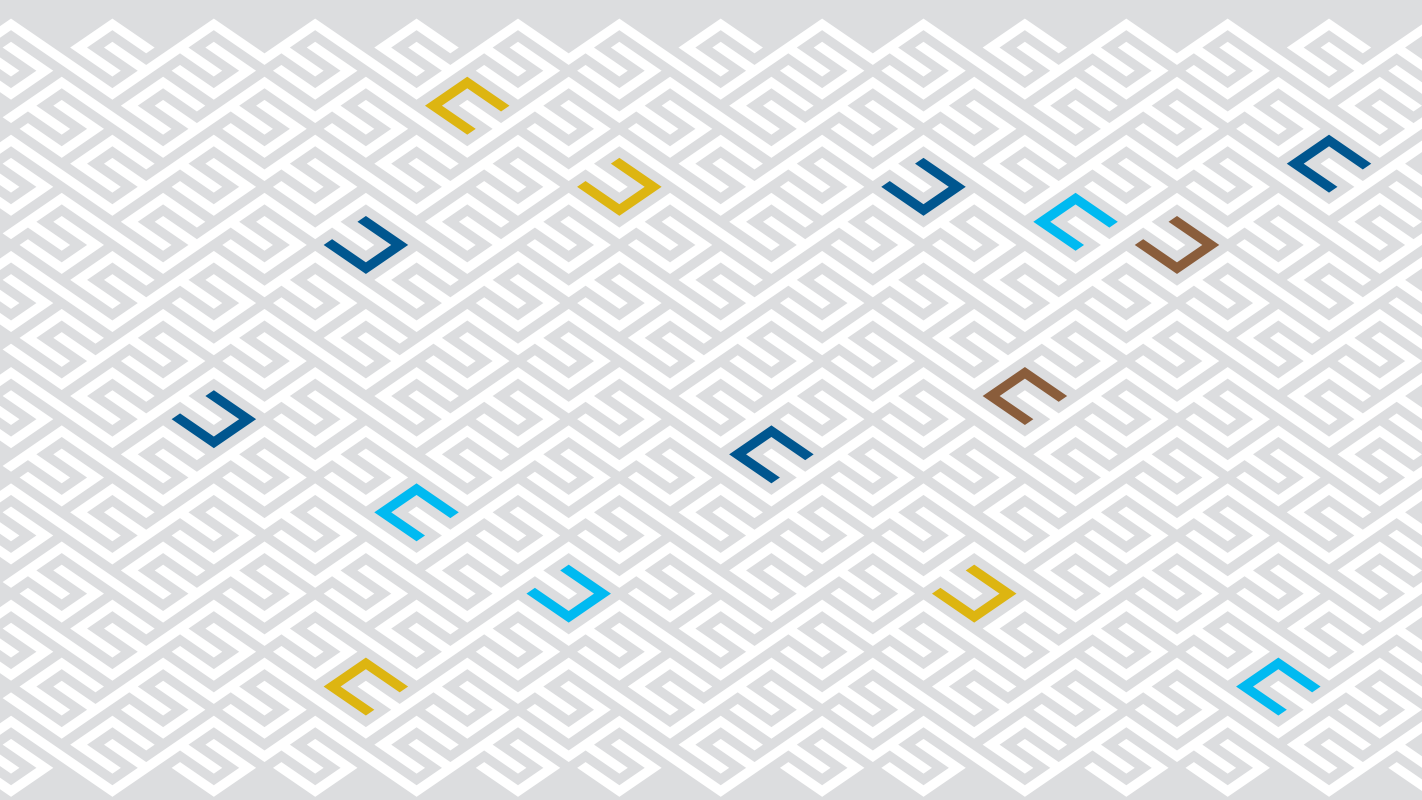


전자금융과 금융보안

E-FINANCE AND FINANCIAL SECURITY



Issue

2016년도 금융 IT·보안 10대이슈 전망보고서

Research

블록체인 활용사례로 알아보는 금융권 적용 고려사항
오픈소스 SW 사용 위험 및 대응 방안
정보보호제품 평가기준 국내외 동향 및 향후 과제

Trend

생체정보를 이용한 금융서비스 현황 비교 분석
OAuth 2.0 개요 및 보안 고려사항



금융보안원
FINANCIAL SECURITY INSTITUTE

본 연구지에 게재된 내용은 금융보안원의 공식 견해가 아니며 연구자 개인의 견해를 밝힙니다. 본 연구지 내용의 무단전재를 금하며, 가공 인용할 때에는 반드시 출처 및 집필자를 명시하여 주시기 바랍니다.

인터넷 홈페이지(www.fsec.or.kr)를 이용하시면 본 연구지에 게재된 자료를 보다 편리하게 보실 수 있습니다.

전자금융과 금융보안

E-FINANCE AND FINANCIAL SECURITY

Issue

- 2016년도 금융 IT·보안 10대이슈 전망보고서

Research

- 블록체인 활용사례로 알아보는 금융권 적용 고려사항
- 오픈소스 SW 사용 위협 및 대응 방안
- 정보보호제품 평가기준 국내외 동향 및 향후 과제

Trend

- 생체정보를 이용한 금융서비스 현황 비교 분석
- OAuth 2.0 개요 및 보안 고려사항

머리말

우리는 지금 금융과 보안 모두가 급속하게 변화해가고 있는 시대를 살아가고 있습니다. 사물인터넷, 클라우드 컴퓨팅, 빅데이터, 모바일, 블록체인 등 혁신적인 기술의 등장으로 그야말로 기술을 지배하는 자가 금융을 지배하는 시대가 도래하고 있습니다.

세계적으로 금융과 ICT부문간 융합을 통한 금융서비스 혁신이 급격히 진전됨과 동시에 국내에서도 금융당국의 규제완화와 핀테크 산업 육성 정책 등에 힘입어 인터넷 전문은행이 등장하고, 최근에는 바이오 인증, 블록체인 기술을 통한 새로운 금융 서비스가 활발하게 도입되거나 검토 추진 중에 있는 등 이용자 중심의 편의성 제고, 금융서비스 시장 확대 및 효율화가 빠른 속도로 진행되고 있습니다.

반면 신·변종 전자금융사기는 결합형으로 나날이 진화하고 있고 크립토락커 등의 랜섬웨어 공격, 진화된 기법을 활용한 DDoS 공격의 지속 시도 등 보안위협 또한 지속적으로 증가하고 있는 것도 사실입니다.

금융과 IT가 융합되는 핀테크 시대에서 금융시장이 신뢰를 받고 금융소비자를 보호하기 위해서는 금융보안이 새로운 선결 과제가 되었습니다.

‘금융보안’이라는 담보 없이는 기술적 발전이나 금융산업이 발전하기 어렵고, 신기술에 대한 최신 보안위협을 적절히 대응하지 못한다면 금융IT융합 발전 또한 기대할 수가 없는 것입니다.

이에 금번 호의 연구보고서에서는 연간 금융 IT·보안 주요 트렌드 분석을 기반으로 주요 이슈를 도출하고 금융보안정책 및 전략 수립 지원을 위한 ‘2016년도 금융 IT·보안 10대 이슈 전망 보고서’를 수록하였습니다.

금융보안원은 금융회사에 다양하고 심도 있는 보안 기술 관련 정보를 제공하여 전자금융과 금융보안의 발전을 위해 지속적으로 분석·연구하는 노력을 지속하겠습니다.

본 연구보고서가 전자금융거래의 안전성과 신뢰성 확보를 통해 전자금융업의 건전한 발전을 위한 기반조성을 이루는데 도움이 되길 바랍니다.

2016년 1월

금융보안원
원장 허창언

Contents

Issue

2016년도 금융 IT·보안 10대이슈 전망보고서	3
-----------------------------------	---

Research

블록체인 활용사례로 알아보는 금융권 적용 고려사항	21
오픈소스 SW 사용 위협 및 대응 방안	43
정보보호제품 평가기준 국내외 동향 및 향후 과제	77

Trend

생체정보를 이용한 금융서비스 현황 비교 분석.....	109
OAuth 2.0 개요 및 보안 고려사항	119

Issue

-
- 2016년도 금융 IT·보안 10대이슈 전망보고서
-

2016 금융 IT·보안


10대 이슈 전망





핀테크 서비스 확대와
보안성 요구 증가



금융거래 정보를 이용한
빅데이터 활성화



바이오인증(FIDO 등)
기술을 활용한 금융서비스 확대




실명확인 방식 전환에 따른
비대면금융거래 확산




금융권 **자율보안체계** 확립과
금융보안거버넌스 강화



블록체인 을 활용한
금융서비스 본격 등장



클라우드 서비스 활성화를 위한
보안 투명성 요구 증대



모바일 및 표적형
랜섬웨어 증가



진화된 기법을 활용한
DDoS 공격의 지속 시도



FDS 구축 확산과
위협정보 공유 확대

2016년도 금융 IT·보안 10대이슈 전망보고서

보안연구부 보안정책팀

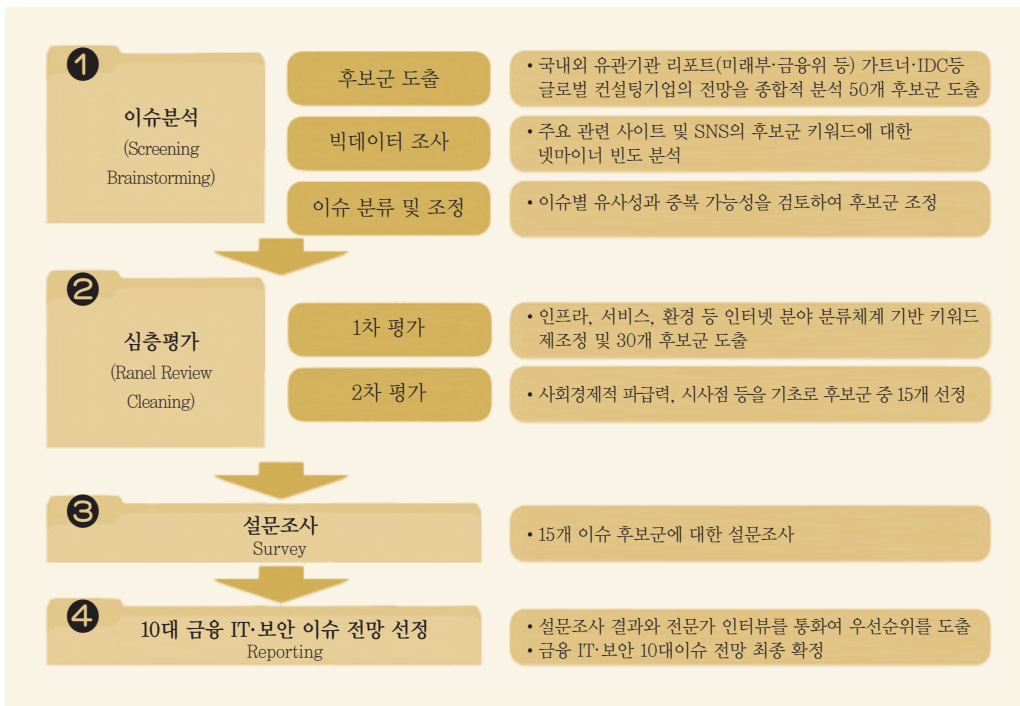
□ 추진목적

- 연간 금융 IT·보안 주요 트렌드 분석을 기반으로 2016년도 10대 이슈 도출을 통해 금융 IT·보안의 정책 방향 및 전략 수립 지원

□ 추진방향

- ‘선정기준 개선’, ‘객관성 및 신뢰성 확보’, ‘주요이슈 전망도출’을 통해 보안담당자는 물론, 최고경영층(CxO)도 관심가질 수 있도록 추진
 - 주제선정에 있어서 보안기술은 물론 정책적 이슈도 적극적으로 고려
 - 흐름 파악은 물론 의사결정에 도움이 될 수 있는 구체적 이슈선정
 - 빅데이터 분석, 전문가 패널 검토를 통해 결과의 신뢰성 확보

□ 단계별 추진방안



□ 2016년 금융 IT · 보안 10대 이슈 전망

※ 노란색은 빅데이터 분석 및 설문조사를 통해 도출된 '이슈 키워드' 명

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 비대면금융거래 확산

5 금융권 자율보안체계 확립과 금융보안거버넌스 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

* 위 표의 순서 구분은 10대 이슈를 나타내기 위함이며, 중요도를 의미하지 않음

1 핀테크 서비스 확대와 보안성 요구 증가

□ 배경

- 다양한 IT 기술과 금융의 융합을 통해 새로운 금융 서비스가 등장하고 핀테크 기업 및 서비스에 대한 리스크 관리 강화 필요성 대두

□ 현황

- 결제·송금분야를 벗어나 투자·대출, 인터넷전문은행, 보험 등 다양한 금융분야에서 핀테크 신규서비스 도입이 예정되어 있음

다양한 핀테크기술분야별 추진현황		
구분	2015년	2016년
인터넷전문은행	예비사업자 인가(11월)	상용서비스 개시(하반기)
생체인식	시범도입(12월, 일부은행)	本格도입(16년, 주요은행)
OPEN API	규격화, 시험·검증(12월, 테스트베드)	本格서비스 제공(하반기)
블록체인 거래시스템	도입방안 내부검토, 핀테크기업과 제휴	외환송금기술 상용화(상반기 목표, S은행)

□ 전망 및 이슈

- (전망) 핀테크 서비스가 간편결제 이외의 다양한 분야로 확대됨에 따라, 사업주체 간 경쟁이 심화되고 신규 보안위협 등장 예상
 - － 금융회사, 핀테크 기업 등 금융서비스 주체의 보안위협에 대한 대응수준에 따라 핀테크 서비스의 경쟁력 확보
- (이슈) 서비스 제공주체 별로 핀테크 서비스는 물론, 신규 보안기술에 대한 투자와 보안성 검증 필요성 증대

2 금융거래 정보를 이용한 빅데이터 활성화

□ 배경

- 금융위원회의 제4차 금융개혁회의('15.6.3)에서 「금융권 빅데이터 활성화 방안」발표를 계기로 금융권은 빅데이터 활용 방안 강구 中

□ 현황

- 해외*는 모든 업권에서 빅데이터가 새로운 방법으로 다양하게 활용되는 반면 국내의 경우 마케팅, 보험사기적발 위주의 초기 활용 단계

* 외국 금융회사는 자동차 운행정보, 기후재난정보 등의 분석을 통해 다양한 금융 상품개발

다양한 핀테크기술분야별 추진현황		
구분	금융회사	주요내용
은행	IBK기업은행	고객감성분석 등 기업이미지 제고에 활용
	SC제일은행	개인 SNS를 이용한 타겟마케팅 활용
보험	삼성화재	도덕적해이 사고 및 고위험군 사고 분석 시스템 개발
	교보생명	위험평가모델을 통한 언더라이팅 업무효율 개선
카드	신한·현대카드	고객마케팅 및 신상품 개발에 활용
	롯데카드	백화점, 마트 등 계열사와 제휴해 마케팅 및 서비스 제공

- 금융보안원은 금융회사와 공동으로 금융거래정보의 빅데이터 활용을 위한 지침 개발 中이며 재식별 가능성을 최소화
- 빅데이터 처리과정에서 개인식별정보 획득에 의한 정보 유출 및 오남용 위협 제기

□ 전망 및 이슈

- (전망) 금융권 빅데이터 활용을 통해 핀테크 기업과 금융회사는 신규 서비스 발굴, 고객 맞춤형 서비스 제공 등 서비스 다양화
- (이슈) 금융권 빅데이터가 점진적 활용 확대를 위하여 정보보호법령상 명확화, 투명한 인프라 운영, 금융회사의 기술적·관리적 비식별화 방안 마련을 통한 정보 유출 및 오남용 위협에 대응

3 바이오인증(FIDO 등) 기술을 활용한 금융서비스 확대

□ 배경

- 스마트폰 등 IT기기의 발전으로 지문정보를 활용한 비대면 본인인증 서비스가 금융 거래*에 활용되면서 금융권 도입 검토 활발

* 애플 스마트폰의 지문 인증 및 결제, 삼성 갤럭시 S6의 삼성페이

□ 현황

- 금융거래시 바이오정보를 활용하여 본인식별 또는 본인인증 등 기존 공인인증서*, 결제 비밀번호 대체 수단으로 일부 활용

* KISA, 웹 표준 전환 성과 발표회-지문인식 및 공인인증서 연계 기술 발표('15.12.17)

- 생체인증(정맥, 홍채 등)을 통해 기존 금융업무를 무인화기기가 대신하거나, 카드 또는 통장 없이 ATM이용 등 금융권 생체인증 도입 추진

금융권 바이오인증 도입 사례	
금융회사	주요내용
신한은행	정맥으로 본인 인증 확인하는 셀프뱅킹 서비스
기업은행	홍채를 인증 자동화기기(ATM) 시범 운영
NH농협은행	비대면 마케팅 채널로 생체인증을 활용한 상품 가입 서비스
메트라이프 생명	성문(음성)인식 방식을 활용한 콜센터 상담 활용
신용카드회사	스마트폰의 지문인식을 활용한 카드결제 서비스

□ 전망 및 이슈

- (전망) 보안업체의 바이오인증 기반 다양한 솔루션 출시*와 전자금융거래시 바이오인증 도입이 금융권 전반으로 확산

* 필기서명인증, 목소리인증, 지문인증 등 FIDO를 기반으로 한 인증 솔루션이 출시 예정

- (이슈) 바이오정보의 안전한 저장·관리를 위한 보안 가이드 마련, 금융사별 다양한 생체 기술 도입시 고객정보 관리 효율화, 기존 인증기술(공인인증서)과 융합시 금융 표준화 요구 증대 예상

4 실명확인 방식 전환에 따른 비대면금융거래 확산

□ 배경

- 금융당국은 국내 핀테크 산업 활성화 정책의 일환*으로 금융거래를 위한 실명확인 시 다양한 비대면실명확인 방식**을 허용함으로써 소비자 편의 제고 및 본격적인 핀테크 산업 활성화 추진

* 「금융거래시 실명확인방식 합리화방안」(‘15.5.18.)

** ①신분증 사본 제출 ②영상통화 ③접근매체 전달시 확인 ④기준계좌 활용 ⑤기타(바이오) 중 2가지 필수
(권고 : ⑥타기관 확인결과 활용, ⑦개인정보 검증 중)

□ 현황

- ‘15년 12월에 은행권의 계좌개설 등 비대면실명확인 서비스 개시 시작으로 ‘16년 증권사와 저축은행 등 제2금융권에서도 창구 방문 없이 계좌 개설과 같은 금융업무 가능
- ‘16년 지점 방문 없이 스마트폰 등으로 모든 은행 업무를 이용하는 인터넷 전문은행 신규 도입

* ‘15년 11월, 한국카카오뱅크와 케이뱅크 예비인가

□ 전망 및 이슈

- (전망) 비대면실명확인 서비스가 도입 확산됨으로써 비대면 계좌개설 등 고객 편의가 제고되고, 다양하고 차별화된 금융서비스에 활용됨으로써 핀테크 산업 활성화에 기여
- (이슈) 신분증 사본 및 개인정보 유출방지를 위한 보안대책 강화 요구, 명의도용 및 대포통장 확산 등 금융사기 방지를 위해 FDS 활용 등 사후 대응 체계 강화 요구

5 금융권 자율보안체계 확립과 금융보안거버넌스 강화

□ 배경

- 금융위·금감원은 금융개혁의 일환으로 각종 규제를 완화하고, 보안규제의 패러다임을 사전규제에서 사후 점검 및 책임강화로 전환

최근 전자금융 관련 규제 완화 내용	
규정 개정 내용	시행일
매체분리 원칙 폐지, 보안프로그램 설치 의무 폐지	'15. 2월
공인인증서 사용의무 폐지, 인증방법평가위원회 폐지, 국가기관 인증 정보보호제품 사용의무 폐지	'15. 3월
금감원 보안성심의 의무 폐지	'15. 6월

□ 현황

- 금융당국은 「금융IT부문 자율보안체계 확립방안*」을 마련('15.6)하고, 금융회사는 자체 보안성 검토 등 자율적 보안 강화 추진
 - * 자체 점검 및 책임 강화, IT보안 역량 향상 유도, 감시체계 강화
- 일부 금융회사는 자체점검·내부통제 및 보안역량 강화 등을 통해 금융보안거버넌스* 체계 확립하여 운영 중에 있음
 - * 금융회사의 전사적인 금융보안을 위해 최고경영층과 보안실무조직, 본점·영업점 등 현업 조직 간의 상호 협력을 통한 적극적인 정보보호 활동

□ 전망 및 이슈

- (전망) 금융회사의 책임과 역할의 강화가 요구되고 최고경영층, CISO, 보안실무조직, 본점·영업점 등 현업조직 간의(전사적) 정보보호거버넌스 활동 확대 예상
- (이슈) 금융보안거버넌스 강화를 위한 세부 실행방안* 마련과 금융회사 규모별·권역별 자율보안 실행역량 확보 방안 요구
 - * 정보보호 조직과 전사적 조직간 협업체계 구축 방법, 위협관리 방법, 투자와 성과관리 방법, 내·외부보안감사 방법, 정보보호 수준 평가 등

6 블록체인을 활용한 금융서비스 본격 등장

□ 배경

- 분산식 원장 기술(distributed ledger technology)을 사용하는 블록체인은 높은 보안성, 거래내역의 투명성, 비용절감 등의 장점으로 글로벌 금융시스템의 새로운 기회로 부상

* ICT업계 종사자 대상 설문조사에서 응답자의 58%는 2020년 중반에 이르러 전세계 GDP의 10%가 블록체인 분야에서 창출될 것으로 예상(2015 survey, World Economic Forum)

□ 현황

- 블록체인은 가상화폐(Bitcoin)에서부터 시작되어 P2P대출, 거래인증 등 최근 핀테크 기술과 융합되어 다양한 분야에 활용

구분	내 용
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 빌려 줌으로써 발생하는 수익을 개인 투자자들에게 분배해주는 서비스. 투자자 및 대출자의 금전은 블록체인을 이용하여 투명성 및 신뢰성을 보장함
주식 거래 (거래 인증)	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 기술을 사용하여 기존에 비해 10분의 1 수준의 수수료 부과

□ 전망 및 이슈

- (전망) 블록체인 기술의 분산성, 보안성, 무결성 등의 특징을 바탕으로 클라우드 펀딩 등 새로운 금융서비스 응용에 활발히 적용되고, 기존 금융 인프라와 보안기술을 보완하는 방식으로 발달 예상
- (이슈) 블록체인 기술 등 새로운 기술 수용을 위한 규제 완화 검토가 필요하며, 블록체인의 활용 분야 및 기술 수용의 방법론* 선택에 있어 금융회사의 비즈니스 목적과 규모에 맞추어 도입 필요

* 독자적인 블록체인 기술 실험 참여 또는 스타트업과 파트너십 등

7 클라우드 서비스 활성화를 위한 보안 투명성 요구 증대

□ 배경

- 정부는 산업 전반의 비용절감 및 생산성 향상뿐만 아니라 클라우드를 기반으로 금융, 의료, 교육, 방송 등 다양한 분야에서 신규 융합서비스가 창출될 수 있도록 클라우드 발전법('15년9월) 시행

□ 현황

- 해외의 경우 클라우드 서비스가 금융거래 데이터 분석, 위험관리 업무, 직원간 협업 등 다양한 목적으로 활용
- 국내 금융권의 경우, 장애, 보안에 대한 우려와 규제와 같은 불안요소로 인해 클라우드 서비스 활성화가 부진한 상황

□ 전망 및 이슈

- (전망) 공공부문의 클라우드 서비스 도입 활성화와 더불어 금융회사는 수익성 하락에 따른 관리비용 절감과 상품서비스 경쟁력 향상을 위한 방안으로 도입 증가 예상

* 빅데이터(Big Data) 분석 및 협업, 개인정보 보호 기술에 활용 등

- 금융부문은 '가상화(Virtualization)' 방식으로 전산센터를 제외한 현업·영업점의 논리적 망 분리가 지속적으로 증가하고 있는 추세
- (이슈) 클라우드 도입 활성화를 위한 금융당국의 여러 규제 완화 요구, 서비스 장애 대응 및 보안성 확보를 위한 인증제의 수요 증가 예상
 - 클라우드서비스 제공자의 경우, 보안 책임 분할/소재의 명확한 규명, 보안관리 및 보안정책의 구체적인 적용 방안 고려
 - 금융회사의 경우, 물리적 기반의 보안기술들과 클라우드 환경에 필요한 보안기술들의 안정적인 통합 가능성 고려

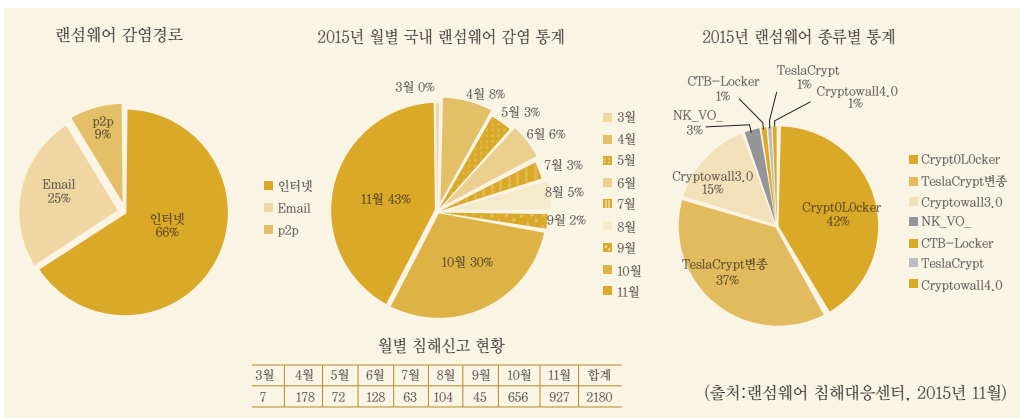
8 모바일 및 표적형 랜섬웨어 증가

□ 배경

- 최근 랜섬웨어의 공격대상이 PC 기반에서 모바일 기기로 확대되고, 공격방식 또한 대규모 공격에서 표적형 공격으로 지능화되는 추세

□ 현황

- 올해 4월 한글버전 크립토락커 유포를 기점으로 증가세를 나타내며, '15년 10월, 11월 두 달간 변종 랜섬웨어의 공격으로 피해 급증



- 랜섬웨어의 유포방식이 드라이브 바이 다운로드, 이메일, 애드웨어 광고 서버 등으로 다양화

□ 전망 및 이슈

- (전망) 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 전망
- (이슈) 무작위로 개인을 낚던 랜섬웨어가 표적형으로 진화하여 금융회사 및 정부로 타겟 확장이 예상되며, 표적형 공격에 대응하기 위한 공동대응체계 강화 필요

9 진화된 공격 기법을 활용한 DDoS 공격의 지속 시도

□ 배경

- 각 기관 및 국가적 유기적인 대응체계 운영에도 불구하고 새로운 DDoS 공격기법과 공격 규모의 증가로 인해 공격 피해가 끊임없이 지속

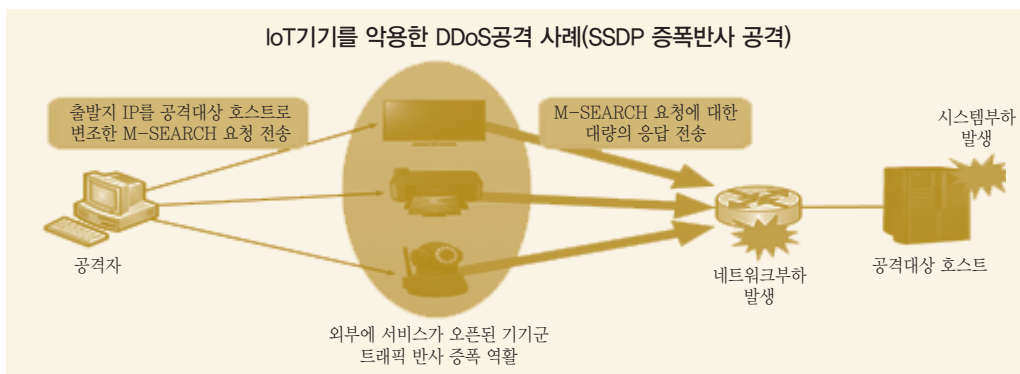
2015년 주요 DDoS공격 사례

구 분	시 기	대 상	특 징
DD4BC 해킹그룹	15년 6월, 7월	한국 (은행, 증권사)	- SSDP, NTP 등 UDP 증폭반사 공격 시도 - 공격 중지 대가로 비트코인 지불 요구
XOR, DDoS 봇넷	15년 8월, 9월	아시아 (교육, 게임사)	- Syn, DNS Flooding 공격 시도 - 리눅스 악성코드를 이용한 DDoS 봇넷 이용
Armada 해킹그룹	15년 10월, 11월	태국, 그리스 (은행)	- DD4BC를 모방한 DDoS공격 해킹그룹

□ 현황

- 최근 DDoS 공격의 특징은 공격 영향력의 강도와 빈도 측면에서 여전히 증가 추세, DDoS 공격에 IoT기기* 활용이 증가

* 무선랜공유기, 네트워크 프린터 등 IoT 기기들이 DDoS 공격에 쓰이기 시작



□ 전망 및 이슈

- (전망) 다양한 산업영역에서 사물인터넷(IoT)형 단말 장치의 사용이 증가함에 따라 사이버 공격 도구로 이용이 예상
- (이슈) 금융사도 보안위협 대응을 위해 IoT 기기의 관리방안 마련이 요구되며, 다양한 장치를 매개로한 DDoS 증폭 공격 시도에 대비 필요

* DDoS 공격에 대비하여 금융보안원에서 디도스 비상대응센터를 운영 중

10 FDS 구축 확산과 위협정보 공유 확대

□ 배경

- 금융회사는 공인인증서 등 한정된 보안수단만으로는 지능화된 이상금융거래 대응에 한계를 노출
- 개별 금융회사의 FDS 운영을 통해 파악된 사고정보 및 이상금융거래 등 사고예방을 위한 위협정보 공유가 필요

□ 현황

- 고도화되는 전자금융사고에 보다 적극적이고 효과적으로 대응할 수 있도록 FDS 도입·구축 확산 중
 - * 금융전산보안강화 종합대책(금융위원회, '13.7)을 통해 은행, 증권 등으로 FDS 확대 구축 권고를 통해 금융회사 본격 구축
- 금융보안원은 전사적 금융권 공동대응을 위해 위협정보를 공유 할 수 있는 이상금융거래정보 공유시스템 구축을 완료

□ 전망 및 이슈

- (전망) 금융권의 FDS 구축 확대 및 이상금융거래정보 공유시스템 구축·운영으로 위협정보에 대한 신속한 공유를 통해 사고예방 및 피해확산 방지에 크게 기여할 것으로 기대
 - 금융고객의 특성상 다수의 금융회사와 거래하고, 편의상 비밀번호를 유사하게 사용하는 경우가 많아 사고 예방에 효과가 클 것으로 예상
- (이슈) 위협정보 공유를 위한 후속절차(개인정보 수집동의 등) 및 정보공유 활성화를 위한 제도적 기반 조성 필요

참고 주요 용어 해설

○ FIDO(Fast Identity Online)

온라인상에서 아이디, 비밀번호 없이 지문, 홍채, 정맥 등 생체인식만으로 보다 간편하게 인증을 처리하는 표준규격을 의미하며 제조자, 서비스사로 구성된 FIDO얼라이언스에서 관련 규격을 제정

○ 금융보안거버넌스

국제표준 정보보호 거버넌스(ISO/IEC 27014)를 기반으로 금융회사의 전사적인 금융보안을 위해 최고경영층과 보안실무조직, 본점·영업점 등 현업 조직 간의 상호 협력을 통한 적극적인 정보보호 활동

○ 블록체인

분산 데이터베이스의 한 형태로, 지속적으로 성장하는 데이터 기록 리스트로서 분산 노드의 운영자에 의한 임의 조작이 불가능하도록 고안, 잘 알려진 블록체인의 응용사례는 암호화폐의 거래과정을 기록하는 탈중앙화된 전자장부로서 비트코인이 있음

○ 랜섬웨어(ransom ware)

인터넷 사용자의 컴퓨터에 잠입해 내부의 파일 등을 암호화해 열지 못하도록 만든 후 돈을 보내주면 해독용 열쇠 프로그램을 전송해 준다면 금품을 요구하는 악성 프로그램

○ DDoS 공격(Distributed Denial of Service Attack)

인터넷 사이트에 '서비스 거부(DoS)'를 유발하는 해킹 기법으로, 대규모의 접속 통신량(트래픽)을 한꺼번에 일으켜 서비스 체계를 마비시키며 불특정 다수의 컴퓨터에 악성 컴퓨팅 코드인 '좀비(Zombie)'를 퍼뜨린 뒤 DDoS 공격에 이용하는 게 특징

○ DD4BC(DDoS for BitCoin)

유럽소재 해킹그룹으로 2014년부터 대규모 비트코인 갈취 공격을 벌인 DD4BC 그룹은 최근 1년 사이 DDoS 공격 범위를 금융기관뿐 아니라 미디어/엔터테인먼트, 온라인 게임, 유통 등 보다 다양한 산업으로 확대

○ FDS(Fraud Detection System)

전자금융거래에 사용되는 단말기 정보 · 접속 정보 · 거래내용 등을 종합적으로 분석하여 의심거래를 탐지하고 이상금융거래를 차단하는 시스템

○ Open API(Open Application Programming Interface)

누구나 사용할 수 있도록 공개된 API. 응용 프로그램을 쉽게 만들 수 있도록 준비된 프로토콜, 도구 같은 집합으로 운영 체제의 상세한 기능은 몰라도 공개된 몇 개의 API만으로 쉽게 응용 프로그램 개발이 가능

Research

- 블록체인 활용사례로 알아보는 금융권 적용 고려사항
- 오픈소스 SW 사용 위협 및 대응 방안
- 정보보호제품 평가기준 국내외 동향 및 향후 과제

블록체인 활용 사례로 알아보는 금융권 적용 고려사항

한 승 우*

I. 서론	23
II. 블록체인 개요	24
1. 블록체인의 개념	24
2. 블록체인 분류	26
III. 블록체인 활용 사례	27
1. 암호화 화폐	27
2. 주식거래(장외시장)	30
3. 전자 공증	31
4. 스마트 계약(Smart Contract)	32
5. IoT(사물인터넷)	33
IV. 금융권 적용 고려사항	35
1. 클라이언트 보호	35
2. 노드유지	36
3. 확장성	38
V. 결론	41
〈참고문헌〉	42

* 금융보안원 보안연구부 보안기술팀(e-mail : swan@fsec.or.kr)

요 약

블록체인은 분산 데이터베이스라고도 불리며, 기존 중앙집중형 네트워크 기반의 인프라를 뛰어넘는 높은 보안성, 확장성, 투명성 등을 보장하기 때문에 큰 관심을 받고 있다.

