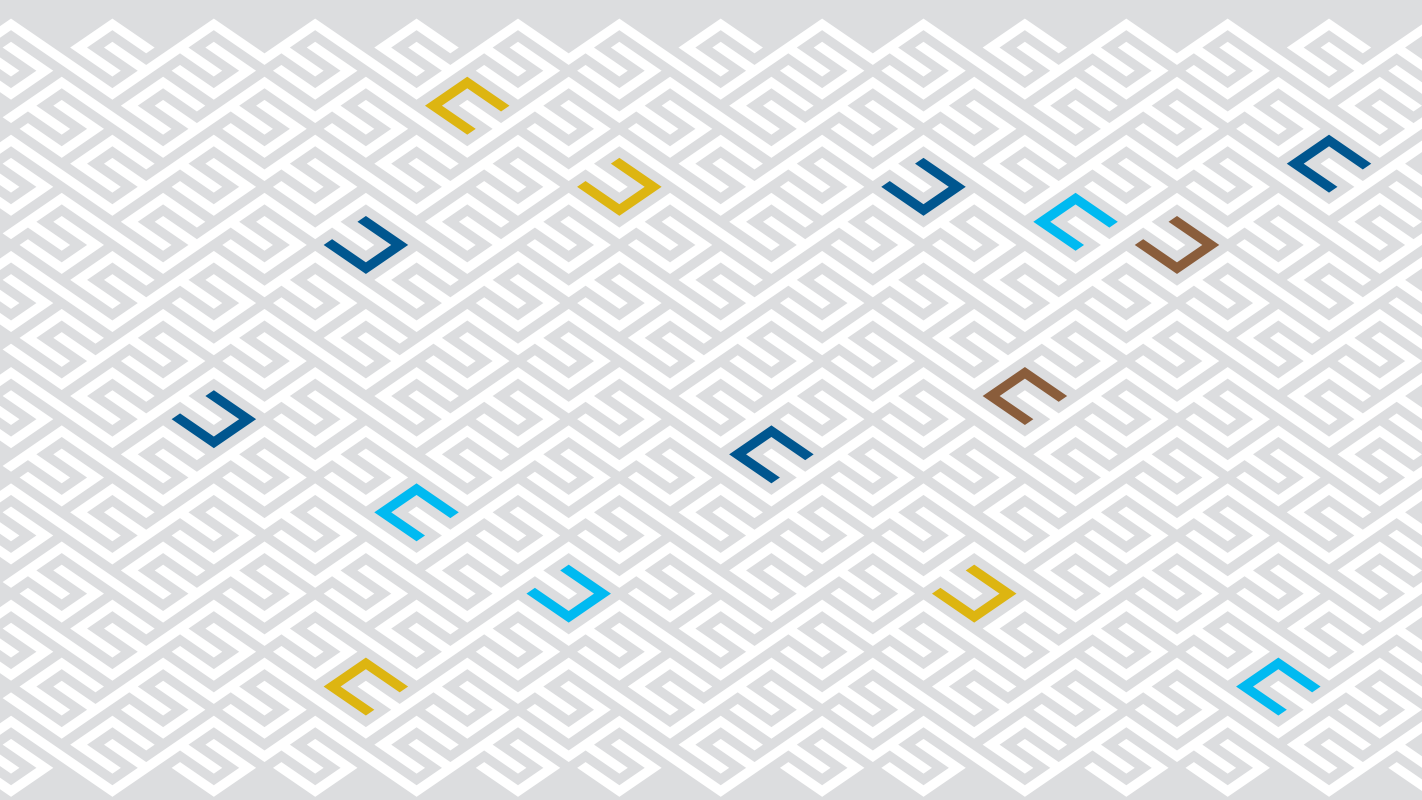


전자금융과 금융보안

E-FINANCE AND FINANCIAL SECURITY



Research

바이오인증 최신 활용 및 보안 동향
금융권 사물인터넷(IoT) 동향 및 향후 전망
금융회사의 보안서비스 제공 현황 및 활용방안

Trend

싱가포르의 핀테크 추진 현황
NIST, 블록암호 운영방식에 관한 권고
타이젠 소개 및 특징 조사



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

Research

- 바이오인증 최신 활용 및 보안 동향
- 금융권 사물인터넷(IoT) 동향 및 향후 전망
- 금융회사의 보안서비스 제공 현황 및 활용방안

Trend

- 싱가포르의 핀테크 추진 현황
- NIST, 블록암호 운영방식에 관한 권고
- 타이젠 소개 및 특징 조사

Contents

Research

바이오인증 최신 활용 및 보안 동향	3
금융권 사물인터넷(IoT) 동향 및 향후 전망	29
금융회사의 보안서비스 제공 현황 및 활용방안	55

Trend

싱가포르의 핀테크 추진 현황	83
NIST, 블록암호 운영방식에 관한 권고	99
타이젠 소개 및 특징 조사	111

Research

- 바이오인증 최신 활용 및 보안 동향
- 금융권 사물인터넷(IoT) 동향 및 향후 전망
- 금융회사의 보안서비스 제공 현황 및 활용방안

바이오인증 최신 활용 및 보안 동향

김 동 진*

I. 서론	5
II. 바이오인증의 이해	6
1. 바이오인증 소개	6
2. 바이오정보 유형 및 특징	8
3. 바이오인증 시스템	11
III. 바이오인증 도입 현황	13
1. 금융권 도입 현황	13
2. 공공부문 도입 현황	16
IV. 바이오인증 보안 동향	19
1. 바이오인증 보안 위협 및 사고사례	19
2. 바이오인증 보안 대응기술 동향	23
V. 결 론	27
〈참고문헌〉	28

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

요 약

바이오인증 기술은 지문, 홍채, 얼굴, 정맥등 개인 고유의 신체적 또는 서명, 음성 등 행동적 특징을 통해 인증하는 방식으로 기존 인증방식 보다 우수한 편의성과 보안성으로 주목 받으며 금융 등 다양한 분야에서 활용되고 있다. 특히, 스마트뱅킹 등 스마트폰 기반 서비스의 확대와 함께 바이오인증 기술 도입 또한 급증하고 있으며, 다양한 활용사례들이 발표되고 있다.

한편 바이오인증 기술과 관련된 다양한 보안 위협이 대두되고 있다. 과거 위조 및 도용이 어려운 것으로 알려졌던 지문 및 홍채정보에 대한 위조 사례가 발표되었으며, 최근 대규모 유출 사고사례 또한 발표된 바 있다.

바이오정보가 위조 또는 유출될 경우 재발급하는 등의 사후조치가 어렵기 때문에 사전에 위조 여부 판별, 다수의 바이오정보 융합, 원본 바이오정보 유출 방지 또는 복원 불가능 등의 사전적 보호방안이 필요하다.

이에 본 고에서는 바이오인증 보안에 대한 관심 재고를 위해 관련 보안 위협 및 대응 기술을 소개하고자 한다.

I. 서론

바이오인증 기술은 지문 인식센서가 탑재된 스마트폰의 등장과 2015년 9월 비대면 계좌 개설을 위한 실명확인 방식으로 인정됨에 따라, 금융권을 중심으로 빠르게 도입되고 있다.

금융고객은 새로운 인증방식으로 바이오인증 기술을 받아들이고 있으며, 특히 스마트폰에서의 금융서비스 이용 시 작은 화면에서의 패스워드 입력 등에 따른 불편함이 바이오인증을 통해 해소 가능하기 때문에 그 편의성으로 인해 더욱 각광 받고 있다.

하지만 도입이 활성화됨에 따라 다양한 보안 위협에 대한 연구 및 시도들이 진행되면서, 여러 위협들이 제시되고 있다. 그중에서도 바이오정보 위조 및 유출에 대한 다양한 사례들이 발표되고 있으며, 바이오정보는 한번 유출되면 폐기 및 재발급이 어렵기 때문에 그 위험성이 더욱 부각되고 있다.

이러한 보안 위협을 개선하고자 다양한 대응방안들이 연구되고 있으며, 바이오정보 위조 판별 기술과 다수의 바이오정보를 융합하여 인증에 사용하는 다중 바이오인증 기술, 바이오 정보를 변환하는 등의 재발급 가능한 템플릿 기술이 대표적이다.

II. 바이오인증의 이해

1. 바이오인증 소개

바이오인증 기술이란, 개인을 식별할 수 있는 고유의 신체적 또는 행동적 특징(이하 바이오정보)을 통해 신원을 확인하는 방식이다. 특히 비밀번호, 공인인증서 등과 같이 인증정보를 소지하거나 기억할 필요가 없기 때문에 기존 인증방식과 비교하여 편리성을 제공하며 분실 및 유출 등으로 인한 악용 우려가 적은 안전한 인증방식으로 평가받고 있다.

이러한 특징으로 인해 [표 1], [그림 1]과 같이 금융권을 비롯해 중요보호시설 출입통제 등 다양한 분야에 도입되고 있으며, 특히 금융권에서는 스마트폰을 활용한 스마트뱅킹 및 간편결제 등 스마트 금융거래를 위한 본인인증 방식으로 국내·외 금융회사를 비롯해 핀테크 업체들에서도 적극 도입 또는 개발 중이다. 공공부문에서도 증명서 발급 시 지문인증 방식이 사용되고 있으며, 최근 행정자치부의 ‘정부청사 보안 강화대책’에 따라 정부청사 출입통제를 목적으로 얼굴인식 방식 도입을 발표하는 등 점차 적용 범위가 확대되고 있다. PC 등 단말 인증부문에서는 대표적으로 마이크로소프트에서 윈도우10의 로그인 방식으로 지문/얼굴/홍채 인증을 지원하고 있다.

[표 1] 바이오인증(인식) 기술 활용 분야	
분야	세부 활용
금융	ATM·키오스크(KIOSK) ¹⁾ , 스마트뱅킹, 전자(간편)결제 등
컴퓨터	PC·노트북·스마트폰·네트워크 로그인 및 접근 제어 등
의료·복지	환자신원확인, 원격진료, 전자 처방전, 진료기록 관리 등
출입통제	주요 시설물 출입관리, 근태관리 등
공공 부문	출·입국심사, 증명서발급, 전자신분증, 선거관리, 범죄자관리 등
사회 복지 부문	연금지급관리, 기타수당관리 등

자료 : 바이오인식정보시험센터 자료 재구성

1) 공공장소에 설치된 무인 종합정보안내시스템으로 광고 및 길안내 등에 사용되어 왔지만, 최근 금융권에서 비대면 금융거래를 위한 무인 셀프점포로 도입 중이다.

[그림 1]

바이오인증 기술 실제 활용 사례



(a) 미국 출·입국심사 - 지문



(b) 인도 주민 등록 - 지문, 얼굴, 홍채



(c) 디즈니월드 - 지문



(d) ATM - 손바닥 정맥

자료 : A.K. Jain, and K. Nandakumar, Biometric Authentication: System Security and User Privacy, IEEE Computer, 2012, 내용 재구성

바이오인증 기술의 도입 증가는 바이오정보 센싱(Sensing)기술의 고도화 및 센서의 소형화에 기인한다. 대표적으로 지문인증의 경우, 센서가 소형화되기 전까지는 주로 공공 및 출입통제를 목적으로 사용되다가, 센서가 소형화되어 스마트폰에 탑재되면서 스마트폰 기반의 다양한 서비스에 적극 활용되기 시작하였다.

2. 바이오정보 유형 및 특징

바이오정보는 크게 신체적 특징과 행동적 특징으로 분류된다. 신체적 특징에는 지문, 홍채, 정맥, 얼굴 등이 해당하고 행동적 특징으로는 서명, 음성 등이 존재한다. 각 바이오정보의 특징은 [표 2]와 같다.

