ISSN 2234-4438
중소기업융합학회 논문지 제6권 제2호 pp. 19-24, 2016 DOI : http://dx.doi.org/10.22156/CS4SMB.2016.6.2.019

# 핀테크 기업의 정보보안체계 관한 연구

강영모, 이영근, 권현정, 한경석, 정현수*
숭실대학교 IT정책학과

# A Study on the Information Security System of Fin-Tech Business

**Young-Mo Kang, Young-Geun Lee, Hyun-Jung Kwon, Keyung-Seok Han, Hyun-Soo Chung***
**IT Policy and Management, Soongsil University**

**요 약** 전통적인 전자상거래방식에서는 정보를 교환할 경우 종이서류에 의한 방법이나 폐쇄형 EDI에 의한 정보교환으로 심각한 문제점은 없었다. 점차 인터넷의 발달로 전자상거래의 규모는 더 커지고 온라인 전자상거래로 변화면서 신원확인, 정보의 변조, 당사자 간의 부인 방지 등 많은 문제점이 발생하였다. 이런 문제점으로 인행 분쟁을 예방하고 사후처리를 위해 전자상거래의 모든 단계에서는 보안 기술을 활용하고 이를 관리하는 인증이 개입하고 있다. 하지만 최근의 모바일 지급결제 서비스 중심으로 핀테크 열풍이 거세게 불고 있다. 카드사 정보유출 사고 및 해킹 등으로 금융서비스의 안정성 확보에 부족하다. 핀테크 산업의 발전과 진화는 정보보호와 동반 성장해야 한다. 따라서 해외의 유명 핀테크 기업의 정보보안체계를 살펴보고 국내 핀테크 기업이 나아가야 할 방향을 제시하고자 한다.

키워드 : 핀테크, 전자상거래, 정보보호, 빅 데이터

**Abstract** A Study on the Information Security System of Fin-Tech Business In traditional electronic commerce, there have not been severe issues of trading information through documents in paper or the closed EDI. The scale of e-commerce has increased as internet develops, however, turning to the online e-commerce, which caused a number of issues such as authentication, information forgery, and non-repudiation between the parties. To prevent conflicts from such troubles and perform the post management, security technologies are applied throughout the process of e-commerce, certificates intervening. Lately, meanwhile, FinTech has been creating a sensation around the mobile payment service. Incidents of information leakage from card corporations and hackings imply the need of securing safety of the financial service. Development and evolution of FinTech industry must be accompanied by information protection. Therefore, this research aims to inquire into the information security system of leading FinTech company in a foreign country

Key Words : Fin-Tech, e-commerce, Information Security, Big Data

## 1. 서론

전자상거래는 전자문서교환(EDI)의 발달에서 시작되었는데 1960년대에 국제 운송회사들이 운송서류를 신속하게 전달할 목적으로 전자문서를 표준화하여 사용한 것이 시초이다[1]. 전사상거래란 독립된 경제주체서 조직과 조직 간에 이루어지는 B2B, 기업과 개인을 대상으로 하여 상품, 서비스 등을 공급하는 거래유형

Received 2016-05-23 Revised 2016-06-11 Accepted 2016-06-13 Published 2016-06-30
*Corresponding author : Hyun-Soo Chung (hsj6553@ssu.ac.kr)