블록체인은 네트워크 접근 권한 및 증명 작업 참여 권한에 따라 별도의 권한이 필요 없는 공개형 블록체인, 네트워크 접근은 자유로우나 증명 작업에는 권한이 필요한 반공개형 블록체인, 네트워크 접근 및 증명 작업에 권한이 필요한 비공개형 블록체인이 있다.

주로 암호화 화폐에서 많이 활용되고 있으며, 초기 비트코인이 개발되고 소스코드가 공개되었기 때문에 이를 바탕으로 유사한 암호화 화폐가 등장하였다. 증권시장에서는 블록체인을 활용한 거래소를 만들어 장외주식을 거래 할 수 있도록 시스템을 구축하였다. 이외에도 전자 공증 시스템, 스마트 계약, 사물인터넷 분야에서도 별도의 블록체인을 이용하거나 비트코인의 블록체인을 이용한 서비스를 선보이고 있다.

금융권에서도 블록체인 기술을 도입하기 위해 세계적인 은행들이 컨소시엄을 구성하여 기술 개발 및 표준화 작업을 진행하고 있다. 국내 금융권에서도 기존 시스템을 대체하기 위한 연구가 진행중이다.

하지만 블록체인 및 활용 기술에 대한 규제로 인해 기술 개발 및 도입이 지연되고 있으나, 규제 개선과 실험적인 기술 개발을 통해 안정적인 블록체인 네트워크 생태계가 마련될 것으로 예상된다.

I. 서론

분산화된 디지털 통화의 개념은 오래전부터 알려졌으나 큰 주목을 받지 못하였다. 1998년 마이크로소프트 연구원이었던 Wei Dai가 제안한 b-money는 분산합의와 계산 퍼즐을 풀게하는 방식을 통해 화폐를 발행하는 아이디어를 최초로 제안하였지만, 실제 구현에 대해서 자세한 방법을 제시하지는 못했다. 2005년 미국의 컴퓨터 과학자였던 Hal Finney가 재사용 가능한 작업증명(Proof-of-Concept) 개념을 소개하였으나, 외부의 신뢰를 필요로 하는 컴퓨팅을 기반을 두는 개념에 대해 구현하지 못하였다.

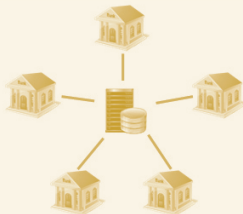
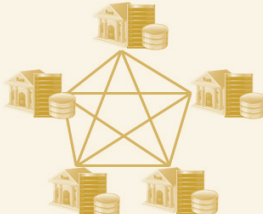
결국 2009년 사토시 나카모토(Satoshi Nakamoto)에 의해 처음 실제로 구현된 탈중앙화된 화폐는 공개키 암호방식과 소유권 관리를 위한 작업증명이라고 알려진 합의 알고리즘이 결합되어 가능하게 되었다. 그것이 바로 비트코인(Bitcoin)이다.

처음에는 주목을 받지 못하였으나, 비트코인을 활용하여 외화송금 서비스가 개발되고 화폐와 같이 물품 구매 등이 가능해짐에 따라 관심을 받게 되었다. 더불어 비트코인 거래를 저장하는 블록체인(BlockChain)에 대한 관심이 커졌는데 이는 기존의 인프라에 비해 안전한 서비스를 제공하고, 비용 절감 측면에서도 효과적이기 때문이다.

비트코인에 대한 전망을 가늠할 수는 없지만, 블록체인에 대한 기술만큼은 무엇보다도 전망이 밝다. 본 보고서에서는 블록체인에 대한 개념과 이를 활용한 사례를 소개하고, 금융권에 적용하기 위해 고려해야 할 사항들에 대해 알아보하고자 한다.

블록체인은 분산 데이터베이스(Distributed Database)라고도 불린다. 기존의 중앙집중형(Centralized) 데이터베이스는 하나의 데이터베이스에 모든 정보를 관리하므로 장애 발생 시 서비스가 불가능하다. 하지만 분산 데이터베이스는 동일한 정보가 담긴 블록체인(파일)이 각각의 네트워크 참가자들에 의해 분산되어 저장·관리되므로 장애가 발생하더라도 가용성(Availability)에 문제가 발생하지 않는다.

[표 1] 중앙집중형, 분산형 데이터베이스 비교

구 분	중앙집중형 데이터베이스	분산형 데이터베이스
구조		
장점	<ul style="list-style-type: none"> · 빠른 거래 속도 · 제어(통제)가 용이함 	<ul style="list-style-type: none"> · 거래의 투명성 · 낮은 구축비용과 확장이 용이
단점	<ul style="list-style-type: none"> · 중앙시스템에 대한 보안 위협 · 높은 관리 비용 발생 	<ul style="list-style-type: none"> · 상대적으로 느린 거래 속도 · 제어의 복잡성

블록체인이 주목을 받는 이유는 신뢰되지 않은 네트워크에서 거래정보를 투명하게 공개하여, 다수의 네트워크 참여자가 공개검증을 수행하므로 공증 주체가 필요 없다는 것이다. 또한, 기존 시스템의 보안 위협과 이를 보호하기 위해 투자되는 비용 등 단점으로 여겨지는 부분을 보완할 수 있다는 점이 가장 큰 장점이다.

[표 2] 블록체인 기술의 장점

구 분	장 점
탈중앙성(P2P based)	공인된 제 3자의 공증 없이 개인 거래 가능
보안성(Secure)	정보를 다수가 공동으로 소유하므로 해킹이 어려움
확장성(Scalable)	공개된 소스에 의해 쉽게 구축·확장 가능
투명성(Transparent)	모든 거래기록에 공개적 접근 가능

자료 : The Fintech 2.0 Paper(Santander, 2015) 재구성

2. 블록체인의 분류

블록체인 네트워크 접근 및 증명 작업 참여 권한에 따라 공개형(Public), 비공개형(Private), 반공개형(Regulated 혹은 Consortium) 3가지로 구분된다.

1) 공개형(Public) 블록체인

현재 가장 일반적으로 이용되는 유형으로 개인 또는 중앙기관 등 어떠한 제약사항 없이 블록체인 네트워크에 참여하여 이용 할 수 있다. 네트워크 참여자들은 컴퓨팅 파워를 이용하여 거래의 정당성을 입증 할 수 있으며, 네트워크에 참여하지 않지만 애플리케이션을 통해 이용자 거래 시 이용될 수 있다. 비트코인이 가장 대표적인 활용 사례이다.

2) 비공개형(Private) 블록체인

개인화된 블록체인으로써 한 중앙기관이 모든 권한을 가지며, 네트워크에 참여하기 위해서는 허가가 필요하다. 한 기관에 권한이 부여되어 있으므로, 규칙변경, 기록 되돌리기 등 기존의 인프라와 유사하다. 또한, 인프라 구축을 위한 비용 절감과 효율성 향상 등의 특징이 존재한다. 나스닥의 비상장 주식거래소 플랫폼인 링크(Linq)가 대표적 활용 사례이다.

3) 반공개형(Regulated 혹은 Consortium) 블록체인

공개형 블록체인과 비공개형 블록체인이 결합된 형태의 성격으로서, 네트워크에 참여하는 것은 자유로우나 미리 선정된 참여자에 의해서 제어된다. n개의 참여자에게 권한을 부여하여 각 참여자의 동의에 의해서 거래를 기록하도록 한다. 일반 이용자들에게는 기록을 열람할 수 있도록 권한을 부여 할 수 있지만, API를 통해 특정 대상에게만 공개할 수도 있다. 일부 기업이나 기관 등의 협업을 위해 컨소시움을 구성하는 모델이 이에 해당될 수 있다.

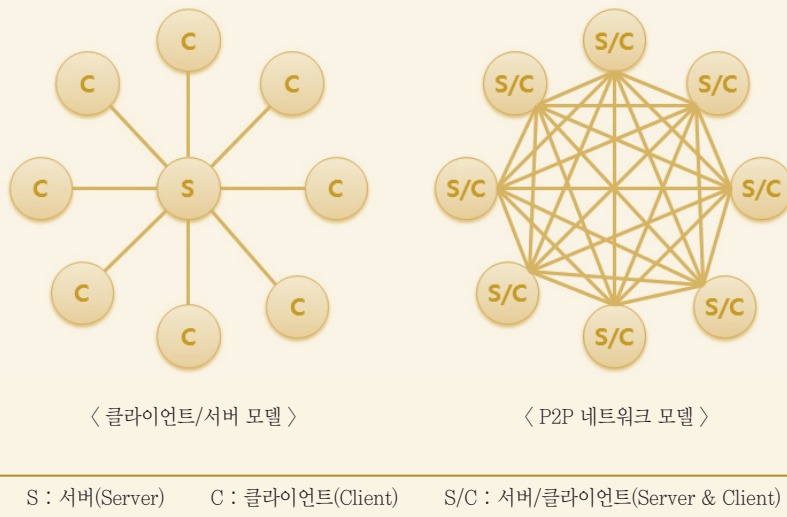
Ⅲ. 블록체인 활용 사례

1. 암호화 화폐

암호화 화폐는 블록체인의 대표적인 활용 사례로 꼽히며, 그 중 비트코인이 가장 큰 가치로 평가되고 있다. 비트코인은 사토시 나카모토란 가명의 프로그래머(또는 집단)에 의해 2009년 처음으로 소개되었다. 중앙기관의 개입을 배제하기 위해 P2P(Peer to Peer) 네트워크²⁾ 기술을 이용하여 거래 기록의 보관, 거래의 최종 승인 등을 네트워크 참여자들이 공동으로 수행하게 만들었다. 이는 분산 컴퓨팅 분야에서 난제로 여겨져 오던 ‘비잔틴 장군 문제’의 해결책으로 제시된 것으로, 제 3의 공인기관이 없이도 당사자 간 메시지를 교환할 수 있는 신뢰를 구축한 것이라고 할 수 있다.

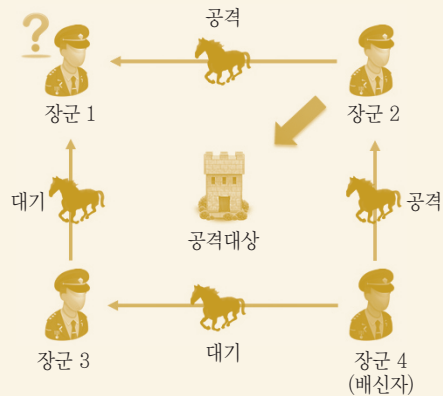
[그림 2]

네트워크 개념도



2) 네트워크 참여자들(Peer Nodes)은 서버와 클라이언트의 역할을 동시에 수행하며, 데이터나 주변 장치 등을 공유하는 방식으로 주로 파일 공유 등의 널리 이용되는 기술이다.

비잔틴 장군 문제



비잔틴 장군 문제(Byzantine Generals Problem)는 1982년 Leslie Lamport 등 3명의 컴퓨터공학자가 마이크로소프트의 의뢰를 받아 연구를 수행하여 발표한 논문³⁾에서 최초로 정식화한 문제이다.

해당 논문에서 중앙통제 시스템이 없는 상황에서 네트워크 참여자간 통일된 의사 결정을 위한 합의(Consensus)를 도출해야 하는 문제를 다음과 같이 가상의 상황으로 설명하였다.

“비잔틴 군대의 여러 부대가 적군의 도시 외곽에 진을 치고 있다. 각 부대를 대표하는 장군이 부대를 통솔한다. 장군들은 오로지 연락병을 통해서만 서로 연락할 수 있다. 적군의 동태를 살핀 다음, 장군들은 합동작전 계획을 결정해야 한다. 그렇지만, 장군들 가운데에는 배신자가 섞여 있을 수도 있고, 그들은 다른 장군들이 합의에 이르지 못하게 하려 한다.”

각 부대의 장군들이 한자리에 모여서 의사 결정을 할 수 없는 상황에서 어떻게 하면 합동 공격시간을 ‘합의’하여 출격할 수 있을지 문제화 하였다. 비트코인은 분산 컴퓨팅 분야에서 발생할 수 있는 이 문제를 작업증명과 블록체인을 도입하여 해결하였다.⁴⁾

네트워크 참여자들은 채굴(Mining)⁵⁾을 통해서 자체적인 화폐인 비트코인(BTC로 표기)⁶⁾을 얻을 수 있으며, 추가적으로 거래 발생 시 블록에 저장할 때 일정량의 수수료를 얻는다.

3) Lamport, L.; Shostak, R.; Pease, M. (1982). “The Byzantine Generals Problem”. ACM Transactions on Programming Languages and Systems 4 (3): 382?401

4) LG경제연구소 김건우 선임연구원, “비트코인, 화폐 논쟁을 넘어 플랫폼으로서의 잠재력 부상 중”

5) 채굴(Mining)이란 특정 조건을 만족하는 해시 값의 앞 부분의 ‘0’개수 보다 많은 0을 가진 해시 값을 만족하는 넌스 값을 찾는 과정

네트워크에 참여하지 않더라도 일반 이용자는 비트코인 지갑을 통해 거래를 할 수 있으며, 공개키 기반 암호화 기술을 통해 은행계좌와 같이 이용될 수 있는 공개주소(Public Address)를 만들어 비트코인을 거래할 수 있다. 거래 정보는 네트워크 참여자들에게 공개 검증 후 블록에 저장되며, 모든 거래 기록들은 공개되어 있으므로 거래 내역을 확인 할 수 있다.

[그림 3]

비트코인 거래 내역

1M1iLA2VNuzXBem7WXLgj6UkYr2MpgWmaH	0.32243114 BTC
▼	
1Fnq8w1VWmpUwyGBUbpvkmwt4jQrurHNw5	0.0035 BTC
1EwwQT9jsRizqv5GjjQXjHbnY4xMzPF3Dt	0.0591 BTC
1DL0Hbs1xVfM6VZFZEgReDHdgxbrpi1gF	0.0024 BTC
1FXnDykYFCIPy9jmxqXqjLTGQX4G151oE	0.0048 BTC
18qUkNjKuejKUGg8gRLjwZf6zGpweq5Pte	0.16 BTC

비트코인 등장 초기에는 지급수단으로 인정하는 곳이 매우 제한적이었으나, 현재는 온·오프라인 구별하지 않고 다양한 분야에서 이용되고 있다. 하지만 익명성과 규제가 적용되지 않아 탈세, 자금세탁 등 악용될 수 있기에 우려의 목소리가 나왔다. 실제 2013년 10월, 마약과 총기류 등 각종 불법 거래를 중계하는 세계 최대 사이트인 실크로드(SilkRoad) 관리자가 FBI에 체포되고 사이트가 폐쇄되었다. 해당 사이트에서는 거래 시 비트코인만을 결제 수단으로 이용하도록 하였다. 랜섬웨어(Ransomware)⁷⁾도 비트코인을 대가로 요구하며, 익명성을 악용하기도 한다. 또한, 비트코인 거래소를 대상으로 해킹을 통해 비트코인을 훔치는 등 끊임없이 해킹 사고가 발생함에 따라 보안성 문제가 대두되고 있다.

6) 보조단위로 밀리코인(0.001 BTC, mBTC로 표기), 마이크로코인(0.000001 BTC, μ BTC로 표기) 및 사토시(0.00000001BTC, satoshi로 표기, 최소단위)가 존재

7) 랜섬웨어란 몸값(Ransom)과 제품(Ware)의 합성어로 이용자 PC의 파일(문서)을 '인질'로 잡고 돈을 요구한다고 하여 붙여진 명칭으로, 익명성 거래가 가능한 비트코인을 요구한다.

2. 주식거래(장외시장)

증권시장에서는 기존의 장외주식과 같이 공식 채널을 이용하지 않고 거래가 이루어지는 비상장주식을 거래하기 위해 블록체인을 활용하고자 한다. 비상장 주식은 공식 채널을 통해 거래가 발생하는 것이 아니며, 기업 정보가 잘 알려져 있지 않아 투자의 어려움이 존재하였다. 국내의 경우, 비상장 주식의 거래는 개인 혹은 브로커를 통해 이루어지므로 사기의 위험성에 언제나 노출되어 있었다. 해외의 경우에는 비상장 주식 거래 시장이 비교적 잘 이루어져 있으나, 비상장 주식 거래를 위해서 일일이 변호사에게 거래를 승인을 받아야 하므로 상당한 시간이 소요되었다.

비상장 주식 시장의 활성화는 벤처기업의 성장과 나아가 국가 경제에도 영향을 미칠 수 있는 부분이다. 나스닥(NASDAQ)은 비상장 기업들의 주식 거래를 위한 플랫폼인 링크(Linq)에 블록체인을 도입하여, 체인닷컴(Chain.com) 등 6개社 비상장기업의 주식을 대상으로 전자증권 발행 서비스를 실시한 바 있다. 다만 기존의 비트코인의 블록체인과는 연계되어 있지 않다는 점으로 미루어보아 개별적인(Private) 블록체인으로 구성된 것으로 보인다.

국내에서도 비상장 주식 유통 플랫폼을 만들어 스타트업이나 비상장기업 등을 대상으로 투자자(주주)에게 전자증권을 발행할 수 있도록 하였으며, 블록체인의 활용으로 시스템 구축 및 보안 투자 비용절감과 투자의 투명성을 확보하였다.

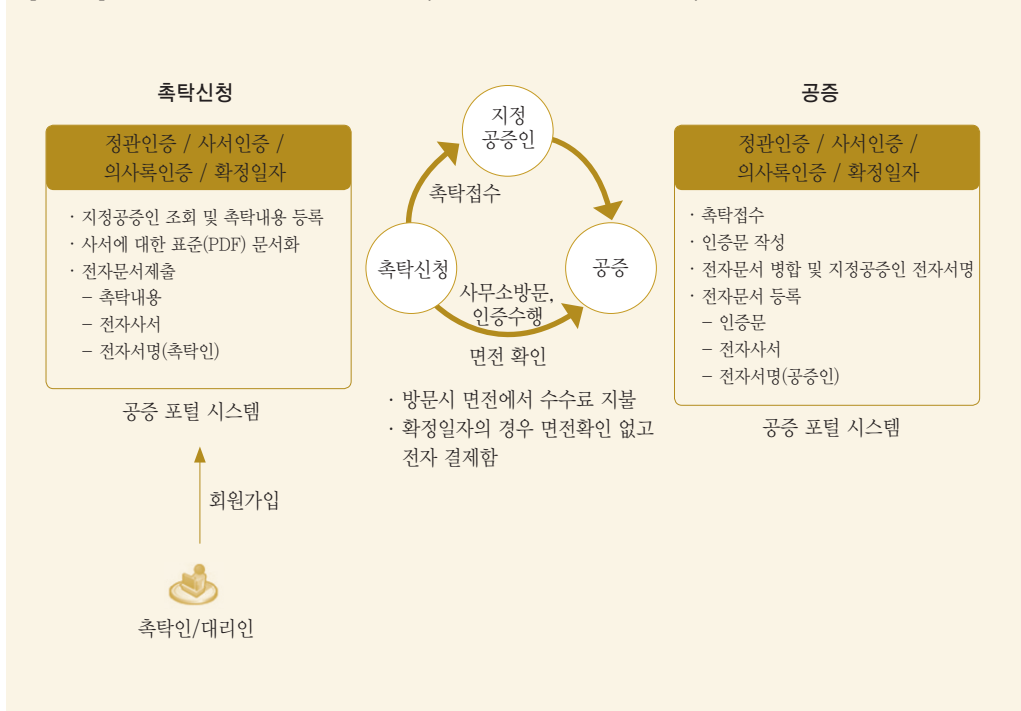
[그림 4] 블록체인 기반 금융상품 오픈 플랫폼 및 서비스 참여자 구성(자료:LG CNS)



3. 전자 공증

전자문서에 의한 다자간 거래 시 발생하는 분쟁 해결을 위한 증명기능으로써, 전자 문서가 변경되지 않았음을 증명한다. 주로 시점확인(타임스탬프)과 해시 함수를 이용하여 증명하며, 인증서, 계약서 등 공적 증명이 필요한 문서 또는 각종 파일들에 적용할 수 있다.

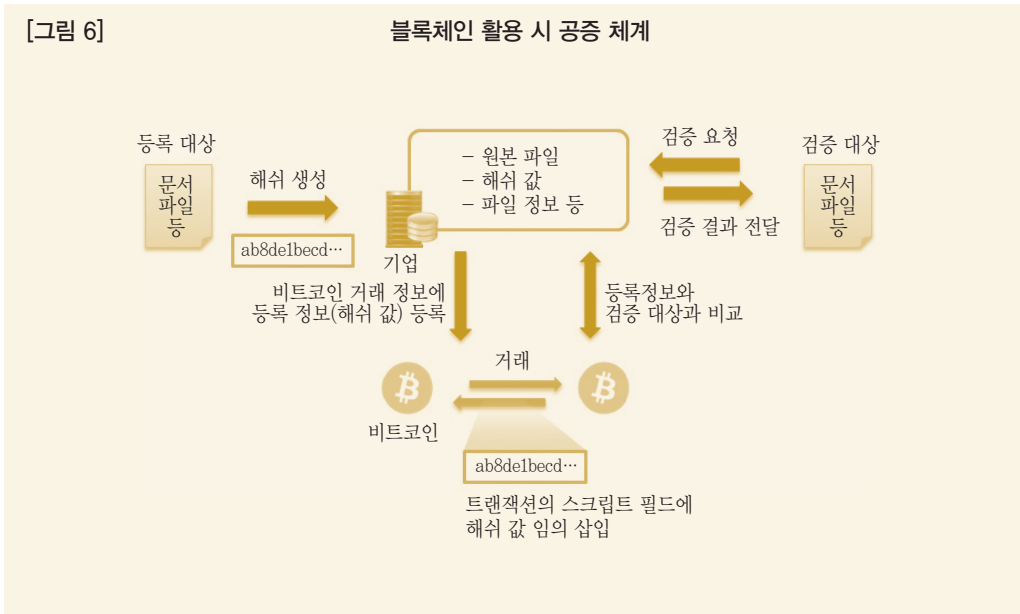
[그림 5] 전자공증 체계 (자료:법무부 전자공증시스템)



전자 공증 시스템을 자체 구축하여 운영하기에는 많은 비용이 수반되므로 이를 위탁하여 운영하는 경우가 많다. 위탁 운영하는 곳이 해킹을 당하여 데이터가 위변조 되었을 경우에는 문서 혹은 파일을 공증하기에는 어려움이 존재한다. 하지만 블록체인을 이용할 경우 저장된 데이터의 불변성을 이용하여 전자 공증 시스템을 구축 할 수 있다.

[그림 6]

블록체인 활용 시 공증 체계



대부분의 서비스들은 비트코인 트랜잭션을 발생시킬 때 스크립트(Script) 필드에 40바이트 가량의 데이터를 입력 할 수 있다. 해당 필드에 공증하고자 하는 문서 혹은 파일의 해쉬 값을 넣음으로써 전자 공증 서비스를 제공한다. 하지만 이용자와 서비스 업체에서 문서를 잃어버릴 경우에는 이를 복원하기 힘들다는 단점이 있다.

4. 스마트 계약(Smart Contract)

스마트 계약은 일정 조건을 만족시키면 자동으로 거래가 실행될 수 있도록 자동화된 시스템을 가리킨다. 예를 들어 3등급 이상의 신용등급, 5천만원 이하의 부채를 지닌 개인에게 투자하고 싶은 사람과 조건에 부합하는 개인이 대출을 신청하였을 때 이를 자동으로 연결시켜주는 시스템이 있으며, 대출 이외에도 온라인 쇼핑, 안전거래(에스크로) 등 다양한 분야에서 응용될 수 있다.

독일의 스타트업인 ‘슬록(Slock)’은 부동산 임대서비스에서 블록체인을 활용한 스마트 계약 서비스를 제공한다. 입주자가 부동산 보증금과 임대료를 지불하면, 스마트폰을 이용해 건물에 부착된 스마트 자물쇠를 계약기간 동안 열 수 있도록 한다. 계약 내용이나 입금내역을 확인할 중간 관리자 없이 입금이 되면 문을 열 수 있도록 플랫폼만 제공한다.

[그림 7]

스마트 계약 작동 원리



스마트 계약은 물품 구매, 권리 이전 등 폭넓게 활용되고 있으며, 최근에는 사물인터넷과 연계되어 이용되고 있다. 조건에 의해 거래가 자동적으로 성립되므로 중간 딜러에 의한 사기 피해를 막을 수 있다. 또한, 거래 정보에 대한 기록이 보존되기 때문에 기록 조작(예 : 계약서 위조, 사고 기록 조작 등) 등의 악의적 행위를 방지할 수 있다.

5. IoT(사물인터넷)

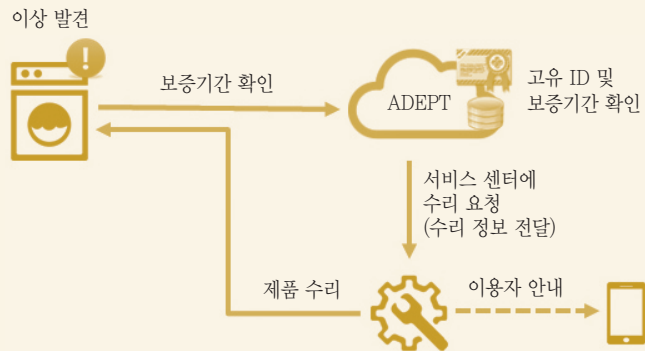
IBM은 삼성과 협력하여 가전제품을 대상으로 블록체인 기반 IoT 플랫폼을 개발하고 있다. 이는 모든 사물들을 인터넷을 통해 연결하여 서로 정보를 공유할 수 있도록 환경을 구성하는 것으로 기존에는 기기들이 한 중앙 장치에 의해 통제되었으나, 이제는 기기 스스로 통제하도록 만든다는 것이다. IBM의 ADEPT(Autonomous Decentralized Peer-To-Peer Telemetry)는 자동 분산 P2P 원격 측정으로 분산된 접근 방식을 택함으로써 IoT의 보안성과 규모를 확장시킨다는 계획을 가지고 있다.

사물인터넷과 스마트 계약을 서로 연계시켜 제품 스스로가 소모성 품목을 재주문 하거나, 기기의 이상이 있을 경우 셀프 서비스 요청 등을 수행 할 수 있다. IBM에서 소개하는 사례는 스마트 세탁기가 스스로 부품의 이상 유무를 확인한다. 문제 발생시 ADEPT 플랫폼 안에 속해있는

기기들의 공유ID와 보증기간을 확인하여, 보증기간에 따라 이용자에게 수리의 필요성을 알리고, 무상으로 서비스하거나 유상일 경우 이용자 확인에 따라 제품을 수리 할 수 있도록 한다. 이용자가 직접 이상 유무를 확인하고 제품 수리 요청을 할 필요가 없이 스스로 판단하고 수행하는데 있어서 진행과정, 결과에 대해서 확인만하면 된다.

[그림 8]

IoT 환경에서 블록체인 활용 예



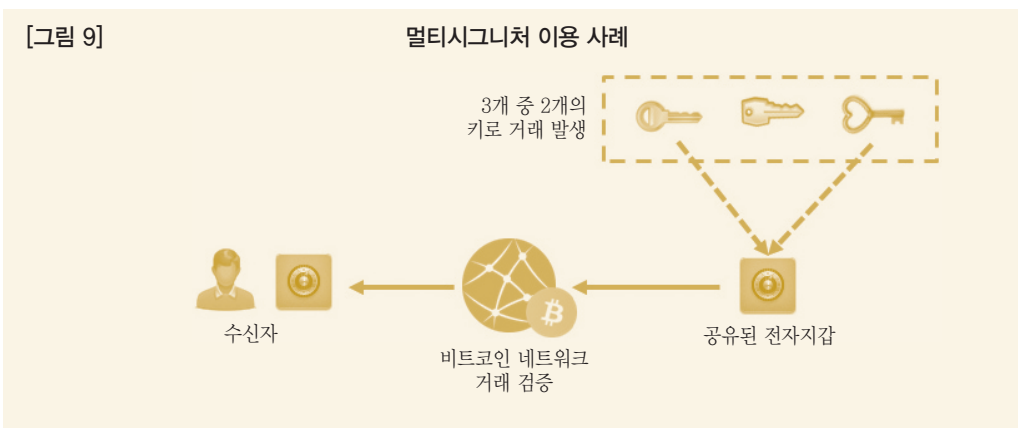
Ⅳ. 금융권 적용 고려사항

IT기업, 금융권 등 다양한 산업분야에서는 블록체인 그리고 암호화 화폐(비트코인)를 적용하기 위해 노력 중이다. 특히 해외 금융사들은 R3CEV 컨소시엄을 통해 기존의 인프라를 대체하기 위한 기술 개발 및 표준화 작업을 진행 중이다. 국내 금융권에서도 블록체인 기술을 적용하기 위해 다양한 노력을 하고 있으며, 이에 금융권에 적용하기 위해서 고려해야 할 부분에 대해 생각해본다.

1. 클라이언트 보호

블록체인은 데이터를 영구적으로 기록하여 보호 할 수 있으나, 애플리케이션을 이용하는 클라이언트에 대한 보호 장치는 미흡하다. 예를 들어 비트코인은 발행되는 화폐를 전자지갑(Digital Wallet)에 보관되고, 이때 이용되는 개인키는 컴퓨터, USB, 클라우드(서버) 등에 저장할 수 있다. 하지만 해킹 혹은 개인의 부주의로 인해 개인키가 도난, 분실될 경우 되찾기가 어렵다.

이러한 문제를 개선하기 위해 멀티시그니처(Multi-Signature)와 같이 다수의 개인키를 생성하여, 특정 조건 이상의 개인키가 있어야만 이용 할 수 있도록 보안장치가 마련되어 있다. (N>M 일 때, N개의 개인키 중 N개가 필요 할 수도 있고, M개가 필요 할 수 있다.) 하나의 개인키는 USB에 보관하고, 다른 하나는 클라우드 서비스 제공업체 서버에 저장하여 상대적으로 안전하게 보관·이용 할 수 있다. 이외에도 종이에 인쇄한 후 소지하여 다닐 수도 있지만, 분실할 경우 제 3자가 무단으로 이용할 수 있거나 찾지 못할 수 있다.



다른 위협은 익명성을 이용한 중간자공격(MITM), 3자 사기 등에 악용될 가능성이 존재한다. 전자지갑을 생성할 때는 본인인증 절차가 없으며, 이메일 주소만 입력함으로써 손쉽게 만들 수 있다. 즉, 수신 주소만으로 실제 거래하는 상대방이 누구인지 알기 어렵다.



비트코인 채굴(Mining) 시 난이도 조절이 이루어지기 때문에 상대적으로 보안성이 높은 것과 달리 전자지갑은 암호로만 보호하므로 상대적으로 안전하지 않다. 하나의 패스워드가 아닌 바이오인식, OTP 등 복합적인 요소와 결합되어 이용 할 수 있는 형태를 고려해야 한다.

2. 노드 유지

가상화 화폐 활성화를 위해서 무엇보다 중요한 것은 안정적인 네트워크를 운영하는 것이다. 다양한 가상화 화폐 중에서도 비트코인은 가장 오래됐으며 안정적인 네트워크를 구축하고 있는데 이는 안정적인 선순환 구조를 만들었기 때문이다. 비트코인의 채굴은 화폐의 가치가 높아질수록 많은 채굴자들이 참여하도록 유도하며, 비트코인의 희소성과 안전성을 높임으로써 더 높은 가치를 만들어 안정적인 네트워크를 운영할 수 있도록 한다.

[그림 11]

비트코인의 선순환구조 (자료: Organic media Lab 재구성)



하지만 비트코인 네트워크를 운영하기 위해 많은 컴퓨터 자원과 전력을 소모하는 것이 비효율적이라는 우려의 목소리도 나오고 있다. 비트코인을 채굴하기 위해서는 연산능력이 필요하기 때문에, 안정적인 네트워크를 위해서는 대량의 컴퓨팅 파워와 전력 소비가 불가피하다. 또한, 51% 공격⁸⁾, 이기적 채굴 전략⁹⁾ 등 컴퓨팅 파워만으로 네트워크를 유지하는 것은 한계가 존재하므로, 효율적으로 네트워크를 유지시킬 수 있는 새로운 채굴 방안이 필요하다. 유사 암호화 화폐에서는 이러한 문제를 해결하기 위해 다양한 시도를 수행하고 있으며, 일부에서는 기존방식과 새로운 채굴 방식을 조합하여 운영하기도 한다.

[표 3]

새롭게 제안된 채굴 방식

구분	세부 내용
소유증명 (PoS, Proof of Stake)	<ul style="list-style-type: none"> · 보유하고 있는 코인의 양에 따라 채굴 할 수 있음 · POS 시스템에서의 51% 공격은 많은 비용이 필요함 · POS 시스템은 더 분산화 되어있지만, 활성화시키기 위해서 열심히 노력해야함 · 적용 대상 : Peercoin, BitShares, Nxt, BlackCoin 등

8) 51% 공격이란 네트워크 전체 해시파워(hash power)의 절반 이상을 차지하는 하나의 마이닝 집단이 블록체인을 조작할 수 있는 힘을 가지게 됨으로써, 이중지불(double-spending)을 감행하거나 채굴된 비트코인을 부정하게 다량으로 확보하는 등 네트워크를 사실상 무력화시킬 수 있는 행위를 말한다.

9) 이기적 채굴(Selfish Mining) 전략이란 블록 생성에 성공하면 공개하지 않고 다음 블록을 찾는데 이용하는 방법으로 다른 경쟁자가 채굴에 성공하더라도 먼저 생성된 블록이 인정될 수 있으므로, 정상 채굴자들의 전력을 낭비한다.

