 지원을 위한 협업 컨소시엄을 구축하고 관련 컨설팅창구를 개설하여 기술상담과 문제해결 지원을 수행하게 한다.

(다) 전문기술력 지원 방안

- 금융업무 현장 요구 및 흐름을 반영하는 전문기술력 지원
  - 이론 및 현장 문제해결 능력 컨설턴트 양성
  - 산업 특화 첨단기술에 대한 선제적인 기술 개발 및 과정 운영
  - 수요 급증 분야에 대한 특화과정 교육 실시
- 국내외 선도기업, 유관기관, 수요기관 공동 협의체 ‘교육센터’ 설립
- 해외 우수교육기관과 연계프로그램 추진, 글로벌 인력 양성

(라) 종합 컨설팅 지원체계 도입 방안

- 맞춤형 컨설팅 지원을 통해 금융사고 현장에서 체감하는 어려움 지원
  - 종합 컨설팅 지원체계 모델 개발
  - 법률부분은 정부에서 지원, 고급 기술분야는 민간 전문가 활용
- 전문 교육 및 컨설팅 지원
  - 관리적·기술적 보호조치 교육과 컨설팅
  - 개선방향 제시로 이용자의 위치정보 보호, 법 위반 사업자 예방

(마) 컨설팅 전문가 역량 강화 프로그램

- 효과적 컨설팅 지원체제로 기업체 지속성장 동력 창출
- 맞춤형 컨설팅 지원체제로 기업체 경쟁력 강화
- 개방·참여형 컨설팅 지원체제로 기업체 참여 촉진

(바) 연구분야

번호	단 계	연구개발 분야명	방 향	참 고
1	지원센터 설립	지원센터 설립 방안	지원센터 설립 방안	
2	기술교육	전문 기술교육	인공지능 기술 암호화 기술 포렌식 기술 하둡과 맵리듀스 빅데이터	
3	컨설팅	사기방지 기술컨설팅 능력 확보방안	컨설팅 가이드라인 개발 컨설턴트 양성	
4	정보지원	사기방지 정보지원	사기방지 글로벌 기술추세	

		방안	정보	
5	감사기능	감사기능	사기방지 업무 자체감사 기능	
6	전문자격증	사기방지 전문자격증	사기방지 자격검정 방안	

## 11. 핀테크 거버넌스 보안 전략분야(L)

### (가) 분야 명 : 사기방지 업무 자체 운영실태 진단 방안 개발

#### (나) 분야 선정 사유

자체 운영실태 진단은 운영상의 정확성을 확인하기 보다 조직의 시스템들이 적법 하게 제대로 운영되고 있는지, 조직이 예상한 (목표로 정한) 결과를 산출하였는지 평가하고(성과평가), 어떤 점이나 어떤 분야에서 개선이 필요할 것인지 평가한다. 통제 체계(MCS)에 대하여 ‘안심’ (안전)(assurance)할 수 있다거나 또는 유효하다고 하는 판단을 제시 (declaration of validity)하며 개선방안에 대한 제안, 권고안을 작성해야 하고 이를 통해서 조언을 제공하는 역할을 수행해야 하는 것이다.

#### (다) 자체 운영실태 진단 의의

- ‘자체’ (Internal)가 의미하는 것은 조직 스스로가 수행하는 자체 운영실태 진단
  - 내부 대상이 되는 조직에 대하여 기능(직무상)적으로 일종의 조직의 영속적 자기혁신 체제(permanent auto-reformation)라고 할 수 있다.
- 현대적, 실질적 의미의 자체감사

- 성과결과에 초점을 두고, 조직이 초기에 정한 목표와 관련해서 (성과)결과로 나타난 실제 사실과 그러한 일관성 정도를 평가하는 것
- 최근의 개념으로 보다 폭넓게 “검사하고, 평가하고, 권고안으로 개선을 유도하는, 내부통제”와 관계가 있는 활동임.
- 통제(control)와 확인(verification)의 개념과도 구별됨(Audit is not control)
- 자체 운영실태 진단인은 전통적인 통제 방식과 관련된 책임도 맡지 않음.

#### (라) 내부통제, 감찰의 의미

- o 내부통제(Internal control)에 관한 글로벌 스탠더드의 하나인 뉴욕주 정부의 내부통제법(Internal Control Act, 1999)상에서 정의
- o “내부통제(Internal control)란 “조직이 정한 목표와 임무를 성취할 수 있다고 여기도록 합리적인 안심을 확인시켜주기 위한 그 조직 구성원들의 모든 활동, 계획, 태도(조직문화), 정책, 시스템, 자원, 노력의 통합을 의미한다.
- o 내부통제는 “일반적으로 받아들여 질 수 있는 원칙과 기준”에 의하여 조직의 경영(재정) 시스템과 통제(비재정) 시스템을 총괄(Financial Management and Control Systems, FMCS)하는 활동임(Cohen, 2008: 44). control의 의미는 조직에게 위협을 주는 위험성 요인들도 분석하여 제거하게 하는 등 Manage and Master (Command)의 의미

비교요인	자체감사기능 (Internal Audit)	내부통제기능 (Internal Control)
주기성	정기적, 주기적, 계획적으로 시행	지속적, 영속적인 기능
위치	내부에서 시행	경영의 한 부분으로 통합적으로 수행
대상	신뢰에 근거를 둔, 경영 및 통제 시스템(MCS), 결과 등을 검토(평가)	조직의 경영(역량과 수준), 위험성 진단
목표	효과성	관리(건전한 재정경영)
방법론	적법성, 기준(Standards), 모범사례(best practices)에 근거하여 평가, 조언	위험성 제거, 효과적 경영체제 등의 준거들에 근거하여 지속 추진
결과처리	제안(조언, 권고)	(행동전략 등에 의한) 정규정 확보
책임성 수준	조직의 합리적 안정성을 인정하는 '의견' 제시	책임성(Accountability) 확보
직업인	전문경력직에 의한 자문, 고문, 평가	조직, 기업 등의 (최고) 경영책임자

(마) 연구분야

번 호	단 계	연구개발 분야명	방 향	참 고
1	진단 방안	자체 운영실태 진단 방안	자체 운영실태 진단 방안	
2	정책	정책수립 방안	정책수립 방안	
3	효율성	업무효율성 진단 방안	업무효율성 진단 방안	
4	시스템	시스템진단(system audit) 방안	시스템진단(system audit) 방안	
5	성과	성과진단(performance or result audit) 방안	성과진단(performance or result audit) 방안	
6	개선	개선이행 진단 방안	개선이행 진단 방안	

## 12. 핀테크 거버넌스 보안 전략분야(M)

### (가) 분야 명 : 조직별 사기탐지 업무성숙도 평가모델 개발

#### (나) 분야 선정 사유

핀테크 운영 조직별 사기탐지 업무성숙도 평가모델 개발을 통해 사기 탐지실적 수준을 평가한다면 각 시스템의 업무개선과 목표관리에 효율성을 도모할 수 있다고 보여 진다. 정보보호관리에 대한 인식이 확산되면서 정보보호 위험분석의 수요가 증가하고 있다. 그러나, 업무현장에서의 실제 적용가능성을 심각하게 고려하지 않고 해외의 특정 방법론과 도구를 그대로 발표하고 있어 이론적 모델이 현장실무에 적용이 어려운 사례도 발견되고 있다. 업무현장 실정을 고려한 체계적 정보보호관리, 위험 분석 방법론 및 도구 개발을 위해 기존의 연구(보안 관리, 위험 분석, 평가 방법, 보호프로 파일, 평가 프로세스, 자산분류, 위협 및 취약성 등)를 연구할 필요가 있다.

#### (다) 정보보호 성숙도 모델

SEI(Software Engineering Institutes)의 CMM이 소프트웨어 개발업자의 개발능력을 평가하고 조직의 성숙도 수준 측정 모델인 반면 SSE -CMM은 공학, 보증, 위험 프로세스의 3가지 요소로 보안엔지니어링을 나누며 성숙도 평가 모델과 수준을 제시한다. 기존 연구를 근간으로 금융시스템을 대상으로 기술적 관점에서 정보 보호수준 ‘성숙 단계’를 정의한다. 이를 연구소재로 선택한 이유는 정보보호수준 성숙단계 진단은 기존의, 취약점 진단, 위험분석 방법론을 실무현장에서 사용할 수 있도록 종합적으로 결론을 제시 한다는 점이다. 특히 뱅킹시스템 환경의 사이버 거래에서의 안전성 확보를 위한 대안은 현장에서 실무적용 효과가 크게 나타

날 것으로 확신하기 때문이다.

SSE-CMM은 보안엔지니어링을 공학, 보증, 위험 프로세스의 3가지 요소로 나누고 있으며 정보보호 성숙도 평가 모델과 수준을 제시하고 있다. 정보보호 성숙도 측정은 취약점 진단, 위험분석 방법론을 실무 현장에서 사용할 수 있도록 종합적으로 결론을 제시한다. 사이버거래의 일반적인 서비스는 인터넷뱅킹, 모바일뱅킹, 텔레뱅킹 등이다. 사이버거래 처리구조의 한 종류인 banking시스템 정보보호 성숙도 측정방법론 연구 목적은 기존의 취약점 진단, 위험분석 방법론을 실무현장에서 사용할 수 있도록 종합적 결론을 제시한다. 안전성과 편리성을 확보하여 이용자들이 사이버 거래를 편리하게 이용할 수 있는 환경을 구축하는 것이 사이버 거래 활성화의 핵심이다. 특히 업무현장에서 정보보호 성숙도 측정을 통한 사이버뱅킹시스템의 안전성을 확보한다면 현장의 실무처리 결과로 많은 효과가 나타날 것으로 기대한다.