[표 2] 바이오정보 유형 및 특징			
분야	바이오정보	인증 방법	특징
신체적 특징	지문	지문의 형상적 특징을 비교	<ul style="list-style-type: none"> • 편의성, 센서 소형화 수준 높음 (스마트폰 내장) • 땀, 먼지 등에 의한 인식을 저하
	홍채 · 망막	홍채의 무늬 · 형태 · 색, 망막의 모세혈관 분포 패턴 비교	<ul style="list-style-type: none"> • 낮은 오인식률 • 위조가 어려움 • 눈을 뜨고 있어야 하는 불편함
	정맥	손바닥, 손가락 등의 정맥 분포 패턴 비교	<ul style="list-style-type: none"> • 위조가 어려움 • 높은 시스템 구축 비용
	얼굴	눈, 코, 입 등 3차원 얼굴 형상 비교	<ul style="list-style-type: none"> • 낮은 시스템 구축 비용 (스마트폰 카메라 및 웹캠 등 활용가능) • 주변 환경, 노화 등에 의한 인식을 저하
행동적 특징	서명	서명과제(속도, 필압 등), 형상 비교	<ul style="list-style-type: none"> • 낮은 시스템 구축 비용 (스마트폰 터치스크린 활용가능) • 서명 복제 및 위조 가능
	음성	개인 고유 음성패턴 비교	<ul style="list-style-type: none"> • 전화 · 인터넷 등으로 원격 인증 가능 • 목소리 및 주변 환경에 의한 인식을 저하 • 녹음을 통한 도용 가능

가. 신체적 특징

바이오정보가 본인인증에 활용되기 위해서는 보편성(Universality), 유일성(Uniqueness), 불변성(Permanence), 편의성 등의 기본요건을 만족해야 한다. 예를 들어 지문의 경우 나이가 들어도 변하지 않으며, 각 개인뿐만 아니라 일관성 쌍둥이 간에도 지문이 서로 다르고, 센서가 대다수의 스마트폰에 탑재될 만큼 소형화되어 편의성도 높기 때문에 지문인증 방식이 최근 가장 많이, 그리고 보편적으로 도입되고 있다.

정맥 및 홍채는 보편성, 유일성, 불변성을 만족하며, 바이오인증 기술의 정확성에 대한 평가 지표인 본인거부율과 타인수락률²⁾이 [표 3]과 같이 지문에 비해 더 우수하지만 센서 소형화의 어려움과 센서가 비교적 고가인 탓에 ATM 및 출·입국관리소 등을 중심으로 도입되었다. 하지만 홍채인증의 경우, 최근 들어 스마트폰에 탑재 가능할 만큼 센서의 소형화가 가능해짐에 따라, 지문인증에 이어 대중화될 전망이다.

[표 3] 신체적 특징별 인증 정확성(인식률) 비교

구분		본인거부율(FRR)	타인수락률(FAR)
지문		0.1%~0.5%	0.001%~0.01%
홍채		0.0001%~0.1%	0.000083%~0.0001%
정맥	손바닥	0.01%~0.1%	0.00008%~0.0001%
	손가락	0.01%~0.3%	0.0001%~0.001%
얼굴		1%~2.6%	1%~1.3%

자료 : 금융결제원, 바이오인식 기술의 금융서비스 적용 현황 및 발전과제, 2014.7.

얼굴 정보의 경우, 스마트폰 등 이용자 단말에 이미 탑재된 카메라를 통해 획득 가능하기 때문에 편의성은 높은 반면 조명 등 외부 환경의 영향으로 인해 정확성이 떨어질 수 있고, 노화로 인해 얼굴 특징이 변화될 수 있기 때문에 다른 바이오정보에 비해 불변성이 떨어지는 것으로 평가된다. 실제로 [표 3]에서 얼굴에 대한 본인거부율 및 타인수락률이 바이오정보들

2) 본인거부율(FRR, False Rejection Rate)과 타인수락률(FAR, False Acceptance Rate)은 각각 본인을 타인으로 오인해 인증을 거부하는 비율과 타인을 본인으로 오인하는 비율로 본인거부율 및 타인수락률 모두 낮을수록 정확성이 높음을 뜻한다.

중에 가장 높은 것을 확인할 수 있으며, 이는 정확성이 가장 낮음을 뜻한다. 이에 주변 환경 및 밝기에 상관없이 얼굴인식이 가능한 센서 등 개선된 기술들이 개발되고 있지만, 센서 소형화의 어려움 및 비용문제 등으로 건물통제 등에만 사용되고 있다.

이밖에도 스마트워치 및 밴드³⁾ 등 몸에 직접 착용하는 스마트 기기를 통해 측정 가능한 심전도 정보도 인증에 사용되고 있으며, 향후 센싱 기술을 발전 및 센서 소형화 등으로 더 다양한 신체적 특징들이 바이오인증 기술에 활용될 것으로 예상된다.

나. 행동적 특징

현재 도입 중인 바이오인증 기술에는 대부분 신체적 특징이 사용되고 있다. 정적인 정보가 대부분인 신체적 특징과는 달리, 행동적 특징은 동적인 정보로서 정보를 획득하기가 어렵거나, 외부 환경으로부터의 영향을 많이 받을 수 있기 때문이다.

하지만 최근 구글이 자사의 신기술 등을 발표하는 컨퍼런스인 구글 I/O 2016에서 다양한 행동적 특징을 활용한 새로운 인증 방식을 선보여 주목 받고 있다. 이 방식은 현재 Abacus라 불리는 프로젝트를 통해 연구·개발이 진행되고 있으며, 2015년 미국 28개 주의 33개 대학과 시범 테스트를 진행한 것으로 알려졌다.⁴⁾

Abacus는 스마트폰 및 웨어러블 단말 등 이용자가 항상 지니고 다니는 단말을 통해 평소 이용자의 키보드 입력 및 걸음걸이 패턴, 현재 위치 등의 행동적 특징을 계속해서 수집한다. 그리고 이 정보를 기반으로 신뢰점수(Trust Score)를 누적계산하고 인증 필요시 누적된 신뢰점수를 기준으로 인증 여부를 결정한다. 앱 개발사들은 각 앱에서 요구하는 신뢰성 수준에 따라 인증 여부를 결정하는 신뢰점수의 임계값을 결정할 수 있는데, 예를 들어 스마트뱅킹 앱의 경우 높은 신뢰점수를 설정하고, SNS 및 게임 앱 등은 비교적 낮은 신뢰점수를 설정할 수 있다.

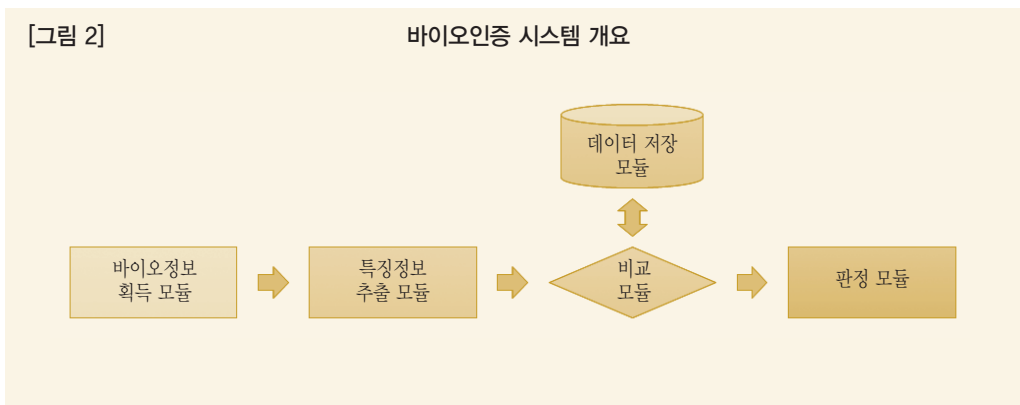
구글은 앱 개발사에서 Abacus를 사용할 수 있도록 2016년 하반기에 관련 기능들을 Trust API(Application Programming Interface)로 제공할 계획이며, 이미 2016년 6월부터 일부 대형 금융회사들과 테스트를 시작할 것이라고 밝힌바 있다.

3) 손목에 착용하는 스마트워치와 유사한 형태의 스마트기기로서, 디스플레이 기능은 최소화하고 다양한 바이오정보(맥박, 심전도 등)를 수집하는데 특화된 기기이다.

4) Sarah Perez, Google plans to bring password-free logins to Android apps by year-end, May 2016.

3. 바이오인증 시스템

바이오인증 시스템은 일반적으로 [그림 2]와 같이, 지문 및 홍채 등의 바이오정보를 획득하는 모듈, 획득한 바이오정보로부터 특징정보를 추출하는 특징정보 추출 모듈, 특징정보를 저장하는 데이터 저장 모듈, 인증 요청자의 특징정보와 저장된 특징정보를 비교하는 비교 모듈 및 판정 모듈로 구성되며, 각 모듈별 세부 설명은 [표 4]와 같다.



[표 4] 바이오인증 시스템 모듈별 설명

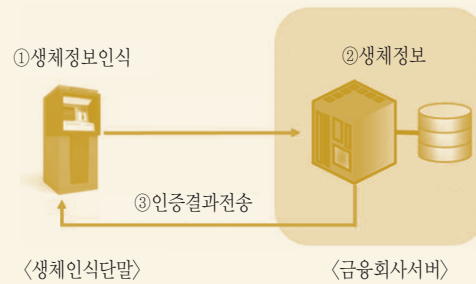
모듈명	설명
바이오정보 획득	바이오정보를 획득하여 샘플(지문 이미지, 음성 레코딩 등)로 변환
특징정보 추출	샘플로부터 실제 바이오정보 비교 대상인 특징정보 추출
데이터 저장	특징정보 저장 · 관리
비교	인증 요청자의 특징정보와 저장된 특징정보 간 유사성 비교
판정	비교 결과 바탕으로 두 특징정보의 출처가 동일한 주체인지 판정

바이오인증 과정은 크게 등록 및 인증 단계로 구분된다. 먼저, 등록 단계에서는 이용자의 바이오정보를 획득 및 특징정보를 추출하여 저장한다. 인증 단계에서는 등록된 바이오정보와 인증 요청자의 것이 동일한 주체의 바이오정보인지 여부를 비교하여 인증 성공여부를 판단한다.

바이오인증 시스템의 유형은 데이터 저장, 비교 및 판정부가 클라이언트 단말에 위치하는지, 또는 서버에 위치하는지 등에 따라 구분된다. 일반적으로 클라이언트 단말이 ATM 및 키오스크 등의 공용 단말의 경우에는 [그림 3]의 (a)와 같이, 바이오정보 저장 및 비교가 서버에서 수행되는 방식이 사용된다. 단말이 스마트폰 등의 개인 모바일 단말인 경우에는 저장 및 비교 등은 단말에서 수행하고, 판정 결과만 서버로 전송하는 [그림 3]의 (b)와 같은 방식이 주로 사용되며, 대표적으로 업계표준으로 자리 잡은 사실표준(De-facto)인 FIDO (Fast Identity Online) 방식이 이에 해당한다.

[그림 3]

바이오인증 시스템 유형별 개요



(a) 서버 저장 및 비교 방식



(b) 클라이언트 저장 및 비교 방식(FIDO)

III. 바이오인증 도입 현황

바이오인증 기술은 [표 1]과 같이 매우 다양한 분야에서 활용되고 있으며, 본 고에서는 바이오인증 기술이 가장 적극적으로 도입되고 있는 금융 및 공공부문을 중심으로 도입 현황에 대해 알아본다.

1. 금융권 도입 현황

가. 국내 도입 사례

국내 금융권의 경우, 과거에는 주로 내부 직원의 접근제어 및 내부통제 등을 목적으로 지문인증 등의 바이오인증 기술이 도입되었다. 이후 스마트폰 기반 बैं킹 및 간편결제 시 인증 방식으로 지문인증이 도입되기 시작하였으며, 바이오인증 기술이 금융권에 본격 도입됨에 따라, 손바닥 정맥인증뿐만 아니라 얼굴근육 및 홍채 인증까지 도입 추진 중이다.

국내 금융권의 바이오인증 기술 도입 사례는 [표 5]와 같다. 은행들의 경우에는 대부분 ATM 및 스마트뱅킹 서비스 등에 바이오인증 기술을 직접 적용하였다. 반면, 대부분의 카드사들은 삼성페이 등 바이오인증 기술이 적용된 간편결제 플랫폼을 통해 자사 카드 결제 서비스를 제공함으로써, 바이오인증 기술을 간접적으로 도입한 형태이다.