위임소유증명 (DPoS, Delegate Proof of Stake)	<ul style="list-style-type: none"> · 101명의 선출된 대표자(Delegate)들이 순번을 정해 돌아가면서 블록을 생성함 · 지분에 대한 권한을 위임받은 대표자는 각 지분보유자가 자기 지분을 가지고 투표를 해서 선출함 · 주주의 지분에 따라 의사결정이 이루어지는 기업의 운영방식과 흡사 · 단, 투표 참여율이 낮을 경우 상대적으로 적은 지분을 가지고도 블록생성권한을 독점할 수 있다는 단점이 존재 · 적용 대상 : BitShares 등
중요성증명 (PoI, Proof of Importance)	<ul style="list-style-type: none"> · 경제활동을 장려하기 위한 PoS의 확장개념 · 사용자 균형 및 트랜잭션 수를 기초로 보상을 계산 · 단, 보상을 위해 자신에게 반복적으로 화폐를 보내지 못하도록 함 · 적용 대상 : NEM 등
속도소유증명 (PoSV, Proof of Stake Velocity)	<ul style="list-style-type: none"> · 화폐의 보유량과 이용량에 따라 보상 · 소셜 미디어 및 기타 소액 결제를 위해 설계됨 · 쌓아두는 것보다 화폐의 사용을 장려하기 위해 만들어짐 · 적용 대상 : Reddcoin 등
시간소유증명 (PoST, Proof of Stake-Time)	<ul style="list-style-type: none"> · 화폐 보유량으로만 결정하는 것이 아닌 화폐에 나이를 적용시킴 · 보유하고 있는 기간이 길어질수록 지분의 확률이 낮아지도록 함 · 적용 대상 : Vericoin 등

3. 확장성 고려

금융권에 블록체인을 적용하기 위해서는 실명인증, 제한된 참여 등 제약사항이 많을 것으로 예상된다. 미국의 나스닥 프라이빗 마켓은 프라이빗 블록체인 형태로 운영중이며, R3CEV 컨소시엄은 공개되진 않았지만 컨소시엄 혹은 프라이빗 블록체인의 형태로 운영될 것으로 예상된다. 프라이빗 블록체인의 경우 기존 시스템에서 크게 변경되는 건 데이터베이스가 투명하고 안전하게 운영한다는 것이지만, 신뢰성이 배제될 가능성이 존재한다. 이러한 문제를 해결하기 위해 등장한 것이 바로 대안체인(Alternative Chains)이다. 대안체인은 비트코인의 제약사항들로 시도할 수 없었던 새로운 실험들(증명방식 등)을 수행하면서 생태계를 확장시키기 위해 고안된 것이다.

특징에 따라 3가지로 구분되며, 서로 독립적인 블록체인을 이용하는 개별 블록체인, 기존 블록체인을 이용하되 추가적인 기능을 제공하는 형태인 메타체인(Meta Chain), 마지막으로 서로 다른 블록체인으로 구성되나 서로 연계될 수 있는 사이드체인(Side Chain)이 있다.

[표 4] 대안체인의 종류별 특징 (자료 : www.jeffpaik.com 재구성)

구분	개별 블록체인	메타체인	사이드체인
개념	 <p>비트코인 블록체인은 여러 기술적 측면에서 제한이 많고, 이미 네트워크가 구축되어 실질적인 실험이 불가능함. 개별 블록체인은 네트워크가 쌓이기 전 충분한 개발과 실험을 통해 비트코인 블록체인에서는 불가능한 여러 기능을 제공함</p>	 <p>메타체인은 비트코인 코드를 변경할 필요 없이 비트코인 블록체인 위에서 여러 추가적 기능을 제공함. 비트코인의 기술적 한계를 공유하는 반면 비트코인의 네트워크 효과와 안정성이 보장됨</p>	 <p>사이드체인이라고도 불리는 상보적 블록체인은 개별 블록체인을 비트코인 블록체인에 연결하여 비트코인의 네트워크를 공유하는 동시에 기술적 문제를 해결하고 여러 실험을 가능하게 함</p>
사례	Ethereum, Bitshares	Counterparty, ColorCoin	Factum, Blockstream

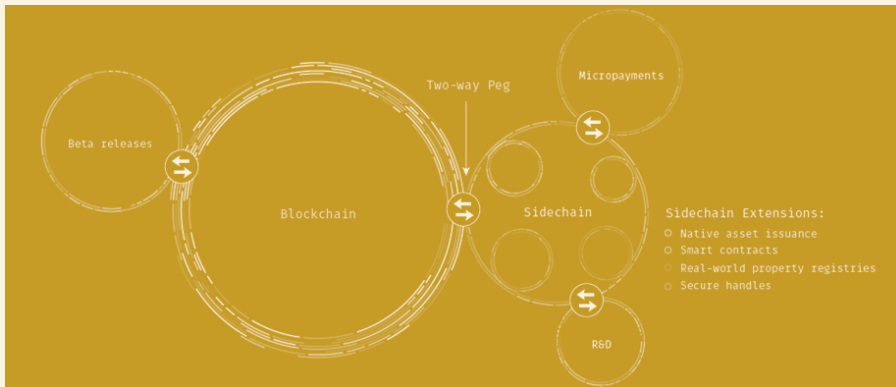
Ethereum은 비트코인과 별개의 블록체인 네트워크를 구축한다. 비트코인은 블록생성에 10분이라는 시간이 필요하지만, 이 문제를 해결하기 위한 대체 가능한 합의 알고리즘에 대해 실험함으로써 블록 생성 시간을 12초로 획기적으로 줄였다.

ColorCoin은 비트코인의 블록체인을 이용하면서 트랜잭션 위에 추가적인 데이터 로더를 더해 필요한 기능을 구현하도록 로직을 구현하였다. 별도의 블록체인이 필요 없어 비트코인의 블록체인, 트랜잭션, 주소 체계 등을 그대로 이용하지만 추가된 프로토콜에 의해 별도의 코인을 생성할 수 있다.

Blockstream은 비트코인과는 별도의 블록체인을 가진다. 블록 생성 주기, 합의 방식, 마이닝 방식 등 비트코인에서 구현되지 않은 독립적이고 실험적인 특성들이 있다. 가장 큰 특징은 비트코인의 블록체인과 사이드체인에 구현된 화폐가 양방향으로 화폐의 가치가 교환될 수 있도록 기능이 구현한 것으로 이를 ‘Two-way Peg’이라고 한다. 사이드체인은 기존의 비트코인의 시스템에서 제공하지 못하는 다양한 기능을 구현할 수 있도록 도와준다.

[그림 12]

사이드체인 형태 (자료 : Blockstream)



V. 결론

블록체인은 복제할 수 없는 거래 장부를 구현했다는 점에서 큰 관심을 받고 있다. 스페인 산탄데르(Santander) 은행의 보고서에서는 블록체인 기술을 적용하면, 글로벌 은행들은 2022년까지 해외송금, 증권거래, 규정준수 등과 관련된 인프라 비용을 연간 150~200억 달러(한화 약 18~24조원)를 절감할 것으로 예측하고 있다.¹⁰⁾ 앞서 소개한 활용 사례와 같이 기존 시스템을 대체함으로써 안전한 서비스를 제공할 수 있지만, 블록체인 네트워크를 누가 구성하고 운영할지는 의문이다. 비트코인과 같이 안정적인 블록체인 네트워크를 유지하기 위해 네트워크 참여자에게 비용을 지불하기 때문에 가능할 수 있는 것이다. 만약 정부기관들이 블록체인 네트워크를 운영한다고 가정하면, 정부가 사회적 발생 비용을 책임질 수 있지만 이용자들이 참여할 수 없는 형태라면 높은 신뢰를 받을 수 있는 네트워크인지 의문을 가지게 될 것이다.

어쩌면 가까운 미래에는 하나의 통일화된 화폐를 사용 할지도 모른다고 생각한다. 비트코인이 될 지 다른 화폐가 될 지는 예상할 순 없다. 다만, 안정적인 블록체인 네트워크를 기반으로 생태계가 만들어지면, 이와 연동될 수 있는 메타체인 및 사이드체인의 형태가 공존하는 생태계가 조성될 것이다. 현재의 사회적 형태를 고려하면, 어느 하나의 통일화된 화폐를 기반으로 각국의 화폐가 교환될 수 있는 모델을 고려해 볼 수 있다.

하지만 블록체인과 암호화 화폐와 관련된 규제는 해결해야 할 숙제이다. 국내의 경우 블록체인 기술을 금융권에 적용하기 위해서는 기존 중앙집중식 전산설비시스템을 전제로 규정되어 있는 현행 전자금융거래법 및 감독규정의 개정이 필요하다. 암호화 화폐의 경우 국내뿐만 아니라 해외에서도 논란이 있는 부분이다. 법정 화폐로 인정하는 국가나 주정부가 있어 각기 다른 규제가 마련되고 있다. 최초로 법정 화폐로 인정한 독일에서는 1년 미만 보유하고 소득이 발생한 경우 자본이득세를 부여하는 등 금융상품에 대한 과세를 실시하고 있으며, 뉴욕 금융감독청(DFS)은 비트코인을 이용한 자금세탁을 방지하기 위한 엄격한 규제안을 내놓기도 하였다.

이러한 규제 이외에도 양자컴퓨터와 같이 강력한 컴퓨팅 파워를 통해 블록체인 네트워크 생태계에 위협을 줄 수 있는 기술들이 등장함에 따라 안정적인 네트워크를 유지할 수 있는 다양하고 공정한 합의 방안 마련에도 지속적인 연구가 필요할 것이다.

10) Santander, The-Fintech-2-0-Paper : rebooting financial services

〈참고문헌〉

- [1] Wei Dai, “B-Money”, 1998
- [2] “bitcoin”, <http://bitcoin.org/en/>
- [3] Stoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008
- [4] “비트코인의 역사”, <http://aboutbitcoin.or.kr/>
- [5] Ethereum, “차세대 스마트 컨트랙트와 탈중앙화된 어플리케이션 플랫폼”
- [6] 이동규, “비트코인의 현황 및 시사점”, 2013
- [7] LG CNS, “Block Chain 기술과 응용사례를 통해 본 확장가능성”, 2015.8
- [8] KIBT, “블록체인 개요”, 2015.8
- [9] O’reilly, “Mastering Bitcoin”, 2014
- [10] Wikipedia, “Proof-of-stake”, <https://en.wikipedia.org/wiki/Proof-of-stake>
- [11] “비트코인 기술로 증권거래소 만든다”, <http://www.bloter.net/archives/209009>
- [12] “Hands On With Linq, Nasdaq’s Private Markets Blockchain Project”,
<http://www.coindesk.com/hands-on-with-linq-nasdaqs-private-markets-blockchain-project/>
- [13] “The Inevitable Failure of Proof-of-Stake Blockchains and Why a New Algorithm is Needed (Op-Ed)”,
<http://cointelegraph.com/news/114359/the-inevitable-failure-of-proof-of-stake-blockchains-and-why-a-new-algorithm-is-needed>

오픈소스 SW 사용 위협 및 대응 방안

김 동 진*

I. 서론	45
II. 오픈소스 SW에 대한 이해	46
1. 오픈소스 SW 개요	46
2. 오픈소스 SW 라이선스	48
III. 금융권 오픈소스 SW 도입	53
1. 금융권 오픈소스 SW 도입 배경	53
2. 금융권 오픈소스 SW 도입 사례 및 효과	54
IV. 오픈소스 SW 보안 위협	61
1. 보안 위협 원인	61
2. 취약점 및 보안사고 사례	63
V. 오픈소스 SW 보안 관리	67
1. 오픈소스 SW 거버넌스	67
2. 오픈소스 SW 보안 관리 방안	69
VI. 결 론	74
〈참고문헌〉	75

* 금융보안원 보안연구부 보안기술팀 (e-mail : dongjink@fsec.or.kr)

요 약

오픈소스 SW는 소스코드가 공개되어 자유롭게 활용 가능한 SW를 말하며, 이용 시 개발 기간 및 비용 절감 효과로 인해 최신 ICT 서비스 개발의 필수 요소로 자리 잡았다. 최근 국·내외 금융권에서도 핀테크 서비스 등 소비자들의 다양한 요구에 발맞춰 금융 서비스 경쟁력 확보를 목적으로 적극 도입 중이다.

하지만 여전히 많은 조직들에서는 오픈소스 SW를 단순히 무료 SW라고 인식하는 한편, 무분별한 사용 및 관리로 인한 라이선스 위반 및 보안 위협에 노출되어 있다. 더욱이 미션 크리티컬(Mission-Critical) 업무와 개인정보 등 중요 정보를 다루는 금융권의 경우, 이러한 위협에 더욱 큰 피해가 예상된다.

특히 2014년 이후, Heartbleed 및 Shellshock 등 오픈소스 SW 보안 취약점으로 인한 해킹 사고가 이어지고 있지만, 촉박한 개발 기간 등으로 인해 여전히 많은 조직들이 오픈소스 SW 관리에 소홀한 상황이다.

이러한 위협에 대한 가장 효과적인 해결 방안으로 알려진 오픈소스 SW 거버넌스(Governance)는 전담 조직 구성, 구성원 및 개발자의 인식 변화, 관련 솔루션 도입 등의 도입 장벽이 존재한다. 그리고 이로 인해 소규모 조직 등에서는 도입이 어려운 실정이다.

본 고에서는 이러한 현실적 어려움을 고려하여 비교적 도입이 쉬운 오픈소스 SW 보안 관리 방안과 여기에 함께 사용 가능한 무료 지원 서비스 및 관련 규격들을 제시한다. 그리고 이러한 방안 도입과 함께 오픈소스 SW 사용에 대한 올바른 인식 변화를 통해 최종적으로는 각 조직별 거버넌스 체계 확립에 도움이 될 것으로 기대한다.

I. 서론

오픈소스 SW(Open-Source Software, 이하 ‘OSS’)는 일반적으로 소스코드가 공개된 SW를 의미하며, 자유롭게 이용, 수정, 재배포 등이 가능하다. 이러한 특성과 더불어 OSS 활용을 통해 효과적으로 SW 개발 기간 및 비용 감축이 가능하기 때문에 매우 널리 사용되고 있다.

과거 금융권의 경우 다양한 금융 규제 등으로 인해 OSS 도입이 미진하였다. 하지만 핀테크 활성화 정책과 금융 소비자들의 다양한 요구에 부합하기 위해 스마트폰, 빅데이터, 클라우드 기반의 다양한 금융 서비스 개발이 필요해졌고, 이에 대한 경쟁력 확보를 위해 OSS 도입이 점차 증가하고 있다. 해외 글로벌 금융사는 물론이고, 국내 금융권에서도 증권부문을 중심으로 OSS 사용이 활성화되고 있다. 대표적으로 코스콤과 한국거래소에서는 차세대 거래 시스템과 같은 미션 크리티컬(Mission-Critical) 서비스를 OSS 기반으로 구축하여 운영 중이다. 이처럼 OSS의 안정성 증대와 급변하는 금융 서비스 요구로 인해 금융 시스템의 OSS 전환은 향후 지속될 전망이다.

하지만 OSS 사용 증가와 함께, 라이선스 위반 및 보안 관련 문제들 역시 급증하고 있으며 금융권도 이러한 문제로부터 자유롭지 못한 상황이다. 특히 금융권의 경우 보안사고 발생 시 개인정보 유출 및 금전적 피해로 인한 경제·사회적 파급효과가 매우 심각하기 때문에 더욱 주의해야한다. 대표적으로 2014년 OSS에서 발견된 Heartbleed 및 Shellshock 취약점으로 인해 대량의 개인정보 유출 및 기타 피해가 발생한 바 있다. 이러한 OSS 관련 보안 문제는 조직 내 무분별한 사용 및 사후 관리 미흡 등 대부분 관리적 문제에 기인한다.

OSS 거버넌스(Governance)는 ICT 서비스 개발에 있어서 OSS 도입부터 폐기까지 전 과정에서 컴플라이언스 및 보안성을 보장하기 위한 방법이며, 중요 서비스를 OSS 기반으로 개발 및 운영 중인 조직이라면 반드시 도입해야한다. 하지만 소규모 조직이나 극히 일부에만 OSS를 도입하는 경우, 거버넌스 도입 자체가 큰 부담으로 작용할 수 있기 때문에 최소한의 관리 방안도 필요하다.

이에 본 고에서는 도입이 용이한 OSS 사용 및 취약점 관리 기반의 보안 관리 방안을 제시하고자 한다.

II. 오픈소스 SW에 대한 이해

1. 오픈소스 SW 개요

가. 오픈소스 SW 정의

오픈소스 SW는 일반적으로 저작권자가 소스코드를 공개한 SW로서, 국외에서는 FOSS(Free and Open-Source Software), 국내에서는 일반적으로 OSS로 불리고 있다. OSS의 가장 큰 특징은 저작권자가 지정한 라이선스 내에서, 소스코드를 자유롭게 사용 및 수정, 재배포 가능하다는 점이다. 라이선스는 OSS의 사용, 수정, 재배포 및 2차 저작물¹⁾의 소스코드 공개 의무 등 OSS 개발자와 이용자 간에 사용방법 및 조건의 범위를 명시한 사용 허가권이다. 대표적으로 GPL(GNU General Public license) 등이 존재한다.

1985년 설립된 FSF(Free Software Foundation)가 자유 소프트웨어(Free Software) 개념을 정립한 후, 1998년 OSS의 활성화 및 라이선스 인증을 담당하는 OSI(Open Source Initiative)가 결성되면서 OSS가 널리 사용되기 시작하였다. 그리고 최근 급변하는 컴퓨팅 환경 및 다양한 OSS 사용 이점으로 인해, 프로그램 개발자(사)들은 적극적으로 OSS를 사용하게 되었으며, SW 개발에 OSS를 사용하는 것은 매우 일반적이게 되었다.

OSI에서는 OSS 조건으로 [표 1]의 10개 기준을 제시하고 있다.

[표 1] OSI에서 제시한 OSS의 정의(Open Source Definition, OSD)		
순번	인증 기준	설명
1	Free Redistribution	자유롭게 배포 가능해야 하며, 사용에 따른 비용 및 대가를 요구하지 않아야 함
2	Source Code	소스코드가 공개되어야 하며, 난독화 및 전처리된 중간 언어는 허용되지 않음
3	Derived Works	수정 가능하고, 원본 OSS의 라이선스 하에 배포 가능해야 함

1) OSS를 사용하여 개발된 SW 및 시스템

4	Integrity of The Author's Source Code	일부 조건 하에 원본 OSS가 수정되어 배포되는 것을 제한할 수 있어야 함
5	No Discrimination Against Persons or Groups	개인 및 그룹 등 이용자를 차별하지 않아야 함
6	No Discrimination Against Fields of Endeavor	활용 분야를 차별하지 않아야 함
7	Distribution of License	라이선스는 수정 없이 재배포 되어야 함
8	License Must Not Be Specific to a Product	특정 제품에 의존되지 않아야 함
9	License Must Not Restrict Other Software	OSS와 함께 배포되는 프로그램에 제한을 두지 않아야 함
10	License Must Be Technology-Neutral	개별 기술 또는 인터페이스의 스타일을 제한 및 규정하지 않아야 함

자료 : OSI, Open Source Definition 재구성

나. 오픈소스 SW 사용 증가

가트너(Gartner)에 따르면 2010년 세계 2,000개 기업 중 75%가 미션 크리티컬 SW에 OSS를 사용하고 있으며, 2016년에는 99%에 이를 것으로 전망하고 있다.²⁾ 또한 OSS 관리 솔루션 기업인 블랙덕(Black Duck)에 의하면, 2015년 전세계 기업의 75%가 OSS를 사용하고 있으며, 이는 2010년 대비 약 2배에 가까운 수치이다.³⁾ 또한 기업의 약 64%가 오픈소스 프로젝트에 참여하고 있다.

OSS 사용이 급증한 이유는 개발 시간 단축, 비용 절감, 개발 및 사후 지원의 편의성, 높은 코드 품질 등 크게 4가지이다. 특히 스마트폰, 빅데이터, IoT(Internet of Things) 등 최근 급변하는 ICT 기술 및 시장, 그리고 이용자들의 요구 사항에 신속하고 유연히 대응하는데 효과적이기 때문이다. 예로 스마트폰 플랫폼인 안드로이드, 타이젠 등이 OSS에 뿌리를 두고 있으며, 클라우드 컴퓨팅 플랫폼으로는 CloudStack, Openstack이 대표적이다. 그리고 빅데이터 처리를 위한 대표적인 분산 처리 플랫폼인 Hadoop 또한 OSS로서, 최근 주요 ICT 서비스에서 OSS가 매우 핵심적인 역할을 차지하고 있다.

2) Gartner, Predicts 2011: Open-source software, the power behind the throne, 2011

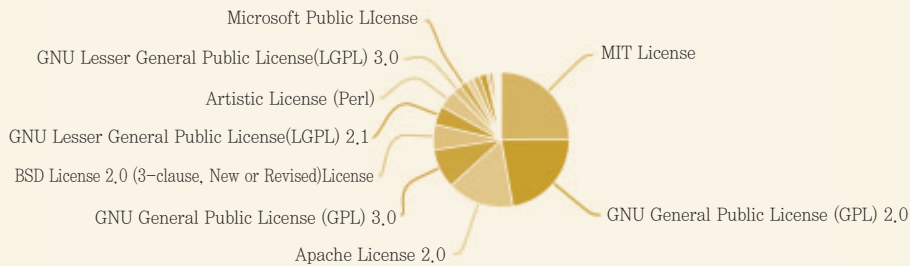
3) Black Duck, How & Why companies are using open source (The 2015 future of Open source survey finds), 2015

OSS 사용이 급증하는 또 다른 주요 이유는 2차 저작물의 소스코드 공개 의무가 없는 라이선스들의 활성화이다. 가장 널리 사용되고 있는 GPL의 경우 이를 사용하여 개발한 2차 저작물, 즉 이용자가 개발한 SW의 소스코드까지 공개해야 한다. 그렇기 때문에 상용 SW 개발 시에는 OSS 사용을 꺼리거나, 사용 사실을 의도적으로 공개하지 않는 경우도 존재한다. 하지만 OSS 사용을 독려하기 위해 2차 저작물의 소스코드 공개 의무가 없는 라이선스의 사용이 활성화됨에 따라 OSS 사용률이 더욱 빠르게 증가하게 되었다. 예를 들어, Apache License, MIT License, LGPL(GNU Lesser General Public License), BSD(Berkeley Software Distribution) 등은 조건 없이 또는 조건 하에 2차 저작물의 소스코드를 공개할 의무가 없다. 이러한 라이선스로 지정된 OSS는 상용 SW 개발에도 사용 가능하기 때문에 개발자(사)는 더 적극적으로 OSS를 도입 및 사용하고 있다.

실제로 2015년 기준, 라이선스별 사용 비율 통계에 따르면 [그림 1]과 같이 2차 저작물의 소스코드 공개 의무가 있는 GPL 라이선스 보다, 의무가 없는 MIT, Apache, BSD, LGPL 라이선스들의 더 높은 것을 확인할 수 있다.

[그림 1]

OSS 라이선스별 사용 비율



자료 : 블랙틱, Top 20 Most Commonly Used Licenses in Open Source Projects

2. 오픈소스 SW 라이선스

일반적인 상용 SW 라이선스는 저작권자의 저작권 및 독점 사용 권리 보호를 목적으로 SW 개발자와 사용자간의 이용방법 및 조건의 범위를 명시한다.⁴⁾ 이와 반대로 OSS 라이선스는 OSS 공유를 위한 일정한 의무 및 책임을 부여하는 것이 목적이다.

OSS 라이선스는 큰 범위에서 OSI 인증 및 비인증 라이선스로 구분 가능하며, GPL, MIT, Apache 등과 같이 잘 알려진 라이선스의 대부분이 OSI 인증 라이선스이다. 현재(2016년 1월) OSI에서 공식적으로 인증한 라이선스는 76개이다.

가. 라이선스 분류

OSI는 OSS 배포자 및 이용자의 라이선스 선택을 돕기 위해 사용 빈도 및 재사용 가능 여부에 따라 라이선스를 8개 카테고리로 분류하고 있다. 각 라이선스 별 의무 조항 등 세부 사항은 한국저작권위원회의 ‘오픈소스 SW 라이선스 종합정보 시스템(OLIS)⁵⁾’ 및 정보통신산업진흥원(이하 ‘NIPA’)의 ‘공개 SW 포털⁶⁾’을 통해 확인 가능하다.

[표 2] OSI의 라이선스 분류 기준	
카테고리	대표 라이선스
널리 사용되는 라이선스 (Licenses that are popular and widely used or with strong communities)	<ul style="list-style-type: none"> - Apache License 2.0 - New BSD license - GNU General Public License (GPL version 2) - Lesser General Public License (LGPL version 2) - MIT license
특정 목적 라이선스 (Special purpose licenses)	<ul style="list-style-type: none"> - Educational Community License - NASA - Open Group Test Suite
기타 라이선스 (Other/Miscellaneous licenses)	<ul style="list-style-type: none"> - Adaptive Public License - Artistic License - zlib/libpng license
유명 라이선스와 중복되는 라이선스 (Licenses that are redundant with more popular licenses)	<ul style="list-style-type: none"> - Academic Free License (Apache 2.0와 중복) - Attribution Assurance Licenses (BSD와 중복) - X.Net License (MIT와 중복)
재사용 불가 라이선스 (Non-reusable licenses)	<ul style="list-style-type: none"> - Apple Public Source License - IBM Public License - Nokia Open Source License

5) 국저작권위원회 오픈소스 SW 라이선스 종합정보 시스템 - <https://www.olis.or.kr>

6) 정보통신산업진흥원 공개 SW 포털 - <http://www.oss.kr>

대체된 라이선스 (Superseded licenses)	<ul style="list-style-type: none"> - Apache Software License v1.1 - Eiffel 1.0 - Lucent 1.0
자체 폐기된 라이선스 (Licenses that have been voluntarily retired)	<ul style="list-style-type: none"> - Intel Open Source License - MITRE Collaborative Virtual Workspace License - Sun Industry Standards Source License(SISL)
미분류 라이선스 (Uncategorized Licenses)	<ul style="list-style-type: none"> - Boost Software License (BSL-1.0) - European Union Public License (EUPL-1.1) - Microsoft Public License (MS-PL)
자료 : OSI, Open Source Licenses by Category 재구성	

또한 OSS 라이선스는 의무 강도에 따라 Strong copyleft⁷⁾, Weak copyleft, Non copyleft로 분류 가능하다. 첫 번째 Strong copyleft는 OSS를 사용한 2차 저작물의 소스코드를 반드시 공개하도록 규정하는 라이선스로 GPL이 대표적이다. 두 번째 Weak copyleft의 경우 특정 조건에서는 2차 저작물의 소스코드를 공개하지 않아도 되는 라이선스이다. 예로 LGPL은 OSS를 라이브러리 형태로 링크하여 사용한 경우 2차 저작물의 소스코드를 공개하지 않아도 되는 라이선스이다. 마지막 Non copyleft는 2차 저작물의 소스코드 공개 의무가 없으며, 일반적으로 상용 SW에도 사용 가능한 라이선스들로써 Apache, BSD, MIT 라이선스가 대표적이다.

대표 라이선스들의 주요 의무사항 비교는 [표 3]과 같다.

[표 3] 대표 라이선스들의 주요 의무사항 비교					
라이선스명	배포시 라이선스 사본 첨부	저작권 고지 사항 유지	소스코드 제공의무와 범위	타 라이선스와 통합 및 배포 허용	수정 시 수정 내용 고지
GPL 2.0	O	O	전체 코드	조건부	X
GPL 3.0	O	O	전체 코드	X	O
LGPL 3.0	O	O	전체 코드	O	O
BSD	X	O	X	조건부	X
Apache 2.0	O	O	X	O	X
자료 : NIPA, 공개SW 라이선스 가이드 재구성					

7) Copyleft : 저작권자가 무료로 자신의 창작물 사용을 허용하는 것, 즉 저작권의 반대 의미

나. 라이선스 위반 및 분쟁

OSS 사용 증가에 따라, 라이선스 위반 및 보안 관련 문제들의 발생이 증가하고 있으며, 많은 기관 및 기업들이 OSS의 부주의한 사용에 따른 피해를 경험하고 있다. 보안 위협에 대해서는 4장에서 별도 기술한다.

SW 개발 시 의도 또는 비의도적인 OSS 라이선스 위반과 이에 따른 분쟁이 빈번히 발생하고 있으며, 이로 인해 법적·경제적 책임을 지는 사례가 증가하고 있다. 예를 들어, GPL을 따르는 OSS를 이용한 경우 어떤 SW 개발자들은 소스코드 공개 의무를 회피하기 위해 OSS 사용 사실을 의도적으로 숨긴다. 비의도적 라이선스 위반은 OSS 라이선스의 인식이 부족한 개발자의 실수인 경우가 대부분이다. 또는 개발에 사용된 외주 개발 모듈이 이미 라이선스를 위반하였는데 이를 모르는 경우에 발생 가능하다.

1) 라이선스 위반 관리

라이선스 의무 이행 및 위반 여부는 FSF, SFC(Software Freedom Conservancy), SFLC(Software Freedom Law Center)와 GPL-Violations 커뮤니티에서 앞장서 관리 감독하고 있다. 이들은 금전적인 목적보다는 OSS 커뮤니티 활성화와 자발적인 라이선스 준수 문화 조성을 목표로 한다.

대표적으로 FSF는 GPL 라이선스인 OSS에 대한 사용을 상담, 지도 및 감시하고 있다. FSF는 라이선스 위반에 대한 신고가 접수되면 이 사실을 위반자에게 통지하고, [표 4]의 단계에 따라 처리한다.

[표 4]	FSF의 라이선스 위반 처리 단계
처리 단계	세부 내용
위반 보고서 작성	이 단계에서는 3가지의 기본정보가 필요하며, Who, What, How로 구성 - (Who) 회사, 조직(단체) 또는 개인 등 누가 라이선스를 위반 했는가에 대한 내용 - (What) 라이선스 위반한 SW - (How) 라이선스 어떤 요구조건을 위반 했고, 어떤 의미인지에 대한 정보
확인	위반 보고서에서 제공된 정보를 확인하는 단계이며, 배포 시 라이선스를 포함 여부, 제공되는 소스코드는 완전한지 여부 등 파악
초기 연락	위반 사항이 확인되면 위반자에게 연락하는 단계로, 먼저 E-Mail을 통해 정보를 공유하고 향후 절차에 대해 안내하고 진전이 없을 경우 변호사 선임
컴플라이언스 이행	위반자에게 라이선스 위반에 대한 조치사항 등을 공유 및 실행한다. 최종적으로 조치사항 등에 대한 실행결과를 확인 및 종료
자료 : NIPA, 공개SW 라이선스 가이드 제구성	

2) 라이선스 위반 주요 사례

라이선스 위반 및 분쟁 사례로는 VMware, 삼성전자, Skype 및 Verizon의 GPL version 2.0(v2) 위반 사례가 대표적이며, 세부 내용은 [표 5]과 같다.

[표 5] 라이선스 위반 및 분쟁 대표 사례			
연도	원고	피고	세부 내용
2015	Christoph Hellwig ⁸⁾ , SFC	VMware	<ul style="list-style-type: none"> - VMware의 ESX 및 ESXi 솔루션이 GPLv2인 리눅스 커널의 코드를 사용하면서 라이선스를 위반 - 진행 중(VMware는 위반 사실을 부인)
2013	유럽 대학생	삼성전자	<ul style="list-style-type: none"> - 삼성전자는 안드로이드 커널의 파일시스템에 GPLv2인 리눅스 커널 드라이버를 사용하면서 라이선스를 위반 - SFC 관여 하에 소스코드 공개 합의
2009	SFLC	삼성전자 외 13개 사	<ul style="list-style-type: none"> - 삼성전자, 휴맥스, JVC, Westinghouse 등이 셋톱박스 SW에 GPLv2인 BusyBox를 사용하면서 라이선스를 위반 - Westinghouse는 침해저작권당 9만불 배상 판결, 이외 비밀 합의
2008	GPL-Violations	Skype	<ul style="list-style-type: none"> - SMC는 제조한 VoIP 전화기에 GPLv2인 OSS 2개가 포함된 리눅스를 사용하면서 라이선스를 위반하였으며, 이를 Skype가 유통 및 판매함 - 소스코드 공개와 함께, 유통업체인 Skype에게도 책임을 물어 벌금 지불 판결
2007	Eric Amderson ⁹⁾ , SFLC	Verizon	<ul style="list-style-type: none"> - Verizon의 서비스에 사용된 무선 라우터에 GPLv2인 BusyBox를 사용하면서 라이선스 위반 - OSS 컴플라이언스 오피스 지정, 소스코드 공개 합의
자료 : 국내·외 관련 기사			

8) 리눅스 커널의 상위 개발자이며, VMware가 무단 도용한 코드 중 상당수를 개발

9) BusyBox 개발자

Ⅲ. 금융권 오픈소스 SW 도입

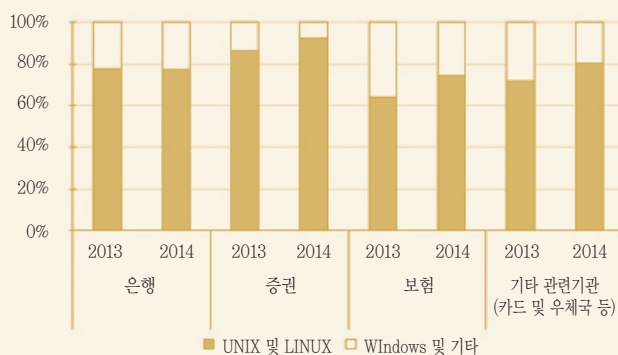
1. 금융권 오픈소스 SW 도입 배경

전통적으로 금융 시스템 고유의 보안성과 특유의 정책 및 규제 등을 고려하여, 금융사들은 자체 개발한 애플리케이션을 선호하였다. 그러나 이러한 생각은 독자적인 시스템 개발 및 운영으로 인한 많은 비용 지출과 금융 시스템이 유지보수가 어렵고, 새로운 서비스와 호환이 어려운 오래된 코드들로 구성되는 원인이 되었다.