#### (라) 정보보호성숙도 측정 단계별 수행방법

위험분석 방법론을 토대로 banking시스템을 중심으로 사이버거래에서의 보안관리 수행과정으로서 정보자산, 위협, 취약성, 대응책을 중심으로 대상 정보 환경의 위험을 측정하는 절차와 기술을 제시한다.

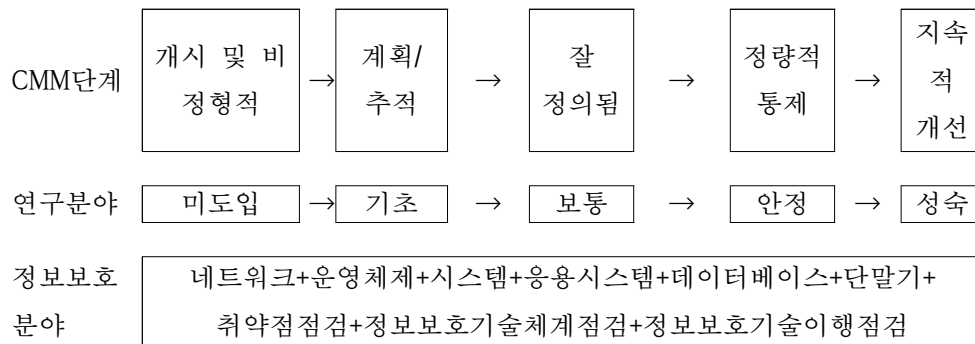
- 위협평가 : 정보시스템 자산에 대한 내외 부로부터의 보안 침해위협을 점검, 평가. 모의 침투, 보안체크리스트 점검
- 취약점평가 : 정보보호취약점 평가 운용 중인 정보시스템 자산이 위협에 노출될 수 있는 가능성과 요소 수준 점검
- 보안체계진단 : 기술적 정보보호 체계 진단 정보시스템에 가해지는 정보보호침해 위험을 회피 또는 감소시킬 수 있는 기술적 분야의 대응체계 진단.



- 위험도측정 : 자산, 위협, 취약점, 보안체계 단계산정, 위험도를 연  
계 분석하여 현재의 위험 수준 평가.
- 정보보호성숙도 수준측정 : 이상의 산출 결과를 바탕으로 정보보호  
성숙도 수준을 종합적 평가.

등급명	A	B	C	D	E
정보보호기능만족도	매우만족	만족	보통	미흡	매우미흡
정보보호성숙도	성숙	안정	보통	기초	미도입
성숙도수준별점수범위	81-100	61-80	41-60	21-40	0-20

(마) 성숙도 단계 연구 소재



13. 핀테크 보안기술 연구개발 분야(D 그룹1)

(가) 분야 명 : **블록체인 핀테크 보안 취약성 실험 및 진단 기술개발**

(나) 분야 선정 사유

블록체인은 가상화폐(Bitcoin)에서부터 시작되어 P2P대출, 거래인증 등

최근 핀테크 기술과 융합되어 다양한 분야에 활용된다. 분산식 원장 기술(distributed ledger technology)을 사용하는 블록체인은 높은 보안성, 거래내역의 투명성, 비용절감 등의 장점으로 글로벌 금융시스템의 새로운 기회로 부상하고 있다. 한국형 인증서 발급 시스템이 가진 맹점을 비트코인 생태계의 근간을 이루는 블록체인이 해결할 수 있을지 주목되고 있으며 핀테크에서 블록체인 보안 시험을 통해 보안 취약성 요소를 진단할 필요가 있다.

#### (다) 블록체인 거래대상

- 비트코인 : 디지털 통화로 발행하고 관리하는 중앙 장치가 존재하지 않는 구조를 가지고, 거래는 P2P 기반 분산 데이터베이스를 이용한 공개키 암호 방식 기반으로 거래를 수행. 거래내역이 가입자간 모두 공개되며, 익명성을 보장할 뿐만 아니라 수수료가 거의 없음
- P2P 대출 : 개인 투자자들이 금전을 맡기면, 대출을 원하는 이용자들의 평판 정보를 분석하여 금전을 빌려줌으로써 발생하는 수익을 개인 투자자들에게 분배해주는 서비스. 투자자 및 대출자의 금전은 블록체인을 이용하여 투명성 및 신뢰성을 보장한다
- 주식 거래 : 나스닥의 프라이빗 마켓은 변호사에게 거래를 승인받도록 하여 거래 속도가 느렸으나, 이 과정을 블록체인으로 대체하여 모든 거래를 자동으로 검증하는데 이용할 계획임
- 해외송금 : 블록체인 기술을 사용하여 중개기관 없이 개인 간 직접 거래하여 수수료 절감. 미국 핀테크 기업(Ripple)은 블록체인 기술 사용으로 기존 10분의 1 수수료로 송금

탈중앙성(P2P-based)	공인된 제3자의 공증 없이 개인간 거래 가능 -불필요한 수수료 절감
보안성(Secure)	정보를 다수가 공동으로 소유하여 해킹 불가능 -보안관련 비용 절감
신속성(Instantaneous)	거래의 승인·기록은 다수의 참여에 의해 자동 실행 -신속성 근대화
확장성(Scalable)	공개된 소스에 의해 쉽게 구축·연결·확장 가능 -IT 구축비용 절감
투명성(Transparent)	모든 거래기록에 공개적 접근 가능 -거래 양성화 및 규제 비용 절감

(\* 주 : KB금융지주 경영연구소)

#### (라) 금융권 동향

- KB국민은행 : 핀테크기업 코인플러그와 블록체인 기반의 새로운 외환 비즈니스 모델 개발을 위한 전략적 제휴(MOU) 체결. 국민은행은 블록체인기술 기반의 해외송금서비스 등 새로운 외환 비즈니스 모델을 개발할 계획. 코인플러그는 우리은행 블록체인 서비스를 개발 중
- 농협 : 비트코인 거래소 코빗과 블록체인을 기술 제휴를 체결.
- 신한은행 : 스트리미에 5억원의 지분 투자를 통해 블록체인 기술 기반 외환송금 시스템을 개발 중.
- KEB하나은행 : 핀테크 인큐베이터 1Q랩에 블록체인 기술 기반의 외환송금 시스템을 개발 중
- 글로벌 대형 금융사는 블록체인 기술을 국제 표준으로 도입 추진

#### (마) 핀테크에서 블록체인 보안 진단분야

- 블록체인 보안성 기술 실험
  - 다양한 핀테크 다양한 방식 ‘블록체인(Blockchain) 기술’을 활용한 보안성 진단
  - 블록체인 개인정보유출, 해킹 안전 진단
- 분산식 원장 기술(Distribute Ledger Technology) 보안성 진단
- 기존 금융 인프라와 보안기술을 보완 방식 진단

o 블록체인 기술의 잠재력 검증

#### 14. 핀테크 보안기술 연구개발 분야(D 그룹1)

(가) 분야 명 : 근거리무선통신 경량암호화 기술개발

(나) 분야 선정 사유

핀테크의 보안을 위해서는 데이터의 무결성을 확보해야하며 이를 위해 암호화(PKI)와 키 관리가 필수적이다. PCI-DSS 준수를 위한 맞춤형 암호화, 키 관리가 필요하다. 한 지불, 결제 관련 핀테크 서비스 사업자라면 PCI-DSS와 같은 최소 요구 조건을 충족시켜야 한다. 강력한 보안체계를 갖추기에 인터넷 공유 기기는 제한적인 요소가 많다. 기기의 크기가 작기 때문에 자원 제약성이 높으며, 보안기술 자체가 아직 미미하다. 또 매시업 보안기술의 부재로 프라이버시 보호도 쉽지 않다. 인터넷 기기에 독자적인 보안체계를 구축할 경우 가격 측면에서 이득이 사라진다. 데이터를 전송할 때 필요한 경량 암호 알고리즘의 경우도 제한적이어서 근거리무선통신 경량암호화 기술개발 연구가 필요하다

(다) 사물인터넷 보안 경량암호화 범위

o 사물인터넷 ‘게이트웨이’ 보안

게이트웨이 보호는 모든 네트워크보안의 숙제이다. 가정에서 쓰이는 사물인터넷 기기들은 대부분 인터넷공유기와 같은 게이트웨이를 통해 데이터를 주고받는다. 사이버공격자가 게이트웨이를 공격해 권한을 탈취할 경우 개인정보, 민감정보 등이 모두 탈취될 수 있다. 공격자는 자동화도구를 통해 비밀번호가 설정돼 있지 않은 공유기에 접속, 호스트 주소(host.ics)를 변조한다. 해당 공유기에 접속한 모든 사용자들은 공격자가

의도하는 파밍 사이트로 접속하게 되고, 개인정보유출 등의 위협에 고스란히 노출된다. 특히 최근에는 공공장소에 있는 공유기의 환경설정을 변조해 파밍용 애플리케이션을 내려 받도록 하는 공격 유형이 나타나고 있다.

#### ○ 개방형 통신 표준 프로토콜

인터넷 기기 대부분이 무선 네트워크 통신이므로 이에 따라 무선 공유기 공격을 통한 보안 위협도 증가할 것이다. 인터넷 공유기기 통신표준은 올조인(AllJoyn)을 채택해 각종 통신에 대한 접근권한을 통제하거나 REST, XMPP, MQTT와 같은 개방형 표준을 사용하면 암호화 적용이 가능하다. 인터넷 통신 표준 올조인(AllJoyn)은 각종 통신에 대한 접근권한을 통제하거나 REST, XMPP, MQTT와 같은 개방형 표준을 사용한다면 암호화 적용하기가 쉽다.