[표 5] 국내 금융권 바이오인증 기술 도입 사례		
기업명	도입 내용	도입 시기
우리은행	국내 은행 최초로 인터넷뱅킹 및 ATM에 지문인증 방식 도입	2001년
KB국민은행	내부 직원의 전산시스템 접근제어용으로 지문인증 방식 도입	2014년
KEB하나은행	스마트뱅킹 이용 시 본인인증을 위해 지문인증 방식 도입	2016년
IBK기업은행	얼굴근육인증 방식 도입	시범적용
씨티은행	ATM에 홍채인증 방식 도입	도입추진
새마을금고	스마트폰 및 홍채인증 기반의 ATM 도입	도입검토

신한은행	금고 직원의 책임자 업무승인 시 지문인증 방식 도입	2006년 이전
NH농협은행	키오스크를 통한 셀프뱅킹시스템에 후지쯔 사의 손바닥 정맥 인증 방식 도입	2015년
NH손해보험	스마트뱅킹 이용 시 본인인증을 위해 지문인증 방식 도입	2016년
주요카드사	직원의 PC 접근제어용으로 지문인증 방식 도입	-
하나카드	삼성페이 등 바이오인증 기술이 적용된 간편결제 플랫폼을 통해 간접적으로 지문인증 등 도입	2015년
롯데카드	간편결제 시스템인 모비페이에 지문인증 방식 도입	2016년
사회	손바닥 정맥인증 기반의 오프라인 결제 방식 도입	시범운영

자료 : 우리금융경영연구소, '국내외 생체인식 기술의 도입 현황과 전망'보고서 및 관련 기사 종합

최근 들어 [표 6]⁵⁾과 같이, 전자상거래 업체들 또한 전용 스마트폰 앱을 선보이면서 쇼핑 고객들의 편리한 간편결제를 위해 바이오인증 기술을 도입하고 있는 추세이다. 그뿐만 아니라 간편 송금 및 결제 서비스를 선보인 일부 핀테크 업체들도 바이오인증 기술을 도입하는 등 전 금융권에서 바이오인증 기술이 각광 받고 있다.

[표 6] 국내 e-커머스, 핀테크 업체의 바이오인증 기술 도입 사례		
기업명	도입 내용	도입 시기
쿠팡 로켓페이	스마트폰 간편결제 인증을 위해 지문인증 도입 ※ 로켓페이, 네이버페이는 현재 TouchID지원 애플 단말만 지원	2016년
11번가 시럽페이		2016년
네이버페이		2015년
페이코		도입검토
토스	간편송금 시 인증을 위해 지문인증 도입 ※ 현재 TouchID지원 애플 단말만 지원하며, 확대예정	2016년

5) [표 6~8] 자료 - 관련 기사 종합

나. 국외 도입 사례

국외 금융회사들은 지문뿐만 아니라 심전도 및 심장박동 등 국내와 비교하여 더 다양한 바이오정보를 사용하고 있다.

미국 및 유럽의 도입 사례는 [표 7]과 같으며, 국내와는 다르게 음성인증 방식도 상당수 도입된 상태이다. 특히 Wells Fargo의 경우 다수의 바이오정보를 융합하여 인증하는 다중 바이오인증 기술도 도입을 계획 중이다.

[표 7] 미국 및 유럽 금융권 주요 바이오인증 기술 도입 사례			
국가	기업명	도입 내용	비고
미국	Bank of America	모바일뱅킹 인증을 위해 지문인증 도입	-
	J.P. Morgan	서비스 로그인 시 인증을 위해 지문인증 도입	-
	Citi group	신용카드 고객 인증을 위해 음성인증 도입	-
	USAA	스마트뱅킹 인증을 위해 얼굴 및 음성, 애플의 지문 (Touch ID ⁶⁾) 도입	-
	Wells Fargo	자사 고객 인증을 위해, 안구인식 및 다중 바이오인증 (얼굴 및 행동적 특징) 기술 도입	-
	다수 금융사	구글 Abacus 프로젝트 Trust API를 통한 다수의 행동적 특징을 활용한 인증방식 내부 테스트	테스트 중
	MasterCard	결제 시스템에 Nymi 사의 스마트 밴드를 활용한 심전도 인증 기술 도입	테스트 중
캐나다	RBC		
	Tangerine	스마트뱅킹 인증을 위해 얼굴, 지문 및 음성 인증 도입	-
영국	Halifax (Lloyds Banking Group)	자사 전자금융서비스를 위한 심장박동 인증 기술 도입	시범운영
	Barclays	Hitachi 사의 손가락 정맥 인증 기술 도입	-
	HSBC	스마트뱅킹 인증을 위해 음성 및 지문(Touch ID) 인증 도입	-
러시아	Sberbank	ATM에서 사용 가능한 모든 거래에 음성인증 도입	-
	Itautech	지점 ATM 거래에 지문인증 도입	-
스코틀랜드	RBS	스마트뱅킹에 지문(Touch ID)인증 도입	-
볼리비아	BBVA Prevision AFP	연금 수령을 위한 얼굴인증 시스템 도입	개발 중
핀란드	Uniqul	얼굴인증 기반의 결제 시스템 개발	-

6) 애플의 스마트기기에 적용된 지문인증 기술.

호주, 중국 및 일본의 도입 사례는 [표 8]과 같으며, 일본은 2011년 동일본 대지진 당시 통장 및 카드가 유실된 고객들이 예금 인출 등 금융거래를 하지 못하는 사례가 속출하자, 이를 계기로 ATM에서 통장이나 카드 없이 생년월일 입력 및 바이오인증만으로 금융거래가 가능한 방식을 대거 도입하였다. 최근 중국의 거대 e-커머스 업체인 Alibaba가 결제 시 인증 방식으로 얼굴인증 방식을 사용한 ‘스마일 투 페이(Smile to Pay)’를 도입하였으며, 이를 시작으로 중국에서도 바이오인증 기술 도입이 가속화될 것으로 예상된다.

[표 8] 기타 해외 금융권 주요 바이오인증 기술 도입 사례		
국가	기업명	도입 내용
호주	St George Bank	스마트뱅킹 인증을 위해 지문인증 도입
	National Australia Bank	폰뱅킹 및 ATM 인증을 위해 음성인증 도입
중국	Alibaba	자사 온라인 쇼핑몰 결제 시 얼굴인증(스마일 투 페이) 도입
일본	NTT Docomo	스마트폰 기반 간편결제를 위한 홍채인증 도입
	Japan Post Bank	ATM 이용시 인증을 위해 손가락 및 손바닥 정맥인증 도입
	Mega Bank	
	Trust Bank	
	Regional Bank	
	Local Bank	

2. 공공부문 도입 현황

국내·외 정부 주도의 바이오인증 기술 도입은 크게 공공부문에서 바이오정보를 활용하기 위한 정부 주도의 바이오정보 수집·관리 형태와 기존 신분증을 대체하기 위한 바이오 eID 카드 형태로 나눌 수 있다.

가. 정부 주도 수집·관리

국내의 경우, 1968년 주민등록증 발급 시 양손 엄지손가락 지문을 날인하는 제도가 최초

도입되었다. 이후 1975년 열 손가락 지문을 모두 등록하게 하는 방식으로 바뀌면서 정부가 국민의 지문을 수집 및 관리하기 시작하였으며, 현재까지는 주로 무인 민원증명서 발급 및 경찰 수사 등 공공부문에서 활용되어 왔다. 최근 발표에 따르면 2017년 1월부터 주민등록증 발급 시 잉크를 사용한 기존 지문 등록방식과 전자식 스캐너(센서)를 사용하는 방식을 선택적으로 병행 가능토록 개선하는 등 바이오정보를 효과적으로 수집·관리하기 위한 노력이 계속되고 있다.⁷⁾

최근 테러가 빈번히 발생하고 있는 사우디아라비아의 경우, 국가안보 강화를 목적으로 바이오정보를 수집 및 관리하기 위한 법안이 2015년 9월 통과되었다. 모바일폰 이용자가 국가안보에 대한 위협 활동에 참여하는 것을 억제하기 위한 보안조치의 일환으로 SIM 카드를 구매하는 모든 사람의 지문을 수집 및 관리하는 내용의 법안으로 사우디아라비아의 내무부(Ministry of Interior)에 의해 추진 중이며, 현재 관련 시스템을 구축중인 것으로 알려졌다.⁸⁾

이를 포함한 해외 주요국의 바이오정보 수집·관리 현황은 [표 9]과 같다.

[표 9] 해외 주요국의 바이오정보 수집·관리 현황	
국가	세부 현황
미국	<ul style="list-style-type: none"> • 일반 국민에 대해서는 바이오정보를 수집하지 않고, 범죄자에 한해 바이오정보 수집 • 2004년 1월 외국인 방문자들의 얼굴 사진 및 지문을 수집하는 'US VISIT'을 도입하였고, 이후 정확한 신원파악을 목적으로 열 손가락의 지문을 모두 수집 및 관리 • 수집된 정보는 FBI 등 정보기관 및 이민국 등에서 활용
영국	<ul style="list-style-type: none"> • 국민의 DNA정보를 수집 및 관리하고 있으며, 비EU 국가 방문객을 대상으로 생체비자(비자 신청시 얼굴 사진 및 지문 수집) 발급을 의무화
일본	<ul style="list-style-type: none"> • 테러 대책 차원에서 2007년 11월 16세 이상 외국인이 입국자에 한해 얼굴 사진 및 양손 집게손가락 지문을 수집 및 관리
사우디아라비아	<ul style="list-style-type: none"> • 테러 등 국가안보 위협 방지를 위해, 모든 모바일폰 SIM 카드 구매자의 지문을 수집 및 관리

자료 : 위키피디아, 주민등록 지문정보DB 사건 및 관련 기사 종합

7) 국민일보, 주민등록번호 변경 신청 내년 5월30일부터 가능, 스캐너 활용 지문등록도 추진, 2016.5.31.

8) Middle East Eyes, Saudi Arabia to gather fingerprints of mobile phone users, Jan, 2016.

나. 바이오 eID 카드

바이오 eID 카드는 일반적으로 IC 칩이 포함된 스마트카드 형태로 홍채, 지문 등의 바이오 정보와 전자서명을 위한 정보 등이 함께 저장되어 실명확인 및 본인인증에 활용 가능하며, 기존의 신분증 위조 및 도용 등의 문제를 개선할 목적으로 도입되고 있다. 쉽게 접할 수 있는 전자여권 역시 바이오 eID 카드로 볼 수 있으며, 바이오 eID 카드는 해외 주요 국가들에서 국민 전체 또는 일부(범죄자, 외국인 등)에 발급되고 있다.

최근 도입 사례로 헝가리의 경우, 2016년 1월부터 ‘One-stop card’라는 이름의 바이오 eID 카드를 국민들에게 발급하기 시작하였으며 영업일 기준 5일만에 3만9천명이 발급 받은 것으로 알려졌다. 이 카드에는 지문 등의 바이오정보 뿐만 아니라 국가별로 사회보장(Social security) 정보, 세금 관련 식별정보 등이 추가로 저장 및 활용되고 있다.⁹⁾

이밖에 최근 터키, 파키스탄, 요르단 등이 바이오 eID 카드를 도입 중이며, 사례는 [표 10]과 같다.

[표 10] 바이오 eID 카드 도입 최근 사례	
국가	세부 현황
헝가리	<ul style="list-style-type: none"> • 2016년 1월, 바이오 eID 카드인 ‘One-stop card’발급을 시작하였으며 영업일 기준 5일만에 3만9천명에게 발급 • 지문정보 등 바이오정보, 전자서명 정보, 사회보장 및 세금 관련 정보 등 저장 • 한번 발급 받은 카드는 19세부터는 6년, 18세 이하는 3년간 유효
터키	<ul style="list-style-type: none"> • 터키의 아나톨리안 지역을 바이오정보 eID 카드 시범 지역으로 선정하여 파일럿 형태로 운영 중 • 해당 카드에는 손가락 및 손바닥 지문 정보를 포함하여 최대 1GB의 정보를 저장할 수 있고, 발급 후 10년 동안 유효
파키스탄	<ul style="list-style-type: none"> • 여행증명서 위조 및 인신매매 등을 방지하기 위해 전자여권을 발행하기 시작하였으며 2017년 완료 예정 • 전자여권에는 바이오정보가 저장되며, 파키스탄 입국심사를 위한 별도의 정보들이 추가될 예정
요르단	<ul style="list-style-type: none"> • 2016년 3월, 요르단의 정보통신기술부(Ministry of Information and Communications Technology)는 손가락 지문 등록을 통해 발급하던 eID에 손바닥 지문까지 포함하도록 변경 • 100여개 주민 및 여권사무소에서 발급 시작
자료 : LTP, The Lastest Governments–Powered Initiatives with Biometric Identification, Jun, 2016.	