최근에는 금융사들에서도 적극적으로 OSS 도입하거나 도입을 검토하고 있다. 먼저 [그림 2]와 같이 2013~2014년 국내 금융권의 운영체제 사용 비율에서 MS 윈도우 계열보다 OSS에 기반한 리눅스의 비율이 점차 증가하는 것을 확인할 수 있다.¹⁰⁾ 또한 2015년 초 코스콤 발표¹¹⁾에 의하면 이미 세계 금융거래의 50% 이상이 OSS를 통해 처리되고 있다. 실제로 OSS 솔루션 기업인 Sonatype 사에 의하면, 2014년에만 약 24만개에 달하는 공개된 Java 컴포넌트가 금융사에 의해 다운로드된 것으로 확인되었다.

[그림 2]

2013~2014년 국내 금융권 운영체제 사용 현황



자료 : 한국은행, 2014년도 금융정보화추진현황 재구성

10) 5천만원 미만 초소형 전산기기 제외

11) 코스콤, 코스콤 이슈 트렌드 2015년 봄호, Vol.258, 2015.

이러한 변화는 빅데이터, 클라우드 서비스 및 스마트폰 중심의 비대면 서비스 등 급변하는 고객들의 요구에 대응하기 위해서는 OSS 도입이 불가피하기 때문이다. 그리고 과거와는 달리 금융사들은 이용자 단말에서 설치 및 실행되는 SW를 직접 개발하여 배포하는 등 SW 벤더의 입장이 되었기 때문이다.

핀테크 활성화 등을 위해 빠르게 변화하는 금융 규제 또한 주요 원인이다. 새로운 서비스 개발을 요구하며, 시스템 및 DB 구성 등에 영향을 주는 규제 및 정책 변화에 발맞춰 대응하기 위해서는 OSS를 도입하는 것이 비용 및 보안 측면에서 더 효과적이라 판단하였기 때문이다.

2. 금융권 오픈소스 SW 도입 사례 및 효과

가. 국외 사례

해외 금융권의 경우 영국, 미국, 일본 등을 중심으로 OSS가 활발히 사용되고 있다. 대표적인 사례로 2013년 영국의 Barclays는 OSS 도입을 통해 SW 관련 비용의 90%를 절감하였다.¹²⁾ 그리고 UK Bank의 경우, 트레이딩 시스템에 OSS를 적극 도입한 결과 [그림 3]과 같이 전체 시스템의 65%를 OSS로 구축할 수 있었고, 자체 개발한 코드는 28%에 불과했다.¹³⁾

미국의 경우에도 2004년 미국 연방금융기관 검사 위원회(Federal Financial Institutions Examination Council, FFIEC)에서 OSS 위험 관리 가이드¹⁴⁾를 발표하였을 만큼, 금융사들의 OSS 사용은 매우 일반적이다. 대표적으로 Bank of America는 2005년부터 OSS를 사용해 왔으며, Wells Fargo & Company는 1997년부터 OSS 스크립트 언어인 PERL을 사용하기 시작하여, 2012년에는 스스로를 OSS의 헤비 유저라고 밝힌 바 있다.¹⁵⁾ 이외에도 JP Morgan, Citi group 등의 주요 금융사들이 OSS를 활발히 사용하고 있다. 은행권뿐만 아니라 뉴욕증권거래소, 시카고선물거래소 등 전 세계의 28개 증권거래소의 미션 크리티컬 서비스들이 OSS 기반 플랫폼 상에서 운영되고 있다.

12) C. Wiedemann, FOSS in Financial Institutions, 2014 FOSS CON Korea 발표자료

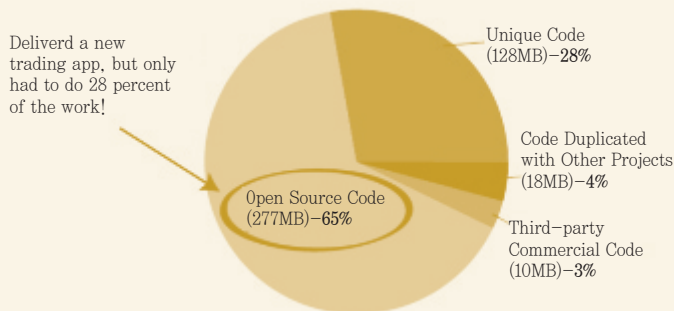
13) Black Duck, Open source component Governance and Management Using COBIT, 2012 ISACA Webinar Program, 2012.

14) FFIEC, Risk Management of Free and Open Source Software, Guide, 2004.10.

15) J. Quitter, Open Source's Promise, American Banker, 2012.07.

[그림 3]

UK Bank의 트레이딩 시스템에 사용된 OSS 비율



자료 : 블랙텍, Open source component Governance and Management Using COBIT, 2012

일본의 경우 증권사들을 중심으로 OSS가 사용되고 있다. Monex 증권의 경우 서비스 인프라 SW부터 애플리케이션 개발에까지 OSS를 도입하고 있다. Daiwa 증권은 높은 신뢰성이 요구되는 은행의 계정계 시스템에 리눅스 서버를 도입하였으며, बैं킹 앱 역시 후지쯔(Fujitsu)에서 공개한 OSS인 W-Bank를 기반으로 개발하였다.

해외 금융권의 대표적인 OSS 도입 사례는 [표 6] 같다.

[표 6]

해외 금융권의 OSS 도입 사례

국가	기업명	사용 OSS	도입 업무
미국	American Express	OpenSSL	인터넷 बैं킹
	American Funds	OpenSSL	인터넷 बैं킹
	Bank of America	Hadoop, OpenSSL	인터넷 बैं킹
	Chicago Mercantile Exchange	Linux	트레이딩 플랫폼
	Citi group	Linux	표준 플랫폼
	E*Trade	OpenSSL	인터넷 बैं킹
	Goldman Sachs	Apache Tomcat, MongoDB, HBase	메시징 시스템 (Symphony)
	JP Morgan	Hadoop	서버 로드 밸런싱, FDS
	MetLife	MongoDB	RDBMS
	Morgan Stanley	Hadoop	트랜잭션 처리
	New York Stock Exchange	Linux, Jboss, Drupal	트레이딩 시스템 외
	Union Bank of California	Linux	IT 표준화 플랫폼

영국	Barclays	OpenSSL, JSON	인터넷/모바일뱅킹
	UK Bank	—	트레이딩 시스템
일본	Daiwa Securities	Linux, W-Bank	계정계 시스템,뱅킹앱
	GMO Click Securities	Apache HTTP Server	온라인 트레이딩 시스템
	Monex Securities	Linux, PostgreSQL, JBoss	온라인 시스템 외
	Nomura Research Institute	Apache HTTP Server, JBoss	증권사 대상 ASP 서비스
	Tokyo Star Bank	Linux, Apache Tomcat	영업사원 인센티브 집계 시스템 외
	Tokyo Stock Exchange	Linux	기간계 시스템
기타	ANZ Bank (호주)	Hadoop	트랜잭션 처리
	AXA Bank Europe (벨기에)	Quantlib	금융 상품 평가
	CaixaBank (브라질)	PostgreSQL	RDBMS
	Deutsche Bank (독일)	Linux	Reuters Market System Data

자료 : 국외 관련 기사

최근에는 OSS를 사용하는 것뿐만 아니라, 직접 OSS 커뮤니티에 참여하여 금융권에 특화된 OSS 개발에 앞장서기도 한다. 대표적으로 JP Morgan 등 주요 금융사들이 리눅스 재단에서 주도하는 OpenMAMA¹⁶⁾라는 OSS 프로젝트에 운영위원으로 참여 중이다. OpenMAMA는 주문 및 거래 시스템에 활용 가능한 메시징 미들웨어이다.

나. 국내 사례

국내 금융권의 경우, 증권 거래 분야를 중심으로 OSS 도입이 추진 중이다. 한국거래소, 코스콤, 대우증권, 한국증권금융이 OSS를 도입한 바 있으며, 차세대 거래 시스템 및 여신 심사 시스템과 같은 중요 시스템부터 내부 업무 시스템에까지 다방면에서 사용되고 있다.

대표적으로 코스콤은 2003년 서버 운영체제와 미들웨어를 시작으로 2013년부터는 실시간 모니터링 및 시스템 차세대 거래 시스템(Exture++)을 OSS 기반으로 구축하는 등 금융권 OSS 도입의 선도적 역할을 해오고 있다. 이뿐만 아니라, OSS를 전방위적으로 도입하기 위해 도입에서 폐기까지 모든 사이클에 필요한 규칙을 정리하는 한편, 실무에 적용 가능한 완성도 높은 OSS 목록 역시 제작한 것으로 알려져있다.

이를 포함한 국내 금융권의 OSS 도입 사례는 다음과 같다.¹⁷⁾


[표 7] 코스콤의 OSS 도입 사례	
기업명	코스콤
도입년도	2013년
배경 및 개요	<ul style="list-style-type: none"> - 사내 시스템에 대한 실시간 운영 상황 모니터링 시스템인 파워워치(PowerWatch)에 OSS인 PostgreSQL 기반 DBMS 도입 - 기존 오라클 DBMS 사용에 따른 과도한 유지보수 비용 및 SW 종속성 개선 <p>[그림 4] 코스콤의 파워워치 시스템 구성도</p>
사용 OSS	PostgreSQL 기반 DBMS인 Enterprise DB의 Postgre Plus Advanced Server(PPAS)
도입효과	<ul style="list-style-type: none"> - TCO 5년을 기준으로 상용SW보다 8배에 달하는 비용 절감 효과 - 버그나 문제점 없이 안정적 운용 가능하다는 점 확인

[표 8] 한국증권금융의 OSS 도입 사례	
기업명	한국증권금융
도입년도	2009년
배경 및 개요	<ul style="list-style-type: none"> - 이미지 시스템과 연계된 여신심사 프로세스의 관리가 요구됨에 따라 여신심사 프로세스 지원 - IT-PMS 프로세스 지원 - 이미징 시스템 및 계정계 통합단말(x-frame)과 연동
사용 OSS	uEngine BPMS(Business Process Management System)
도입효과	<ul style="list-style-type: none"> - 여신심사 및 IT-PMS 프로세스 지원 - 이미징 시스템 및 계정계 통합단말(x-frame)과 연동이 가능해짐

[표 9] 대한 생명, KDB 대우증권의 OSS 도입 사례	
기업명	대한 생명, KDB 대우증권
도입년도	2011년, 2012년
배경 및 개요	<p> - 업무신청, 결제 및 처리 등 다양한 내부 서비스의 지속적인 변화 - 이에 대응해 효율적인 프로세스 제어를 수행하기 위한 관리 프로그램 필요 </p> <p>[그림 5] uEngine BPMS 개요</p> <p>The diagram illustrates the uEngine BPMS architecture, divided into four layers: Users, Interface Layer, Application Layer, and Resource Layer. The Users layer includes roles like 업무처리자 (Business Processor), 업무관리자 (Business Manager), and 시스템 관리자 (System Manager). The Interface Layer contains a Portar and a BPM (Business Process Management) component. The Application Layer includes a 그룹웨어 (Groupware) and a 분석시스템 (Analysis System). The Resource Layer includes a 문서저장소 (Document Repository), 지식분류 통합검색 (Knowledge Classification Integrated Search), DB (Database), and KM (Knowledge Management). Arrows indicate the flow of data and processes between these components and layers.</p>
사용 OSS	uEngine BPMS
도입효과	<p> - 자체적인 유지보수 가능 - 공개 모듈 이식 등으로 유연하게 성능 개선에 대처할 수 있는 프로세스 관리 시스템 구축 - 비용 절감(상용 솔루션 대비 최대 1/3 비용 소요) </p>

[표 10] 메리츠화재의 OSS 도입 사례	
기업명	메리츠화재
도입년도	2010년
배경 및 개요	<p> - 전자정부 표준프레임워크에 기반한 필수 시스템의 안정성 확보를 위한 자체 프레임워크 도입, 통합 앱(APP) 메타 저장소, 운영환경, 배치 프레임워크 등의 추가 확장 필요 - 보상업무를 포함한 기간업무시스템의 완성, IT거버넌스 체계의 강화, 고객 중심형 시스템 구성, 포털, 보험상품 교체 판매 등을 지원하기 위한 상품 시스템, 자동차보험 업무 지원, 신개념의 채널시스템, 콜센터, 대리점과의 연계업무 등에 대한 차별화된 시스템 구현 </p>
사용 OSS	전자정부 표준프레임워크(eGovFrame) 기반 자체확장
도입효과	<p> - SI 사업자에 대한 종속에서 벗어나 자체 기술 경쟁력 확보 - 업무 프로세스의 생산성 향상과 비용절감 </p>

[표 11] 한국주택금융공사의 OSS 도입 사례

기업명	한국주택금융공사
도입년도	2013년
배경 및 개요	<p> <ul style="list-style-type: none"> - 상품 중심의 단순 정보전달형 앱에 대한 개선 필요성 대두 - 신뢰성, 신속성, 접근성을 만족하는 하이브리드 앱 개발 요구 증가 </p> <p>[그림 6] 한국주택금융공사의 스마트 주택금융 앱 화면</p> 
사용 OSS	PhoneGap, jQuery Mobile
도입효과	<p> <ul style="list-style-type: none"> - 주택금융 정보는 물론 금융서비스의 신청 및 조회까지 가능한 하이브리드 앱 마련 - 콘텐츠 업데이트, 보안 네이티브 모듈 연동, 각 운영체제별 접근성 기능까지 모두 탑재 </p>

[표 12]

농협정보시스템의 OSS 도입 사례

기업명	농협정보시스템
도입년도	2011년
배경 및 개요	<p> - 사내 보안 정책 강화로 일반 메신저 사용 금지에 따라 조직 커뮤니케이션 수단 필요 - 상용 메신저를 도입 하자는 의견이 있었지만 사용자 수를 기준으로 적용되는 라이선스 비용, 유지관리 등의 문제로 적합하지 않다고 판단 - 이에 XML에 기반 한 실시간 메시지 지향 공개 표준 통신프로토콜인 XMPP (Extensible Messaging and Presence Protocol)을 활용하기로 결정 </p> <p>[그림 7] 농협정보시스템의 사내 메신저(아리톡) 구조도</p>
사용 OSS	XMPP, Openfire, Spark, Quartz, PostgreSQL
도입효과	<p> - 조직 커뮤니케이션 채널로써 정보 전달성, 신속성 향상 - 조직 내 정보유통의 질을 향상시켜 의사 결정 유효성 증대, 비용 절감 </p>

Ⅳ. 오픈소스 SW 보안 위협

1. 보안 위협 원인

일반적으로 OSS 개발 및 관리에는 수많은 개발자들이 참여하기 때문에 코드의 품질이 더 높고 보안상 더 안전할 것으로 인식된다. 하지만 OSS의 경우에도 공개된 소스코드 및 부주의한 사용 등으로 인한 다양한 보안 위협에 노출되어있다.

가. 공개된 소스코드로 인한 위협

최근 OSS로부터 고위험성 취약점 발견되고 있으며 이로 인한 해킹사고 또한 계속해서 발생하고 있다. 실제로 2014년 미국의 NVD¹⁸⁾에 새롭게 등록된 7,937개의 취약점 중에서 약 4,300개가 OSS에서 발견된 취약점이었다.¹⁹⁾ 2014년 Sonatype 사의 OSS 저장소로부터 금융사가 다운로드한 Java 컴포넌트들 중 약 15,000개(7.5%)에 알려진 취약점이 존재했던 것으로 확인되었다. 또한 미국 FS-ISAC²⁰⁾에서는 OSS의 약 26%에 고위험도 취약점이 존재한다고 발표하였다. 그리고 국가정보원에서 발표한 2015 국가정보보호백서에서는 OSS에 존재하는 위험성 높은 취약점으로 인해 보안위협이 크게 고조되었음을 강조하였다([그림 8]). 트렌드마이크로(TrendMicro)의 2015년 보안 예측 보고서에서는 OSS에 대한 취약점 악용 시도가 더 많아질 것으로 예측하기도 하였다.

이처럼 OSS에서 많은 취약점이 존재하는 가장 큰 이유는 소스코드가 공개되어 있다는 점이다. 소스코드가 공개된 만큼 공격자 입장에서 공격 대상 선정 및 악의적인 역분석이 매우 용이하기 때문이다. 애플의 iOS에 비해 소스코드가 공개된 안드로이드에서 더 많은 취약점이 발견되는 것도 같은 이유이다.

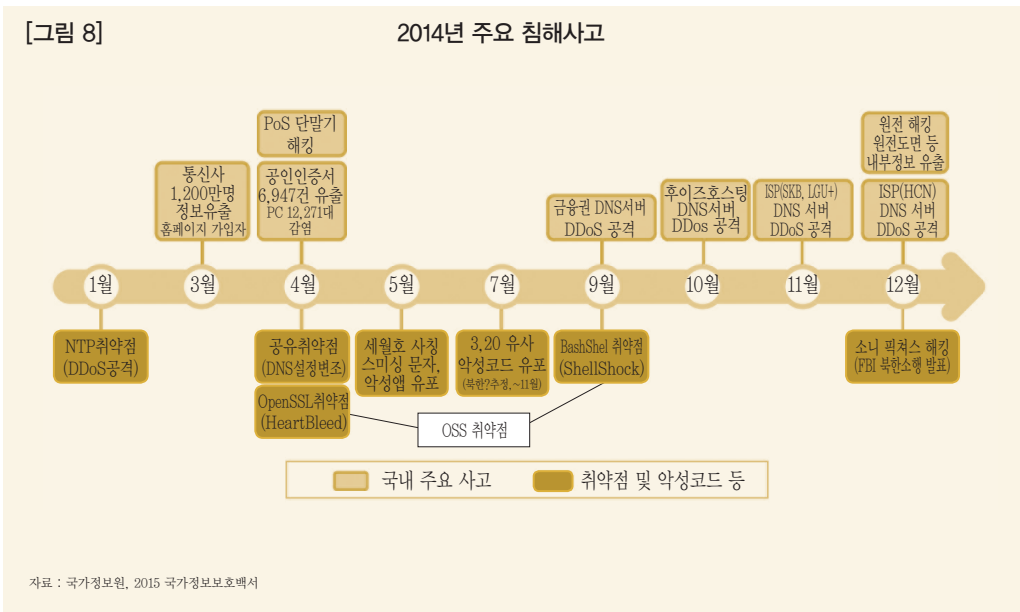
18) NVD(National Vulnerability Database) : 미국 정부 산하 국립표준기술연구소(National Institute of Standards and Technology, NIST)에서 운영하는 공개 취약점 DB

19) 조시행, 오픈소스와 보안, FOSS CON Korea 발표자료, 2015.12.03

20) FS-ISAC(Financial Services Information Sharing and Analysis Center) : 금융권의 해킹 및 사이버테러 방지와 기반보호시설에 대한 취약점 평가 업무를 담당하는 정보공유분석센터

[그림 8]

2014년 주요 침해사고



나. 관리적 보안 위협

OSS 커뮤니티에 많은 개발자들이 참여하고, 코드가 공개된 만큼 보안 패치 등의 해결책이 빠르게 제공되는 것도 사실이다. 하지만 이는 커뮤니티 참여자가 많거나, 기술 지원 전문 업체가 존재하는 경우에 해당한다. 그렇지 못한 경우에는 관리 소홀로 인해 보안성이 더 취약할 수밖에 없다. 또한 보안 패치가 빨리 이루어졌다 하더라도 이용자 측에서 체계적인 버전 관리가 이루어지지 않거나, 버전 변경에 따른 호환성 문제 등을 우려하여 이용자가 패치를 적용하지 않는 경우도 있다.

실제로 2014년 금융사들에서 다운로드한 OSS 중 상위 100개(다운로드 횟수 기준)를 대상으로 29개 금융사에서 사용되는 버전을 분석한 결과, 각 컴포넌트 별로 평균 27개의 다른 버전이 사용되는 것으로 드러났다.²¹⁾ 이를 통해 보안 패치가 제공되더라도 패치 미적용으로 인해 계속해서 보안 위협에 노출될 수 있음을 알 수 있다.

또한 SW 개발 시 OSS 사용 여부가 확인되지 않거나, 소스코드를 확보하기 어려운 외주 개발 모듈 등에 대해서는 OSS가 사용되었는지 여부조차 확인하기 어렵다. 이 경우에는 보안 패치가 적용되기 더 어렵기 때문에 이를 고려한 OSS 사용 관리 및 외주 개발 모듈에 대한 별도 관리가 필요하다.

21) L. constantin, Software applications have on average 24 vulnerabilities inherited from buggy components, PCWorld, 2015.04.

2. 취약점 및 보안사고 사례

2014년 2, 3분기에는 각각 Heartbleed, Shellshock라 불리는 OSS 취약점으로 인한 대규모 보안사고가 발생하였다. 이를 시작으로 2015년에는 Freak, Ghost, Venom 등 더 많은 OSS 관련 취약점이 발견되었다. 이와 같은 OSS 취약점의 공통된 특징은 크게 두 가지로, 첫 번째 최초 OSS가 배포된 시기와 취약점이 발견된 시기 차이가 크며, 두 번째는 최초 사고 이후에도 지속적으로 공격 시도가 이어진다는 점이다.

먼저 최근 2년간 취약점이 발견된 OSS의 배포 및 취약점 발견 시기를 비교한 결과는 [표 13]과 같다. 매우 널리 사용되는 Bash 셸(Shell)의 경우 Shellshock 취약점이 약 25년 동안 발견되지 않은 채 사용되었으며, Ghost 및 Venom 취약점도 배포 후 10여년 만에 발견된 취약점이다. 이를 통해, OSS의 코드 품질에 허점이 존재하며 OSS 이용자 및 참여자 수와 보안 수준이 반드시 비례하지 않는 것을 알 수 있다.

[표 13] 최근 OSS 취약점의 배포 및 발견 시기

취약점명 (OSS)	Heartbleed (OpenSSL)	Shellshock (Bash Shell)	Freak (OpenSSL)	Ghost (GNU C Library)	Venom (QEMU)
배포 시기	2011년	1989년	1990년	2000년	2004년
발견 시기	2014년	2014년	2015년	2015년	2015년

자료 : 조시행, 오픈소스와 보안, 2015 FOSS CON Korea

또한 Heartbleed 및 Shellshock의 경우 최초 공격 이후 약 1년이 지난 지금까지도 이를 악용한 공격이 계속되고 있다.²²⁾ 두 취약점은 각각 2014년 4월, 9월에 보안 패치가 공개되었지만, 2015년 2, 3분기에만 이를 악용한 공격이 각각 약 10만 건, 7만 건 확인되었다. 이는 SW 개발에 사용된 OSS에 대한 버전 및 보안 패치 관리가 정상적으로 수행되지 않는 경우가 적지 않음을 의미한다.

22) 트렌드마이크로 블로그, One Year After Shellshock, Are Your Servers and Devices Safer?, 2015.07.

가장 대표적인 OSS 취약점인 Heartbleed와 Shellshock에 대한 세부 내용은 다음과 같다.

가. Heartbleed 취약점

Heartbleed는 암호화 라이브러리인 OpenSSL에 존재하는 취약점이다. OpenSSL은 웹 서버와 이용자 간의 데이터 암호화 및 전자 서명에 사용되며, Apache와 같은 웹 서버, 이메일 서버 등에 가장 많이 사용되는 OSS 이다. Heartbleed 취약점은 악용될 경우 웹 서버의 개인 키 및 세션 쿠키를 비롯해 금융 서비스 이용자들의 비밀번호 및 신용카드 정보 등까지 탈취 가능한 매우 위험한 취약점이다.

취약점 발표 당시(2014년 4월) 웹 서버²³⁾의 약 17%(약 50만대)가 공격에 노출되어 있는 것으로 보고되었다. 실제로 캐나다 국세청(Canada Revenue Agency, CRA)은 이 취약점 공격으로 인해 900명의 개인정보가 유출 당했으며, 영국 등에서도 피해가 잇달았다. 이 밖에도 구글, 페이스북 등 해외 유명 웹 서비스 회사들도 자사 사이트에 Heartbleed 취약점이 존재함을 발표하고, 신속히 보안 패치를 적용하였다. 취약점 발표 당시 Heartbleed로 인한 국내 금융권의 영향을 조사한 결과, [표 14]과 같이 전체 142개사 중 12개사가 Heartbleed 취약점이 존재하는 OpenSSL 버전을 사용하는 것으로 확인되었다.

[표 13] 국내 금융권의 Heartbleed 영향 조사 결과

구분	금융회사	취약한 버전 사용 회사	조치	미조치
은행	19	2	2	0
금융투자	44	1	0	1
보험	34	4	4	0
카드	8	3	2	1
기타	37	2	2	0
합계	142	12	10	2

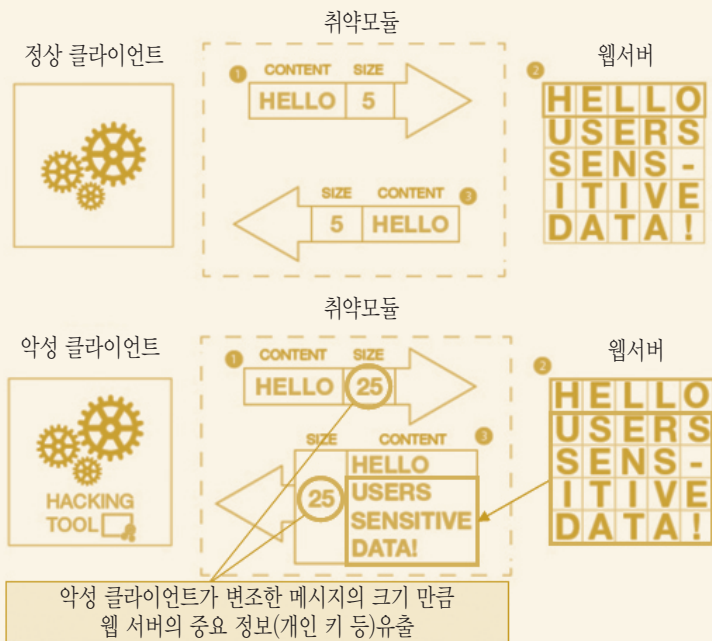
자료 : 금융위원회 보도자료, 2014.04.16.

23) 인증기관(Certificate Authority, CA)으로 부터 인증 받은 웹 서버

세부 취약점 악용 방법은 [그림 9]과 같으며, 악성 클라이언트가 웹 서버에게 어떤 요청을 보낼 때, 메시지 크기 값을 비정상적(최대 64KB)으로 조작하여 보냄으로써 취약점을 악용한다. 이로 인해, 웹 서버에 저장된 중요 정보가 조작된 크기만큼 클라이언트에게 유출된다.

[그림 9]

Heartbleed 악용 방법 개요



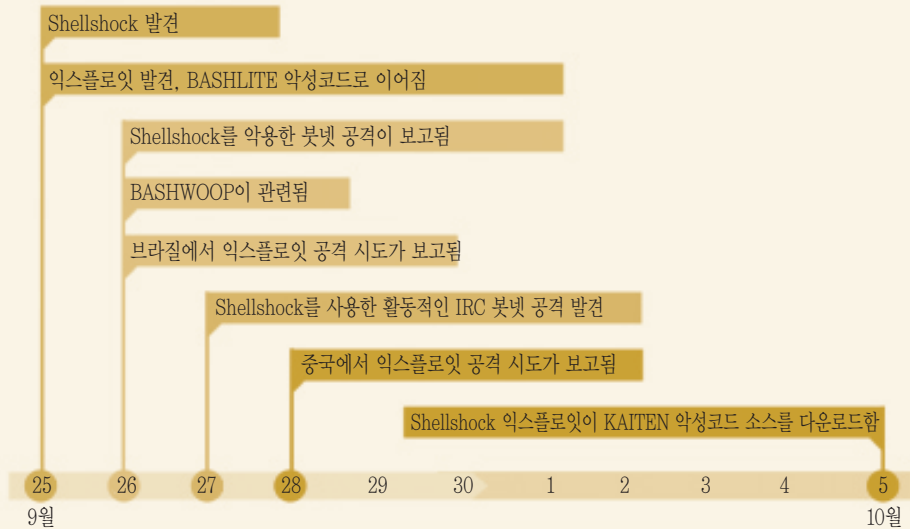
자료 : <http://www.forumsys.com/api-security/how-to-fix-openssl-heartbleed-security-flaw/>

나. Shellshock 취약점

Shellshock는 리눅스 및 맥 계열 운영체제에서 컴퓨터에 명령을 내리는 인터페이스인 Bash 셸에 존재하는 취약점이다. 취약점 발표 당시 리눅스 계열 서버를 사용하는 금융사의 시스템을 포함하여 5억개 이상의 시스템이 공격 위협에 노출된 상태였다. 또한 취약점 악용 방법이 비교적 쉽고, 리눅스 계열 시스템을 완전히 장악 가능한 매우 위험성 높은 취약점이다. 이로 인해, [그림 10]과 같이 취약점 발견 시점으로부터 약 10여일 만에 공격이 빠른 속도로 확산되었으며, 봇넷, DDoS 및 제 3의 악성코드 전파 등 다양한 형태 공격에 활용되기도 하였다.

[그림 10]

2014년 Shellshock 취약점 악용 공격 과정



자료 : 트렌드마이크로, 2014년 4분기 보안위협 보고서

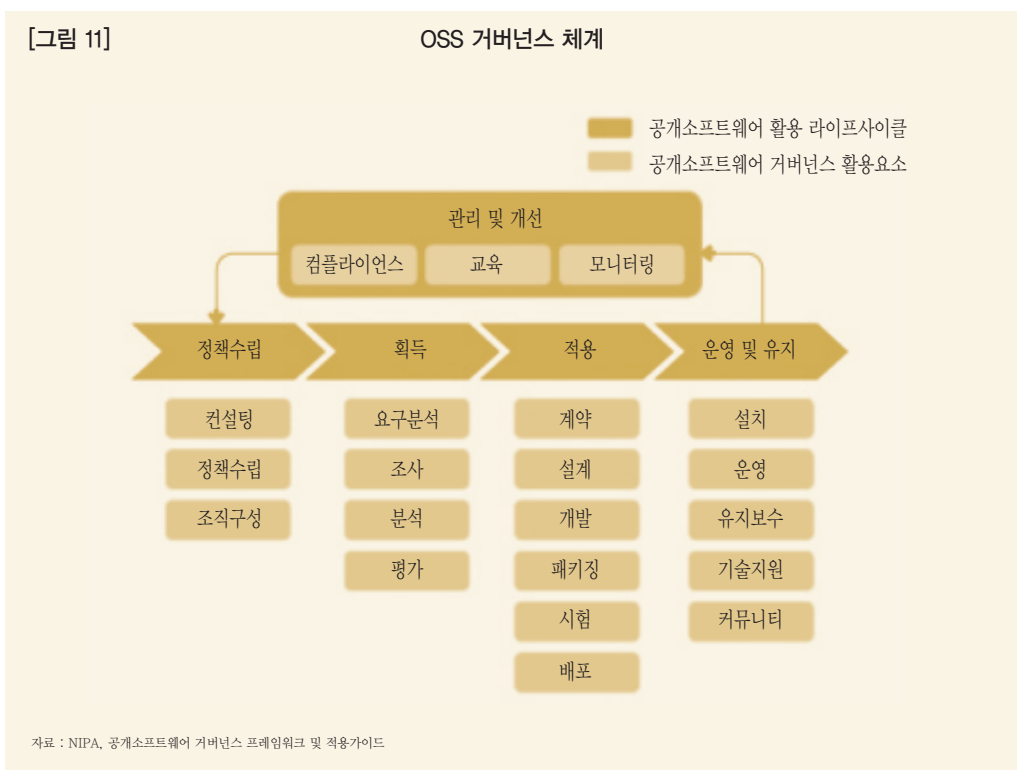
가장 먼저 Shellshock 취약점을 공격받은 대상은 CGI²⁴⁾ 웹 서버이다. 악의적인 시스템 명령어를 포함한 비교적 간단한 문자열이 HTTP 메시지를 통해 전달되면 CGI는 Bash 셸에게 명령어를 전달하여 실행되도록 한다. 이를 통해, 시스템 강제 재시작, 계정 탈취, 파일 및 디렉터리 삭제뿐만 아니라, 악성코드 다운로드 및 실행 등 주요 악성행위가 모두 가능하다.

24) CGI(Common Gateway Interface) : 웹 서버에 요청된 페이지를 애플리케이션에 전달 및 처리하기 위한 인터페이스

V. 오픈소스 SW 보안 관리

1. 오픈소스 SW 거버넌스

OSS 보안 위협을 완화 및 개선하기 위한 가장 바람직한 방안은 OSS 거버넌스 체계를 도입 및 구축하는 것이다. OSS 거버넌스의 주요 목적은 OSS를 효과적으로 활용하고, 라이선스 관리 및 컴플라이언스를 통해 OSS 사용에 따른 다양한 위험 요소를 제거 및 예방하는 것이다. 이를 위해 [그림 11]과 같이 SW개발 정책수립부터 개발 및 배포 후 유지보수까지 SDLC²⁵⁾ 전 단계에 걸쳐 OSS 사용을 계획 및 관리해야한다.



NIPA에서는 거버넌스 각 단계별 주요 활동 내용을 [표 15]와 같이 제시하고 있다.