#### ○ 인터넷, 프라이버시 보호

인터넷 산업이 성공하기 위해서는 프라이버시를 간과해서는 안된다. 아무리 좋은 서비스라도 프라이버시 보호가 안된다면 소외된다. 인터넷은 많은 요소기술 통합으로 보안 취약성 발생 능성이 높다. 하지만 이러한 특징으로 인해 보안이나 프라이버시 보호가 쉽지 않다. 디바이스, 네트워크, 플랫폼, 서비스 등 모든 산업군에서 프라이버시 문제는 발생할 수 있다. 사물인터넷이 성공하기 위해서는 프라이버시 보안 강화 등이 반드시 필요하다.

#### ○ 사물인터넷 엔드투엔드 암호화

사물인터넷 기기와 서버 간 통신을 보호해주는 암호 모듈은 통신 암호화를 위한 암호 알고리즘을 이미 보유하고 있고, 가상사설망(VPN) 기술 등을 사용한다. 보안 Protocol은 사물인터넷 기기 간 CoAP(Constrained Application Protocol)과 DTLS(Datagram Transport Layer Protocol)가 있다. 자원 한정적인 노드와 네트워크 환경에서 DTLS 패킷의 크기를 제한해 부하를 줄이고, 추후 추가될 그룹키 관리기법을 통해 보안도 강화한다. 개인식별정보를 삭제한 뒤 정보를 수집하더라도 다른 정보와 결합을 통

해서 식별정보를 알 수 있다. 데이터 수집 단계에서 노이즈를 추가하거나 암호화를 하는 방법 등으로 프라이버시를 보호해야 할 것이다.

o 개인정보처리시스템 간 암호화

개인정보처리시스템간에 개인정보를 전송할 때 암호화를 지원하기 위하여 공중망을 이용한 VPN(가상사설망)을 구축할 수 있다. VPN은 기반이 되는 보안 프로토콜의 종류에 따라 IPsec VPN 방식, SSL VPN 방식, SSH VPN 방식 등으로 구분할 수 있다.

(라) 연구개발 분야

o 인터넷 디바이스별 경량암호화 프레임워크 구조 설계

o 근거리 무선통신 별 구조와 기능 정의

o 종단간(P2P: Point to Point) 암호화

15. 핀테크 보안기술 연구개발 분야(D 그룹1)

(가) 분야 명 : 랜섬웨어 실시간 대응' 보안 솔루션 기술개발

(나) 분야 선정 사유

랜섬웨어(Ransomware)는 ‘파일을 인질로 잡아 몸값을 요구하는 소프트웨어’란 의미로, 랜섬웨어에 감염되면 사용자 컴퓨터에 저장된 문서, 그림 파일 등에 암호가 걸려 해당 자료들을 열지 못하게 된다. 시그니처/행위기반 탐지 기술을 우회하는 자동 알고리즘을 탑재하는 등 진화된 변종 랜섬웨어로 인한 피해 급증과, 리눅스, 맥 OS, IoT기기 등 공격 대상이 더욱 확대될 것으로 전망된다. 무작위로 개인을 낚던 랜섬웨어가 표적형으로 진화하여 금융회사 및 정부로 타겟 확장이 예상되며, 표적형 공격에 대응하기 위한 공동대응체계 강화가 필요하다. 이를위해 랜섬웨

어 실시간 대응’ 보안 솔루션을 연구한다.

#### (다) 현황

최근 국내에서 랜섬웨어로 인한 피해가 급증하고 신·변종 랜섬웨어가 지속적으로 발견되고 있으며, 기업뿐만 아니라 개인 사용자들에게까지 피해가 확산되고 있다. 특히, 악성코드 제작자들에게 금전적인 이득을 취할 수 있는 방법으로 여겨지면서 광범위한 대상을 향한 무차별적인 공격이 진행되고 있다. 백신으로 랜섬웨어 악성코드를 제거해도 암호화된 파일은 복구하기가 어렵다. 왜냐하면 암호화된 파일을 복원하기 위해서 암호 해독기가 필요한데 대부분 공격자의 서버에 저장되어 있기 때문이다. 또한 피해자가 공격자의 요구에 따라 대가를 지불해도 파일 복구가 된다는 보장이 없다. 특히 최근 랜섬웨어 공격은 백신 프로그램을 우회하기 위해서 다양한 신·변종 악성코드를 활용하는 지능형 위협 공격의 양상을 띠고 있다.

#### (라) 랜섬웨어 공격 기능

o 점차 고도화되는 랜섬웨어는 네트워크 레벨의 샌드박스 기반 보안 제품을 회피하기 위해서 기능이 세분화된 모듈화된 다수의 악성코드를 사용하여 구성한다. 이러한 과정에서 네트워크상의 보안 솔루션 탐지를 회피하기 위해 암호화 통신을 사용한다. 악성코드 역사에서는 ‘파일 암호화’ 기능을 보유한 ‘트로이목마’ 종류의 악성코드로 꾸준히 명맥을 이어 왔다.

o 악성코드 감염을 통해서 ‘금품 요구’라는 직접적인 해킹의 목적을 노출시키는 측면에서는 ‘가짜 백신’ 또는 ‘화면 잠금 바이러스’와 같은 스케어웨어(scareware)류 악성코드의 진화된 형태라고 볼 수 있다. 스케어웨어란 겉보기에는 합법적으로 판매되는 보안 프로그램과 유사하

지만 실제로는 보안 기능이 없이 오직 금전적인 이득을 목적으로 하는 소프트웨어를 말한다.

o 현재 테슬라크립트(Teslacrypt), 크립토월(CryptoWall), 티어랙(Teerac) 등 감염 방식 및 세부 동작 기능에 따라 다양한 이름으로 명명된 랜섬웨어가 전파되고 있다.

o 랜섬웨어류 악성코드의 핵심적인 특징은 ‘컴퓨터 이용자(피해자)에게 가치 있을만한 문서, 이미지와 같은 컴퓨터 내 주요 파일을 무단으로 암호화 한 후에 돈을 요구하는 명백한 범죄 양상’ 이다.

o 랜섬웨어류 악성코드의 핵심적인 특징은 ‘컴퓨터 이용자(피해자)에게 가치 있을 만한 문서, 이미지와 같은 컴퓨터 내 주요 파일을 무단으로 암호화 한 후에 돈을 요구하는 명백한 범죄 양상’ 이다.

(마) 랜섬웨어 실시간 대응 보안 솔루션 기술개발 분야

o 반복적인 파일검색, 다량의 파일암호화 등 행위 진단 실시간 차단 자동수행

o 이메일의 첨부파일 또는 본문 내 URL 링크를 통해서 들어오거나 다양한 경로도 특정 URL을 직접 클릭하도록 유도하는 경우 의심스런 이메일 첨부파일의 실행을 차단하거나 의심 URL을 차단하는 기술개발

o 만약 적절한 차단이 이뤄지지 못 했다면 의도된 악성코드가 네트워크를 통해서 유입 시점에서는 ‘악성코드 전용 샌드박스’ 등을 이용해서 네트워크 레벨에서 최대한 신속하게 악성 여부를 판단해서 차단하는 기술

- 반복적인 파일 검색, 다량의 파일 암호화 등의 행위를 악성으로 진단하고 실시간 차단까지 자동 수행 기술개발

- 실제 랜섬웨어 관련 악성코드가 엔드포인트 시스템에 직접 감염되면서 일련의 운영체제 레벨의 의심 행위 감시

- 의심스런 URL을 실시간으로 차단기능, 랜섬웨어로 의심할 수 있



는 파일을 실행시키지 않은 상태에서, 가상의 분석 환경에서 상세한 분석

#### 16. 핀테크 보안기술 연구개발 분야(D 그룹1)

(가) 분야명 :금융정보 양자암호(Quantum Cryptography)통신기반 구축 기술개발

(나) 양자 컴퓨터 트래픽 암호화

양자암호(Quantum Cryptography)는 양자의 역학적 특성을 이용한 암호화기술이다. 비공개 채널로 키를 주고 받고 공개적인 채널로 암호문을 보내는 방법이다. 공격자가 키를 읽기 위해 펄스를 측정하는 순간 펄스가 변화되어 펄스리듬이 흔들리며 이는 데이터가 무용지물이 되는 결과가 된다(As the noise is increased, the distinction between the two logic levels become less clear). 수신자는 이러한 펄스변화를 통해 해커의 공격 징후를 파악할 수 있어 데이터를 폐기하고 새로운 키를 재송신 받아 도청 없는 통신이 가능하다. 양자 암호란 양자 컴퓨터를 이용한 알고리즘에 의한 공격에 내성이 있는 암호를 말하며 기존에 알려진 암호로는 Hash기반 암호, Code 기반 암호, Lattice 기반 암호, MQE(다변수 2차 다항식) 기반 암호 등이 제안되었다. 현재 IoT 환경에서 쓰이고 있는 인증 프로토콜들의 대부분은 앞으로 나올 양자컴퓨터를 이용한 공격에 대해서는 안전성이 보장되지 않았다. 따라서, 자원이 제한되는 IoT 환경의 특성에 맞게 인증 암호부분을 경량으로 개선하고, 양자 컴퓨터 공격에 내성을 가지는 프로토콜로 사용하여야 한다.

(다) 양자암호통신 기술

○ 양자암호통신 기술은 정보의 저장/전송/측정/제어 등 정보를 다루는 전체 또는 부분의 물리 영역에서 양자 역학에 기반 한 양자 정보를 활용하고, 양자 중첩/불확정성 원리/비복제성 원리/양자 얽힘 등 다양한 물리 현상을 이용함으로써 암호가 제공하는 다양한 기능들의 안전성을 극대화한다.