9) LTP, The Lastest Governments–Powered Initiatives with Biometric Identification, Jun, 2016.

IV. 바이오인증 보안 동향

1. 바이오인증 보안 위협 및 사고사례

최근 바이오인증 기술 도입이 활발해지며 주목 받기 시작함과 동시에 다양한 보안 위협 사례가 공개되고 있다.

바이오인증 기술은 기존 인증 방식에 존재하는 보안 위협이 대부분 그대로 존재한다. 예를 들면, 전송구간 도청 및 인증정보 위·변조, 클라이언트 및 서버 상의 악성코드 설치, 인증결과 조작 등의 위협이 모두 존재하는데, 이는 대부분의 인증 시스템에 공통적으로 존재하며 대응방안 또한 대부분 유사하다. 다른 인증기술과 비교하여 바이오인증 기술에서 더 심각한 보안위협은 바이오정보 위조 및 유출이며, 본 고에서는 두 위협에 대해 알아본다.

가. 바이오정보 위조

바이오정보 위조는 타인의 바이오정보를 위조하여 불법적으로 인증을 시도하는 것이다. 바이오정보는 개인의 신체적·행동적 특징으로 불법 복제 및 도용으로부터 안전한 것으로 알려져 있었다. 하지만 최근 프린트된 지문, 실리콘 지문, 고해상도 사진 등 위조된 바이오정보를 통해 인증에 성공하는 사례들이 발표됨에 따라 위조 위협으로부터 안전하지만은 않다는 것이 밝혀지고 있다.

위조된 바이오정보를 악용하여 인증 우회가 가능한 이유는 미리 등록된 특징정보와 비교 특징정보가 완전히 일치하지 않고 일부 차이가 있더라도 인증에 성공할 수 있기 때문이다. 또 다른 이유는 바이오정보 센싱의 기술적 수준이 부족할 수 있기 때문이다. 예를 들어, 일란성 쌍둥이의 바이오정보 중 얼굴의 경우 지문과는 달리 유사성이 매우 높기 때문에 눈·코·입의 상대적인 위치 및 크기 등과 같은 비교적 단순한 특징으로 비교한다면, 쌍둥이 서로 간의 얼굴인증이 성공할 수도 있다.

바이오인증 기술 도입 초기, 바이오인증 우회를 위해 바이오정보를 위조하기 보다는 타인의 손가락 등 신체 일부분을 절단하는 등의 비윤리적 범죄가 우려되었다. 하지만 최근 위조 기술의 발달에 따라 점차 더 간단한 위조 방법을 통해 인증을 우회하는 시연 및 사고 사례가 발표되고 있다.

먼저 스마트폰 등을 통해 가장 보편적으로 사용되고 있는 지문의 경우, 2005년 지문인증

시스템이 적용된 고급차량 절도를 위해 차주의 손가락을 절단한 사고를 시작으로 지능화된 위조 방식이 등장하고 있다. 2008년 이후에는 목제용 접착제, 실리콘, 점토, 3D 프린터 등을 활용하여 제작한 위조지문으로 공공기관에서 불법 본인인증 및 온라인 결제 등을 성공한 사례가 발표된바 있다.

그리고 2016년에는 총 비용 \$500 미만으로 일반 2D프린터를 이용하여 출력한 위조 지문을 통해 최신 스마트폰의 바이오인증을 우회한 사례가 미국 미시간주립대 연구진들에 의해 발표되었다.¹⁰⁾ 연구진들은 지문을 스캔한 후에 일반 2D 프린터와 AgIC 은(Silver) 전도성 잉크를 사용하여 전용 종이¹¹⁾에 출력하고, 출력한 지문으로 [그림 4]와 같이 인증에 성공한 것으로 알려졌다.

[그림 4]

위조 지문을 이용한 스마트폰 언락



(a) 삼성 갤럭시 S6 언락



(b) Huawei Honor 7 언락

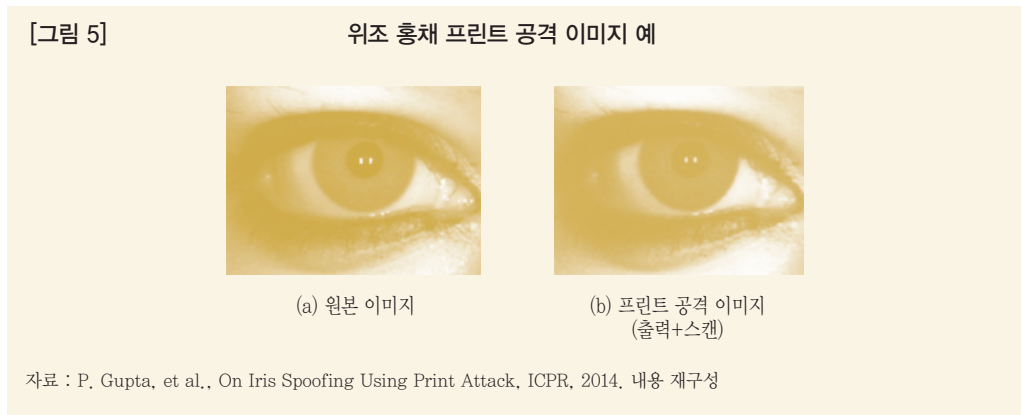
자료 : K. Cao, and A.K. Jain., Hacking Mobile Phones Using 2D Printed Fingerprints, Tech, report, 2016.

홍채의 경우에도 최근 위조 사례가 발표되었다. 2014년 독일의 CCC라는 해커단체는 구글

10) K. Cao, and A.K. Jain., Hacking Mobile Phones Using 2D Printed Fingerprints, Tech, report, 2016.

11) 전자회로를 손쉽게 프린트할 수 있도록 고안된 특수 잉크 및 용지로서, 이를 통해 출력한 그림은 전도성을 갖게된다.

검색을 통해 획득한 러시아 푸틴 대통령의 사진으로부터 고해상도 홍채 사진을 출력하여 위조 홍채를 제작하였다. 이러한 위조 방식을 프린트 공격(Print attack)이라 부르며, 인도의 연구진에 따르면 콘택트렌즈 착용 등의 홍채인식 성능저하 요소가 없는 상태에서 [그림 5]의 (a) 원본 사진을 (b)와 같이 출력 및 스캔하여 프린트 공격을 시도할 경우 최대 62.37% 인증 성공률을 보이는 것으로 알려졌다.¹²⁾



이밖에도 위조 지문을 사용한 실제 사고들이 발생하였으며, 대표적인 사례들은 [표 11]과 같다.

[표 11] 바이오정보 위조 사고사례		
사고 사례	시기	세부 현황
불법 부동산 명의 이전	2014. 10.	<ul style="list-style-type: none"> 박모씨 등 4명은 중국 위조범에 의뢰하여 3D 프린터를 이용한 실리콘 위조지문을 제작 주민센터의 지문센서가 위조여부를 탐지하지 못해 인감증명서 등 필요 서류를 발급받아 50억대 부동산을 불법으로 명의 이전
근태관리 악용	2013. 3.	<ul style="list-style-type: none"> 브라질 상파울루 의사인 Ferreira는 동료의사 등 6명의 실리콘 위조지문을 제작하여 교대로 근태관리를 악용, 실근무를 하지 않고 급여를 수령하다 적발됨
지문인식 지불시스템 해킹	2008. 2.	<ul style="list-style-type: none"> 네덜란드 최대의 식품품 체인업체가 지문인식 지불시스템(Tip2Pay)을 도입하였으나, 실리콘으로 제작한 위조지문에 의해 인증이 우회됨
차량 절도를 위한 손가락 절단	2005. 3.	<ul style="list-style-type: none"> 말레이시아 4인 강도는 지문인식시스템이 도입된 벤츠 S-클래스 차량을 절도하기 위해 차량주인인 회계사 Kumaran의 손가락을 절단 해당 지문인식시스템이 살아있는 생체조직 여부를 판별하는 기능을 탑재하고 있어, 절단한 손가락으로 차량구동이 불가하여 검거

12) P. Gupta, et al., On Iris Spoofing Using Print Attack, ICPR, 2014.

나. 바이오정보 유출

모든 인증 방식에서 인증정보의 유출은 심각한 보안위협으로 인식되지만, 바이오정보의 유출은 더욱 심각하다. 바이오정보의 변하지 않는 특성(불변성)으로 인해, 한번 유출될 경우 비밀번호 및 공인인증서 등과 같이 폐기 후 변경 및 재발급하는 것은 매우 어렵기 때문이다. 그나마 지문의 경우 다른 손가락의 지문으로 대체 가능하지만, 홍채 및 정맥 등은 더욱 제한적이다.

바이오정보 유출 위협은 바이오인증 시스템 전반에 존재하며, [표 12]과 같이 바이오인증 단계에 따라서 바이오 샘플, 특징정보 및 템플릿 형태로 유출될 수 있다. 먼저 바이오정보 획득 단계에서 바이오 샘플 형태로 유출될 경우, 앞서 기술한 위조 방식을 통해 손쉽게 인증 우회에 악용될 수 있다. 바이오 특징정보 및 템플릿 형태로 유출될 경우에도 재전송 및 힐 클라이밍 공격¹³⁾에 악용될 수 있다.

[표 12] 바이오인증 단계별 바이오정보 유출 형태		
바이오정보 형태	설명	유출 가능한 단계
바이오 샘플	센서를 통해 획득한 원본 정보 (예: 지문 및 얼굴 이미지 등)	바이오정보 획득, 전송구간
바이오 특징정보 (Feature)	바이오 샘플로부터 추출한 특징정보 (예: 지문의 끝점, 분기점, 중심점 등)	특징정보 추출
바이오 템플릿 (Template)	특징정보를 비교 및 DB에 저장하기 위한 형태	특징정보 추출, 데이터 저장, 비교, 전송구간

바이오정보 유출의 경우, [표 13]과 같이 바이오정보가 저장된 서버를 공격하여 대규모 유출사고가 발생한바 있다. 미국 연방 인사관리처는 해킹에 의해 전/현직 공무원의 지문정보 560만건을 유출 당했으며, 미국 에너지국에서도 직원 수백 명의 사진 및 지문정보가 유출되었다.

13) 바이오정보 비교 결과가 인증 성공 임계값 이상이 되도록 템플릿을 지속적으로 수정·전송하는 공격.

[표 13] 바이오정보 유출 사고사례		
사고 사례	시기	세부 현황
미국 연방 인사관리처 지문 유출	2015. 6.	<ul style="list-style-type: none"> 중국집단의 APT공격에 의해 DB가 해킹되어 미국 전·현직 공무원의 개인정보 2,200만 건* 및 지문정보 560만 건 유출 * 미국 전체 인구의 약 7% 수준 개인 신상정보, 건강기록, 금융정보 및 퇴직관련 기록 등이 유출되어 신용정보 도용 뿐만 아니라 정부부처 임직원 행세까지 가능해 미국 역사상 가장 파급력이 큰 유출사고 중 하나로 기록됨 미국 연방 인사관리처는 올해 1,000여 명의 사이버보안 전문가를 채용할 계획
미국 에너지국 지문정보 유출	2013. 1.	<ul style="list-style-type: none"> 서버 14대, 워크스테이션 20대 등이 해킹되어 직원 수백 명의 개인정보, 사진 및 지문정보 유출

2. 바이오인증 보안 대응기술 동향

바이오인증 기술과 관련된 보안 위협을 개선하기 위해 다양한 대응기술들이 연구되고 있으며, 바이오정보 위조 및 유출 위협에 대한 대응기술을 중심으로 알아본다.

