정 보 보 호 학 회 지
제 29 권 제4호, 2019. 8

안전한 핀테크 서비스를 위한 지침

나 재 훈*

요 약

디지털 전환(Digital Transformation)은 산업 각 분야에서 진행되고 있는 혁신이며, 금융권에서도 디지털 전환의 영향이 크게 미치고 있다. 전산화 되어 있지만 폐쇄적인 네트워크로 구축되어 있던 금융 네트워크가 점점 데이터의 공개를 필요로 하였으며, 그 공개된 데이터를 기반으로 새로운 서비스가 창출되는 산업적 태동이 있었다. 개별적 서비스의 처리나 단계(부품)의 개선이 아니라 플랫폼의 개방을 통한 융합화와 이를 조화롭게 통제하는 거버넌스의 필요성이 대두되었다. 이러한 동향에 편승하여 새로운 기업(스타트업)이 창출하였고, 공개된 정보를 기반으로 융합 서비스를 창출하여 서비스의 발전이 눈부시게 진행하고 있다. 핀테크 서비스가 공개 API(Application program interface)로 제공되고 있으며, 이를 이용하여 빠른 발전을 하고 있으나, 공개성으로 인하여 취약점마저도 공개되어 정보보안의 위협으로 작용 될 수 있으므로, 개방형 플랫폼의 정보보안을 중심으로 핀테크 정보보안 표준의 동향을 살펴본다.

Ⅰ. 서 론

디지털 전환(Digital Transformation)은 4차 산업에 매우 중요한 영향을 주고 있다. 디지털 기술을 타산업에 적용하여 그 가치를 제고하는 결과를 나타내고 있으며, 이를 통하여 제조산업이 선진국으로 회귀하는 현상을 보이고 있다. 순차적이고 단방향적으로 가치가 창출되었던 경제의 구조에서 디지털 전환으로 인하여 기업 간 다양한 주체들의 상화작용과 협력적 활동으로 가치가 창출되고 있다[1].

핀테크는 금융을 뜻하는 Finance와 기술을 뜻하는 Technology의 합성어로 IT기술을 접목시킨 금융사업을 의미한다[2]. 지급결제, 송금/전자화폐, 펀딩, 자산관리 등 여러 분야에서 서비스를 제공한다. 국제 핀테크 시장이 커짐에 따라, 국내에서도 국내 핀테크 기술을 개발 및 서비스의 출시가 집중되고 있다. 핀테크 기술을 개발하여 사용자에게 좋은 서비스를 제공하는 것도 좋지만, 핀테크 기술을 안전하게 사용하기 위한 보안기술도 간과 되어서는 안된다.

본 논문에서 핀테크 개방형 플랫폼의 진화와 개방형 플랫폼의 위협 및 취약점, 그리고 개방형 플랫폼을 중심으로 안전한 핀테크 서비스 제공과 이용 시에 필요한 정보보안 지침의 내용의 국제표준 동향에 대하여 살펴본다.

Ⅱ. 핀테크 서비스와 개방형 플랫폼

2.1. 개방형 플랫폼

개방형 플랫폼은 개방형 표준에 근거하여 표준문서가 제정(게재)되고, 완전하게 문서화된 외부 응용 프로프램 인터페이스(API: Application Program Interfaces)를 제공하는, 소프트웨어 시스템을 의미한다. API는 원래 프로그램의 의도하지 않은 다른 기능으로 소프트웨어를 이용할 수 있도록, 소스코드의 수정을 하지 않고서도 허용을 하고 있다. 이러한 인터페이스를 이용하여 제삼자는 기능을 추가하기 위하여 플랫폼에 통합을 할 수 있다. 개방형 플랫폼을 이용한다는 것은, 플랫폼 벤더가 아직 완료하지 못한 또는 기존에 생각하지 못한 기능을 개발자가 추가할 수 있는 것이다[4].