인 B2C등 거래하는 경제주체에 따라 또는 중계업자가 관여하는 여부에 따라 다양하게 분류할 수 있다. 좀 더 구체적으로 설명하면 다음 3가지로 나누어 정의할 수 있다. 첫째 커뮤니케이션 관점에서의 전자상거래를 보면 정보의 전달, 상품과 서비스의 배달, 지불까지의 과정이 컴퓨터 네트워크나 다른 매체를 이용하여 모두 전자적으로 이루어지는 거래활동이다. 둘째 비즈니스 프로세스 관점에서는 기존의 상거래와 업무처리과정을 자동화하여 사람의 개입을 최소화하고 정확성과 신속성, 효율성을 높이는 것을 목표로 삼는다. 셋째 서비스 측면에서의 전자상거래는 상기의 두 가지 특성을 최대한 활용하여 중간 유통마진을 최소화하고 고객에게 보다 저렴한 가격과 높은 품질의 서비스를 제공하는 것을 추구한다. 이처럼 바라보는 관점에 따라서 전자상거래는 여러 가지로 정의될 수 있으며 보다 광의의 전자상거래는 새로운 비즈니스기회의 창출과 개발, 이를 통한 부가가치의 극대화의 수단으로 정의할 수 있다. 따라서 정보통신의 발달로 시간과 동간을 초월하여 정보화의 자동화와 정보 유통을 통하여 업무의 효율성과 생산성이 높아졌다. 하지만 전자상거래를 위해서 정보를 교환할 경우 기존의 종이서류에 의한 방법이나 폐쇄형EDI에 의한 정보교환에서는 볼 수 없었던 문제점들이 발생한다. 전자상거래로 인한 정보교환의 문제점으로는 거래 당사자의 신원확인, 교환된 정보의 변조 여부와 관련된 무결성, 당사자 간의 거래 사실의 부인 방지 등을 들 수 있다[2]. 또한 최근의 스마트폰의 발달과 비금융기관의 적극적인 전자상거래 시장 진입 그리고 모바일 뱅킹, 모바일 신용카드 등을 이용한 전자결제 증가로 기존과 다른 결제수단이 형성되어 가고 있다. 특히 고객의 경제적인 위험을 내포하고 있는 핀테크의 결제수단은 정보보호가 없다면 발전할 수 없다. 따라서 정보보호를 바탕으로 산업을 발전시켜야한다. 해외 핀테크의 정보보호전략을 살펴보고 이를 바탕으로 국내 핀테크의 산업의 정보보안체계를 제시보고자 한다.

## 2. 국내 전자금융거래현황

통계청의 온라인 쇼핑동향 자료에 따르면 2016년 3월 온라인쇼핑 거래인은 5조 1,926억 원으로 전년 동월대비 20.9%증가, 온라인쇼핑 거래액 중 모바일쇼핑 거래액은 2조 6,796억 원으로 50.6%증가했다. 이중 모바일 거래액 비중은 51.6%차지했다[3].

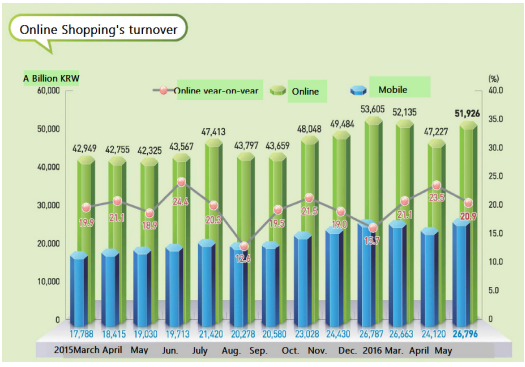


Fig. 1. Online Shopping's Turnover

한국은행에 따르면 현재 17개 금융기관에 등록된 인터넷뱅킹(모바일뱅킹 포함)등록 고객 수는 1억 1,529만 명으로 전분기말대비 1.8%증가했다[4].

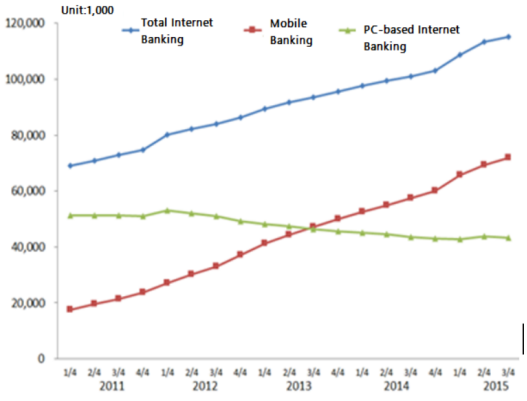


Fig. 2. Demostic Banking Service Usage[5]