가. 위조 판별

위조 판별(Liveness detection)은 바이오정보가 실제 사람의 것인지 또는 위조된 것인지 여부를 판별하는 기술로서 크게 하드웨어 및 소프트웨어 기반 기술로 분류되며, 대표적으로 위조 지문을 판별하는 방식은 다음과 같다.

하드웨어 기반 방식은 센서를 통해 맥박 및 체온 등을 추가로 측정하여 획득한 바이오정보가 살아있는 사람의 것인지 여부를 확인하는 방식이다. 대표적으로 빛 투과율, 정전용량, 혈류 및 혈중 산소함량 등을 측정하여 위조 지문을 탐지하는 특허들이 등록되어 있다. 하드웨어 방식은 소프트웨어 방식에 비해 위조 판별 성능은 더 높지만 새로운 신체적 특징을

측정하기 위해 기존 센서를 변형하거나 새로운 센서가 추가되어 시스템 소형화가 어려워지는 한계가 존재한다.

소프트웨어 기반 방식은 획득한 바이오 샘플을 분석하여 위조 여부를 확인한다. 대표적으로 실제 지문에만 존재하는 땀샘을 짧은 시간 동안 두 번 이상 측정하여 발한현상을 검출하거나, 센서에 지문을 접촉한 채로 손가락을 일정각도 회전하도록 하여 회전 전/후 피부의 왜곡정도를 측정함으로써 실제 지문과 위조 지문의 구분한다. 또한 샘플의 품질을 기준으로 위조 여부를 판단하는 방식이 존재한다. 소프트웨어 방식 적용을 위해서는 분석 소프트웨어를 추가 또는 업데이트하면 되기 때문에 적용은 쉽지만, 하드웨어 방식에 비해 정확도가 떨어지는 단점이 존재한다.¹⁴⁾

위조 지문 판별 방식의 분류 및 특징은 [표 14]와 같다.

[표 14] 위조 지문 판별 방식 비교				
위조 판별 방식		원리	장점	단점
하드웨어	광학	빛 투과/흡수/산란 정도, 다중스펙트럼 영상 측정	고해상도, 정밀한 영상	고비용 및 큰 공간 차지
	전기학	사람 피부의 전기학 특성 (정전용량 등) 측정	다수의 위조 지문 방지 가능	전기학적 특성을 가진 위조 재료에 취약
	생리학	체온 등 사람의 생리학적 특성 측정	비교적 구현이 쉬움	탐지 원리 노출시 비교적 쉽게 우회가능
소프트웨어	발한 작용 기반	땀샘에서 발한 작용 검출	오직 생체 지문에서만 검출 가능	검출이 어려움
	변형기반	손가락을 움직여서 피부의 왜곡정도 및 탄성을 검출	—	위조 재료의 탄성이 실제 피부와 유사할 경우 우회가능

자료 : TTA, 위조 지문 탐지 기술, 기술보고서, 2010. 내용 재구성

14) TTA, 위조 지문 탐지 기술, 기술보고서, 2010.

나. 다중 바이오인증

다중 바이오인증 기술은 인증 시 다수의 바이오정보를 융합하는 방식으로, 하나의 바이오 정보만을 사용하는 단일 바이오인증 기술과 비교하여 본인거부율 및 타인수락률을 낮춤으로써 정확성을 개선하기 위한 방식이다. 보안 측면에서는 다수의 바이오정보를 동시에 사용함으로써, 사용된 모든 바이오정보 위조에 성공하지 않는 이상 인증 우회가 어려운 장점이 있다. 이뿐만 아니라, 바이오정보가 유출된다 하더라도 다수의 바이오정보가 융합되어 있기 때문에 템플릿 등의 구조 파악이 어려우며, 복원 공격 등으로부터 더 안전하다. 하지만 특징정보간의 호환성 문제, 융합된 바이오정보 비교시 복잡도 문제 등 기술적으로 해결해야 할 문제점들이 존재하며, 이에 대한 개선이 필요하다.

다중 바이오인증 기술은 먼저, 융합 방식에 따라 다중 모달/알고리즘/인스턴스/센서로 구분되며 각 방식에 대한 설명은 [표 15]와 같다.

[표 15] 다중 바이오인증 융합 방식	
융합 방식	세부 설명
다중 모달 (Multi-modal)	2개 이상의 서로 다른 바이오정보를 융합 (예 : 지문 + 얼굴, 지문 + 정맥 등)
다중 알고리즘 (Multi-algorithm)	단일 바이오 샘플에 다수의 특징정보 추출 알고리즘을 적용하여 특징정보 추출 및 융합
다중 인스턴스 (Multi-instance)	단일 모달로부터 다수의 인스턴스를 획득 및 융합 (예 : 엄지 지문 + 검지 지문, 왼쪽 눈 홍채 + 오른쪽 눈 홍채 등)
다중 센서 (Multi-sensor)	단일 인스턴스를 다양한 센서로 획득하여 융합 (예 : 얼굴 2D이미지 + 3D이미지, 지문 광학센서 + 정전센서 등)

자료 : ISO/IEC TR 24722 Information technology-Biometrics-Multimodal and other multibiometric fusion 내용 재구성.

다. 재발급 가능한 템플릿 기술

재발급 가능한 템플릿¹⁵⁾ 기술은 바이오정보 유출 위협에 대한 대응기술로서, 바이오 템플릿이 유출되더라도 이를 폐기하고 새로운 템플릿을 재발급 가능하도록 하는 기술이다. 재발급 가능한 바이오인식(Renewable Biometric) 기술이라고도 불리며, 이에 대한 내용이 ISO/IEC 표준¹⁶⁾으로도 제정된 바 있다.

재발급 가능한 템플릿 기술의 가장 큰 특징은 바이오 템플릿 대신 별도의 비교정보를 사용한다는 점이다. 비교정보는 템플릿을 이용하여 생성하며, 재발급(생성) 가능한 알고리즘에 의해 생성되기 때문에 유출되더라도 폐기 및 재발급 가능하며 비교정보로부터 템플릿 역추출 및 복원은 불가능하기 때문에 템플릿은 안전하다.

세부적으로, 바이오정보 등록 및 비교 시 바이오 템플릿을 그대로를 저장 및 비교하지 않는다. 그 대신, 등록 단계에서 템플릿을 이용하여 별도의 비교(인증)정보를 생성하고, 이 비교정보를 본래 템플릿 대신 등록(저장)한 후에 인증 단계에서 비교한다. 이때 바이오 샘플 및 템플릿은 비교정보 생성 직후 안전하게 폐기하기 때문에 유출 우려가 적다. 비교정보 생성 전까지는 바이오 샘플 및 템플릿에 대한 유출 위협이 여전히 존재하지만, 일반적으로 바이오 샘플 획득부터 템플릿 및 비교정보 생성까지는 원자적(Atomic)으로 수행되기 때문에 템플릿이 그대로 저장 및 전송되는 것 보다는 더 안전하다.

인증 단계에서는 등록 단계에서 생성한 보조데이터와 인증 요청자의 템플릿을 결합하여 비교정보를 생성(복구)하고, 이를 비교정보와 비교하여 인증 여부를 판정한다. 인증 요청자의 샘플 및 템플릿 역시, 비교정보 생성 직후 폐기한다.

재발급 가능한 템플릿 기술은 바이오정보 유출에 대한 효과적인 대응기술이며, 실제 활용을 위해서 계속 연구가 진행 중이다.

15) 바이오 특징정보들의 집합으로 바이오정보는 템플릿 형태로 비교 및 저장됨.

16) ISO/IEC 24745, Information technology—Security techniques—Biometric information protection.

V. 결론

바이오인증 기술은 금융, 공공·사회복지 등 다양한 분야에서 활용되고 있다. 특히 스마트폰 상에서의 스마트뱅킹 및 간편결제 시 본인인증 방식으로 적극 활용 중이며, 은행, 카드사, 전자상거래 및 핀테크 업체 등 금융 관련 전 분야에서 도입 중이다.

하지만 바이오인증의 편리함 이면에 바이오정보 위조 및 유출과 같은 위협이 존재한다. 먼저 위조 위협의 경우, 앞서 소개한 위조사례를 통해 쉽게 구할 수 있는 재료들로도 위조 및 인증 우회가 가능함을 알수 있다. 그리고 바이오정보 유출의 경우에도 대규모 유출 사례들이 존재함을 확인하였다.

이러한 보안 위협에도 불구하고, 대응기술들에 대한 관심 및 도입은 부족한 상황이다. 첫 번째 이유는 대응기술의 기술적 한계이다. 위조 판별의 경우 각 기법별로 장/단점이 존재 하며, 다중 바이오인증 및 재발급 가능한 템플릿 기술은 계속 연구가 진행 중이다.

두 번째 이유는 바이오인증 관련 보안위협에 대한 인식 부족이다. 아직까지 바이오정보 유출 등으로 인한 대규모 피해사례는 보고되지 않았지만, 악용시 큰 피해가 예상되기 때문에 바이오인증 기술에 대한 보안위협성을 인식하고 대비하여야 한다.

이처럼, 바이오인증 기술의 보안성 제고를 위해서는 관련 기술의 고도화 및 보안의식 개선 등의 노력이 필요한 상황이며, 본 고가 이러한 필요성을 인식하는 계기가 되기를 기대한다.

〈참고문헌〉

- [1] 금융보안원, 바이오정보 사고사례 및 대응방안 조사, 2016.
- [2] 금융보안원, 바이오정보 템플릿 재발급 기술 조사, 2016.
- [3] 금융보안원, 생체정보를 이용한 금융 서비스 현황 비교 분석, 2015.
- [4] A.K. Jain et al., 50 years of biometric research: Accomplishments, challenges, and opportunities, Pattern Recognition Letters, 2016.
- [5] A.K. Jain, et al., Biometric Template Security, EURASIP Journal on Advances in Signal Processing, 2008.
- [6] A.K. Jain, and K. Nandakumar, Biometric Authentication: System Security and User Privacy, IEEE Computer, 2012.
- [7] K. Cao, and A.K. Jain., Hacking Mobile Phones Using 2D Printed Fingerprints, Tech. report, 2016.
- [8] ISO/IEC 24745, Information technology–Security techniques–Biometric information protection.
- [9] ISO/IEC TR 24722, Information technology–Biometrics–Multimodal and other multi-biometric fusion.
- [10] TTA, 위조 지문 탐지 기술, 기술보고서, 2010.

금융권 사물인터넷(IoT) 동향 및 향후 전망

황 증 모*

I. 서론	31
II. 사물인터넷 개요	32
1. 정의	32
2. 기술 구성요소	33
III. 사물인터넷 동향 및 적용사례	36
1. 사물인터넷 플랫폼 동향	36
2. 금융권 국내·외 적용사례	40
IV. 향후 전망 및 보안 고려사항	43
1. 금융권 사물인터넷 전망	43
2. 보안 고려사항	48
V. 결론	53
〈참고문헌〉	54

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

요 약

사물인터넷이란 기기, 센서, 인터넷 등을 통해 사람과 사물, 사물과 사물 간 상호 소통하고 정보를 생성, 가공, 공유, 활용하여 부가가치를 창출하는 기술 또는 사업 모델을 말한다. 가트너(Gartner)는 사물인터넷으로 연결된 스마트폰, 가전기기, 웨어러블 디바이스, 자동차 등의 사물들이 2020년에는 250억 개에 이를 것으로 예측하고 있으며, 시스코(CISCO)는 기업들이 창출할 수 있는 사물인터넷의 부가가치는 향후 10년 간 14.4조 달러로 예측하고 있다. 또한 맥킨지(McKinsey)는 2025년까지 인류의 삶에 가장 큰 변혁을 일으킬 ICT 기술 중 하나로 사물인터넷을 꼽고 있으며, 사물인터넷은 거의 모든 산업분야에서 널리 활용될 것으로 분석하고 있다.