25) SDLC(Software Development Life Cycle) : 효과적인 SW 개발을 위해 개발 전 과정을 단계로 나누어 설명하는 모델

[표 15]

OSS 거버넌스 단계별 주요 활동 내용

단계	활동 내용	비고
정책수립	<ul style="list-style-type: none"> - 목표와 전략에 따라 반드시 지켜야 할 규정과 지침을 수립함 - OSS 적용과 전략수립을 위한 자문 서비스를 제공함 - 효율적인 인력 구성과 역할과 책임에 따른 운영 방안을 제시함 	순차 수행
획득	<ul style="list-style-type: none"> - 고객 또는 사용자의 고민, 요구사항 등을 분석함 - 새로운 OSS 또는 특정 분야에 적합한 OSS를 찾음 - OSS 속성을 구분하고 상태나 수준을 정리함 - 각 속성에 가중치를 부여하고 평가 모델을 적용하여 채점함 	
적용	<ul style="list-style-type: none"> - OSS 도입 및 활용, 배포에 대한 일련의 책임과 의무에 대해 조건과 규정을 체결함 - 요구 분석 결과에 따라 기능과 사양을 미리 구성함 - OSS 프로그램을 변경 및 결합함 - OSS 설치가 편리하도록 단일 프로그램으로 묶음 - 요구 수준에 맞는지 품질과 성능을 확인함 - OSS를 저장매체, 웹사이트, 장비 등을 통해 전달함 	
운영 및 유지	<ul style="list-style-type: none"> - OSS를 운영할 수 있는 장비에 탑재함 - OSS를 실행시켜 정상적인 상태로 지속적으로 가동시킴 - 최상의 운영 상태를 유지하도록 제반 작업을 수행함 - 추가적인 요구 사항을 반영이나 문제 해결 등 공학적인 OSS 서비스를 제공함 - 소스코드 기여, 재정적 지원, 활동 교류, 참여방법을 제시함 	
관리 및 개선	<ul style="list-style-type: none"> - 라이선스 의무사항 준수 및 법적 문제를 해결함 - OSS 도입, 활용, 배포에 대한 이해력을 높이기 위해 지식을 전달하고 스킬을 향상시킴 - OSS 적용 이후의 상황을 파악하고 피드백을 수렴함 	비순차 및 비정기 수행

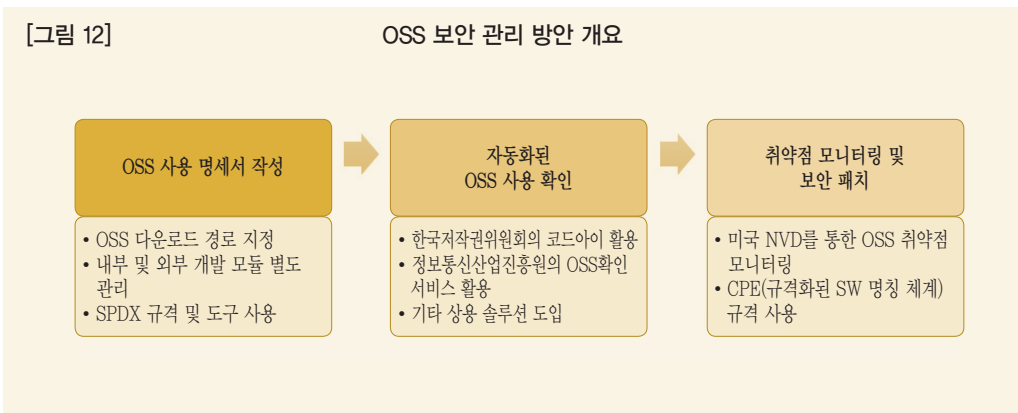
자료 : NIPA, 공개소프트웨어 거버넌스 프레임워크 및 적용가이드 제구성

또한 각 조직의 OSS 거버넌스 성숙도를 총 5단계인 위험노출, 측정단계, 관리단계, 참여단계, 활성화 단계로 구분하고 있다. 위험노출 수준인 조직은 OSS의 특성을 인지하지 못한 채 무분별하게 사용하여, 관련 위험에 노출된 상태이다. 반대로 활성화 단계에서는 자동화된 프로세스 및 도구에 의해 OSS 사용이 관리되어 관련 위험으로부터 비교적 자유로울 뿐만 아니라, OSS 커뮤니티에 후원 및 직접 참여하는 상태이다.

하지만 높은 수준의 성숙도에 이르기 위해서는 기업 경영진 및 개발자들의 인식 변화, OSS 관리 전담조직 신설, 조직 내 별도 OSS 저장소 운영 등 장기간에 걸친 많은 노력이 필요하다. 라이선스 관리와는 달리, OSS 보안 위협 개선을 위한 활동은 거버넌스 성숙도에 상관없이 공통적으로 수행되어야 한다. 하지만 현재 거버넌스 체계들은 보안 위협 개선보다는 OSS를 효율적으로 이용하고 라이선스를 관리하는 것에 초점을 두고 있다.

2. 오픈소스 SW 보안 관리 방안

OSS 거버넌스는 보안 위협 완화를 위한 매우 효과적인 방안이지만, 단 기간 내 도입이 어려우며 일반적으로 SW 개발 초기부터 적용해야하는 단점이 존재한다. 그렇기 때문에 비교적 도입이 쉽고, 이미 개발이 완료된 시스템에도 적용 가능한 OSS 보안성 개선 방안이 필요하다. 이에 본 고에서는 OSS 사용 명세서(Bill of Materials, BOM) 및 보안 취약점 관리 기반의 OSS 보안 관리 방안을 제시한다. 세부적으로 3단계로 구성되며, [그림 12]와 같다.



OSS 사용 명세서는 어떤 SW 및 시스템에 사용된 OSS들의 목록으로 세부적으로는 사용된 OSS의 명칭, 버전, 다운로드 위치(URL) 및 라이선스 등이 기록되어야 한다. 미국 FS-ISAC을 중심으로 30개 주요 금융사 및 OSS 솔루션 기업들로 구성된 워킹그룹에서 발표한 보고서²⁶⁾에서는 OSS 보안성 개선 방법으로 OSS 사용 명세서 도입을 권장하고 있다.

가. 1 단계 : OSS 사용 명세서 작성

첫 번째 단계에서는 사용된 OSS를 식별하고 사용 명세서를 작성한다. 이때 SW가 조직 내부 또는 외주 개발사 등 외부에서 개발되었는지에 따라 서로 다른 고려사항이 존재한다.

먼저 내부에서 개발된 경우, 개발자가 직접 사용한 OSS의 명세서를 작성하도록 한다. 또한 사용된 OSS가 명세서에서 누락되지 않도록 OSS 획득 경로를 제한하여 개발자 스스로가

26) FS-ISAC Third Party Software Security Working Group, Appropriate Software Security Control Types for Third Party Service and Product Providers Ver.2.3, 2015.10.

OSS 사용 사실을 인지하도록 하는 것이 바람직하다. 예로 Github, SourceForge 등 대표적인 OSS 저장소 또는 PIP, Maven과 같은 패키지 인스톨러를 통해서만 OSS를 조달 가능하도록 제한한다.

일부 SW 모듈을 외주 개발하는 경우에는 외주 개발사에게 OSS 사용 명세서를 요구해야 한다. 이와 함께 명세서에 누락된 OSS로 인한 라이선스 위반 및 보안사고 발생 시 책임 소재를 계약서상에 명시하는 것이 바람직하다. 기본적으로 OSS로 인한 문제 발생 시 개발 사뿐만 아니라 이를 배포 및 판매한 벤더에게도 책임이 있기 때문이다.

OSS 사용 명세서는 조직별로 자체 형식을 사용하기 보다는 규격화된 명세서 형식과 명칭 및 버전 정보 표기 방식을 사용하는 것이 효율적이다. 만약 각 부서별 또는 조직별로 서로 상이한 형식을 사용할 경우 OSS 사용여부 중복 검토, 조직간 공유 시 비효율성, 명세서 작성 및 형식 변환 도구 자체 개발 등 다양한 추가 비용이 발생할 수 있기 때문이다.

OSS 사용 명세서 형식 관련 규격들은 [표 16]와 같다. 이들 중 SPDX가 가장 주목 받고 있으며, 국내·외 글로벌 기업들에서 따르고 있다.

[표 16] OSS 사용 명세서 관련 규격	
규격 명칭	설명
ISO/IEC 19770-2:2009	SW 식별 및 태그를 최적화하기 위한 규격
SPDX(Software Package Data Exchange)	리눅스 재단 및 워킹 그룹에 의해 운영되며, OSS 패키지 정보, 라이선스 정보를 추적 및 공유하기 위한 규격
OVAL(Open Vulnerability and Assessment Language)	미국 MITRE가 제정 및 관리하는 시스템 정보 및 상태를 표현, 평가 결과를 보고하기 위한 표준

SPDX의 목적은 여러 OSS가 통합되거나 다른 코드에 포함되는 경우에도 사용된 OSS 및 라이선스를 식별 및 추적하는 것이다. SPDX 보고서 예는 [그림 12]와 같으며, 실제 정보는 RDF²⁷⁾ 규격으로 관리된다. SPDX 보고서 작성 및 형식 변환을 위한 다양한 유·무상 도구²⁸⁾들이 존재하며 이를 활용하는 것이 효율적이다.

[그림 13]

SPDX 보고서 예

Spreadsheet Version		Version SPDX	Creator			Created		Data License	Creator Comment							
1.1.0		SPDX-1.1		Person: Gary O'Neill			2010-02-03 0:00		CC0-1.0		This is an example of an SPDX spreadsheet format					
				Organization: Source Auditor Inc.												
				Tool: SourceAuditor-V1.2												
Package Name	Package Version	Package File Name	Package Supplier	Package Originator	Package Download Location	Package Checksum	Package Verification Code	Verification Code Excluded Files	Source Info	License Declared	License Concluded	License Info From Files	License Comments	Package Copyright Text	Summary	
SPDX Translator	Version 0.9.2	spdxtranslator-1.0.zip	Organization: Linux Foundation	Organization: SPDX	http://www.spdx.org/tools	2d4e1c67a2d281ced849ee1bb76e7391b93eb12	4e3211c67a2d281ced849ee1bb76e7391b93eb12	SpdxTranslator, SpdxTranslator, Spdx.txt	Version 1.0 of the SPDX Translator application	(LicenseRef-3 AND LicenseRef-4 AND Apache-2.0 AND MPL-1.1 AND LicenseRef-1 AND LicenseRef-2)	(LicenseRef-3 AND LicenseRef-4 AND Apache-2.0 AND Apache-2.0 AND MPL-1.1 AND LicenseRef-1 AND LicenseRef-2)	Apache-1.0, Apache-2.0, LicenseRef-1, LicenseRef-3, LicenseRef-4, LicenseRef-2, MPL-1.1	The declared license information can be found in the NOTICE file at the root of the archive file	Copyright 2010, 2011 Source Auditor Inc.	SPDX Translator utility	
File Name	File Type	File Checksum	License Concluded	License Info in File	License Comments	File Copyright Text	Artifact of Project	Artifact of Homepage	Artifact of URL	File Comment	User Defined Columns...					
src/org/spdx/parser/DOAPProject.java	SOURCE	2d4e1c67a2d281ced849ee1bb76e7391b93eb12	Apache-2.0	Apache-2.0		Copyright 2010, 2011 Source Auditor Inc.										
Jena-2.6.3/jena-2.6.3-sources.jar	ARCHIVE	3ab4e1c67a2d281ced849ee1bb76e7391b93f125	LicenseRef-1	LicenseRef-1	This license is used by Jena	(c) Copyright 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009 Hewlett-Packard Development Company, LP	Jena	http://www.openjena.org/	UNKNOWN	This file belongs to Jena						
Reviewer		Review Date			Reviewer Comment											
Person: Joe Reviewer		2010-02-10 0:00			This is just an example. Some of the non-standard licenses look like they are actually BSD 3 clause licenses											
Person: Suzanne Reviewer		2011-03-13 0:00			Another example reviewer.											

자료 : NIPA, 공개소프트웨어 거버넌스 프레임워크 및 적용가이드

나. 2 단계 : 자동화된 OSS 사용 확인

OSS 사용 명세서 작성 후에는 자동화 도구를 사용하여 OSS 사용 여부를 다시 한 번 확인한다. 1단계와는 상호보완적 단계로서, 개발자가 사용한 OSS를 실수로 명세서에 누락할 경우 자동화 도구로 식별하여 추가 가능하다. 또한 개발자가 OSS를 수정 및 개작하거나, 코드의 일부분만 사용할 경우 자동화 도구로는 식별에 실패할 수 있기 때문이다.

OSS 사용 확인을 자동화하기 위해서는 방대한 양의 OSS DB 구축, 라이선스 및 소스코드 비교 기술이 필요하다. 이로 인해 미국 FS-ISAC 등에서는 전문 솔루션을 사용할 것을 권장한다. 대표적인 솔루션 및 업체로는 Black Duck, Open Logic, Palamida, Sonatype,

27) RDF(Resource Description Framework) : 웹상의 자원 정보를 표현하기 위한 규격으로 XML(eXtensible Markup Language)를 사용하기도 함

28) SPDX 관련 도구 - <http://spdx.org/tools>

Veracode 등 있으며, OSS 사용 확인뿐만 아니라 거버넌스 수준의 서비스를 제공한다.

솔루션 도입으로 인한 비용이 부담되는 경우, 정부 공공기관에서 무료로 지원 중인 OSS 검사 서비스를 이용할 수 있다. 현재 한국저작권위원회의 OLIS와 NIPA의 공개 SW 포털에서 무료 서비스를 제공 중이다. OSS 도입 및 라이선스 관련 컨설팅 서비스도 지원 중이며, 각 홈페이지를 통해 서비스 신청이 가능하다.²⁹⁾

한국저작권위원회는 OSS 사용 확인을 위해 코드아이(CodeEye)라는 도구를 개발하여 웹과 클라이언트 버전을 각각 서비스 중이다. 공개 SW 포털은 상용 솔루션을 사용하는 것으로 알려져 있다. 대표적으로 코드아이의 주요 기능은 [표 17]과 같다.

[표 17] 한국저작권위원회 코드아이(CodeEye)의 대표 기능

규격 명칭	설명
라이선스 검사	DB에 수집된 수천만 건(상시 업데이트)의 소스코드와 유사성을 검사하여 OSS 사용 여부 및 사용 라이선스를 검사해주는 기능
GPL 전문 검색	사용자가 검색 요청한 소스코드에서 GPL 라이선스 개발 템플릿의 유·무를 판별하여 GPL 라이선스 사용 유·무를 검사하는 기능
주석 검사	DB에 수집된 수천만건(상시 업데이트)의 소스코드 및 주석의 유사성을 검사하여 OSS 사용 여부 및 사용 라이선스를 검사해주는 기능
소스코드 비교	사용자의 소스코드와 DB에 저장된 OSS 소스코드 비교를 통해 각 파일별 유사라인 검출을 쉽게 확인이 가능하도록 제공하는 기능
검사 결과보고서	코드아이 검사 결과를 이용자가 쉽게 볼 수 있는 보고서 형식으로 제공하는 기능
SPDX 결과보고서	검사 결과를 종합보고서, 검사완료보고서, 제외파일 보고서, 파일별 보고서, SPDX 보고서 총 다섯 가지 형식의 보고서 제공

자료 : 한국저작권위원회, 오픈소스 SW 라이선스 종합정보 시스템

다. 3 단계 : 취약점 모니터링 및 보안 패치

OSS 사용 명세서가 작성되면, 명세서 상의 OSS에서 취약점이 발견되었는지 여부를 지속적으로 모니터링해야 한다. 취약점 모니터링은 각 OSS 커뮤니티에서 운영하는 버그신고 게시판, 공개된 보안 취약점 DB, 취약점 정보 제공 업체를 통해 가능하다. 하지만 대부분의 취약점 DB들이 미국의 NVD를 참조하기 때문에 이를 대상으로 취약점을 모니터링한다.

29) 세부 사용법은 홈페이지 및 사용자 매뉴얼 참고(코드아이 사용자 매뉴얼 - https://www.olis.or.kr/oss/codeEye/CodeEye_Manual.pdf)

NVD에서는 규격화된 명칭 체계인 CPE(Common Platform Enumeration)를 사용하여 SW의 명칭 및 버전을 관리한다. CPE의 표현 방식은 [그림 14]와 같으며, 대부분의 알려진 SW 및 OSS들의 명칭이 CPE 규격에 따라 등록된 사전³⁰⁾을 제공함으로써, 명칭 및 버전에 대한 일관성을 제공한다. 현재(2016년 1월) 약 10만여개의 SW 및 세부 버전들이 CPE 사전에 등록되어 있으며 계속해서 증가 중이다.

[그림 14]

CPE의 구조(예 : OpenSSL)

cpe:/a:openssl:openssl:1.0.2d

타입 벤더 제품명 버전

이에 명세서 작성 시 OSS 명칭 및 버전 정보를 CPE 규격에 따라 기재하고, 이를 활용하여 취약점 모니터링 시 취약점 존재 여부를 [그림 15]와 같이 NVD를 통해 효율적으로 확인할 수 있다. NVD 취약점 정보는 XML 및 RSS 형태로도 배포되기 때문에 자동화가 용이하다.

취약점이 확인된 경우, 보안 패치 정보는 OSS 사용 명세서에 기재된 출처 정보를 통해 확인할 수 있다. 명세서 상의 출처가 불분명한 경우에는 NVD를 통해서도 확인 가능하다. 일반적으로 NVD에는 취약점 보안 패치 및 해결 방안이 제공된 취약점만 공개되며, 보안 전문 업체 및 제조사의 보안 패치 정보에 대한 링크가 함께 제공된다.

[그림 15]

NVD에서 CPE를 활용한 취약점 조회

CPE 사전

취약점 목록

자료 : 미국 NVD 웹페이지 재구성

30) CPE 사전 - <https://nvd.nist.gov/cpe.cfm>

VI. 결론

운영체제 및 데이터베이스 등을 비롯하여, 스마트폰, 빅데이터, 클라우드 및 IoT 등 주요 최신 ICT 기술의 중심에 OSS가 존재하며, 금융 규제 변화에 발맞춰 비용 절감 및 금융 서비스 경쟁력 확보를 위해 금융권에서도 점차 이에 기반 한 서비스를 개발 및 제공 중이다. 그리고 최근에는 OpenMAMA와 같이 금융에 특화된 OSS들도 존재할 뿐만 아니라 금융사들이 커뮤니티에 직접 참여할 만큼 금융 산업에서 OSS는 반드시 필요한 요소가 되었다. 실제로 앞서 기술한 바와 같이 세계 주요 금융사와 함께 국내 금융사들도 OSS 도입 범위를 점차 확대해가고 있는 상황이다.

OSS 관련 위협 중 라이선스 위반도 중요한 문제이지만, 개인정보와 같은 민감한 정보들을 다루는 금융권의 경우에는 보안 위협이 더 심각한 문제이다. 이에 대한 해결 방안으로는 OSS 거버넌스가 가장 효과적이지만 이를 도입하기 위해서는 전담 조직 구성, 구성원 및 개발자의 인식 변화, 관련 솔루션 도입을 위한 비용 등의 추가 노력이 필요하다. 하지만 이와 같은 도입 장벽과 촉박한 개발 기간 등으로 인해 많은 조직들에서는 여전히 OSS 관리에 소홀한 실정이다.

이에 본 고에서는 도입이 용이한 OSS 보안 관리 방안과 이와 함께 사용 가능한 무료 지원 서비스 및 관련 규격들을 제시하였다. 제시 방안에서는 OSS 식별 및 사용 명세서 생성 도구, 공공기관의 무료 OSS 점검 서비스, 공개 취약점 DB 등을 활용한다. 이를 통해 취약점과 관련된 OSS 보안 위협은 개선 가능하지만, 모든 위협을 해결하기에는 부족한 면이 있다.

OSS를 효과적 도입하고 안전하게 활용하기 위해서는 제시한 방안을 도입하는 한편, 장기적 관점에서 OSS에 대한 조직 전체 및 개별 구성원의 인식부터 변화시켜야 한다. 그리고 최종적으로는 각 조직에 적합한 OSS 거버넌스 및 컴플라이언스 체계를 수립해야 한다.

〈참고문헌〉

- [1] FS-ISAC Third Party Software Security Working Group, Appropriate Software Security Control Types for Third Party Service and Product Providers Ver.2.3, 2015.10.
- [2] Black Duck, Open Source Drives Innovation In Financial Services, Tech. Report, 2013.
- [3] 정보통신산업진흥원, 공개소프트웨어 거버넌스 프레임워크 및 적용가이드, 2015.08.
- [4] 정보통신산업진흥원, 공개SW 라이선스 가이드, 2014.03.

정보보호제품 평가기준 국·내외 동향 및 향후 과제

황 증 모*

I. 개 요	79
II. 국내외 정보보호제품 평가기준	80
1. 기존 평가기준	80
2. CC인증 개요	82
3. CC인증 구성	84
4. 국내 CC인증 체계	92
III. 국내외 CC인증 동향	95
1. 국제 동향	95
2. 국내 동향	98
IV. 향후과제	100
V. 결 론	105
〈참고문헌〉	106

* 금융보안원 보안연구부 보안기술팀(e-mail : koyangee@fsec.or.kr)

요 약

미국에서 세계 최초의 정보보호제품 평가기준인 TCSEC이 개발된 이래, TCSEC을 근간으로 하여 ITSEC, CTCPEC 등 다양한 평가기준이 도입되었다. 국가마다 상이한 평가기준들은 국제적으로 상호인정이 되지 않아 해외 진출 시 해당 국가에서 다시 평가해야 하는 문제점이 존재하였으며, 이러한 문제점을 해결하기 위해 공통평가기준인 CC 인증으로 단일화되고 ISO/IEC 15408 국제표준으로 채택되어 현재까지 활용되고 있다.

CC인증은 하드웨어, 소프트웨어 등 IT제품의 보안요구사항과 평가 과정에서 그 제품에 적용되는 보증수단에 대한 공통 요구사항들을 제시함으로써 국가간 중복 인증에 따른 시간 및 비용을 절감하고 국제 표준 규격을 만족하는 정보보호제품을 보증한다. 다양한 보안 위협으로부터 중요 자산을 보호하고 보안수준을 향상시키기 위한 기업들의 니즈에 따라 매년 CC인증제품 수가 급증하고 있으며 평가제품 또한 다양화되고 있는 추세이다.

국내는 2002년 CC인증을 국내 평가기준으로 도입, 2005년 국내 정보보호제품 평가기준을 CC로 단일화함으로써 전 IT 제품군을 평가할 수 있는 기반을 마련하였으며, 국내용 532건, 국제용 77건, 총 609건의 정보보호제품이 CC인증을 획득하였다. 이는 정보보호제품 CC 평가 의무화, CC 평가·인증제도의 국제용, 국내용 이원화 및 지속적인 평가기관 추가 지정 등 CC인증을 활성화하려는 다양한 시도가 있었기 때문이다. 그 결과 초기 국내 정보보호업체의 걸림돌로 여겨지던 CC인증이 국내에 안착할 수 있게 되었다.

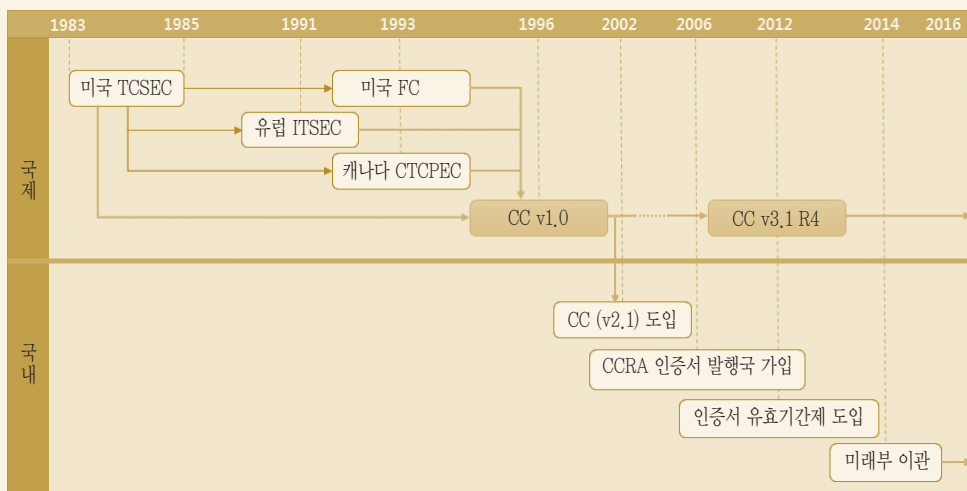
하지만 국내 정보보호제품이 국제적인 경쟁력을 확보하고 국내 CC인증이 향후 보다 활성화되기 위해서는 국제적으로 인정되는 보호프로파일의 적극적인 개발을 통한 인증대상 정보보호제품의 다양화, 급증하는 평가·인증 수요에 대한 대응책 마련, 국내 정보보호제품의 글로벌 시장 진출을 위한 국제용 CC인증제품 확보 등 지속적인 노력이 필요할 것이다.

I. 개요

정보기술이 급속도로 발달하고 기업이 보호해야 할 정보 및 자산이 증가함에 따라 악의적인 해커의 불법 공격 및 내부자의 도덕적 해이로 인한 정보유출 등을 미연에 방지하기 위한 정보보호의 중요성이 점점 커지고 있다. 이러한 정보보호 대책의 일환으로 정당하지 않은 사용자로부터 정보를 보호하기 위해 다양한 정보보호시스템이 도입되어 운영되고 있으며, 세계 각국은 이러한 정보보호시스템의 보안성에 대한 신뢰성 확보를 위해 다양한 평가기준을 개발해왔다.([그림 1])

[그림 1]

국내외 평가기준 발전과정



TCSEC, ITSEC 및 CTCPEC 등 미국, 유럽 등 여러 나라에서 개발되어 활용되고 있던 다양한 평가기준은 정보보호제품 공통평가기준(Common Criteria, 이하 CC인증)으로 단일화 되었다. 이에 국가마다 상이한 평가기준을 연동시켜 평가결과를 상호인정하기 위한 기반이 마련되었으며, ISO/IEC 15408 국제표준으로 채택되어 활용되고 있다. 국내도 보안성이 검증된 정보보호제품을 도입·운용할 수 있는 기반을 마련하기 위해 2002년 CC인증 제도를 도입하고 CCRA²⁾ 인증서 발행국에 가입하여 현재까지 CC인증체계를 유지하고 있다.

2) CCRA(Common Criteria Recognition Arrangement) : 국제 공통평가기준 상호인증 협정

본 고에서는 기존 정보보호제품 평가기준 및 CC인증에 대해 살펴보고, 국내외 CC인증 동향을 분석함으로써 국내 CC인증 제도의 국제 경쟁력을 제고하기 위한 향후 과제를 도출해 보고자 한다.

II. 국내외 정보보호제품 평가기준

1. 기존 평가기준

가. 미국 TCSEC

오랜지북으로 잘 알려진 TCSEC(Trusted Computer System Evaluation Criteria, 1983-1999)은 1983년 NCSC에 의해 초안이 만들어지고, 1985년 미국방성 표준(DoD STD 5200.28)으로 채택된 미국 최초의 정보보호제품 평가 기준이다. TCSEC는 컴퓨터 시스템의 보안을 효과적으로 평가하기 위해 보안정책(Security Policy), 책임성(Accountability), 신뢰성(Assurance), 문서화(Documentation) 등 4개의 보안 요구사항을 정의하고, 보안 요구사항을 만족하는 수준에 따라 7가지의 평가 등급을 제시하고 있다.

[표 1] TCSEC 평가 등급		
Division	등급	설명
Division D	D (Minimal Protection)	외부에 공개되어 보안이 전혀 고려되지 않은 시스템
Division C	C1 (Discretionary Security Protection)	데이터에 대한 읽기, 쓰기 권한을 사용자별로 정의, 사용자가 다른 사용자의 데이터를 임의로 접근 불가
	C2 (Controlled Access Protection)	각 사용자의 작업 내용을 기록, 감사할 수 있는 기능 제공
Division B	B1 (Labeled Security Protection)	각 데이터별로 보안 레벨이 정의되어 있으며, 낮은 보안 레벨을 지닌 사용자는 높은 보안 레벨이 정의된 데이터 접근 불가

	B2 (Structured Protection)	데이터를 접근하는데 필요한 구조화된 보안 정책이 시스템 내에 일정하게 유지, 각 사용자는 자신의 작업에 대한 최소한의 권한만 부여 받음
	B3 (Security Domain)	하드웨어 자원을 포함한 보안관리자 기능 및 위험 시 자가진단에 의해 시스템을 정지시키는 기능 존재하며, 운영체제 내부에 보안과 관련된 코드와 무관한 것들은 모두 제거
Division A	A1 (Verified Design)	수학적으로 보완이 완전하다는 것이 증명된 시스템으로 현존하지 않음

1988년 3월 발표된 TCSEC 관련 지침에서는 최소한 1992년까지 C2등급 이상, 2003년까지 B3등급 이상 충족할 것을 요구하였고, 이에 정보보호제품 개발사들은 이러한 TCSEC 보안 요구사항을 만족시키기 위해 지속적인 노력을 기울인 결과 보안수준이 상당히 향상되었다. 하지만 TCSEC은 호스트 환경의 보안을 위주로 평가하고 있어 그 범위가 제한적이며, 기밀성, 무결성, 가용성 중 기밀성을 최우선으로 하는 군사 및 정보기관에 적용하기에는 무리가 없었지만 무결성 및 가용성이 요구되는 금융 및 데이터처리 분야에 적용하기에는 부적합한 한계가 존재했다.

나. 유럽 ITSEC

ITSEC(Information Technology Security Evaluation Criteria)은 1991년 독일, 프랑스, 네덜란드, 영국 유럽 4개국이 평가제품의 상호 인정 및 평가기준이 상이함에 따른 정보보호 제품의 평가에 소요되는 시간, 인력 및 비용을 절감하기 위해 미국의 TCSEC 내용을 참조하여 제정되었다. ITSEC은 TCSEC에 상응하는 기밀성을 제공할 뿐만 아니라 무결성 및 가용성에 관한 평가기준도 포함하는 포괄적인 표준안을 제시하고 있다. ITSEC은 식별 및 인증(Identification and Authentication), 접근통제(Access Control), 감사(Audit), 객체 재사용(Object Reuse), 정확성(Accuracy), 서비스 신뢰성(Reliability of Service), 데이터 교환(Data Exchange) 등 7개의 보안기능 요구사항으로 분류되어 평가된다.

ITSEC의 등급은 TCSEC과의 호환을 위한 F-C1(C1), F-C2(C2), F-B1(B1), F-B2(B2) 및 F-B3(B3~A1) 및 F-IN(무결성 강화), F-AV(가용성 강화), F-DI(전송데이터의 무결성 강화), F-DC(전송데이터의 비밀성 강화) 및 F-DX(전송데이터의 비밀성과 무결성 강화) 등 총 10개로 구분된다

다. 캐나다 CTCPEC

캐나다 CTCPEC(Canadian Trusted Computer Product Evaluation Criteria, 1993)은 캐나다의 CSE(Communications Security Establishment)가 1989년 개발을 시작하여 1993년 버전 3.0을 완성한 평가기준으로 비밀성, 무결성, 가용성, 책임성의 4가지 분류로 구분되며 각 기능에 대한 세부 보안 요구사항을 기술하고 있다. 보증의 평가등급은 T1~T7의 7등급으로 구분되며, T0은 부적합 판정을 의미한다. 평가 시 제품의 서비스 수준 전체를 평가하여 해당 보증등급에 부합하는지를 결정한다. 기능에 대해서는 제품에 존재하는 기능에 대한 서비스 수준을 명시하며, 만약 제품이 목표하는 서비스 수준의 요구사항에 부합하지 못하고 또한 그 이하의 서비스 수준의 요구사항에도 부합하지 못하면 T0 등급으로 평가되며, 제공하지 않는 서비스의 수준은 명시하지 않는다.

2. CC인증 개요

정보보호시스템의 공통평가기준으로 현재 국내외에 널리 사용되고 있는 CC인증은 국가마다 상이한 평가기준을 연동시키고 평가결과를 상호인정하기 위해 제정된 평가기준으로 1999년 6월 ISO/IEC 15408 국제표준으로 승인되었다. CC인증은 미국의 TCSEC, 유럽의 ITSEC, 캐나다의 CTCPEC 등을 기반으로 개발되었으며, 각국에서 활용되고 있던 다양한 평가기준을 단일화하여 공통의 언어와 이해를 기반으로 한 CC를 개발하게 되었고 개발자 및 사용자 등 IT 제품 시장의 요구사항을 반영하여 발전해 왔다.

CC인증은 하드웨어, 소프트웨어 등 IT제품의 보안요구사항과 평가 과정에서 그 제품들에 적용되는 보증수단에 대한 공통의 요구사항들을 제시함으로써 독립적으로 수행된 보안성 평가의 결과들을 비교할 수 있도록 한다. CC 개발 연혁은 [표 2]와 같다.

[표 2] CC 개발 연혁			
연도	CC 개발 내용	관련 표준화	주관
1993	개발합의	—	미국, 영국, 독일, 프랑스, 캐나다, 네덜란드
1994	CC V0.6	—	
	CC V0.9	—	CCEB (CC Editorial Board)
1996	CC V1.0	—	
1997	CEM V0.6	—	CCIB (CC Implementation Board)
	CC V1.02 (Alpha)	—	
	CC V2.0 (Beta)	—	CCIMB (CC Interpretations Management Board)
	CC V2.0 (Draft)	—	
1998	CC V2.0	—	
1999	CC V2.1	ISO/IEC 15408:1999	
2003	CC V2.2	—	CCMB (CC Management Board)
2005	CC V2.3	ISO/IEC 15408:2005 ISO/IEC 18045:2005	
2006	CC V3.1 R1	—	
2007	CC V3.1 R2	—	
2009	CC V3.1 R3	ISO/IEC 15408:2009	
2012	CC V3.1 R4	—	

CC인증은 CCRA에 의거하여 협정 가입국에서 평가·인증을 받은 제품은 협정에 참여한 어떤 국가에서도 다시 평가를 거치지 않고 동일한 효력을 가지게 된다. 즉, 정보보호 제품을 상호인정 함으로써 여러 국가에서 다시 평가해야 하는 부담을 줄여 국가 간 교역장벽을 낮춤으로써 수출을 용이하게 하고 글로벌 시장형성을 촉진하고자 한다.

CCRA는 인증서를 발행하는 인증서 발행국(Certificate Authorizing Members)과 인증서는 발행하지 않고 이를 인정하는 인증서 수용국(Certificate Consuming Members)으로 구분되며, 우리나라는 국제 활동에 능동적으로 참여하기 위하여 2006년 5월 CCRA 인증서 발행국으로 가입하였다.