2.2. 개방형 플랫폼의 진화

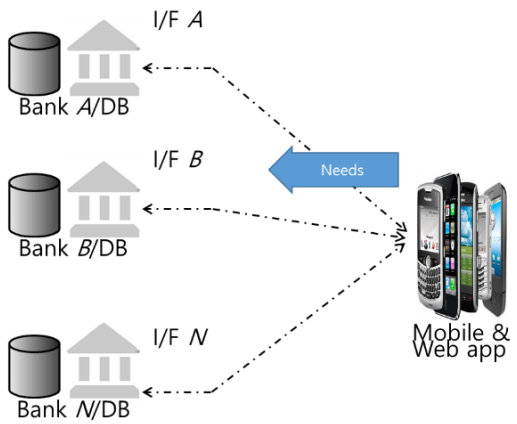
개방형 API는 기업이 보유한 서비스, 데이터 등을

본 논문은 2019년도 과학기술정보통신부의 재원으로 정보통신방송표준개발지원사업의 일환으로 수행되었음.[2017-0-00472, 안전한 웹기반 개방형 핀테크 플랫폼 표준 개발]
* 한국전자통신연구원 정보보호연구본부(jhnah@etri.re.kr)

쉽게 활용할 수 있도록 하여 웹서비스 및 애플리케이션 개발을 지원하는 개방 지향적인 성격을 갖는다. 사용자는 일방적인 웹 검색 결과나 사용자 인터페이스(UI) 등을 제공 받는데 그치지 않고 직접 응용프로그램과 서비스를 개발할 수 있어 사용자 참여를 유도하는 사용자 중심의 비즈니스 모델이다[3].

핀테크의 등장으로 금융회사와 핀테크 기업 간의 연대가 중요해지면서 국내외 금융 회사들은 이를 위한 수단의 하나로 개방형 API 기술에 주목하고 있다. 금융기업들은 제한된 리소스(인적 그리고 기술적)를 가지고 고객들의 다양한 니즈와 개인화된 서비스들을 감당하기에 어려움이 있다. 그리고 핀테크(FinTech) 기업들은 적은 인력으로 동일한 기능을 제공하기 위하여 여러 금융기업들에게 서로 다른 접근방법으로 개발하는 것은 또한 매우 큰 어려움을 갖는 것이고, 그들이 개발한 제품을 실제적이고 충분한 데이터를 배경으로 검증할 수 있는 테스트 환경이 없다는 것 또한 큰 애로 사항이다. 그러므로 금융기업들로부터 데이터와 서비스를 교환하고 종합하는 그리고 핀테크 제품을 시험하는 개방형 플랫폼에 대한 요구가 있는 것은 당연한 것이다.

[그림 1]의 금융 서비스의 구조는 금융 서비스 제공자가 일방적으로 서비스를 구축하여 이용자들에 제공하는 형태를 보이고 있다. 이는 각 금융사가 자신의 데이터와 서비스를 자신들의 방식으로 이용자들에게 제공하는 것이며, 각 금융사를 접속하기 위해서는 각기 다른 앱을 이용하여 접속을 하여야 한다는 것이다. 이것은 새로운 서비스를 개발하기 위하여 유사한 기능에 대하여 금융사가 개별적으로 개발을 하여야 하며, 유지보수 또한 금융사가 책임을 갖으며, 기업 경쟁력에 매우 부적합 구조를 보이고 있다.