이에 글로벌 선진국 및 기업들은 사물인터넷을 국가 및 산업 경쟁력 확보의 핵심 기반 기술로 인식하고 다양한 전략을 수립하고 있다. 특히 국가경쟁력을 좌우할 새로운 수익 창출의 신성장 원동력이 될 것으로 전망되는 사물인터넷 플랫폼을 주도하기 위해 글로벌 표준 플랫폼인 oneM2M, 산업단체 플랫폼인 OIC, AllSeen 등 다양한 플랫폼이 개발 중이다.

금융권은 헬스케어, 스마트홈, 제조업 등 타 분야에 비해 사물인터넷의 활용이 아직까지는 초기단계에 머물러 있으나, 사물에 대한 정보를 수집·분석하여 금융상품에 적용시키는 등 사물인터넷을 적용하는 사례가 꾸준히 증가하고 있다. 또한 엑센츄어(Accenture) 딜로이트(Deloitte)등은 가까운 미래에 금융회사는 다양한 사물로부터 수집한 정보를 이용하여 고객의 금융·비금융 관련 니즈에 만족할 수 있는 개인 맞춤형 조언을 제공하게 될 것이며, 타 업종과 파트너십을 맺어 특정 고객에게 가치 있는 정보를 제공하게 될 것으로 예상하고 있다.

따라서 금융회사는 향후 사물인터넷으로의 서비스가 이전되는 환경에 대비하여 사물인터넷 생태계 내 다양한 분야와 전략적 제휴를 맺고 고객의 니즈를 만족시킬 수 있는 신규 사업을 창출해 나가야 할 것이다. 이와 더불어 증가하는 보안위협에 대응하기 위해 다양한 보안상 고려사항을 준수해야 할 것이다.

I. 서론

사물인터넷(IoT, Internet of Things) 기술의 발전과 보급에 따라 컴퓨터가 다양한 소형 기기에 내장되고 항상 인터넷으로 연결되어 정보를 수집, 전송, 공유 및 분석하며 지능형 서비스를 제공하는 초연결(Hyper-Connectivity) 사회가 점점 현실화 되고 있다. 이에 구글, 애플 등 세계 각국의 주요 IT 업계의 사물인터넷 사업 진출이 가시화되고, 사물인터넷 관련 스타트업 및 관련 투자 규모가 급증하는 등 관련 생태계가 빠르게 조성 중이다.

개인 기기, 스마트홈, 스마트카, 헬스케어 등 다양한 분야의 애플리케이션이 개발되어 서비스 중이며, 사물인터넷 서비스 실현을 위해 요구되는 기반 설비, 단말, 통신 인프라 등 플랫폼 및 인터페이스 또한 많은 기업이 참여 중이다. 또한 모바일, 하드웨어, 빅데이터, 클라우드 컴퓨팅, 인공지능 등 타 IT기술과 융합하여 빠르게 발전하고 있다.

이에 본 고에서는 사물인터넷의 정의, 구성요소 및 최근 동향을 살펴봄으로써 사물인터넷에 대한 기술적 이해를 돕고자 한다. 또한 국내·외 금융권 적용사례 및 향후 전망을 통해 다가올 미래에 사물인터넷 기술이 금융권에 얼마나 많은 영향을 미칠 수 있을지 예상해봄으로써 금융회사들이 향후 사물인터넷이라는 신기술을 활용하는데 도움이 되고자 한다.

II. 사물인터넷 개요

1. 정의

사물인터넷이란 기기, 센서, 인터넷 등을 통해 사람과 사물, 사물과 사물 간 상호 소통하고 정보를 생성, 가공, 공유, 활용하여 부가가치를 창출하는 기술 또는 사업모델을 말한다. 사물인터넷은 MIT의 Kevin Ashton이 1999년 처음으로 제안한 용어로서 M2M(Machine to Machine), 유비쿼터스(Ubiquitous) 등 기존의 기술이 인터넷, 네트워크 및 컴퓨팅 기기의 발전과 더불어 사물 자체가 스마트 디바이스화 되는 개념으로 진화한 ICT 기술이다. 사물인터넷 초기 기술인 M2M은 사물과 사물 간의 통신을 통해 다양한 서비스를 제공하는 기술로서, RFID 센서를 활용한 교통카드, ATM 기기, 바코드 등이 대표적인 예이다. 최근에는 통신기술의 발달로 인한 네트워크 인프라의 확장, 통신을 담당하는 센서의 생산 비용 절감, 다양한 소형 단말 기기의 대중화 등으로 인해 네트워크가 연결되어 있는 곳이라면 언제 어디서든 사람, 사물, 서비스 간 상호 연결하여 정보를 공유할 수 있는 사물인터넷 기술로 발달하게 되었다. 즉, 사물인터넷은 기존 사물 간 정보만 공유하던 M2M 개념을 넘어 사물들끼리 정보를 공유 및 활용하고 의사결정을 수행하는 단계의 기술을 포함한 개념으로 정의할 수 있다.

가트너(Gartner)는 스마트폰, 가전기기, 웨어러블 디바이스, 자동차 등 사물인터넷에 연결된 사물들이 2016년 64억 개에 이를 것으로 보고 있으며, 2020년에는 그 수가 급증하여 250억 개의 사물이 다양한 분야에서 활용될 것으로 예측하고 있다. 또한 시스코(CISCO)는 향후 10년 뒤 기업들이 창출할 수 있는 사물인터넷의 부가가치가 14.4조 달러로 예측하고 있으며, 맥킨지는 사물인터넷을 2025년까지 인류의 삶에 가장 큰 변혁을 일으킬 ICT 기술 중 하나로 꼽는 등 사물인터넷은 새로운 블루오션으로 떠오르고 있다. IDC(International Data Corporation) 보고서에서는 사물인터넷에서 생성된 데이터의 양은 기하급수적으로 증가할 것이며, 이러한 사물인터넷 기반 데이터들은 거의 모든 산업 분야에서 널리 활용되어 다양한 신규 사업을 창출할 것으로 전망하고 있다.

2. 기술 구성요소

사물인터넷의 기술 구성요소는 크게 ① 센싱 기술, ② 서비스 인터페이스 기술, ③ 통신 및 네트워크 기술로 분류할 수 있다. 센싱 기술은 센서로부터 수집한 정보를 처리 또는 보관하거나 해당 정보를 가공·활용하여 서비스로 구현하기 위한 구성요소이다. 서비스 인터페이스 기술은 정보의 저장, 처리, 추출, 가공뿐만 아니라 상황인식, 보안기능 등 사물인터넷 서비스를 제공하기 위해 필요한 다양한 인터페이스를 플랫폼 등으로 제공하는 기술 요소를 의미한다. 마지막으로 통신 및 네트워크 기술은 사물들의 네트워크 종단 간(End to End)에 정보를 교환할 수 있는 통신 기술요소이다.

가. 센싱 기술

센싱 기술은 온도, 습도, 조도, 초음파, 위치, 속도, 표정, 열, 가스 등과 같은 주변 환경의 다양한 물리량을 측정하고, 측정된 정보들을 서비스에 활용 가능한 형태로 변환하기 위한 신호처리 및 알고리즘을 실행해주는 인터페이스 제공 기술이다. 또한 2개 이상의 센서들이 융합된 다중 센서(또는 멀티 센서)들을 이용하여 기존의 독립적이고 개별적인 센서보다 더 지능적이고 다양한 정보를 추출할 수 있다.

이와 같이 정보처리 능력을 내장하고 있는 스마트 센서는 스스로 상황을 감지하여 정보를 직접 처리하거나 인터넷을 통해 사람 또는 사물에게 전달한다. 센서의 통신반경은 1~10m이며, 센서들이 서로 연결되어 있는 네트워크를 센서 네트워크라고 한다. 센서 네트워크가 구성되기 위해서는 모든 사물들이 고유한 식별체계 및 주소를 가지고 있어야 한다. 최근 사물인터넷의 인기와 더불어 IP주소에 대한 수요가 급증하고 있어 기존 32비트 주소 체계인 IPv4로는 증가하는 사물들에게 주소를 모두 할당하기 어려워 128비트 주소체계인 IPv6로 이동하고 있다. 또한, 사물인터넷 환경에서 사물이 항상 운영되어야 하는데, 센싱 기술을 이용하여 태양에너지 또는 열에너지를 지속적으로 전력으로 공급할 수 있다.

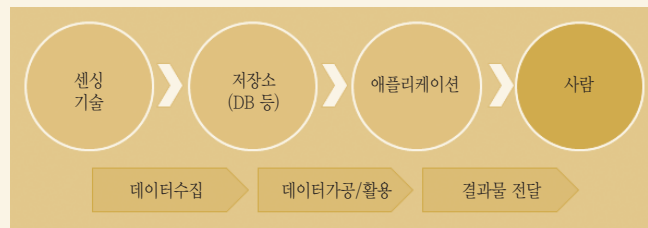
나. 서비스 인터페이스 기술

서비스 인터페이스 기술은 사람 또는 사물을 사물인터넷 환경의 서비스 또는 애플리케이션과 연동해주기 위해 다양한 인터페이스를 제공하는 기술로서, 사물인터넷 내·외부에서 이루어지는 모든 센싱, 정보처리, 가공, 처리, 저장 등의 주요 기능들을 이용 가능하게 해준다.

즉 서비스 인터페이스는 [그림 1]과 같이 센싱 기술을 이용하여 주변의 데이터를 수집하여 DB에 저장하고, 저장된 데이터를 의미 있는 정보로 가공한 후 응용프로그램을 통하여 해당 정보를 자체 활용하거나 주변의 사물 또는 사람에게 전달하는 수행 과정을 거침으로써 데이터를 의미 있는 결과물로 해석, 표현, 처리가 가능하게 해주는 기술을 의미한다.

[그림 1]

사물인터넷 서비스 인터페이스의 수행 과정



따라서 각종 센서가 수집한 막대한 양의 정보를 저장하고 분석하여 처리하는 빅데이터 기술, 현재 시점에 수집되고 있는 정보와 과거에 축적된 데이터 속에서 가치 있는 정보를 추출해 내는 데이터 마이닝 기술 등이 서비스 인터페이스 기술에 속한다.

다. 통신 및 네트워크 기술

사물인터넷에서 통신 및 네트워크 기술은 다양한 사물들을 물리적, 논리적으로 연결하여 센서가 수집, 보관, 가공한 정보를 전송할 수 있게 해주는 유무선 기술로써, 와이파이(Wi-Fi), 3G · 4G · LTE, 블루투스, ZigBee, NFC, RFID, BcN(Broadband convergence Networks), 이더넷, 위성통신 등이 이에 해당된다.

저전력, 저성능의 특성을 갖고 있는 사물인터넷 기기들은 전력 소모를 줄여주고 처리해야 할 데이터의 양을 최소화함으로써 컴퓨팅 부하를 줄여주어야 한다. 또한 안정적인 인터넷 환경과는 달리 단거리 통신을 수행해야 하기 때문에 연결이 비교적 불안정하다. 이러한 사물인터넷의 제약을 극복하기 위해 최근 다양한 네트워크 기술들이 개발되고 있다. IBM에서 개발하고 OASIS(Organization for the Advancing open Standards for the Information Society)에 의해 사물인터넷의 표준 규약으로 사용되고 있는 경량형 메시징

프로토콜인 MQTT(Message Queue Telemetry Transport), IETF의 CoRE(Constrained RESTful Environments) 워킹 그룹에서 소형기기에 적합하도록 개발한 경량형 웹 전송 프로토콜인 CoAP(Constrained Environment Application Protocol)가 대표적인 예이다. 이러한 프로토콜들은 저전력, 저성능의 사물인터넷 환경에서 통신 및 네트워크 서비스를 제공할 때 TCP, HTTP와 같은 무거운 통신 프로토콜 대신 많이 사용된다.

또 하나 각광받는 기술 중 하나가 2013년 애플에서 발표한 아이비콘(iBeacon)인데, 아이비콘은 BLE(Bluetooth Low Energy)를 활용한 근거리 데이터 통신 기술로서 통신 가능 범위가 최대 70m에 이른다. 기존 블루투스 기술은 장치를 사용하려면 페어링(기기 간 연결)을 해주어야 하며 전력소모가 심한데 반해 BLE는 페어링이 필요 없어 저전력으로 통신이 가능하다.

