2016년도 금융 IT · 보안 10대이슈 전망보고서

(보안연구부 보안정책팀, 2016.1.5)

□ 추진목적

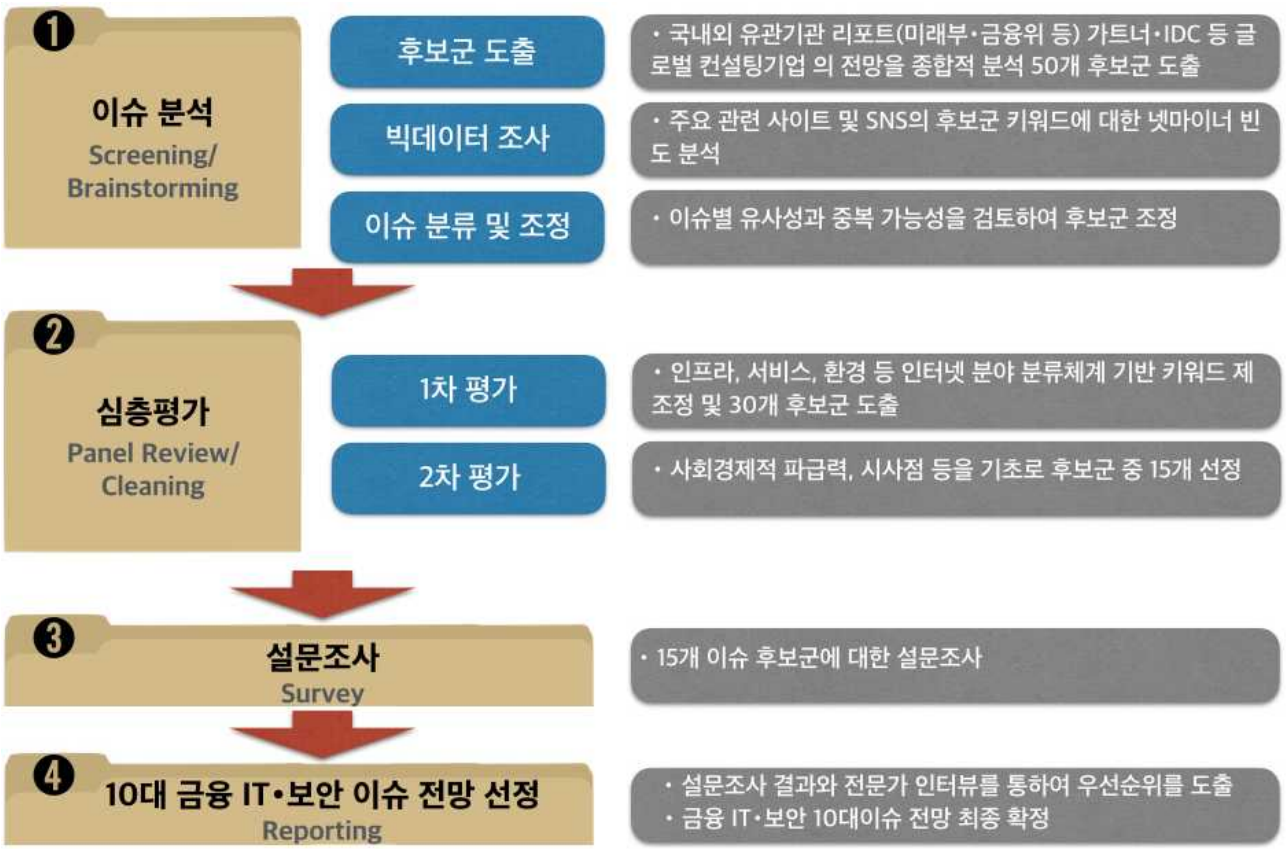
○ 연간 금융 IT · 보안 주요 트렌드 분석을 기반으로 2016년도 10대 이슈 도출을 통해 금융 IT · 보안의 정책 방향 및 전략 수립 지원

□ 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

※ 붉은색은 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)	본격도입(16년, 주요은행)
OPEN API	규격화, 시험·검증(12월, 테스트베드)	본격서비스 제공(하반기)
블록체인 거래시스템	도입방안 내부검토, 핀테크기업과 제휴	외환송금기술 상용화 (상반기 목표, S은행)

□ 전망 및 이슈

○ **(전망)** 핀테크 서비스가 간편결제 이외의 **다양한 분야로 확대**됨에 따라, **사업주체 간 경쟁이 심화**되고 **신규 보안위협 등장 예상**

- 금융회사, 핀테크 기업 등 **금융서비스 주체의 보안위협에 대한 대응수준**에 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

<금융관련 빅데이터 활용사례>

구분	금융회사	주요내용
은행	IBK기업은행	고객감성분석등 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 중**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 정보보호 **법령상 명확화**, 투명한 인프라 운영, 금융회사의 **기술적·관리적 비식별화 방안 마련**을 통한 정보 유출 및 오남용 위협에 대응

3 바이오인증(FIDO 등) 기술을 활용한 금융서비스 확대

□ 배경

○ 스마트폰 등 IT기기의 발전으로 **지문정보를 활용**한 비대면 본인인증 서비스가 금융거래*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, 홍체 등)을 통해 **기존 금융업무를 무인화기기가 대신**하거나, 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)** 보안업계의 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 **허용**함으로써 소비자 편익 제고 및 **본격적인 핀테크 산업 활성화 추진**

* 「금융거래시 실명확인방식 합리화방안」('15.5.18.)