○ 각각의 응용 기술은 서로 독립적인 기술이라기보다는 다양한 요소기술을 공유하거나 상호 보완 활용되며, 양자의 이중성 불확정성, 중첩 및 얽힘현상 등 양자역학적 원리와 현상에 바탕을 두고 있는 다양한 요소기술을 개념적으로 분류하면 양자 상태의 생성, 유지(저장), 제어, 전송, 측정을 위한 기술 및 양자 알고리즘으로 나눈다

○ 양자암호통신 기술은 양자적 현상에 기반한 다양한 요소기술이 융합되어 개발되는 응용기술의 한 분야라고 할 수 있으며, 이러한 응용 기술에는 양자암호통신을 포함하여 양자중계기, 양자프로세서 및 양자컴퓨터, 양자기반 정밀계측, 양자기반 초고속통신 등이 있다.

#### (라) 양자암호통신 실용화 전망

○ 현재의 양자암호통신 기술은 이제 막 상용화가 시작되는 태동기며, 우선 국가 주요 기간망, 군사망, 금융망 등에 우선적으로 보급될 것으로 판단된다.

○ 보안을 적용할 수 있는 통신 채널의 물리적인 거리, access망 및 가입자망을 통한 네트워크 topology의 다양성, 비용 문제 등의 제한으로 인해 아직은 일반 사용자들이 양자암호통신 기술을 사용하기에는 많은 제한이 있는 것이 사실이다.

○ 각 분야의 요소 기술들이 발전하면 양자암호통신 장비의 소형화 및 대량 생산화가 가능해 질 것이며, 양자 스위칭 및 routing 기술이 발전되면 멀지 않은 미래에 양자암호통신 장비도 일반 가정에서 사용될 것으로 기대된다. 또 Home network를 관리하는 장비에 통합운영될 수 있다.

\* 세계 각국의 과학자들이 관련 연구에 몰두하고 있어 실용화 가능성도 점점 높아지고 있다. 우리나라도 한국과학기술연구원(KIST)에서 양자통신을 연구하고 있고, 지난 10월 20일 통신사 SK텔레콤에서 국내 최초로 양자통신 시제품 공개를 발표했다. 사회적 관심도가 높지 않고 연구의 출발도 늦었고 지금도 몇몇 연구자와 기관만 연구로 선진국과의 기술격차가 너무 크다.

(마) 연구 소재

- o 핀테크 보안 해킹시도를 원천 봉쇄할 양자암호통신 실용화 주요기술 소재 연구
- o 통신 채널의 물리적 거리, access망 및 가입자망을 통한 네트워크 topology의 다양성, 비용 문제 등 양자암호통신 기술 사용제한 사항 조사
- o 핀테크 무선통신망에 적용할 가능성 분야에 대한 연구.
- o 핀테크 무선통신 보안영역 센싱 트래픽도메인, 근거리 통신, 원거리 통신 금융정보 양자암호 방안 연구
- o 암호통신 장비 소형화, 스위칭 및 routing 기술 발전 시 양자암호통신 활용방안

17. 핀테크 보안기술 연구개발 분야(D 그룹1)

(가) 분야 명 : 사물인터넷 환경의 핀테크 네트워크보안 프레임워크 기술개발

(나) 분야 선정 사유

사물인터넷 환경에서는 보호해야 할 기기의 수가 우리 일상생활의 모

든 사물로 확대되고, 그 특성도 다양화(경량저전력, 초연결성 등)되면서 기존 보안기술 적용에 한계가 있다. 연산 능력과 전원 등과 같은 자원이 제한되어 있는 IoT 환경에서 현재 다른 분야에서 쓰이고 있는 AES, SHA-3 등의 보안 솔루션을 그대로 적용하기에는 각 디바이스에 부담이 된다. 이러한 환경적 특성으로 인해 최근 IoT에 적합한 경량 암호화 관련연구가 많이 진행되고 있다. 알려진 경량 암호 중 경량이며, 안정성 또한 높은 인증 암호의 사용이 필요하다. IoT 환경에서의 보안을 위한 필요사항으로는 데이터 기밀성, 데이터 무결성, 디바이스 무결성, 시스템 가용성, 사물과 사물 간의 디바이스 인증 및 서버 인증, 접근제어 및 인가, 네트워크 오용 방지, 프라이버시 보호, 추적성 방지, 부인 방지 등이 있다. 이 중에서 사물과 사물간 디바이스 인증 및 서버 인증, 접근제어 및 인가, 부인 방지 등을 위해서는 반드시 인증 암호와 인증 프로토콜이 필요하므로, IoT에서 인증 암호와 인증 프로토콜의 역할은 매우 중요하다.

#### (다) 사물인터넷 보안 조건

○ 빠른 알고리즘 : 작은 하드웨어 칩과 빠른 알고리즘 속도는 경량암호의 필요조건 중 하나이다. 이를 달성하기 위해 복호화를 할 때 암호화의 역을 취하지 않아도 되는 inverse-free한 구조를 가진다면 복호화에 대비한 하드웨어를 고려하지 않아도 되므로 칩의 크기가 줄어든다.

○ 경량 보안기술 : 디바이스 수가 많아지고, 보안패치 적용 곤란, 통신 내용 모니터링 곤란에 따른 보안 취약성이 증가 할 것이다. 저사양 기기를 포함해 다양한 기기 특성을 반영한 경량 보안기술(백신, 암호화, 인증 등)개발 및 적용이 필요하다.

○ 보안패치 :기기 운영 신뢰성 보장, 무결성 검증 등을 위해 센서/디바이스 보안패치 적용 기술 개발, 센서/디바이스 모니터링 체계가 필요하다.

o 개방형 플랫폼 : 공개 플랫폼을 통한 기기-서비스 간 허위 데이터 전송/오작동 등 공격이 예상되며 IoT 디바이스가 수집한 단편 정보의 중앙 집중 및 조합으로 사용자 신원정보 유출이 될 것이다. 이를 해결하기 위해 안전한 개방형 플랫폼 이용지침 마련, 디바이스/사용자 서비스 간 상호 인증 및 키관리, 신뢰관리 필요, 기기의 개인 정보수집/추적 방지 및 개인 식별 정보 필터링 기술이 필요하다.

o 프로토콜 : IoT 환경에서 디바이스 사이의 프로토콜로 고려되고 있는 DTLS(Datagram Transport Layer Security)와 HIP(Host Identity Protocol)가 있다. 보안 측면이나 성능적인 면에서 검토가 필요하다.

#### (라) 연구사항

o 사물인터넷 환경에서 보호해야 할 기기의 수가 우리 일상생활의 모든 사물로 확대되고, 그 특성도 다양화(경량·저전력, 초연결성 등)되면서 기존 보안기술 적용에 한계가 있다. 연산 능력과 전원 등과 같은 자원이 제한되어 있는 IoT 환경에서 현재 다른 분야에서 쓰이고 있는 AES, SHA-3 등의 보안 솔루션을 그대로 적용하기에는 각 디바이스에 부담이 된다. 경량 암호 중 경량이며, 안정성 또한 높은 인증 암호 연구가 필요하다.

o IoT 환경에서의 보안을 위한 필요사항으로는 데이터 기밀성, 데이터 무결성, 디바이스 무결성, 시스템 가용성, 사물과 사물 간의 디바이스 인증 및 서버 인증, 접근제어 및 인가, 네트워크 오용 방지, 프라이버시 보호, 추적성 방지, 부인 방지 등이 있다. 이 중에서 사물과 사물간의 디바이스 인증 및 서버 인증, 접근제어 및 인가, 부인 방지 등을 위해서는 반드시 인증 암호와 인증 프로토콜이 필요하다.

o Zigbee, Wi-fi, Bluetooth 등 이동 무선 네트워크 간 상호연동이 되면서, 일정한 보안수준을 유지하기 어렵고, 디바이스 간 통신이 지원되면서, 디바이스인증이 제한적으로 지원이 될 것이다. 클라우드 가상화 서

비스를 통한 좀비 PC 대량생산, 냉장고, 청소 로봇, 의료기기 등 대규모 디바이스에 악성코드를 감염시켜 트래픽 폭증 공격이 가능해질 것이다. 이를 해결하기 위해 이중망 연동을 위한 프로토콜 상호 운용성 기준 마련, 이 기종 저 사양 연결 통신 네트워크 환경에 적합한 보안기술이 필요하다,

o 대규모 기기·네트워크에 대한 보안 상태 모니터링 및 감시가 필요하다. 하드웨어 칩과 빠른 알고리즘, 경량 보안기술, 보안패치, 개방형 플랫폼, 프로토콜이 프레임워크로 연구되어야 한다.

## 18. FDS 알고리즘과 기술개발 분야(D 그룹2)

### (가) 분야 명 : FDS 구축이후 업그레이드 기술개발

#### (나) 금융권의 이상금융거래탐지시스템 도입 현황

금융권을 중심으로 이상금융거래탐지시스템 도입이 잇따르고 있는데, 특히 카드사에 비해 이상금융거래탐지시스템 구축 경험이 적은 증권사들은 잇따라 이상금융거래탐지시스템 도입을 추진하고 있다.

#### (다) FDS 시스템 운용현장에서 발견되는 불편사항

o 사기 기술 진화 수준을 따라가지 못하는 FDS 업그레이드 알려지지 않은 새롭게 등장하는 패턴의 증가(Previously unknown, newly emerging, schemes)로 인해 사기탐지 기능은 항상 시험대에 오르는 결과를 초래한다. 최적화 작업은 지속적으로 이뤄져야할 부분이지만, 사기 거래를 정교하게 잡아내 오탐율을 최소화하는데 가장 중요한 부분이다. 이런 오탐율을 최소화하는 근거는 얼마나 많은 패턴과 경험을 보유했느냐에 따라 달라진다.