[표 3] CC Members (2015년 12월 기준)

연도	국가	인증기관 홈페이지
인증서 발행국 (17개국)	오스트레일리아	http://www.asd.gov.au/infosec/aisep
	캐나다	http://www.cse-cst.gc.ca/
	프랑스	http://www.ssi.gouv.fr/
	독일	http://www.bsi.bund.de/
	인도	http://www.commoncriteria-india.gov.in/
	이탈리아	http://www.ocsi.isticom.it/
	일본	http://www.ipa.go.jp/security/jisec/jisec_e/
	말레이시아	http://www.cybersecurity.my/mycc
	네덜란드	http://www.tuv-nederland.nl/nl/17/common_criteria.html
	뉴질랜드	http://www.dsd.gov.au/infosec
	노르웨이	http://www.sertit.no/
	대한민국	http://itscc.kr
	스페인	http://oc.ccn.cni.es
	스웨덴	http://fmv.se/en/Our-activities/CSEC---The-Swedish-Certification-Body-for-IT-Security/
	터키	http://bilisim.tse.org.tr/tr/icerikkategori/942/950/isoiec-15408-cc-ortak-kriterler.aspx
	영국	http://www.niap-ccevs.org/
	미국	http://www.niap-ccevs.org/
인증서 수용국 (8개국)	오스트리아	http://www.digitales.oesterreich.gv.at/
	체코	http://www.nbu.cz/en/
	덴마크	http://www.nbu.cz/en/
	핀란드	http://www.ficora.fi/en/
	그리스	http://www.nis.gr/
	헝가리	http://www.kormany.hu/en/ministry-of-national-development
	이스라엘	http://www.sii.org.il/20-en/SII_EN.aspx
	파키스탄	http://www.commoncriteria.org.pk/

자료 : CCRA 홈페이지

2. CC인증 구성

CC는 기본개념, 보안기능요구사항, 보증요구사항을 각각 설명하는 세 부분으로 구성된다. “제1부 소개 및 일반모델”은 보안성 평가의 원칙과 일반 개념을 정의하고 평가의 보편적인 모델을 제시하고 있다. “제2부 보안기능요구사항”에서는 정보보호제품이 갖는 다양한 보안 기능에 대한 요구사항을 정의하고 있으며, 이는 보호프로파일(PP, Protection Profile)이나

보안목표명세서(ST, Security Target)에서 명시된 보안기능 요구사항(SFR, Security Functional Requirements)을 표현하는데 기초가 된다. “제3부 보증요구사항”에서는 보증 등급(EAL, Evaluation Assurance Level) 별 요구되는 문서와 내용에 대해 다루고 있다.

가. 보안기능요구사항

보안기능요구사항은 정보보호제품이 고려해야 하는 모든 보안기능과 관련된 요구사항을 적절한 기준에 따라 분류하고, 표준의 형식에 맞추어 제시함으로써 TOE³⁾ 보안 행동을 설명하고자 하는 것으로 뒤에서 설명할 보호프로파일이나 보안목표명세서에서 서술된 보안목적을 만족시키기 위하여 사용되며, [표 4]와 같이 11개의 클래스로 구성되어 있다.

[표 4] 보안기능요구사항		
클래스	패밀리	설명
보안감사 (Security Audit)	보안감사 자동대응(FAU_ARP)	보안활동에 관련되는 정보를 인식, 기록, 저장 및 분석할 수 있도록 6개의 패밀리로 구성되어 있으며 보안관련 사건 발생 시 감사대상사건에 부합하는 시스템 활동을 감사레코드에 기록 저장하여 관리자나 인가된 사용자가 필요시에 감사관련 자료들을 검토할 수있게 함
	보안감사 데이터 생성(FAU_GEN)	
	보안감사 분석(FAU_SAA)	
	보안감사 검토(FAU_SAR)	
	보안감사 사건 선택(FAU_SEL)	
	보안감사 사건 저장(FAU_STG)	
통신 (Communication)	발신 부인방지(FCO_NRO)	데이터 교환시 송수신자의 신원을 보증 및 확인할 수 있는 요구사항
	수신 부인방지(FCO_NRR)	
암호 지원 (Cryptographic support)	암호키 관리(FCS_CKM)	암호키 생성, 분배, 접근 및 파괴 행동 및 암호 알고리즘, 암호키 길이 등에 대한 요구사항
	암호 연산(FCS_COP)	

3) TOE(Target of Evaluation) : CC인증 평가의 대상이 되는 소프트웨어, 펌웨어 및 하드웨어의 집합

사용자 데이터 보호 (User Data Protection)	접근통제 정책(FDP_ACC)	보안기능으로 사용자 데이터 보호정책 및 보호형태, 오프라인 저장, 데이터 유출, 유입 등에 대한 보안기능 요구사항
	접근통제 기능(FDP_ACF)	
	데이터 인증(FDP_DAU)	
	TOE로부터의 사용자 데이터 유출 (FDP_ETC)	
	정보흐름통제 정책(FDP_IFC)	
	TOE 외부로부터 사용자 데이터 유입 (FDP_ITC)	
	TOE 내부전송(FDP_ITT)	
	잔여정보 보호(FDP_RIP)	
	복귀(FDP_ROL)	
	저장된 데이터의 무결성(FDP_SDI)	
	TSF ⁴⁾ 간 전송되는 사용자 데이터 비밀성(FDP_UCT)	
	TSF 간 전송되는 사용자 데이터 무결성(FDP_UIT)	
식별 및 인증 (Identification & Authentication)	인증실패(FIA_AFL)	사용자 신원을 식별하고 검증하는 기능에 대한 요구사항
	사용자 속성 정의(FIA_ATD)	
	비밀정보의 검증 및 생성(FIA_SOS)	
	사용자 인증(FIA_UAU)	
	사용자 식별(FIA_UID)	
보안 관리 (Security Management)	사용자-주체 연결(FIA_USB)	시스템 운영에 대한 융통성을 허용하면서 사용자의 프라이버시 보호를 만족시키기 위한 요구사항
	TSF 기능 관리(FMT_MOF)	
	보안속성 관리(FMT_MSA)	
	TSF 데이터 관리(FMT_MTD)	
	폐지(FMT_REV)	
	보안속성 유효기간(FMT_RAE)	
	관리기능 명세(FMT_SMF)	
프라이버시 (Privacy)	보안 역할 관리(FMT_SMR)	보안속성 및 보안기능 관련 여러 사항을 관리하는 보안기능에 대한 요구사항
	익명성(FPR_ANO)	
	가명성(FPR_PSE)	
	연계불가성(FPR_UNL)	
TSF 보호 (Protection of the TSF)	관찰불가성(FPR_UNO)	보안기능을 제공하는 메커니즘의 무결성 및 보안 기능 데이터의 무결성 관련 기능 요구사항
	안전한 상태 유지(FPT_FLS)	
	외부전송 TSF 데이터의 가용성 (FPT_ITA)	
	외부전송 TSF 데이터의 비밀성 (FPT_ITC)	
	외부전송 TSF 데이터의 무결성 (FPT_ITI)	
	TSF 데이터 내부전송(FPT_ITT)	
	TSF의 물리적 보호(FPT_PHP)	
	안전한 복귀(FPT_RCV)	

4) TSF(TOE Security Functionality, TOE 보안기능성) : 보안기능요구사항을 정확하게 수행하기 위하여 필요한 TOE 기능들을 총칭

	재사용 공격 탐지(FPT_RPL)	
	상태 동기화 프로토콜(FPT_SSP)	
	타임스탬프(FPT_STM)	
	TSF간 전송되는 TSF 데이터의 일관성(FPT_TDC)	
	외부 실체 시험(FPT_TEE)	
	내부 복제 TSF 데이터의 일관성(FPT_TRC)	
	TSF 자체 시험(FPT_TST)	
자원 활용 (Resource utilization)	오류에 대한 내성(FRU_FLT)	처리 능력 및 저장 용량과 같은 요구된 자원의 가용성을 지원하는 보안기능 요구사항
	자원사용 우선순위(FRU_PRS)	
	자원 할당(FRU_RSA)	
TOE 접근 (TOE access)	선택 가능한 보안속성의 범위제한(FTA_LSA)	사용자 세션 설정을 통제하기 위한 기능 요구사항
	동시 세션수의 제한(FTA_MCS)	
	세션 잠금 및 종료(FTA_SSL)	
	TOE 접근 경고(FTA_TAB)	
	TOE 접근 이력(FTA_TAH)	
	TOE 세션 설정(FTA_TSE)	
안전한 경로/채널 (Trusted path/channel)	TSF간 안전한 채널(FTP_ITC)	사용자와 보안 기능 사이의 신뢰된 통신경로 및 보안기능과 신뢰된 IT 제품 사이의 신뢰된 통신 채널에 관한 요구사항
	안전한 경로(FTP_TRP)	

자료 : 정보보호시스템 공통평가기준 CC/CEM V3.1 R4 (IT보안인증사무국)

예를 들어 보안감사 클래스의 보안감사 자동대응(FAU_ARP) 패밀리는 잠재적인 보안 위반을 암시하는 사건을 탐지하는 경우 취해야 할 대응행동으로써, “제2부 보안기능요구사항”에 “TSF는 잠재적인 보안 위반을 탐지한 경우, [할당 : 행동 목록]을 취해야 한다.”라고 정의하고 있으며, 보호프로파일 또는 보안목표명세서 작성 시 [할당 : 행동목록] 등의 매개변수를 구체적으로 명시하여 해당 보안기능요구사항을 기술하게 된다.

나. 보증요구사항

보증요구사항(SAR, Security Assurance Requirement)은 TOE의 보증수준을 측정하기 위한 표준화된 척도로서, 정보보호제품의 보증등급을 결정하는 기준이 된다. 보증등급은 EAL1부터 EAL7까지 7단계로 분류되며 등급별 요구하는 수준을 만족했는지 여부를 평가한다. 보증요구사항은 보안기능요구사항들이 체계적으로 구성되어 TOE의 보안목표를 만족하는

가를 검토하기 위해 사용되며, TOE에 구현된 기능들이 제대로 개발되었는지와 이를 안전한 환경 하에서 개발하였는지를 보증하기 위한 보증 컴포넌트들의 집합으로 이루어져 있다.

[표 5] 보증요구사항

클래스	패밀리	설명
보호프로파일 평가 (Protection Profile evaluation)	보호프로파일 소개(APE_INT)	보호프로파일이 타당하고 내부적으로 일관성이 있으며, 하나 이상의 다른 보호프로파일이나 패키지에 근거하고 있을 경우 그것들을 정확히 실체화한 것임을 입증하기 위해 필요한 활동
	준수 선언(APE_CCL)	
	보안문제정의(APE_SPD)	
	보안목적(APE_OBJ)	
	확장 컴포넌트 정의(APE_ECD)	
보안목표명세서 평가 (Security Target evaluation)	보안요구사항(APE_REQ)	보안목표명세서가 타당하고 내부적으로 일관성이 있으며, 하나 이상의 다른 보호프로파일이나 패키지에 근거하고 있을 경우 그것들을 정확히 실체화한 것임을 입증하기 위해 필요한 활동
	보안목표명세서 소개(ASE_INT)	
	준수 선언(ASE_CCL)	
	보안문제정의(ASE_SPD)	
	보안목적(ASE_OBJ)	
	확장 컴포넌트 정의(ASE_ECD)	
	보안요구사항(ASE_REQ)	
개발 (Development)	TOE 요약명세서(ASE_TSS)	다양한 추상화 수준 및 형태의 관점에서 TSF를 구조화하고 표현하기 위한 요구사항을 정의
	보안 아키텍처(ADV_ARC)	
	기능명세서(ADV_FSP)	
	구현의 표현(ADV_IMP)	
	TSF 내부(ADV_INT)	
	보안정책모델(ADV_SPM)	
설명서 (Guidance documents)	TOE 설계(ADV_TDS)	모든 사용자 역할에 대한 설명서의 요구사항을 제공하며, TOE의 안전한 준비와 운영을 위하여 TOE의 안전한 관리에 관련된 모든 측면이 서술되어야 함
	사용자 운영 설명서(AGD_OPE)	
생명주기 지원 (Life cycle support)	준비 절차(AGD_PRE)	개발 및 유지하는 동안 TOE의 상세화 과정에서 규칙 및 통제를 수립
	형상관리 능력(ALC_CMC)	
	형상관리 범위(ALC_CMS)	
	배포(ALC_DEL)	
	개발 보안(ALC_DVS)	
	결합교정(ALC_FLR)	
	생명주기 정의(ALC_LCD)	
	도구와 기법(ALC_TAT)	

시험 (Tests)	범위(ATE_COV)	TSF가 기능명세, TOE설계, 구현표현에 서술된 대로 동작함을 보증
	상세수준(ATE_DPT)	
	기능 시험(ATE_FUN)	
	독립적인 시험(ATE_IND)	
취약성 평가 (Vulnerability assessment)	취약성 분석(AVA_VLA)	TOE의 개발이나 운영 중에 악용 가능한 취약성이 발생할 가능성을 다룸
합성 (Composition)	합성에 대한 이론적 근거(ACO_COR)	합성 TOE가 기존에 평가된 소프트웨어, 펌웨어, 하드웨어 컴포넌트에 의해 제공되는 보안기능성에 의존하는 경우 안전하게 동작한다는 신뢰를 제공하기 위해 고안된 보증요구사항들을 명세
	개발 증거(ACO_DEV)	
	종속 컴포넌트의 의존성(ACO_REL)	
	합성 TOE 시험(ACO_CTT)	
	합성 취약성 분석(ACO_VUL)	

자료 : 정보보호시스템 공통평가기준 CC/CEM V3.1 R4 (IT보안인증사무국)

다. 보호프로파일 및 보안목표명세서

소비자가 개발자로부터 제품을 구매하려고 하는 경우, 일반적으로 소비자는 제품에 대한 요구사항을 작성하여 개발자에게 제공하고 개발자는 이 요구사항을 바탕으로 제품명세서를 작성하고 이를 기반으로 개발을 진행한다. 이와 같이 사용자의 보안 요구사항을 형식화한 문서가 보호프로파일이고, 보호프로파일을 사용하여 개발자가 작성한 제품명세가 보안목표명세서에 해당한다. 즉 보호프로파일은 구현에 독립적인 제품군(예: 침입탐지시스템)에 대한 요구사항을 명시하고 있으며, 보안목표명세서는 구현에 종속적인 특정 제품(예: A사의 침입탐지시스템)에 대한 제품명세를 명시하고 있다. 따라서 보안목표명세서는 보호프로파일을 준수해야 하며, 이는 제품이 모든 소비자 요구사항을 포함해야 한다는 것을 의미한다. 하지만 보안목표명세서는 보호프로파일보다 더 명세적일 수 있기 때문에 세부사항을 더 많이 포함할 수 있다.

보호프로파일은 소비자의 요구를 명세하기 위해 보안요구사항들을 구현에 독립적인 방식으로 정의한 것으로, 소비자들은 특정 제품에 관계없이 IT 보안성에 대한 요구를 표현할 수 있다. 보호프로파일은 일련의 보안요구사항들을 포함하고 있는데, 이는 공통평가기준에서 선택된 보안요구사항 또는 별도로 명시된 보안요구사항들로 구성되며, 재사용이 가능하다. 보호프로파일은 소비자들이 구체적인 보안 요구사항들을 참조할 수 있는 수단이 되기 때문에 이러한 요구사항에 관심이 있는 소비자 집단, 평가기관 또는 유관기관 등에 의해 개발이

이루어지게 된다.

[표 6] 보호프로파일 구조		
순서	제목	내용
1	보호프로파일 소개 1.1 보호프로파일 참조 1.2 TOE 개요	<ul style="list-style-type: none"> - 보호프로파일 제목, 버전, 작성자 등 기술 - TOE를 간략히 서술한 TOE 개요
2	준수선언 2.1 공통평가기준 준수 선언 2.2 보호프로파일 준수 선언 2.3 패키지 준수 선언 2.4 준수 선언의 이론적 근거 2.5 보호프로파일 준수 방법	<ul style="list-style-type: none"> - 보호프로파일이 어떻게 다른 보호프로파일 및 패키지를 준수하는지 서술
3	보안문제정의 3.1 위협 3.2 조직의 보안정책 3.3 가정사항	<ul style="list-style-type: none"> - TOE, TOE 운영환경, 또는 그 모두에 의해 대응될 위협 및 조직의 보안정책을 서술 - 보안 기능성을 제공하기 위해 운영환경에 요구되는 가정사항을 서술
4	보안목적 4.1 TOE에 대한 보안목적 4.2 운영환경에 대한 보안목적 4.3 보안목적의 이론적 근거	<ul style="list-style-type: none"> - 보안문제정의에서 서술된 문제에 대한 해결책을 간결하고 추상적인 문장으로 표현
5	확장 컴포넌트 정의	<ul style="list-style-type: none"> - 공통평가기준에 명시되지 않은 보안요구사항을 포함할 경우 새로운 컴포넌트로 정의
6	보안요구사항 6.1 보안기능요구사항 6.2 보증요구사항 6.3 보안요구사항의 이론적 근거	<ul style="list-style-type: none"> - 보안기능요구사항 및 보증요구사항 기술
자료 : 정보보호시스템 공통평가기준 CC/CEM V3.1 R4 (IT보안인증사무국)		

보안목표명세서는 TOE 평가를 위한 근거로 사용되는 보안요구사항과 기능명세의 집합으로, 보안요구사항은 보호프로파일로부터 정의될 수 있고, 공통평가기준의 보안기능요구사항 컴포넌트 및 보증요구사항 컴포넌트를 사용하여 직접 정의할 수도 있으며, 공통평가기준에 포함되지 않은 보안요구사항을 사용하여 정의될 수도 있다.

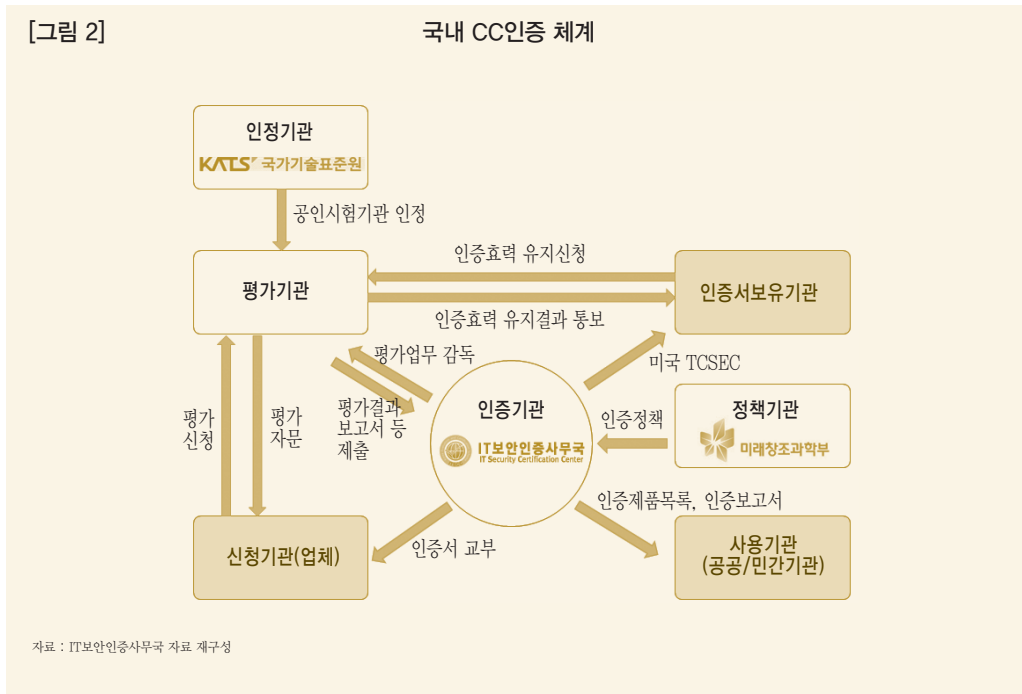
[표 7] 보안목표명세서 구조

순서	제목	내용
1	보안목표명세서 소개 1.1 보안목표명세서 참조 1.2 TOE 참조 1.3 TOE 개요 1.4 TOE 설명	<ul style="list-style-type: none"> - 보안목표명세서 제목, 버전, 작성자 등 기술 - TOE를 서술한 TOE 개요 및 설명
2	준수선언 2.1 공통평가기준 준수 선언 2.2 보호프로파일 준수 선언 2.3 패키지 준수 선언 2.4 준수 선언의 이론적 근거	<ul style="list-style-type: none"> - 보안목표명세서가 공통평가기준, 보호프로파일(존재할 경우), 패키지(존재할 경우) 내용을 준수하는지 서술
3	보안문제정의 3.1 위협 3.2 조직의 보안정책 3.3 가정사항	<ul style="list-style-type: none"> - TOE, TOE 운영환경, 또는 그 모두에 의해 대응될 위협 및 조직의 보안정책을 서술 - 보안 기능성을 제공하기 위해 운영환경에 요구되는 가정사항을 서술
4	보안목적 4.1 TOE 보안목적 4.2 운영환경에 대한 보안목적 4.3 보안목적의 이론적 근거	<ul style="list-style-type: none"> - 보안문제정의에서 서술된 문제에 대한 해결책을 간결하고 추상적인 문장으로 표현
5	확장 컴포넌트 정의	<ul style="list-style-type: none"> - 공통평가기준에 명시되지 않은 보안요구사항을 포함할 경우 새로운 컴포넌트로 정의
6	보안요구사항 6.1 보안기능요구사항 6.2 보증요구사항 6.3 보안요구사항의 이론적 근거	<ul style="list-style-type: none"> - 보안기능요구사항 및 보증요구사항 기술
7	TOE 요약명세	<ul style="list-style-type: none"> - 보안기능요구사항 및 보증요구사항 기술- TOE의 잠재적인 소비자에게 TOE가 모든 보안기능요구사항을 만족시키는 방법을 설명

자료 : 정보보호시스템 공통평가기준 CC/CEM V3.1 R4 (IT보안인증사무국)

4. 국내 CC인증 체계

국내 정보보호제품 평가·인증제도는 「국가정보화 기본법」 제38조 및 동법 시행령 제35조, 「정보보호시스템 평가·인증지침」(미래창조과학부고시 제2013-52호, 2013.8.8.)에 근거하여 운영되며 체계는 [그림 2]와 같다.



정책기관인 미래창조과학부는 정보보호제품 등의 인증에 관한 국가정책 결정, 평가인증 수행규정, 평가기준방법론, 보호프로파일 등을 수립 및 시행한다. 또한 인증기관 지정 및 철회, 인증기관의 인증업무 감독 및 인증자 자격관리, 인증기관 보안관리 실태점검 등의 역할을 담당한다.

인증기관인 IT보안인증사무국은 평가기관의 평가업무 감독 및 평가자 자격관리, 평가기관 보안관리 실태점검, 인증보고서 작성 인증서 발급, CCRA 관련 활동, 인증제품에 대한 사후 관리 및 평가기관 승인 및 취소 역할을 수행하고 있다.

평가기관은 평가업무 수행에 관한 규정 수립 및 시행, 평가계약체결 및 평가수행, 평가관련 간행물 발간, 개발자 대상 개발환경 보안점검 수행 등의 역할을 수행하며, 현재 국내에는

CCRA 협정에 의거 승인서가 발행된 총 7개의 평가기관이 있다

[표 8] 국내 CC인증 평가기관		
평가기관명	지정년도	홈페이지
한국인터넷진흥원	1998	http://www.kisa.or.kr
한국산업기술시험원	2007	http://www.ktl.re.kr
한국시스템보증	2007	http://www.kosyas.com
한국아이티평가원	2009	http://www.ksel.co.kr
한국정보통신기술협회	2009	http://www.tta.or.kr
한국정보보안기술원	2014	http://www.koist.kr
한국기계전기전자시험연구원	2014	http://www.ktc.re.kr
자료 : IT보안인증사무국		

국내 정보보호제품 평가·인증제도는 금융기관 및 공공기관이 주요 자산을 보호하기 위해 보안성이 검증된 정보보호제품을 도입·운용할 수 있도록 하기 위해 1995년 처음으로 그 기반이 마련되었으며, 침입차단시스템 및 침입탐지시스템에 대한 평가기준을 개발하여 적용해 왔다. 2002년 CC인증이 국내 평가 기준으로 도입되어 전 IT 제품군을 평가할 수 있는 기반을 마련하게 되었으며, 2005년 국내 정보보호제품 평가기준을 CC로 단일화하였다. 이 후 2006년 CCRA 인증서 발행국에 가입함으로써 국내 정보보호제품의 해외 진출의 발판을 마련하였다. 또한 정부·공공기관 사용 정보보호제품에 대해 CC 평가를 의무화하였다.

[표 9] 국내 평가·인증제도 연혁	
연도	연혁
1995	「정보화촉진기본법 제15조」에 의거, 정보보호제품 평가 기반 마련
1998	정보통신망 침입차단시스템 평가기준 고시
2000	정보통신망 침입탐지시스템 평가기준 고시
2002	CC 국내 평가 기준 도입
2005	국내 평가기준을 CC로 단일화
2006	정부·공공기관 사용 정보보호제품 CC 평가 의무화
	CCRA 인증서 발행국 가입

2007	CC 평가 · 인증제도 국제용/국내용으로 이원화
	복수 평가기관 제도 도입, 2개 평가기관 추가 지정
2009	2개 평가기관 추가 지정
2010	국내용 평가 · 인증제도 간소화
2012	인증서 유효기간제(3년) 신설
	국가사이버안전센터 산하 IT보안인증사무국을 국가보안기술연구소로 이관
2014	CC인증 정책 업무가 국가정보원에서 미래창조과학부로 이관
	2개 평가기관 추가 지정
2015	국가기관 인증제품 사용 의무 폐지

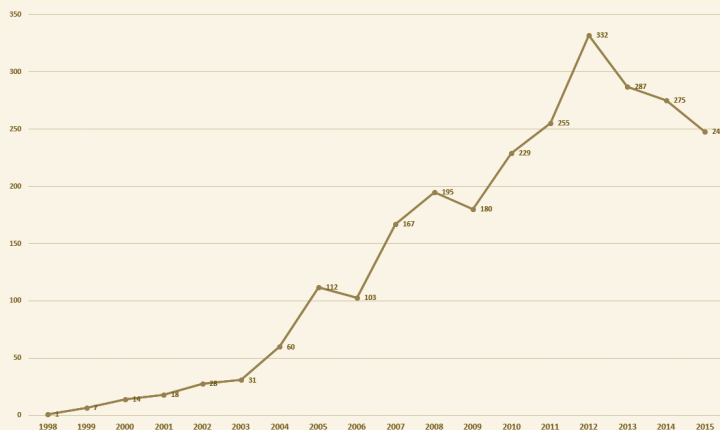
2007년에는 평가기간이 오래 소요되고 평가비용이 높은 국제용 CC인증 제도를 국제용과 국내용으로 이원화하였다. 이는 국내 시장에서는 국내용 CC인증을 허용함으로써 정보보호 업체의 경제적 부담을 완화시키고, 평가수요에 대한 적체를 해소함으로써 적시에 제품이 사용기관에 도입될 수 있도록 하기 위함이었다. 2014년 10월에는 CC인증 정책기관이 기존 국가정보원에서 미래창조과학부로 이관이 되어 수행되고 있으며, 2015년에는 금융기관이 도입하는 정보보호제품을 국가기관 평가 · 인증 제품으로 한정하던 의무가 폐지되어 금융회사 자율적 판단 하에 다양한 정보보호 제품 · 솔루션 활용이 가능하게 되었다.

Ⅲ. 국내외 CC인증 동향

1. 국제 동향

CCRA 홈페이지에 등록된 연도별 CC인증제품 목록에 따르면 CC인증이 1998년도부터 시작된 이래 꾸준히 CC인증제품은 그 수가 증가하고 있으며 초창기와 비교했을 때 최근의 평가 수요는 급증했음을 알 수 있다.

[그림 3] 연도별 CC인증제품 (2015년 12월 기준)

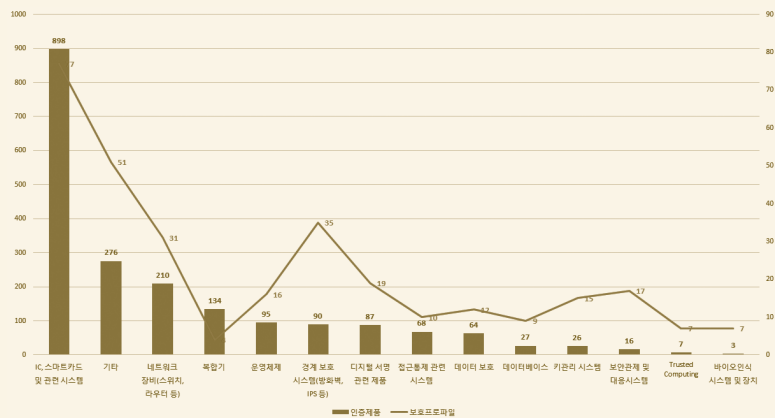


자료 : CCRA 홈페이지 통계자료 재구성

이는 공신력 있는 기관으로부터 보안성에 대한 인증을 취득한 정보보호제품에 대한 수요자의 니즈가 증가하고 있으며, 이러한 니즈를 만족시키고 국제적인 경쟁력을 제고하기 위한 정보보호업체들의 노력의 결과라 할 수 있다. 또한 과거에는 전형적인 보안제품인 방화벽, IDS 등 일부 정보보호제품이 평가되었으나 최근 IT기술의 확대와 인터넷 등의 발달로 인하여 다양한 제품의 평가가 이루어지고 있기 때문에 인증제품 수가 급증한 것으로 보인다.

[그림 4]는 CC인증제품 및 보호프로파일 현황을 제품군별로 분류하여 보여준다. 통계에서 알 수 있듯이 IC, 스마트카드 및 관련시스템 제품군에 대한 인증이 상당부분을 차지하고 있으며, 기존의 IT 제품군 분류 체계에 부합하지 않는 기타 제품군(스마트폰, 태블릿 및 프린터 등 다양한 제품)에서 인증이 활발하게 이루어지고 있음을 알 수 있다. 제품군별 개발된 보호 프로파일 현황은 대체적으로 CC인증제품수에 비례하였다.

[그림 4] 제품군별 CC인증제품 및 보호프로파일 현황 (2015년 12월 기준)

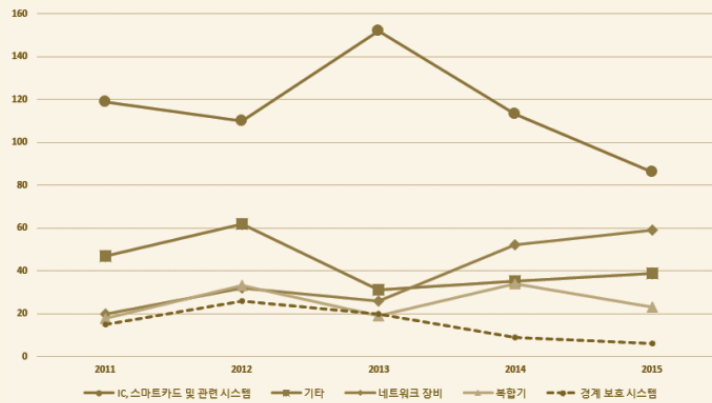


자료 : CCRA 홈페이지 통계자료 재구성

[그림 5]는 최근 5년간 CC인증을 받은 제품군의 통계자료로써 [그림4]의 순위와 거의 동일한 결과를 보여준다. 이는 최근 5년 동안 CC인증을 받은 제품의 수(1,397개)가 전체의 55%를 차지하여 전체 순위에 큰 영향을 미치기 때문이다. 또한 IC, 스마트카드 및 관련시스템 제품군의 CC인증 제품수(581개)는 최근 5년 CC인증을 받은 전체 제품의 22.9%를 차지하고 있어 해당 제품군에 대한 CC인증이 국외에서 활발하게 이루어지고 있음을 알 수 있다. 그래프는 상위 5개 제품군에 대한 통계이며, 그 뒤로 데이터 보호, 운영체제, 접근통제 관련 시스템, 디지털 서명 관련 제품 등의 순으로 나타났다.

[그림 5]

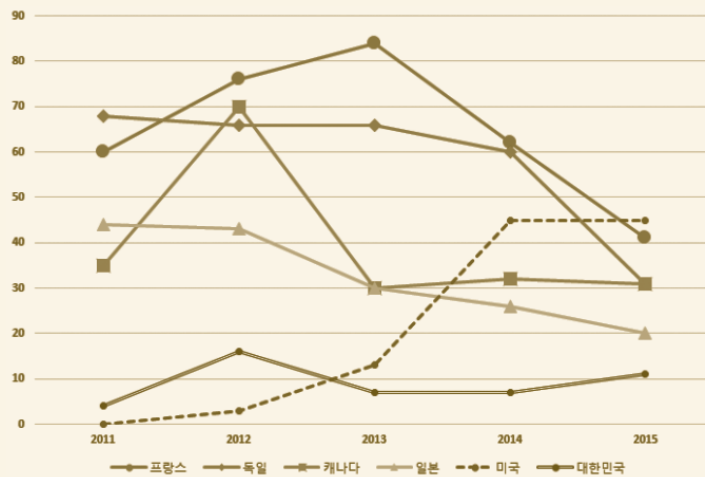
최근 5년 제품군별 CC인증제품 현황



자료 : CCRA 홈페이지 통계자료 재구성

[그림 6]

최근 5년 국가별 CC인증제품 현황



자료 : CCRA 홈페이지 통계자료 재구성

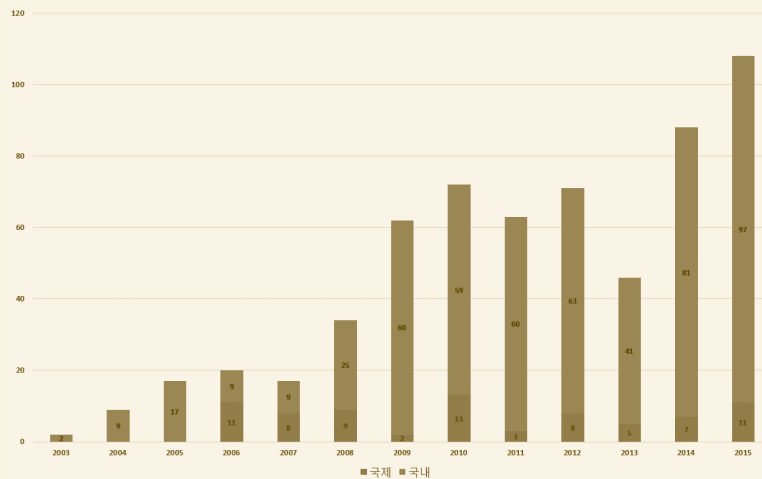
최근 5년간 국가별 CC인증제품수를 비교했을 때 CC인증이 가장 활발한 나라는 프랑스였으며, 독일, 캐나다, 일본, 미국, 스페인, 우리나라 순으로 나타났다. 우리나라는 17개 인증서 발행국 중 7위를 차지하였으며 전체 CC인증제품수의 3.2%를 차지하였다. 특히 미국의 경우 2011년까지는 CC인증이 활발하지 않았으나, 최근 그 성장속도가 두드러져 향후 정보보호제품 시장을 선도할 가능성이 클 것으로 전망된다.