스마트폰뱅킹 등록고객 증가에 따라 전체 인터넷뱅킹 등록고객 중 모바일뱅킹 등록고객이 차지하는 비중(62.3%)은 꾸준히 증가하는 추세이다. 특히 모바일뱅킹 등록 고객 수는 지속적인 증가세를 보이는 반면 PC기반 인터넷뱅킹 등록 고객 수는 2012년 1/4분기 이후 완만한 감소세를 이어가고 있다.

## 3. 해외 핀테크 기업보안체계

### 3.1 페이팔(PAPAL)

페이팔 가입자는 물품 구매 시 추가적인 소프트웨어 설치가 불필요하며 페이팔 ID/PW만 입력하면 카드정보 입력이나 본인인증 절차 없이 결제가 가능하다. 일부국가에서는 휴대폰 단문문자 메시지 또는 OTP(One Time Password)를 통한 추가 인증 절차가 필요하다[2].

#### 3.1.1 보안체계

- 페이팔이 진출한 20개국에 500여 명의 정보 유출 방지 전담 인력 배치, 보안과 리스크 관리 등 인력을 합치면 전 세계 17개 센터7,000명이 보안 업무를 수행하고 있다.
- PCI-DSS 보안표준을 준수하는 동시에 전자 금융 사기를 방지하기 위해 보안업체를 인수하고(Fraud Science)새로운 보안기술을 도입하여 금융사고 발생을 예방한다.
- FDS(Fraud Detection System)를 이용하여 부정거래 행위를 24시간 모니터링한다.
- 송금, 결제 정보가 이메일로 구매자에게 전달되므로 피싱(Phishing)사기 방지를 위해 피싱 사이트 필터링 시스템을 운영한다.

#### 3.1.2 사고배상책임

- PCI-DSS를 준수하지 않은 상태에서 정보 유출 발생이 발생할 경우 카드사는 벌금 부과 및 카드결제 승인 거부 등의 수단으로 해당 회사를 제재한다.
- PCI-DSS를 준수했을 경우 민사소송에서는 면책되지 않지만 공공부문 소송에서는 면책이 가능하다.
- CVC 없이 결제가 이루어진 이후 발생한 사고에 대해서는 PCI-DSS가 준수되었는지 확인 후 보상여부를 결정한다.

### 3.2 알리페이(ALIPAY)

알리페이는 신용카드, 은행계좌등을 가상계좌와 연동하여 입출금, 결제, 송금, 담보거래, 요금납부, 펀드, 보험 등 다양한 금융서비스를 제공하고 있다[2].

#### 3.2.1 보안체계

- PCI-DSS보안표준을 준수하고 있으며, 인증서에 의한 서버인증(VeriSign), 웹 표준(128BitSSL)을 활용하여 거래 및 인증데이터 암호화한다.
- 2005년부터 실시간 모니터링을 통한 전자금융결제 사고 방지를 위해 FDS(Fraud Detection System)도입하여 운영하고 있다.
- 데이터 암호화 기술을 활용한 SSL인증서와 자체 앱(app)을 기반으로 한 OTP서비스를 제공하고 있다.

#### 3.2.2 사고배상책임

- 결제 사고 발생 시 회원에게 피해 금액의 한도 내에서 손해 배상을 하며, 회원이나 제3자에게 책임이 있는 경우 제외한다.
- 배상조건에 부합할 경우 고객 증빙자료를 바탕으로 배상여부를 결정한다.
- 회원의 ID/PW, 검증번호, 신분 정보 유출, 연계은행의 시스템 문제, 천재지변 등 불가항력 발생으로 인한 사고는 배상책임에서 제외한다.