** ①신분증 사본 제출 ②영상통화 ③접근매체 전달시 확인 ④기존계좌 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 확산**됨으로써 비대면 계좌개설 등 고객 편의가 제고되고, **다양하고 차별화된 금융서비스에 활용**됨으로써 **핀테크 산업 활성화에 기여**

○ **(이슈)** 신분증 사본 및 **개인정보 유출방지**를 위한 보안대책 강화 요구, 명의도용 및 대포통장 확산 등 **금융사기 방지**를 위해 FDS 활용 등 **사후 대응 체계 강화 요구**

5 금융권 자율보안체계 확립과 금융보안거버넌스 강화

□ 배경

○ 금융위·금감원은 금융개혁의 일환으로 각종 규제를 완화하고, 보안 규제의 패러다임을 **사전규제에서 사후 점검 및 책임강화**로 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***」 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 금융회사**는 자체점검·내부통제 및 보안역량 강화 등을 통해 **금융보안거버넌스* 체계 확립하여 운영 중**에 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*** **마련**과 금융회사 규모별·권역별 **자율보안 실행역량 확보 방안 요구**

* 정보보호 조직과 전자적 조직간 협업체계 구축 방법, 위험관리 방법, 투자와 성과 관리 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 빌려줌으로써 발생되는 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 적용**되고, **기존 금융 인프라와 보안기술을 보완하는 방식으로 발달** 예상

○ **(이슈)** 블록체인 기술 등 새로운 기술 수용을 위한 **규제 완화 검토**가 필요하며, 블록체인의 활용 분야 및 기술 수용의 방법론* 선택에 있어 **금융회사의 비즈니스 목적과 규모에 맞추어 도입 필요**

* 독자적인 블록체인 기술 실험 참여 또는 스타트업과 파트너쉽 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 분야**에서 신규 융합 서비스가 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 불안 요소로 인해 **클라우드 서비스 활성화가 부진**한 상황

□ 전망 및 이슈

○ **(전망)** 공공부문의 클라우드 서비스 도입 활성화와 더불어 금융회사는 수익성 하락에 따른 **관리비용 절감**과 **상품서비스 경쟁력 향상**을 위한 방안으로 도입 증가 예상

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

- **금융부문은 ‘가상화(Virtualization)’ 방식**으로 전산센터를 제외한 현업·영업점의 **논리적 망 분리가 지속적으로 증가**하고 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

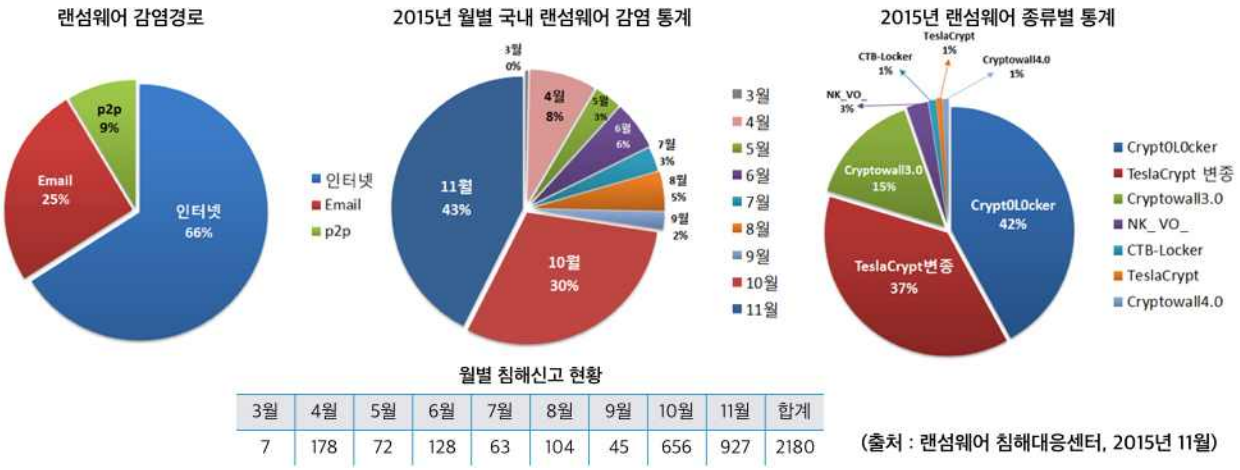
8 모바일 및 표적형 랜섬웨어 증가

□ 배경

○ 최근 **랜섬웨어**의 **공격대상**이 PC 기반에서 **모바일 기기**로 **확대**되고, **공격방식** 또한 대규모 공격에서 **표적형 공격**으로 **지능화**되는 추세

□ 현황

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



월별 침해신고 현황

3월	4월	5월	6월	7월	8월	9월	10월	11월	합계
7	178	72	128	63	104	45	656	927	2180

(출처 : 랜섬웨어 침해대응센터, 2015년 11월)

○ 랜섬웨어의 **유포방식**이 드라이브 바이 다운로드, 이메일, 애드웨어 광고 서버 등으로 **다양화**

□ 전망 및 이슈

○ **(전망)** 시그너처/행위기반 탐지 기술을 우회하는 자동 알고리즘을 탑재하는 등 **진화된 변종 랜섬웨어로 인한 피해 급증**과, 리눅스, 맥 OS, IoT기기 등 공격 대상이 **더욱 확대**될 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 공격규모의 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

< IoT기기를 악용한 DDoS공격 사례(SSDP 증폭반사 공격) >

□ 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

○ **금융회사**는 공인인증서 등 한정된 보안수단만으로는 지능화된 **이상금융거래 대응에 한계**를 노출

○ 개별 금융회사의 FDS 운영을 통해 파악된 사고정보 및 이상금융거래 등 사고예방을 위한 **위협정보 공유가 필요**

□ 현황

○ **고도화되는 전자금융사고**에 보다 적극적이고 **효과적으로 대응**할 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 **위협정보**에 대한 **신속한 공유**를 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, 홍체, 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 준다며 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 금융기관 뿐 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