Ⅲ. 사물인터넷 동향 및 적용사례

글로벌 선진국 및 기업들은 사물인터넷을 국가 및 산업 경쟁력 확보의 핵심 기반기술로 인식하고 다양한 전략을 수립하고 있다. 우리나라도 2014년 5월 ‘사물인터넷 기본계획’을 미래창조과학부에서 발표하고 글로벌, 대기업, 통신사 등 참여자 간 협업 강화, 개방형 플랫폼을 활용한 성과 극대화, 글로벌 시장을 겨냥한 서비스 개발 등을 추진 중이다. 특히 국가경쟁력을 좌우하고 수익창출의 신성장 원동력이 될 것으로 전망되는 사물인터넷 플랫폼을 주도하기 위한 국가 및 기업 간 경쟁이 치열하게 진행 중이다.

사물인터넷 플랫폼이란 사물인터넷 제품이나 서비스를 만드는 핵심 기술로서, 인터넷에 연결된 모든 기기를 하나로 통합 관리할 수 있도록 제공하는 하드웨어 및 소프트웨어를 의미하며 운영체제(OS), 소프트웨어 개발도구, 응용프로그램 및 사용자 인터페이스 등을 포함한다.

이에 본 장에서는 사물인터넷 플랫폼을 주도하고 있는 oneM2M, OIC 및 AllSeen 동향 및 금융기관의 사물인터넷 적용사례를 살펴보고자 한다.

1. 사물인터넷 플랫폼 동향

가. oneM2M (글로벌 표준 플랫폼)

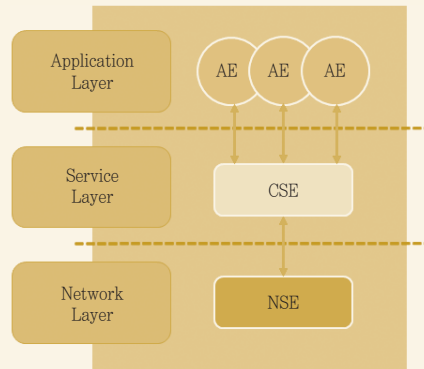
oneM2M은 2012년 7월 글로벌 사물인터넷 플랫폼 표준 기술을 개발하기 위하여 TTA(한국), ETSI(유럽), TTA(북미), ATIS(북미), ARIB(일본), TTC(일본), CCSA(중국), TSDSI(인도)를 비롯한 전 세계 8개 주요 표준화 기관들이 참여하여 결성된 글로벌 표준 단체이다. 이에 한국, 유럽, 미국 등은 개별적으로 진행하던 사물인터넷 플랫폼 표준 작업을 중단하고 oneM2M이라는 단일 사물인터넷 표준을 개발하게 되었다.

oneM2M의 목적은 사물의 위치, 접근방법, 센서, 통신기술 등 다양한 사물인터넷 환경에 구애받지 않고 스마트홈, 스마트카 등 다양한 산업분야에서 공통적으로 사용될 수 있는 사물인터넷 플랫폼 기술 규격을 제공하기 위함이다.

oneM2M은 2015년 1월에 표준 릴리즈 1.0을 발표하였고, 2016년 7월에 표준 릴리즈 2.0을 추가로 발표할 계획이다.

[그림 2]

oneM2M 아키텍처



oneM2M 아키텍처는 [그림 2]와 같이 애플리케이션(Application), 서비스(Service), 네트워크(Network) 레이어의 3개 계층 구조로 이루어져 있으며, 각 레이어는 AE (Application Entity), CSE(Common Service Entity), NSE(Network Service Entity)로 구성된다.

- AE : 다양한 서비스를 제공하는 애플리케이션을 의미
- CSE : 사물인터넷의 다양한 응용프로그램(AE)에게 공통적으로 제공해야 할 서비스 기능들(CSF, Common Service Function)을 포함한 계층으로, 장치 등록, 정보 탐색, 보안, 그룹 관리, 정보 구독·통지, 장치 관리, 데이터 저장·관리·분석, 메시지 관리, 서비스 과금 등 12가지 공통 기능을 제공
- NSE : CSE 간 통신이 가능하도록 통신 기능을 제공

oneM2M 표준은 다양한 응용 도메인에서 요구하는 공통 기능 및 표준 인터페이스를 제시하여 사물인터넷 서비스에 공통적으로 적용 가능한 서비스 플랫폼을 제공한다.

나. OIC의 IOTivity (산업단체 표준 플랫폼)

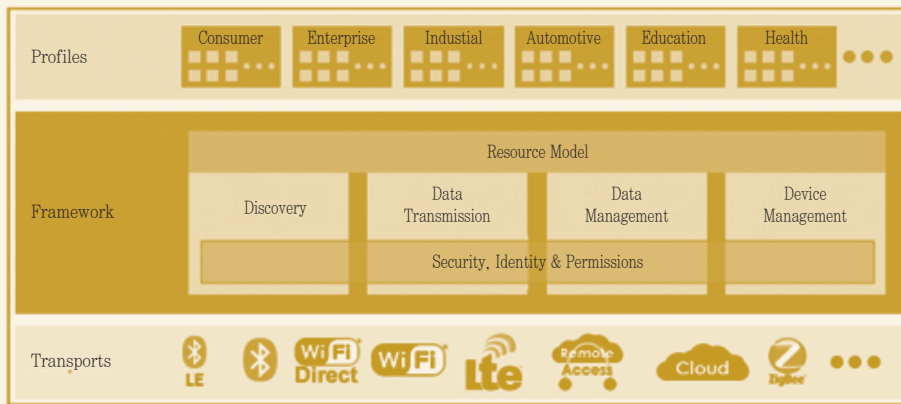
OIC(Open Interconnect Consortium)는 사물 간 상호연결에 대한 다양한 요구사항을 지원함으로써 사물인터넷 서비스를 실현할 수 있는 프레임워크 개발을 목표로 2014년 7월 인텔, 삼성, 윈드리버, Atmel 등의 기업들이 만든 산업표준 단체이다. OIC는 2015년 9월 표준규격 1.0을 발표했으며, OIC 표준 기반의 사물인터넷 미들웨어 오픈소스를 개발하여

현재 릴리즈 버전 1.1.0을 공개한 상태이다.

IoTivity 플랫폼은 장치를 발견하면 이에 대응되는 IoTivity 리소스를 생성하여 맵핑하는 리소스 기반 구조로서, 모든 사물을 리소스로 표현하는 RESTful 아키텍처의 서버-클라이언트 방식으로 동작한다. 클라이언트는 CRUDN(Create, Read, Update, Delete and Notification) 오퍼레이션 명령어를 서버로 전달함으로써 리소스에 대한 상태조작 요청이 가능하다.

[그림 3]

IoTivity 아키텍처



IoTivity는 응용프로그램을 담당하는 프로파일(Profiles), 블루투스, 와이파이 등 사물 인터넷의 다양한 통신 기능을 제공하는 전송(Transports), IoTivity 리소스 발견, 데이터 전송, 데이터 및 디바이스 관리 등 플랫폼의 주요 기능을 담당하는 프레임워크(Framework)의 3개 계층 구조로 이루어져 있다. 프레임워크의 주요 기능은 다음과 같다.

- 리소스 발견(Discovery) : 근접해있거나 원격에 있는 장치 및 자원을 발견
- 데이터 전송(Data Transmission) : 메시지 또는 스트리밍 기반으로 정보를 주고 받는 기능 제공
- 데이터 관리(Data Management) : 센서를 통해 수집한 정보 또는 다른 장치로부터 전달받은 정보를 저장, 분석, 활용
- 디바이스 관리(Device Management) : 장치의 구성, 권한설정 및 진단 등의 기능을 제공
- 보안, 인증 및 권한관리(Security, Identity & Permissions) : 프레임워크 전반에 걸쳐 보안, 인증 및 권한관리 등 보안기능 제공

다. AllSeen 얼라이언스 (산업단체 오픈소스 플랫폼)

AllSeen 얼라이언스는 2013년 12월 쉘컴, Cisco, LG전자, 파나소닉, 하이얼, 샤프, 마이크로소프트, AT&T 등 51개 기업이 참여해 결성된 산업체 컨소시엄으로 쉘컴이 2011년 공개한 오픈소스 프로젝트를 기반으로 참여기업들이 다양한 API 등을 개발하여 오픈소스 사물인터넷 플랫폼인 AllJoyn 프레임워크를 공개하였다.

AllJoyn 프레임워크는 [그림 4]와 같이 크게 AllJoyn Application과 AllJoyn Router 2가지로 구성되어 있다. AllJoyn Application은 ① 애플리케이션, ② 알림기능, 환경설정 등 응용서비스를 제공하기 위한 AllJoyn Service Frameworks, ③ 서비스 광고(타 디바이스에게 자신의 디바이스 존재를 알리는 과정) 및 검색(타 디바이스를 검색하는 과정) 요청, 세션 생성, 인터페이스 정의, 데이터 전달 등의 기능을 제공하는 AllJoyn Core Library로 이루어져 있다. AllJoyn Router는 서비스 광고 및 검색 수행, 세션 관리, 메시지 및 신호 전송, 보안기능 등 통신 기능을 제공하며 다른 AllJoyn Router와 통신이 가능하도록 Bus를 제공한다.

[그림 4]

AllJoyn 아키텍처



처음 AllJoyn 디바이스 실행되면 디바이스 내의 AllJoyn Application이 AllJoyn Router로 서비스 광고 및 검색을 요청하면 AllJoyn Router는 주변의 디바이스들을 검색한 후 요청한 디바이스가 제공할 수 있는 서비스를 다른 디바이스들에게 전달(광고)하게 된다. 검색된 디바이스들은 AllJoyn Router를 통하여 서로 정보를 송수신 할 수 있게 된다.

2. 금융권 국내 · 외 적용사례

금융권은 헬스케어, 스마트홈, 제조업 등 타 분야에 비해 사물인터넷의 활용이 아직까지는 초기단계에 머물러 있으나, 자동차보험 가입자의 운전 습관, 건강 보험 가입자의 건강 상태 등 사물에 대한 정보를 수집 · 분석하여 금융상품에 적용시키는 등 사물인터넷을 적용하는 사례가 꾸준히 증가하고 있다.

가. 국내 적용사례

금융회사	적용사례	설 명
동부화재	smartT UBI ¹⁾ 안전운전 특약 (2016년 4월)	<ul style="list-style-type: none"> 네비게이션 앱(T map)을 실행한 상태에서 500km 이상 주행 및 일정 기준 이상의 안전운전 (속도준수, 여유가속, 안전감속 등) 시 보험료 추가 할인 T map 제휴 기반 상품으로 별도의 OBD 장치 설치 불필요
홍국화재	UBI 보험상품 (적용 예정)	<p>홍국화재운전습관연계보험개념</p> <p>1 자동차에 주행정보 분석기기부착</p> <p>2 KT로 주행정보 실시간전송</p> <p>운전습관빅데이터분석시 고려내용</p> <ul style="list-style-type: none"> ①급제동 ⑤운행시간대 ②급가속 ⑥주행거리 ③급회전 ⑦운행경로 ④장기과속 ⑧지역 <p>3 빅데이터분석통해 운전습관점수와 관련정보애플리케이션 통해고객에게피드백</p> <p>4 운전습관점수 바탕으로보험료할인 혹은할증</p>
우리은행	에셋 매니지먼트 (Asset Management) 담보대출 관리시스템 (적용 예정)	<ul style="list-style-type: none"> 담보관리가 어려워 활성화되지 못했던 자동차, 공장설비등의 담보물건에 위치기반시스템을 적용한 담보대출 관리시스템
	우리비콘 서비스 (2016년 6월)	<ul style="list-style-type: none"> 비콘 서비스를 이용해 영업점을 방문하는 고객 스마트폰으로 상품, 이벤트 안내, 쿠폰 등 은행거래에 필요한 콘텐츠 전송

1) UBI(Usage-Based Insurance, 운전습관연계보험) : 피보험자의 운전거리, 운전형태 등을 활용해 위험을 차별화하여 보험료를 산정하는 보험 상품