### 3.3 구글 월렛(GOOGLE WALLET)

구글 월렛은 전자지갑 서비스로 온라인 오프라인 결제를 모두 지원하며, 지메일, 구글플러스 등 자사 서비스와 연계한 결제부가서비스 제공하고 있다[2].

#### 3.3.1 보안체계

- 웹 표준기술 사용, PIN번호, 실시간 트랜잭션 통지 등의 대책 마련하였다.
- 통신시 SSL암호화 프로토콜 사용, 결제 데이터 저장시 최소 2,048bits암호화한다.
- PIN번호 설정을 통해 구글월렛 앱 접근, ATM 인출등에 사용가능하다.
- 앱을 통한 실시간 거래내역 통지한다.

#### 3.3.2 사고배상책임

- 거래일로부터 120일 이내에 보고된 비인가 된 거래에 대해서는 100%보상프로그램 마련하였다.(미국 내)
- 분실 폰 관리를 위해 온라인(wallet.google.com)에서 원격으로 구글, 월렛앱 또는 카드중지 가능하다.

## 4. 핀테크 기업보안 관리체계

### 4.1 핀테크 보안체계

위에서 살펴본 핀테크 선진국 보안체계를 바탕으로 정리하면 표 5와 같다[6].

Table 1. Advanced Security System

| Category | Features |
|---|---|
| Post-Security Reinforcement | Discovering illegality or fake trade and screening issues after the fact |
| Selective Regulation | Executing regulations in a different manner, according to the trade volume or the credit rating of the consumer |
| Heavy penalty to the parties involved in the incident | Fine the company who caused a severe security incident an astronomical sum of money |
| Heavy penalty to the parties involved in the incident | Operate PCI-DSS, a self-regulative security certification system |
| Responsibility diffusion | Diffusing responsibilities at the electronic payment agency, IT company, and financial consumer |
| Abundant manpower and technology of FinTech businesses | Securing verified high-end FDS, big data analysis technology, and certification technology and fostering security management technology |

위의 표처럼 국내 핀테크 기업 보안체계를 국내시장에 맞추어 구축할 필요성이 있다.

자율 보안 키워드 속에는 금융회사가 보안인증 수단 등을 스스로 결정할 수 있다.

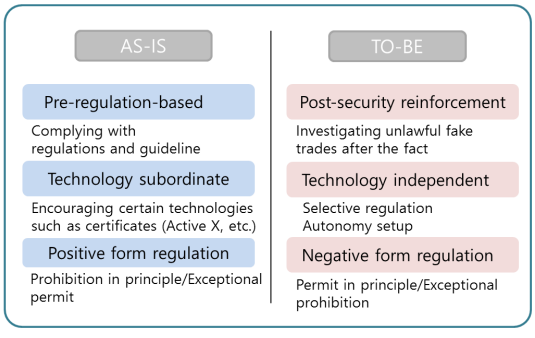


Fig. 3. Changes of Financial Security

공인인증서와 액티브 X 등 특정 기술을 권장했던 과거와 달리 이제는 다양한 기술을 선택할 수 있는 자율성이 주어지게 된다[7-10]. 비대면 금융서비스를 위한 실명 확인 방법으로 금융회사가 기존 대면 방식에서 다양한 방식을 택할 수 있다. 따라서 기업은 미국의 애플 페이, 중국의 알리페이처럼 간편하고, 편리한 서비스를 낮은 비용으로 안전하게 제공하는 것이 핀테크를 성공적으로 발전시킬 것이다.

### 4.2 기업 정보보안

기업은 다양하고 새로운 위협으로부터 기업정보를 지속적으로 관리 가능한 상태를 유지해야 한다[11,12]. 따라서 아래그림은 6하 원칙에 따른 정보유출을 포함한 정보보안 전략을 설계하였다.