- FDS 시스템의 사기탐지 분석기능의 한계

데이터의 분리처리와 분석으로 인한 분석기능 취약성(Fragmented data)을 들 수 있다. FDS의 핵심은 탐지율을 높이는 것이다. 그러기 위해서는 FDS 조직을 통해 분석 역량을 강화하고, 끊임없이 고도화하는 작업이 필요하다. 제품이 개발되어 시스템 Open 즉시 FDS의 정상운영이 가능해야 함실 제적 성과를 바로 낼 수 있는 있는 FDS Package SW 필요하다.

#### (4) FDS 도고화 이후 FDS 업그레이드 연구 소재

##### (1) 운영현장의 불편해소

- FDS 시스템은 실시간 분석이 불가능하다.
- FDS 시스템은 기초적 데이터마이닝, 통계분석만 가능하다.
- FDS 운용 Knowhow 부족으로 분석 어렵다.
- FDS는 बैं킹과는 분리된 시스템이다.
- FDS 단계별 조치 및 안내가이드가 없다.
- FDS 시스템은 실시간 정보수집이 불가능하다.
- FDS 시스템은 운용환경 별로 추가기능 개발 필요하다.
- FDS 시스템의 분석결과 구체적 이상금융거래탐지인자 모른다.
- FDS 시스템 RULE SET이 초기 수준이다(경험 미흡).

##### (2) FDS 도고화 이후 FDS 업그레이드 기술개발

###### ○ MITM 공격

중간자 공격(Man In The Middle, MITM)을 의미하는데, 쉽게 예를 들어 FDS 구성요소인 사용자 단말단 수집정보를 메모리 단계에서 복제해 다른 기기나 조건에서 재사용할 수 있다. 정상적인 A란 기기의 메모리상에서 암호화된 전문을 훔쳐내 이를 비정상인 B기기에서 악용하기 위해 바

꺾치기 할 가능성이 있다

o 피해자가 가해자로 바뀔

FDS의 탐지 패턴을 우회 할 수 있음은 물론 피해자가 가해자로 바뀌어 분쟁이 발생할 소지도 크다며 보안조치가 필요하다.

o 임계치 탐지

FDS 보안체계 우회를 위해 각종 단말 수집 정보를 제거하거나 조작하는 것은 물론 거래 패턴 탐지 우회를 위한 임계치를 탐지하고 예외처리에 대한 악용을 시도할 것으로 예상된다.

o RAT

RAT은 원격 접속 툴(Remote Access Tool)에 의한 승인받지 않은 불법적인 원격조종 기법이다. 이에 대비하기 위해서는 관련한 전용 보안모듈 적용과 화이트 리스트 정책 기반의 통제 방안이 강화되어야 한다

## 19. FDS 알고리즘과 기술개발 분야(D 그룹2)

(가) 분야 명 : 사기방지 빅데이터 분석 Science Map 설계 기술개발

(나) 분야 선정 사유

스마트폰의 보급과 R등 오픈소스 분석 도구의 보급으로 모든 개인이 데이터 분석가의 역할을 하는 것이 가능해졌다. 이중 주목할 만한 움직임은 개인의 삶에서 수집된 데이터를 가공 / 분석해 개인의 삶을 분석/개선하는데 활용하는 Self-Tracking이라는 기술 및 관련 커뮤니티의 발달이다. 이런 개인적 데이터의 분석에는 빅데이터도, 최신 기계학습 기술도 들어가지 않지만, 각 개인이 자신의 문제를 해결하기 위해 찾아내는 해결책이다. 데이터 사이언스는 복잡한 것이 아니라 일상의 문제에 대한 과학적 해결책을 찾으려는 노력에서 필요하다. 개인은 변화하는 시대에 살아남을 수 있는 경쟁력을 확보하게 되며 사기방지 빅데이터\* 분



석 Science Map이 필요한 이유이다.

#### (다) Science Map 기능

Science Map은 데이터 사이언스 분야의 관심 기술을 한눈에 조망한다. 인터랙티브 맵으로 만들어져 있어서 마우스를 올리면 간단한 소개와 공식 사이트로 링크된다.

메모리 가격이 낮아지면서 인메모리 데이터베이스와 관련된 새로운 제품들이 많이 등장했다. 스파크(Spark) 보다 스트리밍 데이터 처리에 보다 좋은 성능을 발휘한다. 빅데이터\* 분석 Science Map은 소셜 미디어와 같은 다양한 데이터 소스에서 나온 데이터를 통해 정보에 대한 이해력을 높일 수 있도록 도와주고, 놓치거나 이용하지 않은 채로 놔두기 쉬운 트렌드 및 변화의 패턴을 정확히 짚어주는 역할을 한다. Science Map을 사기탐지에 활용하기 위해 사기방지 빅데이터\* 분석 Science Map 설계가 필요하다.

#### (라) 데이터 사이언스 활용분야

o 빅데이터' 대용량 데이터 처리에 대한 관심 확대와 함께 널리 사용된다.

- 2000년대 초반, 구글과 야후를 비롯한 온라인 서비스 회사에서 개발한 하둡(Hadoop)과 같은 데이터 처리 기술이 다른 분야에까지 널리 퍼지면서 나타난 현상이다.

o 구글/야후에서 처음 개발된 하둡(Hadoop)과 같은 대용량 처리기술은 클라우데라 / MapR과 같은 솔루션 업체가 주도한다.

o 야후의 내부 프로젝트로 시작된 하둡(Hadoop)이나, 페이스북이 개발·공개한 아파치 카산드라(Apache Cassandra) 등 유명한 오픈소스 프

로젝트 중에는 기업체 프로젝트에서 시작한다.

- 기타 트위터, 링크드인을 비롯한 많은 회사들도 오픈소스 활동에 동참하고 있다.

- 스마트폰 대중화로 인해 언제 어디서나 데이터를 접하고 생산한다. 대용량 데이터를 수집·가공·분석해 가치있는 결과를 끌어내는 데에는 인프라, 분석, 시각화에 이르기까지 다양한 기술이 필요하다.

(마) 핀테크에서의 사기방지 빅데이터\* 분석 Science Map 연구사항

빅데이터 기술을 보안영역에 적용하기 빅데이터 수집기술을 통한 데이터의 수집과 실시간 모니터링, 비정상 행위들을 미리 설정하여 이상 징후를 확인한다. 탐지분석, 빅데이터의 분석기법을 이용한 데이터 및 네트워크 분석 등이 이용된다. 이를 위해 splunk나 flume 등의 수집 플랫폼을 활용하며 금융회사의 보안 모니터링과 모니터링한 데이터 통합보안 관제 제품과의 통합을 통해 높은 수준의 지능적인 모니터링과 연관 분석이 가능하다.

- 분석된 데이터의 의미와 가치를 시각적으로 표현하기 위한 시각화
- 분석결과와 기존 데이터 저장소의 정형 데이터와의 통합
- 애드혹 리포팅, 경고, 운영 프로세스와의 연계

## 20. FDS 알고리즘과 기술개발 분야(D 그룹2)

(가) 분야 명 : Big Data 검색엔진 기반 이상금융거래 탐지 기술개발

(나) 분야 선정 사유

과거 사이버 위협 방어 기술의 핵심기술은 알려진 공격에 대한 공격 시그니처 데이터베이스를 확보하고 고성능 패턴매칭 알고리즘을 구현하여 얼마나 빨리 비교할 수 있느냐에 달려 있었다. 이제는 복합데이터 처리기술의 발달로 내부 망에서 발생하는 다중소스의 누적 데이터에 대한 특성인자를 정의하고 연관성 분석할 수 있는 보안기술로서 빅데이터를 활용한 보안 분석 기술이 부각되고 있다. 가트너 그룹은 빅데이터 분석을 활용한 보안 분석을 통하여 예전에 보이지 않았던 사고패턴을 발견하고 정보 보안을 포함한 기업경영에 대한 선명한 통찰력을 제공함으로써 기업의 비즈니스 가치를 높일 수 있다고 예측하고 있다. 빅데이터를 활용한 보안 분석(big data securityanalytics)은 데이터 분석 기술의 고도화 측면에서 기존에 해결하지 못한 공격위협 분석을 가능하게 할 것으로 예측되고 있다.

#### (다) 사기탐지 방식 진화 방향

전통적 방식과 진화방향을 비교하여 보면 데이터측면에서는 데이터베이스에서 지식베이스로 다시 빅데이터로 진화하고 있다. 분석방법은 전통적 방식이 형태분석, 형상 분석, 외형분석, 행위위주의 분석이라면 진화방향은 행태, 행동, 내면적 움직임 분석, 심리학, 감정까지 분석대상이다. 패턴인식은 패턴매칭에서 휴리스틱 방식이 필요하며 알고리즘은 단위 알고리즘, 사용목적 별 알고리즘에서 통합화 알고리즘, 통합화 분석으로 진화된다. 탐지방식 측면에서는 static 고정식에서 dynamic 유연성 방식으로 변화되고 있다. 사용자의 룰세팅 방식은 완성된 제품의 옵션만을 선택하는 방식에서 지속적 커스터마이징을 전제로 하며 룰세팅 자체를 사용자가 수행한다.

#### (라) 사기방지 빅데이터 적용단계

#### o 저장 - 로딩 및 준비

데이터를 분석하려면 먼저 데이터를 입수해야 한다. 따라서 데이터를 저장할 공간이 필요하며 종종 구문 분석이나 여타 형태의 보강을 통해 최초 사용을 위한 준비를 해야 한다. 이를 흔히 ETL(Extract(추출), Load(로딩), Transform(변환) 또는 ELT(Extract, Load, Transform)라 한다. 여기서 흔히 배치 성능이 중요하며, 확장에는 비용이 수반되기 때문이다. 특히 데이터가 문서와 유사한 형식(예: JSON)일 경우 로딩 작업은 사용자 쿼리에 비해 느린 속도로 변하는 경향이 있기 때문에 사용 편의성은 다소 덜 중요하다.