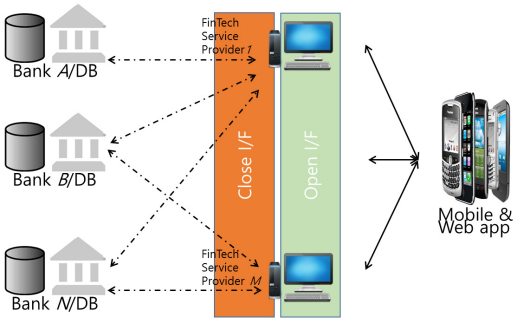


〔그림 1〕 디지털금융 서비스의 기능구조

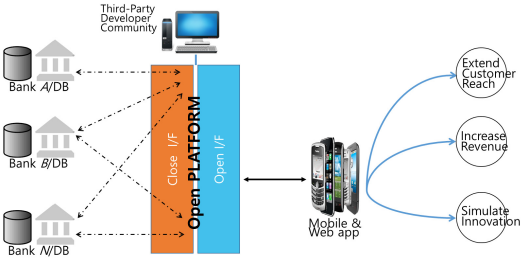
[그림 2]의 핀테크 서비스 구조는 이용자들의 요구사항을 수용하기 위하여 나름 금융사가 투자를 한 결과 금융사의 내부 기술자가 아닌 외부 핀테크 기업을 활용하여 이용자들에 서비스를 제공하는 형태의 구조를 보이고 있다.

이 구조는 핀테크 기업이 금융사를 위하여 서비스 구축을 위하여 소프트웨어를 개발하고 개방형 인터페이스를 사용자들에게 제공하여 주고 있다는 커다란 장점을 가지고 있다. 그러나 유사하거나 동일한 기능을 사용자들에게 각 금융사별로 다른 인터페이스로 서비스를 제공하므로 사용자는 각각의 앱을 설치하여 서비스를 처리하여야 한다.

[그림 3]의 개방형 플랫폼은 표준화된 공개 인터페이스를 제공하기에 이용자는 하나의 앱을 통하여 여러 금융사의 데이터와 서비스를 접할 수 있으며, 더욱이 핀테크 기업은 단일화된 인터페이스로 인하여 동일한 기능에 대하여 단일한 소프트웨어를 개발하므로 생산성에 있어서 매우 큰 이점을 갖으며 향후 유지보수 또한 용이하게 되고, 공개된 데이터와 서비스로 스타트업의 출



〔그림 2〕 핀테크 서비스의 구조



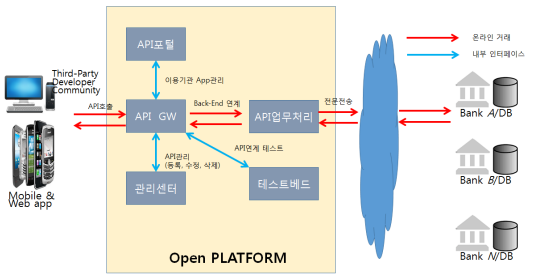
〔그림 3〕 핀테크 서비스를 위한 개방형 플랫폼 구조

현과 새로운 서비스 발굴로 최종 금융사의 기업의 가치가 창출될 수 있는 구조를 보이고 있다.

Ⅲ. 안전한 개방형 플랫폼의 정보보안

[그림 3]의 개방형 플랫폼 구조로 핀테크 서비스가 제공되면 생산성과 효율성 및 기업의 가치에 긍정적인 영향을 주므로 국내 금융권에서는 개방형 플랫폼 구축을 하였다. 그러나 중요한 데이터와 서비스를 안전하게 관리하고 처리하는 것에 대한 고려가 부족하며, 개방형 온라인 인터넷 상에서 서비스의 중단 없이 추가하고 변경하는 것이 원활하게 수행할 수 있어야 하는 것이 핵심 요구사항이다.