2. 국내 동향

2015년 12월 기준, CC인증을 받은 정보보호제품은 인증서 유효기간이 경과하여 효력이 만료된 제품 및 인증 취소된 제품을 포함하여 국내용 532건, 국제용 77건 등 총 609건이다. [그림 7]에서 알 수 있듯이 CC인증이 국내 평가 기준으로 도입된 이래 CC인증을 획득한 제품 수는 해마다 그 수가 증가하고 있다.

[그림 7]

연도별 국내 CC인증제품 (2015년 12월 기준)



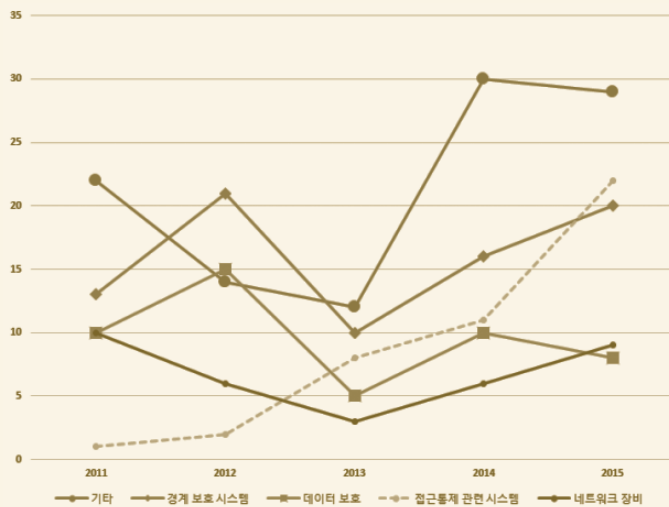
자료 : IT보안인증사무국 홈페이지 통계자료 재구성

이는 정보보호제품 CC 평가 의무화, CC 평가·인증제도의 국제용, 국내용 이원화 및 지속적인 평가기관 추가 지정 등 CC인증을 활성화하려는 다양한 시도가 있었기 때문으로 보인다. 그 결과 초기 국내 정보보호업체의 걸림돌로 여겨지던 CC인증이 국내에 어느 정도 안착되었고, 정보보호업체 또한 CC인증을 별도의 프로세스라기 보다는 제품 개발 라이프사이클의 일부로 여길 만큼 인식 또한 많이 바뀌게 되었다. 하지만 국내용 CC인증을 받은 제품은 꾸준히 증가하고 있는데 반해 국제용 CC인증을 받은 제품은 매우 드물며, 거의 일정한 수준을 유지하고 있어 국내 보안업체들이 글로벌 시장에서 경쟁력을 갖추기 위해서 국제용 CC인증제품을 확보하기 위한 노력이 필요할 것이다.

[그림 8]은 최근 5년간 국내 CC인증을 받은 제품군의 통계자료로써 기타 제품군(취약점 점검도구, ActiveX 보안프로그램 등), 경계 보호 시스템(방화벽, IPS 등)이 가장 큰 비중을 차지하고 있다.

[그림 8]

최근 5년 제품군별 국내 CC인증제품 현황



자료 : IT보안인증사무국 홈페이지 통계자료 재구

IC, 스마트카드 및 관련시스템 제품군에 대한 CC인증이 활발하게 진행되고 있는 국제 동향과는 달리 국내의 경우는 CC인증이 도입된 후부터 지금까지 경계 보호 시스템 제품군이 아직도 주류를 이루고 있어, 국제적인 동향을 예의주시하고 이를 국내에도 반영할 필요가 있다. 그래프는 상위 5개 제품군에 대한 통계이며, 그 뒤로 백신, 운영체제, IC, 스마트카드 및 관련 시스템, 복합기 등의 순으로 나타났다.

IV. 향후과제

1. 인증대상 정보보호제품의 다양화

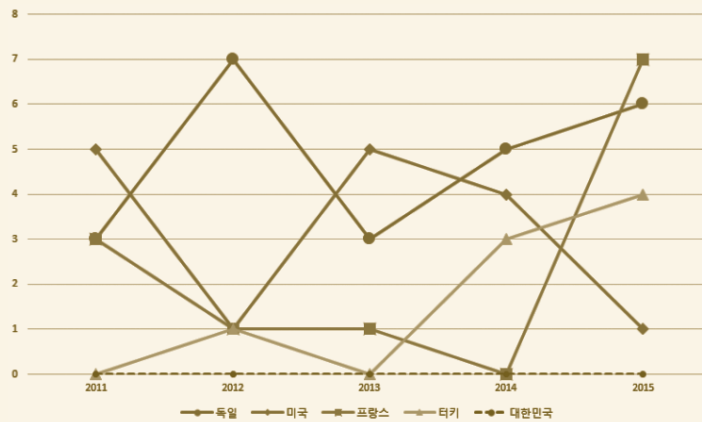
[표 10]은 국내에서 개발되어 인증기관인 IT보안인증사무국 홈페이지에 등록되어 있는 보호프로파일 리스트로써 2011년 “개방형 스마트카드 플랫폼 보호프로파일 V2.2”를 마지막으로 더 이상 보호프로파일이 개발되지 않고 있다.

[표 10] 보호프로파일 리스트		
보호프로파일명	보증등급	등재일
개방형 스마트카드 플랫폼 보호프로파일 V2.2	EAL4+	20110406
보안토큰 보호프로파일 V2.1	EAL3	20100610
네트워크 침입방지시스템 보호프로파일 V2.1	EAL3	20100610
전자여권 보호프로파일 V2.1	EAL4+	20100610
개방형 스마트카드 플랫폼 보호프로파일 V2.1	EAL4+	20100610
네트워크 스팸메일차단시스템 보호프로파일 V2.1	EAL2	20100610
소프트웨어 기반 보안USB 시스템 보호프로파일 V1.0	EAL2	20100423
IP Phone/IP PBX 통합 보호프로파일 V1.0	EAL2	20090814
전자여권 보호프로파일 V2.0	EAL4+	20090506
무선랜 인증시스템 보호프로파일 V2.0	EAL3	20080919
웹 응용프로그램 침입차단시스템 보호프로파일 V1.0	EAL3	20080919
암호기반 전자문서 유출방지시스템 보호프로파일 V1.0	EAL3	20080919
통합 보안관리시스템 보호프로파일 V2.0	EAL3	20080919

보안토큰 보호프로파일 V2.0	EAL3	20080729
역할기반 접근통제시스템 보호프로파일 V2.0	EAL3	20080729
침입차단시스템 보호프로파일 V2.0	EAL4	20080424
침입탐지시스템 보호프로파일 V2.0	EAL3	20080424
가상사설망 보호프로파일 V2.0	EAL3	20080424
등급기반 접근통제시스템 보호프로파일 V2.0	EAL3	20080424
개방형 스마트카드 플랫폼 보호프로파일 V2.0	EAL4+	20080424
지문인식시스템 보호프로파일 V2.0	EAL2	20080424
네트워크 스팸메일차단시스템 보호프로파일 V2.0	EAL2	20080424
네트워크 침입방지시스템 보호프로파일 V2.0	EAL3	20080424
보안토큰 보호프로파일 V1.0	EAL4	20080314
전자여권 보호프로파일 V1.0	EAL4+	20080104
통합 보안관리시스템 보호프로파일 V1.0	EAL3	20070105
무선랜 인증시스템 보호프로파일 V1.0	EAL4	20070105
네트워크 스팸메일차단시스템 보호프로파일 V1.0	EAL3	20070105
안티 바이러스 소프트웨어 보호프로파일 V1.0	EAL3	20070105
국가기관용 침입차단시스템·가상사설망 통합보호프로파일 V1.1	EAL2	20060517
국가기관용 개방형 스마트카드 플랫폼 보호프로파일 V1.1	EAL4+	20060517
국가기관용 가상사설망 보호프로파일 V1.2	EAL3+	20060517
국가기관용 침입탐지시스템 보호프로파일 V1.2	EAL3+	20060517
국가기관용 침입차단시스템 보호프로파일 V1.2	EAL3+	20060517
국가기관용 등급기반 접근통제시스템 보호프로파일 V1.1	EAL3+	20060517
국가기관용 지문인식시스템 보호프로파일 V1.1	EAL2+	20060517
역할기반 접근통제시스템 보호프로파일 V1.0	EAL4	20060310
네트워크 침입방지시스템(IPS) 보호프로파일 V1.1	EAL4	20051221
국가기관용 게이트웨이형 가상사설망 보호프로파일 V1.1	EAL3+	20030430

또한 [그림 9]는 최근 5년 국가별 보호프로파일 개발 현황을 나타낸 것으로 독일, 미국, 프랑스의 순으로 신규 보호프로파일을 개발하여 등록하였다. 하지만 우리나라의 경우 CCRA 인증서 발행국으로 가입한 이래 6개의 보호프로파일을 개발하였지만, 최근 5년간 개발한 보호프로파일은 하나도 없는 실정이다.

[그림 9] 최근 5년 국가별 보호프로파일 개발 현황



자료 : CCRA 홈페이지 통계자료 재구성

국외의 경우, 모바일 카드결제, NFC 결제, 스마트카드용 운영체제, 전자여권 등 “IC, 스마트카드 및 관련시스템” 제품군뿐만 아니라 생체인증 디바이스, 생체인증정보 위·변조 탐지 등 “바이오인식 시스템 및 장치”, 스마트폰, 태블릿 및 프린터 등 “기타” 제품군 등 다양한 정보보호제품들에 대한 보호프로파일 개발 및 CC인증이 활발하게 이루어지고 있다. 그에 반해 우리나라는 정보보호제품 개발 또는 평가·인증 시 활용 가능한 보호프로파일이 많이 개발되어 있지 않아 인증대상 정보보호제품이 다양하지 않은 실정이다.

물론 보호프로파일이 개발되지 않은 정보보호제품이라 하더라도 CC인증을 획득할 수 있으나, CC인증을 획득하기 위해 정보보호업체는 보호프로파일이라는 기준 없이 보안기능요구사항을 도출하여 해당 제품의 보안목표명세서를 직접 작성해야 하므로 상당한 노력과 시간이 소요되게 된다.

따라서 우리나라 정보보호제품의 향후 국제시장 진출의 발판을 마련하기 위해서는 국제적으로 인정되는 보호프로파일을 적극적으로 개발하고, 이 보호프로파일을 근간으로 우리나라의 정보보호제품에 대한 국제용 CC인증을 다수 확보하여야 한다. 즉, 신규 정보보호제품에 대한

보호프로파일을 지속적으로 개발 및 보급함으로써 인증대상 정보보호제품을 다양화하고, 개발업체 및 보안업체가 제품 개발 시 보호프로파일을 참조하여 보안수준이 높고 국제적으로도 경쟁력이 있는 제품을 개발할 수 있도록 유도 및 지원해야 한다.

하지만 이런 보호프로파일은 개발에 많이 비용과 시간의 투입을 필요로 하며 일반적으로 평가기관, 단체 또는 정부기관 등에 의해 작성이 이루어지기 때문에 단기적인 성과를 얻기는 힘들다. 또한 보호프로파일은 소비자의 요구를 정확히 파악하여 명확하고 구체적인 보안요구사항을 도출하고 정의해야하기 때문에 보호프로파일을 개발하는 평가기관 등은 유관기관과 정보 및 기술을 공유하고 소비자의 요구사항을 파악할 수 있는 다양한 채널을 마련해야 한다. 이와 동시에 이러한 소비자의 요구사항을 가장 잘 파악하고 있는 전문기관들이 해당 분야의 보호프로파일을 개발하고 보급할 수 있는 제도적인 체계가 마련될 필요가 있다. 예를 들어 금융기관(소비자)의 요구사항을 지속적으로 파악할 수 있으며, 금융기관의 IT환경, 보안위협 및 대응방안 등을 가장 잘 알고 있는 해당분야 전문기관들이 금융기관에 특화된 정보보호제품에 대한 보호프로파일을 개발한다면 보다 완성도 높고 보안성이 우수한 결과가 도출될 수 있을 것이다.

2. 평가·인증 수요에 대한 대응마련

2015년 3월 금융기관 정보보호시스템에 사용하는 정보보호제품은 국가기관 평가·인증을 받은 장비를 사용해야 하는 의무가 폐지됨에 따라 금융회사 자율적 판단 하에 다양한 정보보호제품을 도입할 수 있게 되었다. 이러한 규제 장벽이 사라짐에 따라 CC 평가·인증 수요도 다소 감소할 것으로 예상되었으나 2015년 한 해 동안 CC인증을 획득한 정보보호제품은 108개로 2002년 CC인증이 국내 평가 기준으로 도입된 이래 CC인증을 획득한 정보보호제품(609개)의 17.7%를 차지할 정도로 오히려 그 수는 급증하였다. 이는 정보보호제품 도입 시 CC인증 의무가 사라져도 대다수의 금융회사, 공공기관 등은 여전히 CC인증을 획득한 제품을 선호하기 때문인 것으로 판단된다. 특히 CC인증이 없는 제품을 사용했을 때 발생한 사고에 대한 책임소재가 명확하지 않을 수 있기 때문에 CC인증 의무화가 폐지되었다 하더라도 대다수의 금융회사들은 여전히 CC인증을 획득한 제품을 도입할 것으로 전망된다.

또한 2012년 CC인증 유효기간제가 도입되면서 CC인증을 받은 제품의 인증서는 3년의 유효기간이 적용되며, 따라서 보안업체들은 CC인증서가 만료되기 전에 효력을 연장하기 위해 재심사를 받아야 한다. 실제 CC인증 유효기간제가 도입된 후 209개 정보보호제품의 CC인증서가 만료되었으며, 86개 정보보호제품이 효력연장을 위한 재심사를 받았고 그 수요는

앞으로 계속 증가할 것으로 예상된다.

이와 같이 평가·인증 수요는 꾸준히 증가하고 있으나 이러한 수요에 대한 대응방안이 적절히 마련되지 않는다면 이는 평가적체로 이어지게 되어 신기술 등장보다 인증정책이 마련되는 속도가 느려져 정보보호업체들의 사업에 직접적인 영향을 미치는 상황이 발생할 수 있다. 따라서 정보보호제품 평가·인증 절차 간소화, 평가기관의 평가자 인력보강 및 금융기관 등 분야별 전문기관을 민간평가기관으로 추가 지정·운영하는 등 평가적체를 해결하기 위한 다양한 방안을 모색하기 위한 지속적인 노력이 필요할 것이다.

V. 결론

세계 최초로 미국의 TCSEC에 의해 정보보호시스템에 대한 평가가 시작되고 CC인증으로 평가기준이 단일화된 이래, 정보보호제품 업체들은 이 평가기준을 준용함으로써 정보보호시스템의 보안성에 대한 신뢰성을 확보하고자 노력하고 있다. 또한 많은 기업들은 다양한 위협으로부터 중요 자산을 보호하고 보안수준을 향상시키기 위해 인증된 정보보호제품을 도입하여 운영 중에 있다. 매년 CC인증제품 수가 급증하고 있으며 평가제품 또한 다양화되고 있어 이러한 안전한 IT 환경을 구축하기 위한 노력은 앞으로도 지속될 전망이다.

국내도 이러한 국제적인 동향에 발맞추어 2002년 CC인증이 국내 평가 기준으로 도입된 이래 CC인증을 획득한 제품 수는 해마다 그 수가 증가하고 있다. 이는 안전한 정보보호제품에 대한 기업의 니즈도 있었지만, CCRA 인증서 발행국 가입, CC평가의 의무화, CC인증의 국제용·국내용 이원화 및 지속적인 평가기관의 추가 지정 등 국내 CC인증체계를 활성화하기 위한 정부의 다양한 시도가 있었기에 가능한 결과이다.

하지만 국내 정보보호제품이 국제적인 경쟁력을 확보하고 국내 CC인증이 향후 보다 활성화되기 위해서는 인증대상 정보보호제품이 다양화될 수 있도록 국제적으로 인정되는 보호프로파일을 적극적으로 개발하고, 이 보호프로파일을 근간으로 우리나라의 정보보호제품에 대한 국제용 CC인증을 다수 확보할 수 있어야 할 것이다. 이를 위해 다양한 분야의 전문기관들이 해당 분야 보안요구사항을 도출하여 보호프로파일을 개발하고 보급할 수 있는 제도적인 체계를 마련하는 등의 노력이 필요하다. 또한 평가적체로 인한 보안업체들의 시장 진입에 걸림돌이 되지 않도록 정보보호제품 평가·인증 절차 간소화, 평가기관의 평가자 인력보강 및 금융기관 등 분야별 전문기관을 민간평가기관으로 추가 지정·운영하는 등 지속적으로 증가하는 평가·인증 수요에 대한 대응책도 마련되어야 할 것이다.

〈참고문헌〉

- [1] 정보보호시스템 공통평가기준(CC/CEM V3.1 R4) 1부
- [2] 정보보호시스템 공통평가기준(CC/CEM V3.1 R4) 2부
- [3] 정보보호시스템 공통평가기준(CC/CEM V3.1 R4) 3부
- [4] 정보보호시스템 공통평가방법론(CC/CEM V3.1 R4)
- [5] 정보보호시스템 공통평가기준(미래창조과학부고시 제2013-51호)
- [6] 정보보호시스템 평가·인증 지침(미래창조과학부고시 제2013-52호)
- [7] 정보보호제품 평가인증 수행규정(2012, 국가사이버안전센터)
- [8] 2015 국가정보보호백서(국가정보원)
- [9] 정보보호시스템 평가·인증 가이드(2004, 한국정보보호진흥원)
- [10] 강수영, 박종혁, “최근 정보보호제품 공통평가기준에 관한 고찰”, 2008
- [11] 김광식, 남택용, “정보보호시스템 공통평가기준 기술동향”, 2002
- [12] 강수영, 박종혁, “안전한 정보보호제품 개발 보증을 위한 인증 제도에 관한 연구”, 2010
- [13] 류재철, 박순태, 이승환, “국외 민간평가기관 평가 동향”, 2003
- [14] IT보안인증사무국 홈페이지, <http://www.itscc.kr>
- [15] CCRA 홈페이지, <http://www.commoncriteriaportal.org>

Trend

- 생체정보를 이용한 금융서비스 현황 비교 분석
- OAuth 2.0 개요 및 보안 고려사항

생체정보를 이용한 금융 서비스 현황 비교 분석

조 현 호*

1. 개요	110
2. 서비스 현황	111
3. 인증방식 비교	115
4. 주요 인증 수단 비교	116
5. 시사점	118

* 금융보안원 보안연구부 보안기술팀 (e-mail : hhcho@fsec.or.kr)

1 개요

- 최근 생체정보를 활용한 이용자 인증이 무인화 기기, 모바일 기반 업무 시스템 등 다양한 서비스에 적용되면서 금융 거래에 필요한 기존 수단(대면확인, 카드/계좌)없이도 금융 거래를 이용할 수 있도록 변화하고 있음
- 본 보고서에서는 생체정보를 활용하는 서비스 현황과 이용되는 생체정보 및 인증 방식 대해 비교 분석함

2 서비스 현황

금융회사	신한은행	기업은행	우리은행	농협은행
서비스명	디지털 키오스크	홍채인증 ATM	우리 삼성페이	NH스마트금융센터
출시일자	2015.12.2	2015.12.14	2015.8.20	2015.12.19
인증방식	서버 저장 방식	서버 저장 방식	FIDO* 방식	FIDO 방식
생체정보	손바닥 정맥	홍채	지문	지문
인증절차	키오스크 방문	ATM 방문	스마트폰-> ATM 태깅	모바일 앱 실행
주요서비스	상품 가입, 발급, ATM 등 은행 창구 업무	ATM 입금, 출금	ATM 출금, 결제	금융상품 가입
기존 거래여부	불필요	필요	필요	필요
생체정보 등록시	비대면	대면	비대면	비대면

* FIDO(Fast IDentity Online) : 기존 비밀번호 방식 대신 생체정보를 이용한 인증 표준

1) 디지털 키오스크*

- (개요) 비대면으로 각종 실명확인, 계좌 발급, 각종 금융업무를 수행할 수 있는 무인화 기기 서비스

* 키오스크(Kiosk) : 공공장소에 설치된 무인 정보단말기로 교통/지도 정보, 서비스 예약, 티켓 발권 등 각종 업무를 처리할 수 있도록 터치스크린과 음성서비스, 동영상 등을 제공하며 산업 전반에서 다양하게 활용되고 있음

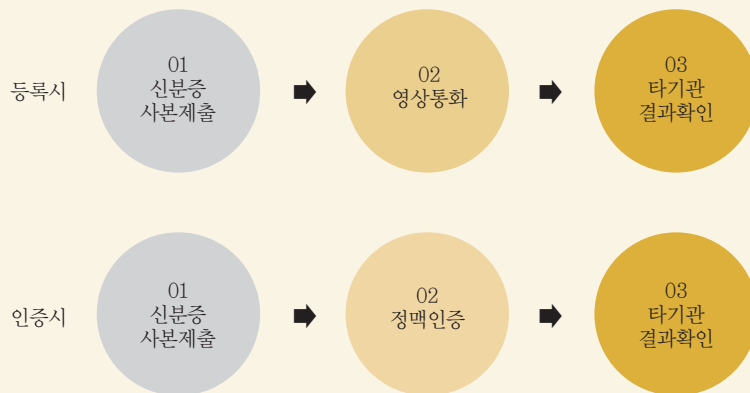
- 금융위는 금융실명제 도입 이후 대면 방식으로 시행되던 실명 확인 방식을 정부의 핀테크 산업 활성화를 위해 복수의 방법을 통한 비대면 방식으로 실명 확인을 할 수 있도록 허용함('15.12.1.)

참고 : 비대면 실명확인 구체적 적용방안

- **(의무사항)** ①신분증 사본 제출, ②영상통화, ③접근매체 전달시 확인, ④기존계좌 활용, ⑤기타 이에 준하는 새로운 방식(생체인증 등) 중 2가지 의무 적용
- **(권고사항)** ⑥타기관 확인결과 활용(휴대폰인증 등), ⑦다수의 개인정보 검증까지 포함하여 이미 선택한 2가지를 제외하고 ①~⑦ 중 추가확인 권고

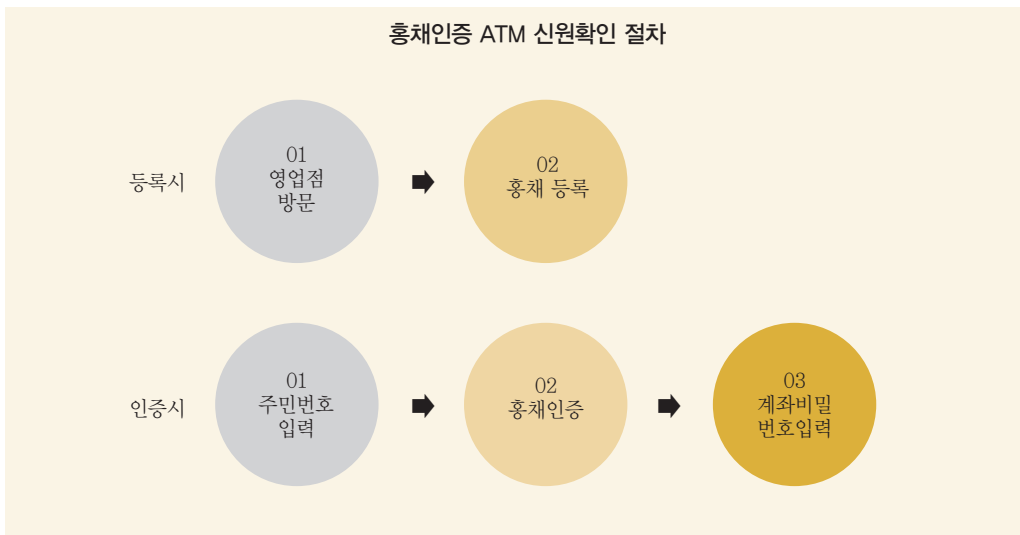
- **(특징)** 최초 서비스 가입 단계부터 비대면으로 본인 확인이 가능하고 기존 창구에서 수행 하던 업무의 90%(107가지)를 디지털 키오스크 서비스를 이용하여 처리 가능

디지털 키오스크 신원확인 절차



2) 홍채인증 ATM

- (개요) ATM 이용시 최초 영업점을 방문하여 등록된 홍채정보를 통해 ATM 기능(입금, 출금, 계좌송금)을 이용 할 수 있는 서비스
- (특징) 실물 카드 또는 통장 없이 홍채인증만 이용하여 금융거래 가능



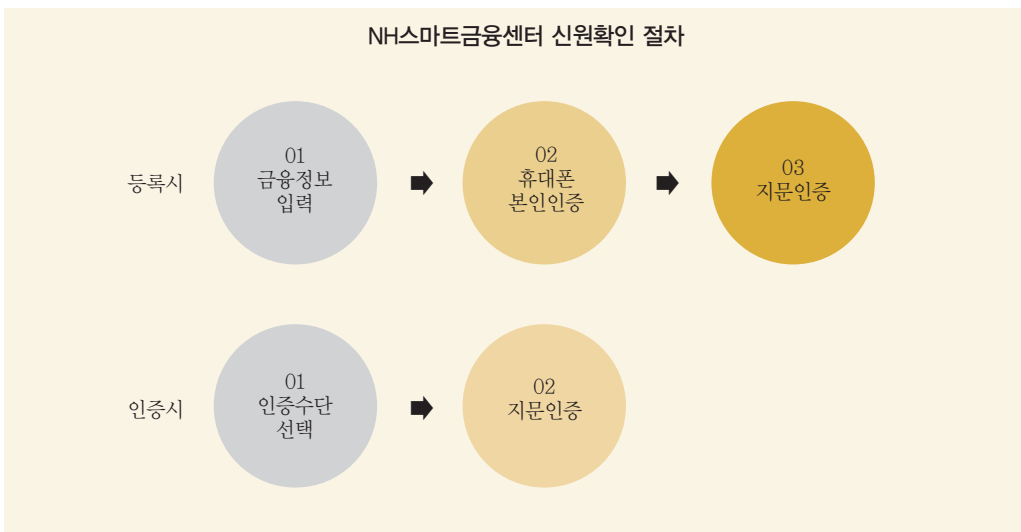
3) 우리 삼성페이

- (개요) 은행 계좌를 삼성페이에 등록하고 ATM에서 삼성페이를 이용해 태깅(Taging)하여 출금 기능을 이용할 수 있는 서비스
- (특징) 삼성페이와 연계하여 별도의 현금카드 없이 등록된 은행 계좌에서 직접 ATM (삼성페이 리더기가 설치된 ATM)을 이용하거나 매장에서 결제 서비스로 이용 가능



4) NH스마트금융센터

- **(개요)** 스마트폰, 태블릿 등 모바일 기기로 금융 상품 가입시 지문인증을 이용하여 본인 인증이 가능한 서비스
- **(특징)** 일반적으로 본인 인증 시 사용되는 공인인증서 외 인증 수단으로 생체정보인 지문 인증을 통해 서비스 이용



3 인증 방식 비교

□ 현재 생체정보를 이용하여 이용자를 인증하는 방식은 서버 저장 방식과 FIDO 방식 2가지로 나뉘지며, 생체정보가 서버에 저장되어 있는 경우 서버 저장 방식, 생체 인식 단말에 저장되어 있는 경우 FIDO 방식으로 구분 할 수 있음

1) 서버 저장 방식

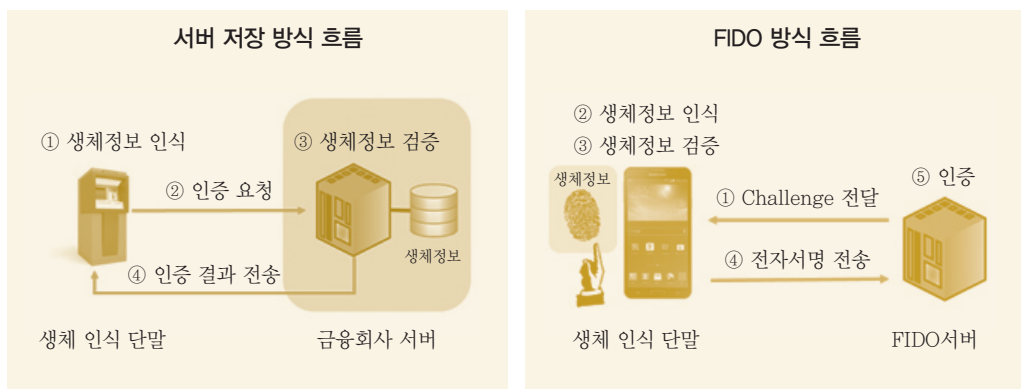
○ (대상 서비스) 디지털 키오스크, 홍채인증 ATM

○ (특징) 개인의 생체정보가 금융회사 서버에 저장되어 있고 생체 인식 단말에서 추출한 생체정보를 전송해 서버에서 비교

2) FIDO 방식

○ (대상 서비스) 우리 삼성페이, NH스마트금융센터

○ (특징) 개인의 생체정보가 생체인식단말에 저장되어 있어 추출한 생체정보를 단말에서 비교 후 전자서명 값이 전송되기 때문에 생체정보가 서버로 전송되지 않음

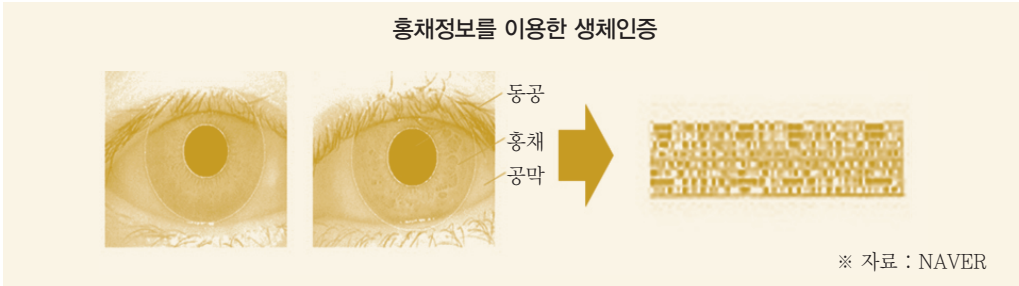


4 주요 인증 수단 비교

- (지문) 입력장치를 통하여 지문을 입력 받아 지문의 패턴을 비교하는 방법으로 현재 생체 인증 수단으로 가장 널리 이용되고 있음



- (홍채) 눈동자의 홍채 패턴을 스캔하여 개인을 식별하는 방법으로 같은 홍채 패턴을 가질 확률이 매우 낮아 보안성이 높음



- (정맥) 정맥인식센서를 통해 개인의 정맥 패턴을 추출하여 개인을 식별하는 방법으로 정밀도와 사용자 편의성이 높음



생체인식 기술별 특징 비교				
구분		인식원리	장점	단점
생체적 특징	지문	<ul style="list-style-type: none"> • 개인의 지문 특성을 DB와 비교 	<ul style="list-style-type: none"> • 편리하며 안전함 • 위조 불가능 	<ul style="list-style-type: none"> • 땀, 먼지 등에 의한 인식을 저하
	홍채	<ul style="list-style-type: none"> • 망막 모세혈관 분포 패턴 분석 • 홍채 무늬, 형태 색깔 분석 	<ul style="list-style-type: none"> • 낮은 오인식률 • 고도의 보안성 • 위조 불가능 • 분실위험 없음 	<ul style="list-style-type: none"> • 불편(눈을 계속 뜨고 있어야 함) • 비위생적(안구질환 우려)
	얼굴	<ul style="list-style-type: none"> • 얼굴 요소의 특징 분석 • 눈, 코, 입 거리 / 얼굴의 열상 / 3차원 얼굴 영상 분석 	<ul style="list-style-type: none"> • 위생적(비접촉식)이며 편리 • 시스템 비용 저렴 	<ul style="list-style-type: none"> • 빛의 세기, 촬영 각도, 자세 등으로 인한 인식을 저하
	정맥	<ul style="list-style-type: none"> • 혈관 패턴의 특징을 파악, 비교 	<ul style="list-style-type: none"> • 편리, 복제 불가능 	<ul style="list-style-type: none"> • 구축 비용 높음
행동적 특징	음성	<ul style="list-style-type: none"> • 음성 특징을 DB와 대조해 개인 인증 	<ul style="list-style-type: none"> • 편리, 전화나 인터넷으로 원격지에서 이용 가능 	<ul style="list-style-type: none"> • 녹음을 통한 도용 가능성 • 목소리 상태에 따른 오인식
	서명	<ul style="list-style-type: none"> • 서명과정(펜의 움직임, 속도, 압력), 모양 특징 분석 	<ul style="list-style-type: none"> • 분실, 도난 위험 없음 	<ul style="list-style-type: none"> • 서명 복제, 위조 가능
※ 자료 : 한국방송통신전파진흥원				

5 시사점

- (다양한 생체인증 활성화) 비대면 실명확인이나 기존 공인인증서를 대체하기 위해 지문, 홍채, 정맥 등의 생체정보를 활용한 서비스가 출시되어, 금융회사의 생체정보를 활용한 새로운 서비스 출시가 가속화 될 것으로 보임
- (생체정보의 안전한 관리) 개인의 생체정보는 비밀번호와 같이 쉽게 변경 할 수 없기 때문에 정보가 유출되지 않도록 안전한 보관 등을 위한 금융회사의 지속적인 노력 필요함
- (생체정보 재사용 방지를 위한 대비 필요) 생체정보를 이용한 본인확인 도입 시 정보가 유출 되더라도 유출된 정보를 재사용 할 수 없도록 방지 대책이 마련되어야 함

OAuth 2.0 개요 및 보안 고려사항

김 동 진*

1. 개요	120
2. OAuth(Open Authorization) 2.0의 개념	121
3. OAuth 2.0의 대표 보안 위협	122
4. 결론 및 보안 고려사항	123
5. 붙임 (세부 내용)	124