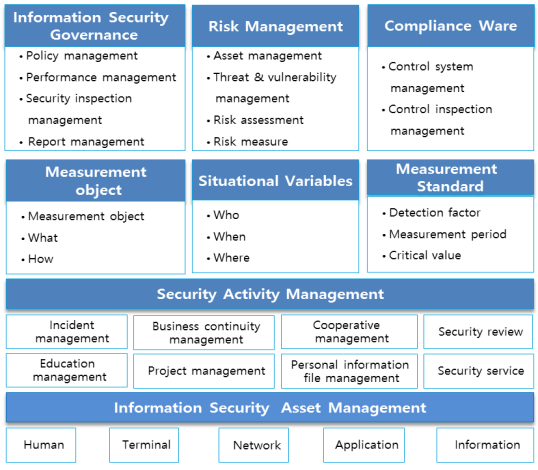


Fig. 4. Information Security Integrated Management System

정보보안통합관리체계를 효과적으로 운영하기 위해서는 다음 세 가지를 고려해야 한다.

첫째, 6하 원칙 행위를 시나리오를 만들어 정보유출을 시도한 당사자를 찾아 어떤 정보를 유출시도를 쉽게 찾을 수 있다. 따라서 정보유출여부의 논란을 줄일 수 있는 정확성을 높인다.

둘째 시스템의 정보를 수집하여 위험관리 대상을 설정, 행위패턴 분석 및 상관관계, 통계/보고서 등 정보유출 분석 모니터링 업무의 전 과정을 하나의 시스템 내에서 수행하도록 한다.

셋째 위험그룹 대상 관리, 소명관리, 통계 등 사전/사후 대응을 위한 프로세스로 설계해야한다. 다양한 상황에 따라 다르게 관리할 필요가 있으며 이상 징후가 포착되었을 때 소명처리를 통해 그 행위를 정당성을 검증해야 한다. 또한 상황에 맞는 통계 및 보고서 활동을 통해 시스템 운영전반에 대한 현황을 식별할 수 있어야 한다.

정보보안에 기업이 소극적인 대응을 하는 경우가 많은데 핀테크 산업에 있어서 기업의 정보를 보호하여 기업 가치를 높일 수 있을 것이다.

## 5. 결론

국내 핀테크 보안업체가 살아남기 위해서는 철저한 시장분석과 연구개발에 집중하여 차별화된 서비스개발이 중요하다. 그러기 위해서는 해외 핀테크 산업의 보안체제를 연구하여 우리나라 실정에 맞는 보안체제를 구축하는 것이 시급하다. 또한 핀테크 산업의 발전하기 위해서는 정보보호기업에 대한 투자가 확대되어야 한다. 또한 유망 핀테크 보안기업, 정보보호 스타트 업 기업을 선정해 투자하고 금융권과 제휴할 수 있도록 지원해야 한다. 높은 인터넷 이용률, 스마트 폰 보급률, 인터넷 뱅킹, 신용카드 등 금융 인프라가 다른 나라에 비해 뒤떨어지지 않는다. 또한 정보보안통합관리체계를 구축하여 기업의 가치를 높일 수 있다.따라서 규제 완화와 보안 강화를 바탕으로 정보 보안 산업육성 전략과 핀테크 보안체계를 구축하려는 노력이 필요하다.

## REFERENCES


[1] H. C. Kim, “Issues and Subjects of the Framework Act on Electronic Document and Electronic Commerce,” *Inha Law Review the Institute of Legal Studies Inha University*, Vol. 15, No.2, pp.292-322, Jul. 2012.

[2] S. S. Jang, A Study on impact of Fin-Tech information on the protection industry, Internet &Security Focus, http://http://www.kisa.or.kr/, 2015. 5.

[3] H. G. Jeon and W. S. Jang, “A study on the Information Security Technology in the Electronic Commerce,” *Journal of Korean Studies Information Service System (KISS)*, Vol. 10, No. 1, pp. 43-55, 2009.

[4] The Statistics Korea, *Shopping Trends,* The Statistics Korea, 2016.