#### o 탐색

이 단계는 분석 모델이 어떨지를 규명하기 위해 데이터 관련 질문을 하는 분석가의 엄청난 상호작용을 요한다. 데이터 과학 용어에서는 이를 흔히 “탐색적 데이터 분석”이라고 한다. 이는 흔히 분석의 가장 복잡한 단계로서 데이터가 아직 잘 파악되어 있지 않으며 조회에 적합한 형태가 아닐 수 있다. 이는 Hadoop에서 점점 더 보편적으로 쓰이고 있는 “데이터 레이크(Data Lake)”와 더불어 이 초기 단계 조회 시간을 단축할 수 있는 도구의 필요성을 촉진한다.

#### o 적용

이 단계에서는 일반적으로 통찰력 있는 정보를 찾아내어 운영하기 위한 모델을 구축한다. 일례로, 분석가는 온라인 게임 사용자들이 진행이 막히게 되는 지점에서 게임을 포기하는 경우가 흔하며 그 지점을 지난 사용자들은 훨씬 더 높은 평생 가치를 가진다는 점을 발견할 수 있을 것이다.

#### o 실행

이 단계에서는 원하는 결과가 가시화되어야 한다. 따라서 조직은 최소한 분석이 바람직한 효과를 거둘 수 있도록 유입 데이터의 흐름을 관찰해야 한다. 아울러 이 과정에서 조직은 분석 통찰력을 증진하기 위해 더

많은 정보가 필요하다는 것을 종종 깨닫게 된다.

(마) 연구 소재

이같은 환경에서 품질관리 방법론은 전통적인 QoS에서 MoS까지 고려하는 목표 관리가 요구된다. Big Data 검색엔진 기반 이상금융거래 탐지 방안은 기능 요구분석은 사용자요구사항이 전제되고 있다.

- 통계 및 분석가를 위한 데이터마이닝
- 프로그래밍을 활용한 데이터마이닝
- 맵리듀스 활용 이상금융거래 탐지

21. FDS 알고리즘과 기술개발 분야(D 그룹2)

(가) 분야 명 : 사기탐지 인공지능 (AI) 질의응답 전문가시스템 기술개발

(나) 분야 선정 사유

사기탐지 업무에는 순간적으로 이상상황에 대한 판단을 통해 차단여부를 결정하는 긴박성 소재가 대부분이어서 이때 자동화된 프로그램에 의해 대처하고 있다. 그러나 모든 경우에 자동화 프로그램으로 해결되는 것은 아니며 운용자의 판단에 의해 관리되어야 할 상황이 발생할 때 전문가의 도움이 필요하다. 이 경우에 필요한 시스템이 사기탐지 전문가시스템이다.

\* 왓슨(Watson) : 자연어 형식으로 된 질문들에 답할 수 있는 인공지능 컴퓨터 시스템, 시험 책임자 데이비드 페루치가 주도한 IBM의 DeepQA 프로젝트를 통해 개발. 왓슨은 IBM 최초의 회장 토머스 J. 왓슨에서 이름을 따다. 2011년 기능 시험으로서 왓슨은 퀴즈 쇼 제퍼디에 참가하였

으며, 이는 유일한 인간 대 컴퓨터 대결이다.

#### (다) 전문가시스템 구성

##### (1) 구성 요소

전통적인 데이터 분석만으로는 사기탐지 기능을 완전히 해결하기 어렵다. 금융분야의 경우 데이터 분석에 기반하지만 Data Driven만으로 할 수 있는 분야는 매우 제한적이며 전문가 Heuristics을 모델화 할 수 있는 지식공학 능력이 필수이다. 지능형 금융정보시스템의 핵심 성공 요인은 지식베이스(Knowledge-base)를 어떻게 잘 만드느냐, 어떻게 잘 관리하는가에 있다. 전문가시스템(Expert systems)은 일반적으로 다음과 같은 요소로 구성된다.

- o 지식베이스획득 인터페이스(Knowledge-Acquisition Interface)
- o 사용자 인터페이스(User Interface)
- o 지식베이스(Knowledge Base)
- o 인터페이스엔진(Inference Engine)

##### (2) 지식베이스(knowledge base)

전문가시스템의 구성 요소의 하나로서, 인공지능 에이전트가 사용될 분야와 관련된 지적 활동과 경험을 통해서 축적한 전문지식 그리고 문제 해결에 필요한 사실과 규칙 등이 저장되어 있는 데이터베이스이다. 전문지식의 표현 방법으로 IF-THEN 형식의 생성규칙이 사용되며, 사실의 표현을 위해서는 프레임 표현이 사용된다.

##### (3) 지식 획득(knowledge acquisition)

지식의 추가와 변경 작업에 대한 방식이 인공지능 에이전트의 사용분야에 따라 다르며, 에이전트의 사용자들의 기준에 따라 달라지기 때문에 이러한 작업은 상황에 맞게 개별적으로 작성되어야 한다. 인공지능 대상의 관련 지식을 지식베이스에 반영하는 작업을 지식 획득(knowledge acquisition)이라고 한다.

#### (4) 추론기관

주어진 문제의 해결을 위해 지식베이스에 있는 규칙들을 탐색, 추론(inference)과 통제(control)를 하는 전문가시스템에서 가장 중요한 부분. 새로운 지식을 추론하기 위해 규칙들을 어떻게 적용할 것인가를 결정하는 규칙해석기(interpreter), 규칙들의 적용순서를 결정하는 스케줄러(scheduler)로 구성된다.

#### (5) 지능형 에이전트

지능형 에이전트 시스템은 환경을 인식하고 성공을 가장 극대화 할 수 있는 행동을 취한다. 이러한 정의에 의하면 인간과 인간들의 조직처럼, 예를 들어 회사처럼 특정 문제를 해결하는 간단한 프로그램들을 지능형 에이전트라고 한다.

#### (라) 연구사항

##### o 시스템 개발 목표 설정

- 문제정의 : 주어진 문제의 유형과 범위, 개발작업에 참여할 인력, 전문가, 소요될 시간, 컴퓨터 시설 등을 함께 고려한다.
- 개념설정 : 정의된 문제를 해결하기 위해 필요한 개념을 정립하고

각 개념 사이의 관계와 제어기능을 정의한다.

- 정형화 : 중요한 개념과 지식을 정형화하여 표현하다.

- 구현 : 표현된 지식을 프로그래밍하는 단계로서 자료구조, 추론과정, 프로그램 제어, 하부 시스템들의 통합 등을 고려한다.

- 검증 : 개발된 시스템이 처음 정의한 요구사항대로 만들어졌는가 평가 과정.

o 시스템 개발 도구

- 사기탐지 인공지능 (AI) 질의응답 전문가시스템 기능요구 사항

- 프로그래밍언어

- 지식공학언어(knowledge engineering language)

- 질의응답 전문가시스템 개발도구(developing tool)

- 시스템 구축 보조(system building aids) :



## 제 6 장 결 론

새로운 패러다임 기술을 맞이하는 대한민국의 과제로서 비트코인을 가  
능케 한 클라우드 블록체인이라는 분산장부 기술은 핀테크 열풍 속에서  
금융의 미래를 바꿀 것이다. 핀테크가 간편하고 편리한 서비스를 안정적  
으로 제공하기 위해서는 고도의 보안 유지가 필요하다.

국내에서도 핀테크에 대한 관심이 높긴 하지만 아직 초기 단계인 국내  
핀테크 기업이 성공적으로 자리매김하기 위해서는 해외 투자를 유치해  
글로벌 사업에서 성과를 거두는 것이 필요하다. 이를 위해 미국과 유럽  
처럼 정부, 지자체 등이 기존 대형 금융기관들과 함께 핀테크 기업 육성  
을 위해 부트캠프 등을 운영하면서 법규제 완화, 필요 기술 공동개발,  
서비스 제휴 등을 추진하는 것이 필요하다. 또 핀테크를 비롯한 차세대  
금융서비스의 합리적인 발전을 위해 과감한 규제 완화 등도 적극 검토해  
야 한다. 유럽처럼 기존 금융기관과 핀테크 스타트업을 위한 금융서비스  
라이선스에 차등을 두는 식의 새로운 규제를 만드는 것도 필요해 보인  
다. 대한민국 정부의 **핀테크 산업 육성 지원책**이 계획에 따라 핀테크 지원  
체계의 운영을 내실화하고 관련 규제개선 및 자금조달 지원의 활성화가  
기대된다.

본 연구에서 핀테크 육성 정책적으로 건의드리는 과제는 클라우드 펀딩 제  
도와 인터넷 전문은행 정책 등의 활성화에 더해 해외시장에서 국제경쟁력을  
갖추기 위한 과제로 ▲ 금융업-ICT업계 연계를 위한 핀테크 클러스터 확대  
▲ 국가 간 지급거래 정보 호환성 제고 ▲ 핀테크 관련 보안 가이드라인 수  
립 ▲ 진입장벽 완화 등을 제시한다. 그리고, 국가 간 지급거래가 활성화를  
위해 지급 거래 정보 호환성 강화를 위한 '지급결제 관련 국제 표준(ISO  
20022)'의 단계적 도입 필요성이 있다. 아울러 금융서비스에 대한 실질적 보안  
역량을 강화할 수 있는 '보안 가이드라인'을 수립해 국내 핀테크 산업의 정보  
보안 능력 키우는 방법도 향후 과제로 제시한다.

또한 핀테크 산업 육성과 관련해 현재 신용정보 주체를 식별할 수 없는 경우 개인신용정보에서 제외해 비식별 빅데이터를 금융회사 등이 이용할 수 있게 하는 '신용정보법', 온라인 소액투자 중개업자의 투자광고 매체 제한을 완화해 크라우드 펀딩을 활성화시키는 '자본시장법' 개정안 등이 발의되어야 한다. 그리고, 핀테크 금융권 특허등록이 필요하다. 그리고 글로벌 핀테크 기업들에게 국내시장을 한 순간에 장악당하지 않기 위해서라도 해외와 같이 ICT기업의 적극적인 금융산업 진출을 도모하기 위한 방안을 마련되어야 한다.