[그림 4]는 개방형 API를 제공하면서, API를 변경, 추가, 삭제하며, 온라인 상에서 자유롭게 시험을 할 수 있는 개방형 플랫폼의 구조를 보이고 있다. 이용자가 직접 API를 접속하는 API GW(게이트웨이)가 있어서 이용자로부터 입력된 요청을 내부 네트워크를 통하여 해당 서버에 맞는 명령어로 전환하여 수행 처리하는 API 업무 처리가 있다. 이러한 API에 관한 인터넷 공지를 담당하는 포털이 있어서, API 사용법, 변경하기 위한 기초정보, 사용 권한 등등을 문서화하여 사용자나 핀테크 개발자에게 공지를 하는 포털이 운영된다. 그리고 개방형 API를 수정 또는 추가 하려고 할 때에 사전에 개방형 플랫폼에 적합한지 그리고 안전한지를 검증하기 위한 테스트베드가 있으며, 검증을 마친 개방형 API를 등록, 수정, 삭제를 관리하는 관리센터가 있다. 이와 같은 구조에서 도메인을 넘나드는 이용자 인증 및 정보의 융합에 따른 안전성을 보장하는 개방형 플랫폼 서비스의 정보보호와 개방형 플랫폼의 각 콤토넌트간의 연동을 통한 각 인터페이스에서 상호작용하여 서비스 및 데이터와 시스템의 안전성을 위한 정보보호 메커니즘이



〔그림 4〕 안전한 핀테크 서비스를 위한 개방형 플랫폼 구조

폭넓게 고려되어야 한다.

3.1. 개방형 플랫폼의 위협 및 취약점

개방형 API는 금융기관의 시스템에서 다른 회사를 통행 새로운 통신 경로를 설정하여 사용자에게 새로운 서비스를 제공하는데, 이러한 통신 경로가 데이터 유출이나 변조 그리고 승인되지 않은 트랜잭션을 초래하는 위협이 있을 수 있다[5].

개방형 플랫폼 위협요인은 개방형 웹 응용 정보보호 프로젝트, 금융보안원, 일본의 은행권의 개방형 API 관련 자료를 기초로 하였으며, 참고를 위한 위협항목 목록을 기술하였다.

3.1.1. 위협 [6, 8]

- 계정 수집 (Account aggregation)
- 계정 생성 (Account creation)
- 광고 사기 (Ad fraud)
- 캡차 공격 (CAPTCHA defeat)
- 카드 크래킹 (Card cracking)
- 카딩 (Carding)
- 캐싱아웃 (Cashing out)
- 크리덴셜 크래킹 (Credential cracking)
- 크리덴셜 스터핑 (Credential stuffing)
- 재고 거부 (Denial of Inventory)
- 서비스 거부 (Denial of Service)
- 신속처리 (Expediting)
- 핑커프린팅 (Fingerprinting)
- 풋프린팅 (Footprinting)
- 스캘핑 (Scalping)
- 스크래핑 (Scraping)
- 스큐잉 (Skewing)
- 스니핑 (Sniping)
- 스패밍 (Spamming)
- 토큰 크래킹 (Token cracking)
- 취약점 스캐닝 (Vulnerability scanning)
- 비인가 접근 (Unauthorized access)

3.1.2. 취약점 [7]

- Glibc 취약점
- 쿼드루터 (Quadrooter)
- 드로운 취약점 (DROWN)
- 제로데이 공격 (Zero-Day attack)
- DB 취약점 (Database vulnerability)
- OS커널 취약점 (Operating System Kernel vulnerability)
- OpenJDK 취약점

3.2. 안전 핀테크 서비스를 위한 정보보안 지침

핀테크 서비스의 안전한 서비스를 위하여 네트워크 인프라에서 종단간(end-to-end) 보호를 위한 서비스 요소들은 우선적으로 개방형 플랫폼, 개방형 API, 그리고 데이터를 들 수 있으며 이것을 핀테크 서비스를 사용하는 사용자, 서비스를 제공하는 제공자, 스타트업 중심의 기술제공 제삼의 기관의 측면에서 분석하여 다음과 같이 23개 분야의 74 지침 항목이 제시되었다[9].