[5] The bank of korea, *Domestic internet banking service usage,* The bank of korea, 2015.

[6] Yu jae-dong, According to credit security level differentiation, increase efficiency of financial transactions, dongA.com http://news.donga.com, 2015. 5.

[7] S. J. Han, “The legal issues on the fintech and e-commerce payment,” *Journal of Korea Information Assurance Society*, Vol. 15, No. 2, Mar. 2015.

[8] S. B. Kim and K. M. Kim, “A Study on the Efficient e-Commerce Policies under the Smart Phone Environment,” *Journal of the Society of Digital Policy & Management*, Vol. 10, No. 1, pp.125-133, Feb. 2012.

[9] H. S. Lee, “The Study of Electronic Payment System in Electronic Commerce,” *Journal of Korea International Accounting Association*, Vol. 6, pp. 145-164, 2002.

[10] Strategy Eye & Digital Media, *Insight Report : The Future of Fintech,* 2014.

[11] J. H. Park, "Study on the Secure Distribution and Storage of Financial institutions' documents - Focused on the authorized electronic address and the Certified e-Document Center System", *Seoul Law Review*, Vol. 21, No. 3, pp. 347-388, Feb. 2014.

[12] S. H. Lee and D. W. Lee, “FinTech-Conversions of Finance Industry based on ICT”, *Journal of Korea convergence society*, Vol. 6, No. 3, pp. 97-102, Jun. 2015.


## 저 자 소 개


**강 영 모(Young-Mo Kang)** [학생회원]

- 1998년 4월 ~ 2010년 7월 :국제 A/GE 대표 역임
- 2015년 10월 ~ 현재 : 위디코(주) 대표
- 보안 및 안전 시스템 특허 5개보유
- 2014년 9월 ~ 현재: 숭실대학교 IT정책학과 박사과정

<관심분야> : 정보경영, 정보통신 행정 및 정책, IT융합 기술, 인공지능 및 지능시스템

**이 영 근(Young-Geun Lee)** [학생회원]

- 1988년 2월 : 공군사관학교 기계공학과 학사
- 2000년 2월 : 국방대학교 무기체계 석사
- 2014년 9월 ~ 현재: 숭실대학교 IT정책학과 박사과정

<관심분야> : 네트워크 중심전, 지휘통제시스템, 국방자원관리 등

권 현 정(Hyun-Jung Kwon) [학생회원]

- 2010년 3월 ~ 현재 : 한국 보건복지부(책임)
- 2014년 9월 ~ 현재 : 숭실대학원 박사과정

<관심분야> : 정보보안,IT정책, IT 융합기술, 인공지능 및 지능시스템

한 경 석(Keyung-Seok Han) [정회원]

- 1979년 : 서울대학교, 국어교육학사
- 1984년 : 서울대학교 경영학 석사
- 1989년 : 미국 퍼듀대학교 대학원, 경영정보시스템 전공 박사
- 1989년 : 미국 휴스턴 대학교 조교수
- 1983년 ~ 현재 : 숭실대학교 경영학부 교수 재직

<관심분야> : Technical MIS, Digital Economity, Agent-Eased Simulation, Web Programming, ERP, 회계정보시스템, E-Business, 전자상거래, 중소기업정보화

정 현 수(Hyun-Soo Chung) [정회원]

- 1982년 2월 : 숭실대학교 전자계산학과 학사
- 1991년 2월 : 숭실대학교 컴퓨터학과 석사
- 1995년 2월 :숭실대학교 컴퓨터학과 박사
- 1982년 2월 ~ 2005년 11월 : ETRI 책임연구원
- 2006년 2월 ~ 2011년 3월 : TANC CTO
- 2009년 2월 ~ 2012년 2월 : 한남대학교 경영정보학과 겸임교수
- 2012년 4월 ~ 현재 : 숭실대학교 숭실융합연구원 교수

<관심분야> : 정보보호, ICBM, IT 감리 & 컨설팅