핀테크는 금융서비스를 기본으로 하는 IT서비스이다. 따라서 금융서비스에서 정의하고 있는 정보기술 요소들을 그대로 유지하면서 추가되는 서비스에 대한 아키텍처를 반영하고 새롭게 수립된 시스템에 맞춘 보안 사항을 추가하면서 시스템 품질을 확보할 수 있다. 핀테크는 일종의 서비스 개념이지 기술은 아니다. 정보기술의 발달로 인한 새로운 금융서비스라고 할 수 있기 때문에 구축하려는 시스템의 범위를 기존 금융서비스와 최대한 연계하여 효율화 하여야 한다. 그리고 이의 지속적인 보안 모니터링이 필요하다.

마지막으로, 디지털 혁신의 시대에 패러다임의 변화에 의한 새로운 시장기회를 주도적으로 발견하고 혁신적인 비즈니스 모델을 창출하는 것이 필요하다. 금융업계는 이러한 현실의 직시와 적극적인 자세로 산업융합의 추세를 비즈니스 모델의 혁신기회로 삼아야 한다. 따라서 ICT를 제대로 이해하고 금융산업과 융합을 통한 혁신적인 비즈니스를 추진할 수 있는 전문가의 영입 및 양성이 필요하다.

## 참고문헌

- [1] 금융위원회, 계좌 개설시 실명확인 방식 합리화 방안, 2015.5
- [2] 테크M, 중요성 커지는 핀테크 보안기술, 2015.9
- [3] KB금융지주 경영연구소, 금융산업에서 생체인식 기술의 활용현황과 전망. 2014.6.
- [4] 플래툰, [맥스서밋 2015] 핀테크가 만들 새로운 금융 패러다임은, 2015.10.5.
- [5] KB금융지주경영연구소, KB 지식비타민: 해외 인터넷 전문은행 동향 및 국내 이슈 점검, 2014. 9. 24, (14-73).
- [6] KB금융지주경영연구소, 국내외 핀테크(FinTech) 동향과 전망, KB 지식비타민(14-60), 2014. 8. 4.
- [7] KB금융지주경영연구소, P2P대출, 대안적 서민금융으로서의 가능성 점검, KB 지식비타민(14-9), 2014. 2. 4.
- [8] KDB산업은행, ICT업계의 금융업진출에 따른 시장영향분석, 산업이슈, 2014.7.
- [9] 강민형, 산업융합시대, 금융업의 새로운 기회, 우리금융경영연구소,
- [10] <핀테크 국내외 산업 동향과 전망>, 한국과학기술기획평가원, 2015년 06월
- [11] <구글·애플·아마존·페이팔, 핀테크 연합 ‘FIN’ 설립>, IT뉴스, 2015년 11월
- [12] <美·日·EU 22개 은행 핀테크 연합 결성... 한발 늦은 한국 핀테크>, 아주경제, 2015년 10월
- [13] <소프트어공학센타 웹진 138호~142호: 인사이드 이슈> 개발자를 위한 Fintech Payment Architecture
- [14] 금융위, 금융규제개혁 기본방향 및 진입규제 개선방안, 2008. 6. 26.

- [15]김정균, 정보통신기술(ICT)과 은행의 미래, 우리금융경영연구소,
- [16]김종현, 국내모바일 전자지갑 시장동향과 전망, 우리금융경영연구소,
- [17]김종현, 카카오의 금융업 진출의 영향 및 시사점, 우리금융경영연구소,
- [18]머니투데이, [급부상하는 핀테크의 세계 ③] 핀테크 스타트업, 금융서비스 재창조한다, 2014. 9. 28.
- [19]머니투데이, [급부상하는 핀테크의 세계 ①] IT, 금융으로 진격하다, 2014. [20] 9. 28.머니투데이, [급부상하는 핀테크의 세계/국내 사례 ⑥]
- [21]비바리퍼블리카 ‘토스’ ... ‘진짜’ 간편한 계좌이체 서비스로 승부한다, 2014. 10. 5.
- [22]아이티 투데이, 소액이체 앱, 모바일뱅킹 앱 넘어설까, 2014. 11. 30.
- [23]우리금융경영연구소, 글로벌 금융테크(FinTech)기업 현황 및 은행에 대한 시사점, 경제연구실, ISSUE & INSIGHT 2014-10호, 2013. 7. 18.
- [24]전상욱, 은행업 패러다임의 변화와 대응 방향, 우리금융경영연구소,
- [25]전자신문, IT강국 대한민국, 핀테크 요람을 만들자, 이슈분석, 2014.10.6.
- [26]천대중, 해외 인터넷 전문은행 동향 및 시사점, 우리금융경영연구소,
- [27]주간금융경제동향 이슈브리프, 제4권 제30호, 2014. 7. 30.
- [28]한경닷컴, 의사·대기업 때려치우고 모바일 결제시장 도전장 “실패하면 또 창업하죠, 2014. 10. 14.
- [29] 경찰청 보도자료, “ ‘파밍(Pharming)’ 등 신종금융사기주의!” , 2013.6.참조
- [30] 박대우 호서대학교 벤처전문대학원 교수/prof1@hoseo.edu
- [31] 금융보안원 핀테크 서비스와 보안기술 구조
- [32] 한국정보통신기술협회 IC Tagging과 생체 인증
- [33] 라온시큐어 라온시큐어 ‘터치엔 원패스’ 구성도
- [34] 한국전자인증 [https://www.crosscert.com/solution/03\\_2\\_06.jsp](https://www.crosscert.com/solution/03_2_06.jsp)
- [35] [네이버 지식백과] USIM카드 [Universal Subscriber Identity Module]

Card]

- [36] (한경 경제용어사전, 한국경제신문/한경닷컴 ) USIM카드
- [38] 보안뉴스 김경애 기자 2채널 분할 입력, boan3@boannews.com
- [39] 이민형 기자 kiku@ddaily.co.kr 사물인터넷 ‘게이트웨이’ 보안
- [40] 이상진 고려대학교 사이버국방학과 교수 · 디지털포렌식연구센터장/
- [41] 금융보안원, 이상금융거래탐지시스템 기술 가이드, 2014. 8
- [42] 국내 금융권의 이상금융거래탐지시스템 도입 현황 및 한국우정의 대응
- [43] [DBGuide.net] 연재 글 - 데이터 수집 #1 오픈 소스 수집기 비교
- [44] 2015 데이터산업 백서.
- [45] 지급결제와 정보기술 제60호 (2015. 4),
- [46] 부정위험 탐지를 위한 데이터마이닝 적용방안 연구, 감사연구원
- [47] 전자통신동향분석 제27권 제5호 2012년 10월
- [48] 정보통신단체표준(국문표준) TTA.KO-12.0178
- [49] CIOCISO 방창완 편집국장
- [50] 지급결제와 정보기술 제60호 (2015. 4)
- [51] 모바일시대를넘어AI시대로 정보화진흥원 제7호 (2010. 8. 25)
- [52] 한국휴렛팩커드 Technical white paper ! A Heterogeneous Approach to Big Data Analytics, 빅데이터 분석에 대한 이중 접근방식
- [53] 김자봉, 최근전자금융의 발전과 주요이슈, 2006
- [54] KISA 2010.침해사고대응팀 CERT 구축운영안내서, CERT의 정의 및 목적,2010.
- [55] 이상탐지를 위한 Hybrid Product of Experts 모델과 학습 알고리즘, 서울대학교 김일권, 장병탁
- [56] 나종희+,이태훈+, 클라우드 컴퓨팅의 보안위협과 통제모델에 대한 고찰
- [57] Internet & Security Focus 2013 4월호 28 FOCUS
- [58] 통신 채널상의 보안성을 극대화하는 기술, 양자암호통신기술의 현재

와 미래, 방송통신기술 이슈&전망 2014년 제 34호

[59] 핀테크의 현황과 과제 - 해외사례와 국내에서의 시사점을 중심으로  
-서강대학교 경영학부 교수 정유신, 2015. 1. 21

[60] 지급결제와 정보기술 제60호 (2015. 4)

[61] 금융보안원, 전자금융과 금융보안 창간호, 2015, 07

[62] KB금융지주경영연구소, 국내외 금융권의 정보보안 최근 동향과 전망 2015. 3. 11 (15-19호)

[63] 안랩, '가짜백신, 어떻게 설치되고 얼마나 유해할까?'