3.2.1. 정보보호 정책·조직

- 정보보호최고책임자 지정 및 실무조직
- 정보보호정책 수립 및 공표

3.2.2. 외부자 관리

- 위탁업체 선정 및 관리

3.2.3. 정보자산 관리

- 정보자산 식별 및 등급부여
- 정보자산별 책임자 지정

3.2.4. 정보보호 교육

- 정보보호 교육계획 수립 및 이행
- 실무자 정보보호 교육 이수

3.2.5. 인적 보안

- 비밀유지서약서
- 직무분리
- 퇴직 및 직무변경 관리

3.2.6. 위험 관리

- 취약점 점검 정책 수립 및 점검 수행

3.2.7. 침해사고 대응

- 침해사고 대응절차 마련 및 교육 시행
- 침해사고 대응 관련 로그 보존 및 모니터링

3.2.8. 장애 대응

- 백업정책 수립 및 복구절차 마련

3.2.9. 이용자 보호

- 개인정보 처리 관련 이용자 보호
- 개인·신용정보 접근 및 거래지시 권한 관련 안내
- 이용자 고충 처리방침 마련 및 공개
- 이용자 보안 주의사항 안내

3.2.10. 물리적 보안

- 보호구역 지정 및 출입 통제
- 보호구역 반출입 관리
- 사무실 환경 보안 정책 수립 및 이행

3.2.11. 개발 보안

- 설계 시 보안 요구사항 도출 및 반영
- 시큐어 코딩 적용 및 보안 취약점 점검·보완
- 테스트 시 이용자 개인·신용정보 사용 제한
- 소스 프로그램 및 전산원장 대상 접근·변경 통제

3.2.12. 암호 통제

- 중요 정보 암호화 정책 수립 및 이행

3.2.13. 접근 통제

- 중요 정보자산 계정 및 접근 권한 관리
- 중요 단말기 지정 및 접근 통제

3.2.14. 시스템 보안

- 주요 시스템 등의 악성코드 감염 및 정보유출 방지
- 인터넷망을 통한 원격관리 통제
- 주요 시스템 목적 외 기능·프로그램·포트 등 제거
- 중요 서버 독립 운영 및 정보보호시스템 적용
- 공개용 웹서버 보호대책 마련
- 중요 보안패치 적용 지침 수립 및 이행

3.2.15. 네트워크 보안

- DMZ 구간 구성
- 내부망 사설IP 활용 및 주요 시스템 배치
- 무선 네트워크 이용 최소화 및 보안대책 수립·적용
- 대외기관과 통신 시 보안통신 적용

3.2.16. 거래 당사자 인증

- 이용자 인증 방법의 적정성
- 이용기관 인증 방법의 적정성
- 고위험 전자금융거래 인증 방법의 적정성
- API 접근 요청 처리 시 권한의 적정성 검증
- 운영기관 정보처리시스템 인증
- 이용자 인증 우회방지
- 접근키 등 유출 위험 완화 대책
- 이용기관 인증정보 추측방지
- 인증 및 거래 관련 기록관리
- 인증키 관리

3.2.17. 거래정보의 기밀성 및 무결성

- 거래정보 등의 기밀성
- 거래정보 등의 무결성
- 안전한 암호 알고리즘 사용
- 안전한 키관리
- 안전한 암호 프로그램 관리

3.2.18. 정보처리시스템 보호대책

- 관리자 및 책임자 지정·운영
- 중요 패치 수행
- 운영체제 계정 추가인증
- 서버접근 중요단말 보호
- 서버 해킹 방지
- 보안성 검증 및 취약점 점검
- 공개용 서버 설치 및 접근통제
- 이용기관 침해사고 대응

3.2.19. 고객단말기 보호대책

입력정보보호
이용기관 고객단말기 보호대책
이용기관 서명 인증서 관리

3.2.20. 정보유출 방지대책

- 접근계정 관리
- 정보시스템 로그 기록 및 분석
- 이용기관 정보유출 방지대책

3.2.21. 이상금융거래 방지대책

- 이상금융거래 모니터링 및 탐지
- 이상금융거래 탐지 시 대응
- 중요거래 고객통지

3.2.22. 시스템 가용성 확보 및 비상대책

- 업무지속성 확보방안 수립
- 주요 전산장비 이중화
- 백업·소산 관리

3.2.23. 시스템 가용성 확보 및 비상대책

• 이용기관 물리적 접근통제

Ⅳ. 결 론

플랫폼의 개방화는 디지털 전환에서 금융산업에 디지털 기술을 접목하여 금융 서비스의 단순 간편화를 넘어 데이터의 공유, 융합서비스의 출현이라는 매우 중요한 의미를 갖고 있다. 이렇게 신규 서비스가 출현하고 있으며, 이에 발맞추어 정보보안 기술도 개발되어야 하며, 글로벌 연동을 위한 상호운용을 위한 표준은 필수불가별한 결과인 것이다.