* 금융보안원 보안연구부 보안기술팀 (e-mail : dongjink@fsec.or.kr)

1 개요

- 핀테크 활성화의 일환으로 금융권의 오픈 API 제공을 위한 핀테크 오픈플랫폼 구축이 추진됨에 따라, 금융정보 제공 시 안전한 인증 방법으로 OAuth 2.0 및 관련 보안기술에 대한 관심 급증
- 이에 OAuth 2.0의 개념을 알아보고 금융권에서 도입 시 고려해야 할 보안사항을 조사
 - ※ OAuth 2.0의 기술 상세 내용은 [붙임] 참조

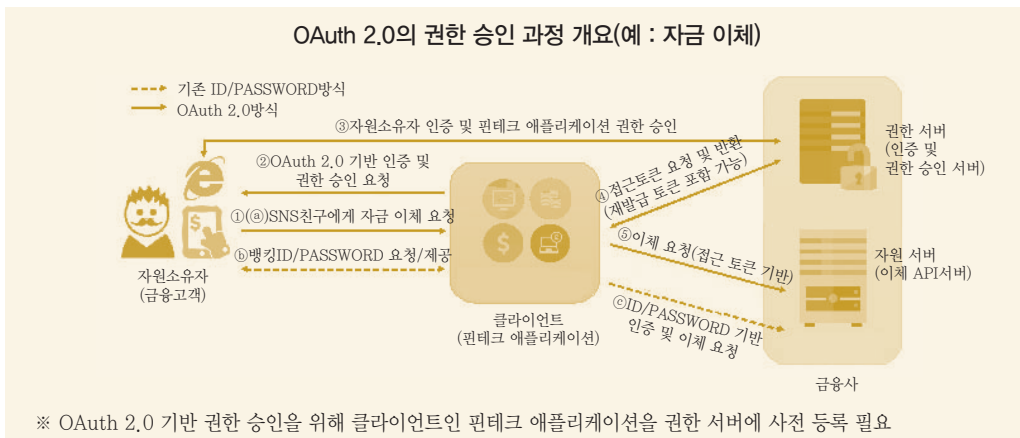
2 OAuth(Open Authorization) 2.0의 개념

□ 배경

- (정의) 제3의 앱이 자원의 소유자인 서비스 이용자를 대신하여 서비스를 요청할 수 있도록 자원 접근 권한을 위임하는 방법
- 예시) 인스타그램은 SNS 친구 찾기를 위해 페이스북의 오픈 API를 사용하여 자원 소유자의 친구 목록에 접근하며, 이때 OAuth 2.0 기반으로 인증 및 권한 승인



- (금융거래 적용) OAuth 2.0을 이용하여 금융고객(자원소유자)의 बैंकिंग ID/PASSWORD를 핀테크 애플리케이션에 직접적으로 제공하지 않고, 접근 토큰(Access Token)*을 기반으로 계좌 이체 등에 대한 권한을 위임
- * 자원에 대한 접근 권한을 자원 소유자가 인가하였음을 나타내는 자격증명(Credentials)



3 OAuth 2.0의 대표 보안 위협

○ 통신구간 보안위협

- (중간자 공격) 클라이언트의 자격증명*을 네트워크 단에서 도청 및 변조함으로써 정상 클라이언트로 위장하여 보호된 자원에 불법 접근

* 권한 승인 방식에 따라 접근 토큰 외에도 재발급 토큰(Refresh token) 및 권한 코드(Authorization code)가 존재

- 2014년 초에 발표된 은닉 리다이렉트(Covert redirect)¹⁾는 중간자 공격 위협으로, 보호된 자원에 불법 접근 및 유출 가능성이 검증됨

○ 클라이언트 유형별 보안 위협

- (웹서버) 클라이언트가 웹 서버일 경우 모든 서비스 이용자의 접근 토큰을 저장 관리하고 있어 악의적인 공격에 의한 토큰의 탈취 위협
- (이용자 단말) 악성코드 감염 단말기에서 자격증명이 공격자에게 노출 가능 및 권한 서버와 자원 서버에 대한 서비스 거부 공격 가능

○ 자원 소유자 대상 보안 위협

- (파밍 등) 파밍(Pharming) 또는 클릭재킹(Clickjacking)*을 통해, 자원 소유자의 인증 정보 탈취 및 권한 승인 유도

* 인터넷 이용자에게 투명한 악성 웹 페이지와 정상 웹 페이지를 겹쳐서 보여줌으로써 공격자가 의도한대로 마우스 클릭을 유도하는 공격

1) 리다이렉트 목적지 주소를 변조하여, 어떤 정보가 공격자에게 전달되도록 하는 방법(출처 : <http://oauth.net/advisories/2014-1-covert-redirect/>, <http://www.tetraph.com/blog/covert-redirect/covert-redirect-vulnerability-related-to-oauth-2-0-and-openid/>)

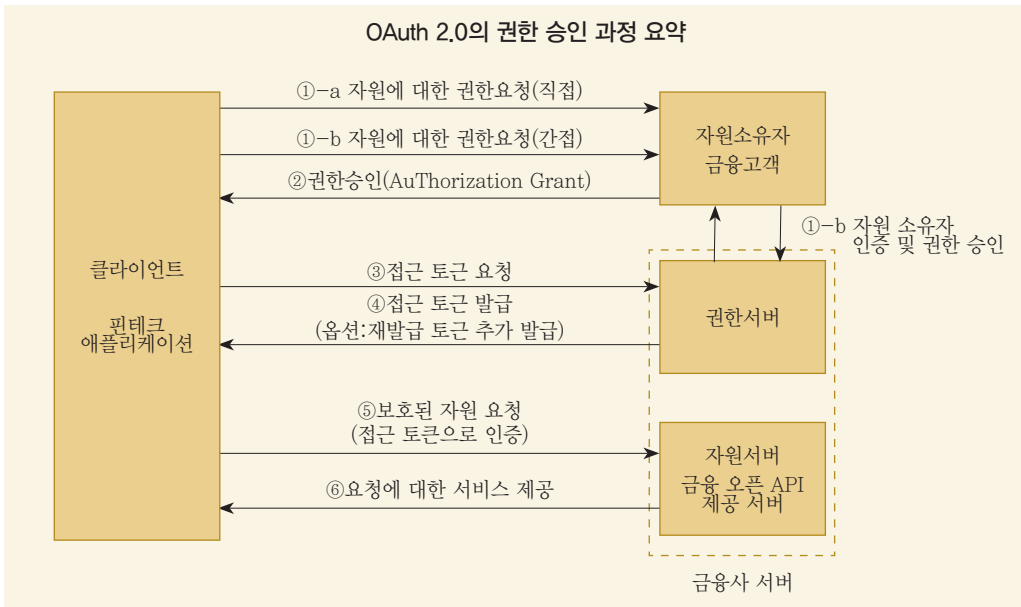
4 결론 및 보안 고려사항

- 오픈 API의 기본이 되는 OAuth 2.0에 대한 다양한 보안 위협이 존재하므로, 도입 시 보안성 검토 및 보안대책의 수립 필요
 - (보안성 강화) 권한 및 자원 서버에서 클라이언트의 요청을 처리 시, OAuth 2.0에 정의된 클라이언트에 대한 검증 절차 강화
 - 등록된 정보와 접근 토큰 요청 시 제출된 클라이언트 정보 비교, 클라이언트의 IP 주소 및 기타 시스템 정보 비교
 - 클라이언트 유형 및 권한 승인 방식 중 비교적 안전한 웹 애플리케이션 및 권한 코드 승인 방식에 대한 우선 적용 고려
 - 접근 토큰의 불법 유출 및 악용에 대비하여 접근 토큰의 유효 기간을 짧게 설정(또는 일회용)하고, 재발급 토큰과 분리 저장하는 방안 고려
 - (관리대책 수립) 클라이언트에 대한 신뢰성 확보를 위한 등록 절차를 마련하여 관련 서류나 현장 실사 등 적정성 검증

5 불임 (세부 내용)

□ OAuth(Open Authorization) 2.0의 권한 승인 개요

○ OAuth 2.0의 권한 승인 과정은 6단계로 요약됨



단계	세부 내용
① 단계	클라이언트가 자원 소유자에게 자원에 대한 접근 권한을 직/간접 요청 · ①-a : 자원 소유자에게 직접 요청 · ①-b : 권한 서버를 중개자로 간접적으로 요청(권장)* * 리다이렉트(Redirect) URI를 통해 자원 소유자를 권한 서버로 리다이렉션 시키며, 권한 서버가 클라이언트를 식별할 수 있도록 식별 정보를 함께 전달
② 단계	클라이언트에게 자원에 대한 접근 권한을 승인(4가지 권한 승인 방법 정의)
③ 단계	클라이언트가 권한 서버에게 접근 토큰을 요청
④ 단계	권한 서버는 클라이언트를 인증 및 부여 받은 권한을 검증하고, 검증된 경우 클라이언트에게 접근 토큰을 발급 · 권한 승인 방법에 따라, 선택적으로 접근 토큰의 유효기간 만료 시 접근 토큰 재발급을 위한 재발급 토큰(Refresh Token) 추가 발급
⑤ 단계	클라이언트가 자원 서버에게 접근 토큰으로 인증 및 자원을 요청
⑥ 단계	자원 서버는 접근 토큰을 검증하고, 검증된 경우 서비스 제공

□ OAuth 2.0의 역할 구성

○ OAuth 2.0의 권한 승인 과정은 6단계로 요약됨

OAuth 2.0의 역할 및 금융권 예		
역할	설명	금융권 예
자원 소유자 (Resource owner)	보호 자원에 대한 접근 권한을 부여할 수 있는 개체(일반적으로 이용자)	핀테크 업체의 금융 서비스를 사용하는 금융고객
클라이언트 (Client)	자원 서버에 보호 자원을 요청하고 관련 서비스를 제공하는 애플리케이션	금융 오픈 API를 사용하여 금융 서비스를 제공하는 핀테크 애플리케이션
자원 서버 (Resource server)	보호된 자원에 대한 서비스 API를 제공하는 서버	금융 오픈 API(예금 조회/이체, 결제 등)를 제공하는 금융사의 서버
권한 서버 (Authorization server)	클라이언트가 보호된 자원에 대한 제한된 접근할 수 있도록 자원 접근 권한을 위임 및 관리하는 서버	금융 서비스에 대한 제한된 접근 권한을 핀테크 애플리케이션에게 위임 및 관리하는 금융사의 서버

○ (권한/자원 서버) 권한 서버와 자원 서버는 구축 및 운영 방식에 따라, 동일 또는 별도 서버로 존재 가능하며, 하나의 권한 서버가 발급한 접근 토큰이 여러 자원 서버에 유효할 수 있음 (1:N 구성 가능)*

* 권한 서버와 자원 서버간의 관계 및 상호운영방식은 OAuth 2.0 표준의 범위를 벗어남

○ (클라이언트 유형) 클라이언트는 자격증명을 안전하게 보관 및 관리할 수 있는지 여부에 따라 크게 비밀(Confidentiality) 및 공개(Public)로 구분

OAuth 2.0의 클라이언트 분류		
유형	특징	클라이언트 종류
비밀	안전한 서버에서 실행되며, 클라이언트의 자격증명이 안전하게 보호 관리되기 때문에 보안성이 높음	- 웹 애플리케이션
공개	자원 소유자의 단말에서 실행되기 때문에 공격자가 클라이언트 자격증명에 접근 가능하며 자격증명의 기밀성을 보장하기 어려움	- 이용자 에이전트 애플리케이션 - 네이티브 애플리케이션

○ 클라이언트는 구축 방식에 따라 웹 애플리케이션(Web application), 이용자 에이전트 애플리케이션(User-agent-based application), 네이티브 애플리케이션(Native application)으로 분류

OAuth 2.0의 역할 및 금융권 예	
클라이언트 유형	설명
웹 애플리케이션	웹 서버 상에서 실행되는 애플리케이션으로 자원 소유자는 HTML 및 웹 브라우저 또는 별도의 웹 클라이언트를 통해 접속
이용자 에이전트 애플리케이션	웹 브라우저 등 이용자의 에이전트 상에서 실행되는 애플리케이션으로 클라이언트 측 스크립트(자바 스크립트 등) 및 웹 브라우저 확장 프로그램 형태 등으로 배포
네이티브 애플리케이션	PC, 스마트폰 등과 같은 이용자 단말에 직접 설치 및 실행되는 애플리케이션

- (클라이언트 등록) OAuth 2.0에서는 API 요청을 한 클라이언트를 식별 및 검증하기 위해, 먼저 권한 서버에 클라이언트를 등록하도록 정의
 - 일반적으로 권한 서버(또는 API 개발자 사이트)에서 제공하는 HTML 양식을 통해 개발자(사)가 직접 등록함
 - 등록이 완료되면, 권한 서버는 클라이언트 자격증명 정보 중 하나인 client_id, client_secret*를 발급하며, 클라이언트 개발자는 이 자격증명을 애플리케이션 개발 시 포함시킴
 - * 접근 토큰 요청 및 오픈 API 호출 시 등록된 정상 클라이언트인지 검증하는데 사용됨

구글의 클라이언트 등록 정보 및 화면

사용자 인증 정보

클라이언트 ID 만들기

애플리케이션 유형

☒ 웹 애플리케이션

☐ Android 자שה 알아보기

☐ Chrome 앱 자שה 알아보기

☐ iOS 자שה 알아보기

☐ PlayStation 4

☐ 기타

클라이언트 유형 선택 (구글에서 추가 유형 제공)

클라이언트 이름

이름

웹 클라이언트 1

승인된 리디렉션 URL

여기에 자바스크립트 원본 또는 아래의 리디렉션 URI(또는 두 항목 모두)를 입력하세요. @ 와일드 카드(http://*.example.com) 또는 경로(http://example.com/subdir)를 포함할 수 없습니다.

http://www.example.com

승인된 리디렉션 URI

프로토콜이 있어야 합니다. URL 조각 또는 상대 경로는 포함할 수 있으며 공개 IP 주소를 사용할 수 없습니다.

http://www.example.com/oauth2/callback

사용자 인증 정보

사용자 인증 정보 OAuth 동의 화면 도메인 확인

클라이언트 ID를 통해 사용자 인증 및 권한 승인 화면에 표시될 클라이언트 정보

이메일 주소

kdjorang@gmail.com

제품 이름

제품 이름

홈페이지 URL (선택사항)

Product logo URL (선택사항)

http://www.example.com/logo.png

최종 사용자에게 로고가 다음과 같이 표시됩니다.

최대 크기: 120x120픽셀

개인정보취급방침 URL (선택사항)

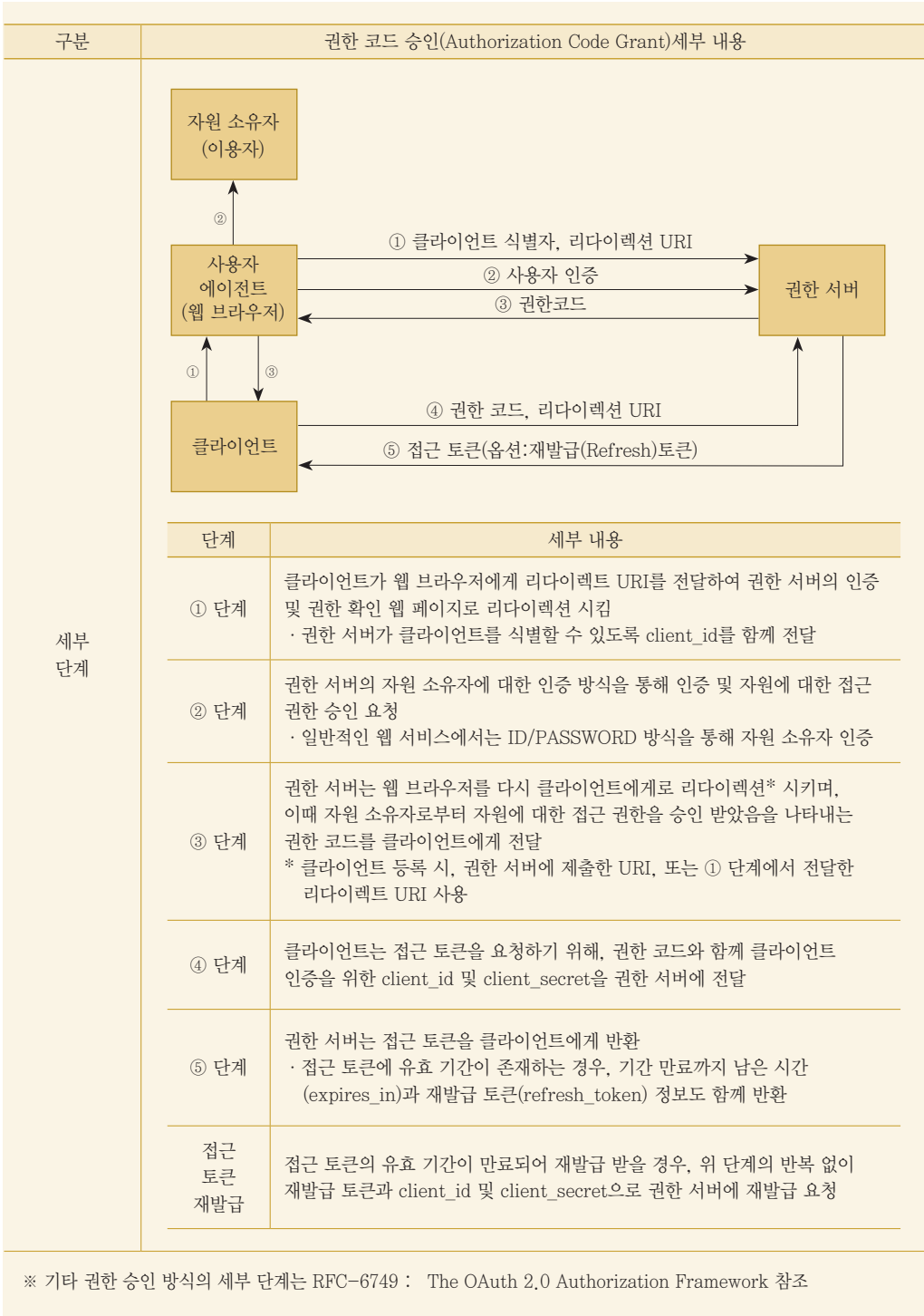
서비스 약관 URL (선택사항)

□ OAuth 2.0의 권한 승인 방법

- 클라이언트 유형, 자원에 대한 장기적 접근 여부 및 제공 서비스의 특성 등에 따라, 총 4가지 권한 승인 방법을 정의

OAuth 2.0의 권한 승인 방법 비교	
권한 코드 승인 (Authorization Code Grant)	암묵적 승인 (Implicit Grant)
<ul style="list-style-type: none"> ○ 클라이언트 유형 <ul style="list-style-type: none"> · 서버 웹 애플리케이션 · 네이티브 애플리케이션(백엔드 서버 사용) ○ 장기적 접근 <ul style="list-style-type: none"> · 재발급 토큰을 통해 지원 ○ 보안성 <ul style="list-style-type: none"> · 사용자 웹 브라우저를 통해 접근 토큰이 노출되지 않도록 권한 코드 사용 · 클라이언트는 권한 코드를 사용하여 권한 서버에게 직접 접근 토큰을 요청 · 중요 자격증명 정보가 서버에 저장되기 때문에 다른 권한 승인 방법에 비해 안전함 	<ul style="list-style-type: none"> ○ 클라이언트 유형 <ul style="list-style-type: none"> · 이용자 에이전트 애플리케이션 ○ 장기적 접근 <ul style="list-style-type: none"> · 재발급 토큰 미지원으로 인해 접근 토큰의 유효 기간이 짧으면 장기적 접근 불가 ○ 보안성 <ul style="list-style-type: none"> · 접근 토큰이 웹 브라우저에 전달 및 저장되기 때문에 웹 브라우저, 클라이언트, 이용자에 대한 신뢰가 높은 경우에 적합 · 접근 토큰 유출을 고려하여, 접근 토큰의 유효 기간에 대한 적절한 조절이 필요함
자원 소유자 비밀번호 자격증명 승인 (Resource Owner Password Credentials Grant)	클라이언트 자격증명 승인 (Client Credentials Grant)
<ul style="list-style-type: none"> ○ 클라이언트 유형 <ul style="list-style-type: none"> · 모든 클라이언트 유형 가능 · 일반적으로 API 제공 업체가 배포한 애플리케이션 ○ 장기적 접근 <ul style="list-style-type: none"> · 재발급 토큰을 통해 지원 ○ 보안성 <ul style="list-style-type: none"> · 자원 소유자의 비밀번호가 애플리케이션에 노출되고, 피싱 위험이 존재 · 접근 토큰 발급 요청 시에만 비밀번호가 사용되기 때문에 클라이언트에 인증정보를 저장할 필요 없음 	<ul style="list-style-type: none"> ○ 클라이언트 유형 <ul style="list-style-type: none"> · 클라이언트가 데이터를 소유하고 있거나, 접근 위임이 이미 허용된 경우 ○ 장기적 접근 <ul style="list-style-type: none"> · 재발급 토큰 미지원 · 클라이언트 인증만으로 즉시 접근 토큰 재발급 가능 ○ 보안성 <ul style="list-style-type: none"> · 클라이언트 인증만으로 접근 토큰을 발급하기 때문에 안전한 인증 방식 사용 및 인증 정보의 규칙적인 변경이 필요함

○ 비교적 안전한 권한 코드 승인 방식은 세부 5단계로 구성



□ OAuth 1.0과 2.0 비교

OAuth 1.0과 2.0의 주요 차이점 비교		
특징	OAuth 1.0	OAuth 2.0
역할 (역할 명칭 변경 및 세분화)	- 이용자(User)	- 자원 소유자(Resource Owner)
	- 소비자(Consumer)	- 클라이언트(Client)
	- 서비스 제공자(Service Provider)	- 자원 서버(Resource Server) - 권한 서버(Authorization Server)
API 호출 인증 및 보안	- 서명	- HTTPS(SSL/TLS) 기본 - 서명 : 자원 서버가 별도 서명을 요구하는 경우
클라이언트 지원 유형	- 웹 애플리케이션	- 웹 애플리케이션 - 이용자 에이전트 애플리케이션 - 네이티브 애플리케이션

- OAuth 2.0은 1.0의 알려진 보안 문제 등을 개선한 버전으로 1.0을 대체(하위 호환성 미지원)
 - 기존 서비스 제공자(Service Provider)를 자원 및 권한 서버로 분리하여 다수의 서비스 제공자(서버)로 구성 웹 서비스에서 발생 가능한 권한 동기화 문제 개선
 - 오픈 API 요청 시 클라이언트 인증 방법으로 서명 대신, HTTPS를 의무화하여 서버 및 클라이언트 개발 편의성 개선
 - 다양한 유형의 클라이언트와 이를 고려한 권한 승인 방법을 정의하여 유형별 클라이언트들에 대한 일관된 구현 가능
 - 접근 토큰 재발급을 위한 재발급 토큰(Refresh Token)을 도입함으로써 접근 토큰의 유효 기간 단축 및 보안성 개선
 - 접근 토큰의 유효 기간이 과도하게 긴 경우, 접근 토큰이 유출된 경우 공격자에 의해 장시간 악용 가능
 - 기타 다양한 확장성 지원

□ OAuth 2.0 도입에 따른 보안적인 이점

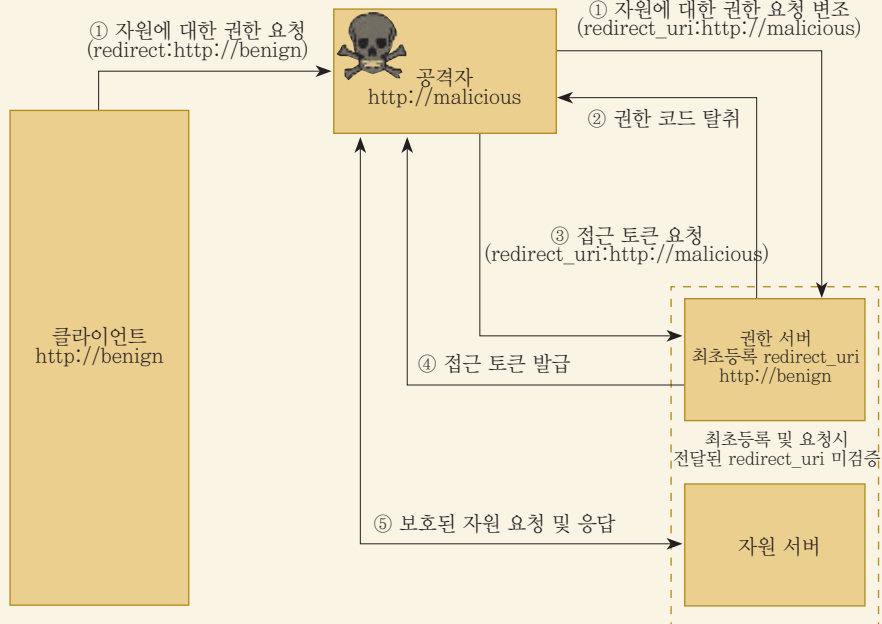
- 자원 소유자가 클라이언트에 비밀번호를 제공할 필요가 없으며, 피싱 등의 위협 감소
- 클라이언트 개발자는 자원 소유자의 비밀번호에 대한 안전한 저장 및 노출을 고려하지 않아도 됨
- 자원 소유자의 모든 권한이 아닌, 클라이언트에게 반드시 필요한 권한만 제한적으로 제공 가능
- 자원에 대한 클라이언트의 접근을 각 클라이언트별로 차단 및 권한 취소가 가능하며, 권한의 범위를 제어 가능
 - 비밀번호 방식의 경우, 클라이언트의 권한 취소를 위해서는 비밀번호를 변경해야하며, 접근 권한을 재부여할 클라이언트에게 비밀번호 제공 필요
 - 클라이언트별 API 호출 가능 횟수 제한, 일부 자원에 대한 접근만 허용하는 등의 권한 범위 제어 가능



□ OAuth 2.0의 보안 위협 및 대응 방안

- (중간자 공격) 2014년 초에 공개된 은닉 리다이렉트(Covert Redirect) 는 중요 자격증명 정보인 권한 코드 및 접근 토큰 등의 유출로 이어질 수 있는 보안 위협

구분	상세 설명
공격 방법	공격자가 클라이언트와 권한 서버 간의 권한 승인 요청을 가로채서, 전달 인자 중 redirect_uri* 값을 공격자의 서버로 변조하여, 권한 코드 및 접근 토큰 탈취 * 권한 서버가 클라이언트에게 발급하는 권한 코드, 접근 토큰 등이 전달될 주소
위협 원인	URI 값은 최초 클라이언트 등록 시 권한 서버에 제출되지만, 최초 제출된 URI와 요청 시 전달된 URI의 미검증 및 정상 클라이언트 여부 미검증이 원인
파급 효과	발표자에 의하면, 위협 공개 당시 페이스북, 구글 등 주요 오픈 API 제공사 대부분이 위협에 노출되어 있는 상태였음
대응 방안	최초 등록된 URI와 요청 시 함께 전달된 URI 비교 및 클라이언트의 IP 주소, 기타 시스템 정보 비교를 통한 클라이언트 검증 절차 준수



※ 은닉 리다이렉트 위협은 RFC-6819에 4.2.4, Threat: Open Redirector 로 정의되어있음

- RFC-6819에는 권한 코드 승인 방법과 관련된 12개의 보안 위협을 정의 및 대응 방안을 제시하고 있으며, 금융권 OAuth 2.0 적용 시 검토 필요

분류	보안 위협
권한 코드 유출	<ul style="list-style-type: none"> · 권한 코드 도청 및 유출 · 권한 서버의 DB로부터 권한 코드 유출 · 권한 코드 피싱 · 위조 클라이언트로 인한 권한 코드 유출 · redirect_uri 에 대한 CSRF(Cross Site Request Forgery)²⁾ 공격을 통해 권한 코드 획득
서비스 거부 (DoS)	<ul style="list-style-type: none"> · 반복된 권한 요청을 통해 권한 서버에 대한 서비스 거부 공격 · 악의적으로 생성된 권한 코드를 통해 권한 서버에 서비스 거부 공격
불법 권한 획득	<ul style="list-style-type: none"> · 권한 코드 추측(guessing)을 통한 권한 획득 · 악의적인 클라이언트의 권한 획득 · 클릭재킹(Clickjacking) 공격을 통한 권한 획득
신분/세션 도용	<ul style="list-style-type: none"> · 자원 소유자 신분 도용 · 이용자 세션 도용
분류	대응 방안
권한 코드 유출	<ul style="list-style-type: none"> · SSL/TLS 기반의 HTTPS를 통해 클라이언트와 권한/자원 서버 간 통신 구간 보호 · 권한 코드 발급 시 클라이언트 인증 절차 준수 · 권한 코드의 유효 기간을 짧게 설정 · SQL 인젝션에 대한 대응 · redirect_uri 검증
서비스 거부 (DoS)	<ul style="list-style-type: none"> · 이용자별 발급 가능한 접근 토큰 개수 제한 · 비정상 권한 코드를 일정 횟수 이상 권한 서버에 전송하는 경우, 해당 클라이언트와의 연결 차단
불법 권한 획득	<ul style="list-style-type: none"> · 권한 코드에 메시지 서명 적용 · 권한 코드에 1회성 임의 값을 추가 · 인증 및 권한 부여 웹 페이지에서는 iFrame을 비활성화 하도록 서버 옵션 추가
신분/세션 도용	<ul style="list-style-type: none"> · CAPTCHA* 사용 · * 변형된 이미지를 사용하여 사용자가 실제 사람인지를 확인하는 방법 · 1회성 인증 정보를 SMS 등의 별도 망으로 발급

- OAuth 2.0에서 다루지 않는 이용자 단말과 통신 구간에 대한 보안 위협 및 대책 고려 필요

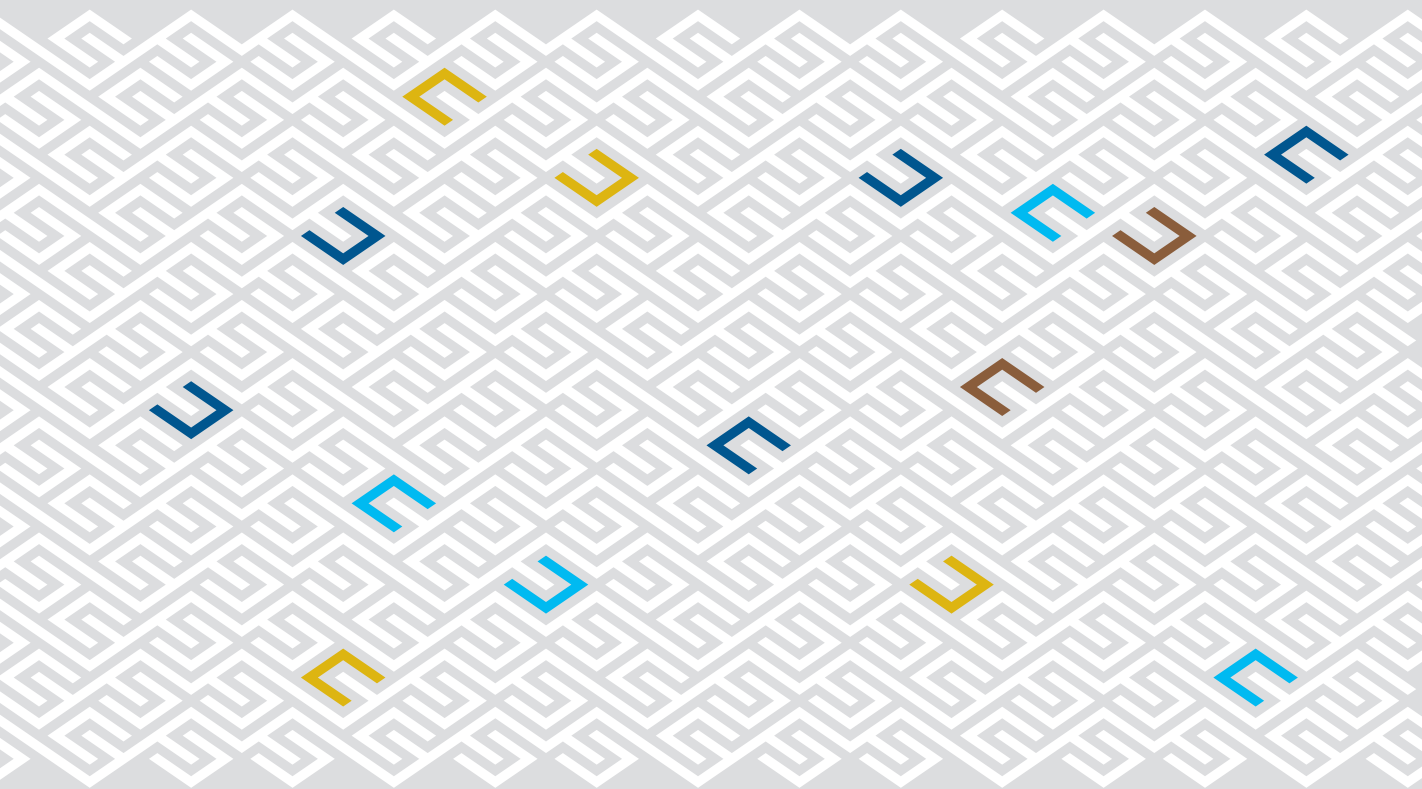
2) 이용자가 자신의 의지와는 무관하게 공격자가 의도한 악성 행위를 특정 웹 사이트에 요청하게 하는 공격
(출처 : https://ko.wikipedia.org/wiki/사이트_간_요청_위조)

전자금융과 금융보안

발 행 2016년 1월
발 행 인 허 창 언
발 행 처 금융보안원
주 소 서울특별시 영등포구 의사당대로 143
금융투자협회 빌딩 8, 9F

(비매품)

본 문서의 내용은 금융보안원의 서면 동의 없이 무단전재를 금합니다.
본 문서에 수록된 내용은 고지없이 변경될 수 있습니다.



금융보안원
FINANCIAL SECURITY INSTITUTE

전자금융과 금융보안 | 제3호