[http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu\\_dist=3&seq=16067](http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=3&seq=16067)

[64] 한국IDG, '랜섬웨어로부터 PC 지키기'(2014/01/21)

- US-CERT, Crypto Ransomware

<https://www.us-cert.gov/ncas/alerts/TA14-295A>

[65] KISA, 한글버전 랜섬웨어 '크립토락커' 확산 주의 당부

[http://www.kisa.or.kr/notice/press\\_View.jsp?mode=view&p\\_No=8&b\\_No=8&d\\_No=1364](http://www.kisa.or.kr/notice/press_View.jsp?mode=view&p_No=8&b_No=8&d_No=1364)

[66] International Journal of Software Engineering and Its Applications  
Vol. 6, No. 4, October, 2012

[67] International Journal of Security, Privacy and Trust Management  
(IJSPTM), Vol. 1, No 5, October 2012

[68] Data Industry White Paper Wenke Lee and Salvatore J. Stolfo  
Computer Science Department Columbia University 500 West 120th  
Street, New York, NY 10027 {wenke,sal}@cs.columbia.edu

[69] Christos Faloutsos Carnegie Mellon University, christos@cs.cmu.edu  
March 2015 Ab

[70] Cognizant Fraud Control - IT Interventions and Solutions 2011,

[71] Nicholas Carlson. <http://www.businessinsider.com/these-startups-are-replacing-banks-2014-2>. 2014

- [72] Julian Skan, Richard Lumb, Samad Masood and Sean K. Conway, “The Boom in Global Fintech Investment,” Accenture, 2014.
- [73] CB Insights, <https://www.cbinsights.com/blog/fin-tech-periodic-table/> 2014
- [74] <http://www.softwareplatform.net56>
- [75] <http://techpageone.dell.com> : Big data use case summary
- [76] <https://www.bodnara.co.kr>
- [77] [https://www.crosscert.com/solution/03\\_7\\_01.jsp](https://www.crosscert.com/solution/03_7_01.jsp)
- [78] [https://www.crosscert.com/solution/03\\_2\\_06.jsp](https://www.crosscert.com/solution/03_2_06.jsp)
- [79] <http://www.dbguide.net/db.db?>
- [80] <http://youtu.be/rKctE8UiXLU>
- [81] <http://www.bispro.co.kr/fds>
- [82] [http://www.splunk.com/content/splunkcom/ko\\_kr/resources/machine-data.html](http://www.splunk.com/content/splunkcom/ko_kr/resources/machine-data.html)
- [83] [http://hochul.net/blog/datacollector\\_sqoop\\_flume\\_scribe\\_chukwa/](http://hochul.net/blog/datacollector_sqoop_flume_scribe_chukwa/),  
<http://techpageone.dell.com> : Big data use case summary
- [84] <http://m.technbeyond.co.kr/>
- [85] <http://blog.saltlux.com/bigdata-analysis-overview/198>
- [86] <http://ieeexplore.ieee.org/xpl/login.jsp?>
- [87] <http://www.entrust.com>
- [88] <http://techpageone.dell.com> : Big data use case summary
- [89] <http://www.softwareplatform.net> 지급결제와 정보기술 제60호 (2015. 4)
- [90] [http://www.cs.cmu.edu/~abeutel/kdd2015\\_tutorial/tutorial.pdf](http://www.cs.cmu.edu/~abeutel/kdd2015_tutorial/tutorial.pdf)
- [91] ONLINEMCA.COM @Beta <https://www.google.co.kr>
- [92] <http://aistory.egloos.com/4493798>:
- [93] <http://ko.hortonworks.com/blog/how-big-data-is-revolutionizing>
- [94] [https://casiis.llnl.gov/technical\\_focus\\_area/machine\\_learning](https://casiis.llnl.gov/technical_focus_area/machine_learning)

- [95] <http://www.droid-sec.com/2014/03/deep-learning-in-android-malware-detection/>
- [96] <https://ko.wikipedia.org/wiki/>
- [97] <http://word.tta.or.kr>
- [98] [http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu\\_dist=3&seq=16067](http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=3&seq=16067)
- US-CERT, Crypto Ransomware  
<https://www.us-cert.gov/ncas/alerts/TA14-295A>[http://www.kisa.or.kr/notice/press\\_View.jsp?mode=view&p\\_No=8&b\\_No=8&d\\_No=1364](http://www.kisa.or.kr/notice/press_View.jsp?mode=view&p_No=8&b_No=8&d_No=1364)
  - Trend Micro, Ransomware Definition
- [99] <http://www.trendmicro.com/vinfo/us/security/definition/Ransomware>
- McAfee, Defeat Ransomware: Ensure Your Data Is Not Taken Hostage  
<http://www.mcafee.com/kr/resources/solution-briefs/sb-quarterly-threat-q1-2015-2.pdf>
  - Symantec, Ransomware: A Growing Menace  
[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/ransomware-a-growing-menace.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf)
- [100] <https://ko.wikipedia.org/wiki/>
- [101] CNBC, <http://www.cnbc.com/id/101734664,2014>.
- [102] 보드나라 : [www.bodnara.co.kr](http://www.bodnara.co.kr)



## 부록 국내 FinTech 단체

단체명	추진 주체	일 시	주요내용
핀테크 지원센터 (금융감독원의 지원센터 통합 추진)	금 융 위 원 회	'15.3	-핀테크 기업/금융사/정부 주도의 민관 합동 지원 협의체 구성 -자금조달부터 행정/법률상 애로사항 등을 원스톱 해결 -위원장 취임사(3/16) : 비금융분야와 융합, 해외진출 등을 통한 성장동력 확보의 첫걸음 - 핀테크 생태계 구축
핀테크 지원센터 (2014년 버전)	금 융 감 독 원	'14.11	-핀테크 창업기업들의 관련 법규-제도, 행정절차 등 상담 -IT전문 변호사, 지급결제 전문가 등 IT 전문 상담원 6명 상주 -스타트업과의 협업 지원을 위한 금융사 중심의 센터와 행정 법률 검토 지원을 위한 금융당국 창구로 이원화 (3월말)
한국핀테크포럼 fintechkorea.kr	스타 트업 얼라이언스, 은행권 창업재단	'14.11.28	-핀테크 이해당사자들을 위한 교류, 정보 공유,협력의 장 마련 -규제 개선 논의 창구 -매월 정기모임 (3/10, 4차모임 주제 : 핀테크보안) -손에 잡히는 핀테크 세미나 개최 (3/25)
창조경제연구회 kcern.org	미 래 창 조 과 학 부의	'09.06	-창조경제 포럼 및 세미나 개최 등 학술활동 진행 사업 -창조경제의 학문적 체계 확립과 적용을 위한 수탁 연구 사업

	비영리 사단법 인		-관련 단체 및 정부기관 협력 사업 -창조 경제 연구 확산을 위한 온오프라인 출판사업 -창조 경제 연구 플랫폼 구축 사업
--	-----------------	--	--

단체명	추진 주체	일시	주요내용
IBK기업은행 핀테크 지원센터	IBK기 업은 행		
NH핀테크협 력센터	NH금 융지 주	‘15. 03.16	- NH농협은행과 제휴희망기업에게 원스톱 업무협의 지원 - 핀테크스타트업 지원프로그램 운영 : 기술력 이외의 기반이 약한 기업에 금융지원/기술상담/법률자문/특허출원 지원 - 사전 상담을 거쳐 1:1 멘토링 제공
신한퓨처스 랩	신한 금융 지주 액센 추어	‘15. 03.16	- 글로벌 경쟁력 있는 핀테크 스타트업 기업 육성을 위한 후원 - 전 계열사를 동원하여 멘토링, 인프라/테스트 환경 제공 - 액센추어를 통하여 해외투자 유치 및 해외진출 지원 - 국내 스타트업 유관기관과 핀테크 로드쇼 진행 예정(4월중)
KB핀테크허 브센터	KB금 융지 주	‘15. 3	- KB 계열사 업무 협의 지원 창구로서 사업모델 확대 기회 제공 - 지원이 필요한 기업에 투자(KB인베스트 150억), 대출 소개 - 송금/지급/결제/대출/자산관리 등 전담

			<p>추진분과 운영</p> <ul style="list-style-type: none"> <li>- 본인인증수단, 제휴 등 공동이슈에 신속 대응 체계 마련</li> </ul>
D. CAMP	은행권 청년창업재단	‘14’5	<ul style="list-style-type: none"> <li>- 전국은행연합회 회원금융기관이 출범한 창업지원센터</li> <li>- 예비 창업자와 멘토, 투자자가 한자리에 모여 교류의 장</li> <li>- D.OFFICE : 글로벌 비즈니스센터, 스타트업을 위한 입주공간</li> <li>- D.DAY : 매달 마지막주 금요일 스타트업 데뷔 무대</li> <li>- D.PARTY : 기업, 기관, 투자자 등과의 네트워킹 행사</li> <li>- D.MATCH : 스타트업과 인재를 연결</li> <li>- D.CISION : 창업에 대한 성찰의 기회</li> </ul>

단체명	추진주체	일시	주요내용
B2B 핀테크 연구센터	웹캐쉬	‘15’3	<ul style="list-style-type: none"> <li>- B2B 핀테크 : 금융과 IT의 결합을 통해 기업의 업무프로세스 속에 금융을 융합</li> <li>- B2B 분야의 핀테크 연구 및 사례조사</li> <li>- 비즈니스 상품 개발 및 확산</li> <li>- 금융기관 대상 핀테크 전략수립 컨설팅</li> </ul>
글로벌 핀테크 연구소	서강대학교	‘15’2	<ul style="list-style-type: none"> <li>- 핀테크 발전에 관한 기술 교류, 협력 및 국가 핀테크 정책 지원</li> <li>- 미래 지향적 기술 선도로 관련 산업 육성 발전에 기여</li> <li>- 차세대 핀테크 기술의 선도적 역할 수행</li> </ul>

# 국내외 핀테크 관련 기술 및 정책 동향 분석을 통한 연구분야 발굴

인 쇄 : 2016 년 2월

발 행 : 2016 년 2월

발행인 : 백 기 승

발행처 : 한국인터넷진흥원(KISA, Korea Internet&Security Agency)

서울시 송파구 중대로 135 (가락동 78)

Tel: (02) 405-5118

인쇄처 : 남서울대학교 인쇄실

Tel: (041) 581-0643

[비매품]

1. 본 연구보고서는 정보통신진흥기금으로 수행한 정보통신연구개발사업의 연구결과입니다.
2. 본 연구보고서의 내용을 발표할 때에는 반드시 한국인터넷진흥원의 정보통신연구개발사업의 연구결과임을 밝혀야 합니다.
3. 본 연구보고서의 판권은 한국인터넷진흥원이 소유하고 있으며, 당 진흥원의 허가 없이 무단 전재 및 복사를 금합니다.