금융기업이 제삼자에게 API를 공개할지라도, 그것이 표준으로 개발되지 않는다면 각자의 API에 따른 개발은 비생산적이고 비효율적인 것이다. 전체적이고 종합된 방법으로 핀테크 개발자들이 필요한 제어와 궁극적으로 고객을 위한 종대종 보호를 보증할 수 있도록 국제표준화가 선행되어야 한다고 미국, 영국 등의 의견이 있었으며, 2017년 9월 ITU-T SG17 제네바 회의에서 신규 표준아이템 X.sfop: Security framework of open platform for FinTech services가 한국의 제안으로 신설되었고, 표준개발이 마무리 단계에 있으며, 내년(2020년) 상반기에 표준제정을 예정하고 있다. 이는 국내의 기술을 국제적 기술로 승화시키며, 국제 경쟁력을 높이는 표준화로 평가되고 있다. 이 표준 아이템에 대하여 한중일간에 긍정적이고 적극적인 논의가 진행되었으며, 일본의 은행권에서 상용중인 개방형 API에 대한 경험을 이 표준에 반영하기를 의도하고 있으며, 중국은 알리바바의 표준전문가를 ITU-T SG17 회의에 참여하여 표준화를 진행하였다.

참 고 문 헌

[1] 제4차산업혁명과 산업의 디지털 전환:위기와 전략 (1), 2017.04. 소프트웨어정책연구소

[2] 금융위원회, “핀테크”, 금융용어사전, 2015, http://fsc.go.kr/know/wrd_list.jsp

[3] 해외 금융회사의 오픈 API 구축 동향 및 시사점, 2015.12. 지급결제와 정보기술 제62호, 금융결제원

[4] Open platform, https://en.wikipedia.org/wiki/Open_platform

[5] Report of Review Committee on Open APIs: Promoting Open Innovation https://www.zenginkyo.or.jp/fileadmin/res/news/news290713_3.pdf

[6] OWASP Automated Threats to Web Applications. https://www.owasp.org/index.php/OWASP_Automated_Threats_to_Web_Applications

[7] Top Open Source Security Vulnerabilities. https://resources.whitesourcesoftware.com/blog-whitesource/top-open-source-security-vulnerabilities

[8] Report of Review Committee on Open APIs: Promoting Open Innovation. https://www.zenginkyo.or.jp/fileadmin/res/news/news290713_3.pdf

[9] 금융권 오픈API 이용기관 자체 보안점검 가이드, 금융보안연구원 https://www.fsec.or.kr/common/proc/fsec/bbs/147/fileDownLoad/1786.do

〈저 자 소 개〉

나 재 훈 (Jae Hoon Nah)

종신회원

1985년 2월 : 중앙대학교 컴퓨터공학과 학사

1987년 2월 : 중앙대학교 컴퓨터공학과 석사

2005년 2월 : 한국외국어대학교 정보공학 박사

1987년~현재 : 한국전자통신연구원 정보보호연구본부 전문위원/책임연구원

2009년~현재 : ITU-T SG17 WP4 부의장, Q7 라포처

2018년7월~현재 : TC307 대표전문위원

2011년~2012년 : 한국정보보호학회 학회지 편집위원장

2011년~현재 : 한국정보보호학회 학회지 정보보호 국제표준 특집호 책임 편집위원

<관심분야> 블록체인보안, 핀테크보안, P2P보안, 웹메쉬업보안, 익명인증