나. 국내 적용사례

금융회사	적용사례	설 명
이탈리아 Generali Seguros	Pago Como Conduzco (2013년 2월)	<ul style="list-style-type: none"> • 통신회사인 텔레포니카(Telefonica)와 제휴하여 사물인터넷 기술을 활용한 자동차 보험 상품 출시 • 보험가입자 차량에 설치된 센서로부터 지속적으로 운전자의 기본 정보와 운전 습관 등 세부적인 기록을 제공받고, 3개월마다 고객의 운행 정보를 분석해 보험료를 최대 40% 할인 • 스마트폰 애플리케이션을 통해 자동차 운행 데이터를 고객에게 실시간으로 제공해주고, 수집된 데이터는 텔레포니카의 클라우드 서비스와 결합해 고객에게 맞는 보험상품을 설계
미국 Progressive	SnapShot (2011년 3월)	<ul style="list-style-type: none"> • 운행시간, 시간대, 운전경로, 운전습성 등을 바탕으로 최대 30%까지 보험료 할인해주는 보험상품 • 2013년까지 누적 2백만 건 판매(전체 보험료의 10%) • 비가입자 대비 19%이상 보험 유지 기간 늘어남
미국 Oscar	Health Insurance (2014년 1월)	<ul style="list-style-type: none"> • 고객 중 희망자에 한해 스마트밴드(Oscar Misfit)를 무상으로 제공 • Oscar 앱에서 매일 주어지는 걷기 목표를 달성하면 1달러(연간 최대 240달러)를 지급하며, 향후 자전거, 수영 등으로 확대 예정
미국 BP	Million Step Challenge (2014년)	<ul style="list-style-type: none"> • MSC 프로그램에 가입하면 Fitbit activity tracker를 무료로 제공하며, 100만보 달성 시 500 포인트 제공 • 추가 100만보마다 250포인트를 제공하며, 최대 1000포인트(\$1000의 인센티브 제공) 적립
미국 State Farm	Drive Safe & Save(DSS) (2012년)	<ul style="list-style-type: none"> • Onstar 등 이용하여 주행거리, 차량의 회전, 감속 및 가속 등의 요소를 근거로 보험료를 할인

영국 CoverBox	CoverBox Car Insurance	<ul style="list-style-type: none"> • GPS 및 블랙박스를 기반으로 특정시간 운행 제한, 운행거리 및 운전자의 습관에 따라 보험료 할인 또한 온라인으로 실시간 모니터링이 가능
미국 PayPal	PayPal Beacon (2013년 9월)	<ul style="list-style-type: none"> • 고객이 매장에 진입하면 비콘을 통해 고객의 페이팔 계정 정보가 매장 POS 시스템에 표시 • 고객이 구매를 결정하면 점원은 결제정보를 고객의 스마트폰에 전송 후 고객이 결제 승인
터키 DenizBank	비콘 기반 서비스	<ul style="list-style-type: none"> • 영업점 방문 시 비콘을 통해 대기 번호표를 모바일 뱅킹앱으로 교부 • 대기번호가 가까워지면 고객에게 알림서비스를 제공하여 대기 시간 동안 다른 업무 처리 가능
뉴질랜드 Westpac	비콘 기반 서비스	<ul style="list-style-type: none"> • 영업점 방문목적 등 원하는 업무를 사전에 등록 • 고객이 영업점 방문 시 비콘 신호를 이용하여 영업점 직원이 고객의 내방 사실 인지, 등록된 정보를 바탕으로 빠른 상담업무 수행
호주 St. George Bank	비콘 기반 서비스	<ul style="list-style-type: none"> • 고객이 영업점 방문 시 최근 금융상품, 시장 정보 등 제공 • 만족도, 개선사항 등 설문을 유도하여 상품 및 서비스 개선에 활용

Ⅳ. 향후 전망 및 보안 고려사항

1. 금융권 사물인터넷 전망

가트너(Gartner)에 따르면 2020년 사물인터넷의 경제적 부가가치가 1.9조 달러로 글로벌 GDP의 2.1%를 차지하고, 이 중 제조, 헬스케어, 금융 부문에서 부가가치 기여도가 높을 것으로 예상하고 있다. 또한 기 언급했듯이 사물인터넷에 연결되는 기기의 수는 2020년 250억여 개에 이를 것으로 전망된다.

따라서 이러한 사물인터넷에 연결된 센서들이 수집한 정보들은 산업 전 분야의 다양한 기업들에게 새로운 사업 기회를 창출하고 수입의 원동력이 될 것으로 전망된다. 물론 사물인터넷에 연결된 모든 사물들이 금융분야에 활용되지는 않겠지만 딜로이트(Deloitte)의 보고서에 따르면 2013년에는 사물인터넷에 연결된 사물들의 약 25%, 2015년에는 약 33%가 금융분야에 활용되고, 2020년에는 그 비율이 50% 이상 상승할 것으로 예측하고 있다. 따라서 2020년 금융회사들은 사물인터넷 환경의 절반 이상의 사물들로부터 수집되는 정보들을 활용하여 수익 창출 및 신규 서비스 개발 등이 가능할 것으로 전망된다.

엑센츄어(Accenture)²⁾는 가까운 미래에 사물인터넷이 금융분야로 확산되어 금융회사를 이용하는 고객들의 생활에 자연스럽게 동화될 것으로 예상하고 있으며, 고객들 또한 언제, 어디서, 어떻게 그들이 원하는 서비스를 받을 수 있을지 잘 알고 있을 것으로 보고 있다. 이러한 환경에서 금융회사는 사물인터넷으로부터 수집한 정보들을 활용하여 자신들의 고객을 보다 더 잘 이해할 수 있도록 끊임없이 노력해야 하며, 결국엔 금융회사의 이러한 노력이 고객의 삶을 변화시킬 것으로 보고 있다. 엑센츄어는 이러한 금융회사에 특화된 사물인터넷 환경을 Bank of Things라는 용어로 정의를 하고 있다.

Bank of Things 환경에서의 금융회사는 다양한 사물로부터 수집한 정보를 이용하여 고객의 금융·비금융 관련 니즈에 만족할 수 있는 개인 맞춤형 조언을 제공(advice provider)하게 될 것이며, 타 업종과 파트너십을 맺어 특정 고객에게 가치있는 정보를 제공(value aggregator)하게 될 것이다. 또한 고객을 다른 서비스 제공자와 연결(access facilitator)해줌으로써 고객의 삶을 변화시킬 것이다.

이와 같이 Bank of Things 환경에서 고객의 삶을 변화시키는 금융회사의 다양한 역할에 대해 엑센츄어는 세 가지(개인뱅킹, 기업뱅킹, 산업뱅킹) 미래 가능 시나리오를 제시하고 있다.

2) 출처 : Accenture, The Bank of Things - How the Internet of Things will transform Financial Services, 2014

- 개인뱅킹 시나리오

Yumi Sato는 퇴근길에 차가 고장났다는 경고등을 확인했다. 그녀는 자동차 수리비가 얼마나 나올지 걱정이 되어 집에 도착하자마자 스마트폰의 뱅킹앱을 실행하여 계좌잔고가 얼마 남지 않은 것을 확인하였다. 뱅킹앱은 집 안의 스마트 냉장고, 전기계측기 및 수조 등 스마트홈 기기들로부터 자료를 자동으로 다운로드 받아 현재 소비한 전기세, 수도세 등을 실시간으로 계산하여 Yumi의 자산을 파악한 후 몇 가지 제안을 한다. 한 가지는 휴가를 위해 6개월 간 모은 적금을 자동차 수리비에 사용하거나, 다른 한 가지는 신용카드 한도를 높이는 것이다. 마지막으로 뱅킹앱은 그녀의 운전습관을 분석한 데이터를 토대로 자동차보험이 줄어든 것 까지 계산하여 보여준다. Yumi는 적금을 수리비에 이용하기로 결정했으며, 뱅킹앱은 다시 여행자금을 위한 적금을 들 수 있는 가이드를 제시한다.

- 기업뱅킹 시나리오

Hawkins Weill(H+W)은 세계적인 의료기기 제조업체이다. H+W에게 있어서 제품이 생산되어 소비자에게 전달되기까지의 공급망을 관리하는 것은 기업의 수익과 직결되는 중요한 문제이다. 따라서 공급망 단계 단계 별 데이터를 수집하여 관리해줌으로써 재고를 줄이고, 수익을 극대화할 수 있다. H+W와 거래하는 은행 또한 H+W 제품의 공급망에 대한 데이터를 수집하여 대차대조표, 상품회전률 등을 보다 면밀히 분석함으로써 H+W에 대한 투자를 동적으로 결정할 수 있다. 몇 달 전 은행은 H+W가 현금흐름 문제가 발생할 수 있다는 것을 예측하고 선제적으로 H+W에게 대처할 것을 제안하였다.

- 산업뱅킹 시나리오

John Martin 가족은 100년 이상 밀을 재배해 왔다. 다양한 센서들이 그의

농장의 토양, 농작물, 축산물 및 농기계 상태들을 매일 업데이트 해준다. John은 주거래 은행에 센서로부터 얻은 데이터들을 전송하면 은행은 농장 부동산 가치, 농작물의 잠재적 수익률 등을 계산하여 대출가능 금액 등을 제시해준다. 지난 몇 년간의 은행의 분석은 John이 농장을 경영하는데 큰 도움을 주었다.

딜로이트³⁾는 금융분야 업권별 사물인터넷의 다양한 활용 시나리오를 제시하고 있는데, 금융회사가 향후 사물인터넷을 업무에 적용 시 참조할 수 있도록 해당 보고서의 내용을 정리하여 소개한다.

가. 은행권(Banking)

사물인터넷은 향후 은행의 보증 절차를 개선하고, 새로운 시장에 진출하는 등 은행에게 다양한 기회를 제공할 수 있을 것으로 전망하고 있다. 바이오 센서 및 위치 센서가 수집한 사람의 신체적, 행동적 정보 또는 기업의 제조, 운송 정보를 분석함으로써 개인 또는 기업의 신용평가가 가능할 것이다. 하지만 이러한 신규 기술을 도입하기에 앞서 무수히 많은 사물인터넷 정보들 중 어떤 정보가 신용평가에 적절한지를 분석하고, 사람의 신체적, 행동적 정보 수집으로 인한 사생활 침해 관련 잠재적 위험을 어떻게 해결할 수 있을지를 우선적으로 고민해야 한다.

또한 은행은 물품 구입/대여 관련 금융상품 운용 시 물품에 부착된 센서로부터 물품의 상태를 모니터링함으로써 자산의 잔여가치를 정확히 분석할 수 있다. 모니터링을 통해 수집된 자산 상태에 따라 구입/대여한 이용자에게 할인을 적용하거나 위약금을 부과할 수 있을 것이다.

나. 자본시장(Capital Markets)

자본시장에서 사물인터넷 센서로부터 수집된 정보를 분석한다면 트레이딩 및 투자 활동을 자동화하는 데 더욱 도움을 줄 것으로 예측하고 있다. 또한 인간의 개입을 배제하고 사물

3) Deloitte University Press, The derivative effect - How financial services can make IoT technology pay off, 2015

인터넷 기반의 실시간 데이터 흐름을 분석함으로써 기업은 시장거품 여부를 더 정확히 평가할 수 있을 것으로 전망했다. 물론 일부는 자동화된 인공지능이 투자자의 요구나 지정학적 사건의 변화를 확실히 감지하지 못 하기 때문에 잘못된 결정을 내릴 수도 있다고 보고 있다.

다. 보험업(Insurance)

보험업권은 이미 센서로부터 수집된 정보들을 이용하여 자동차 보험에 적용하는 등 사물 인터넷을 널리 활용하고 있다. 하지만 얼마전 발생한 테슬라의 자동주행 사고사례와 같이 자동주행 자동차의 보급으로 운전자가 책임을 지는 자동차 사고보험에서 자동차 제조사가 책임을 지는 생산물배상책임보험으로 변화할 것이다. 이 경우 보험사들은 사물인터넷을 통해 자동차의 결함 관련 정보를 보다 정확히 수집이 가능할 것이다. 하지만 자동차 사고율의 급감과 전통적인 보험담보 적용이 힘들어져 보험료 수익이 상당히 줄어들 것으로 전망된다.

또한 UBI(운전습관연계보험)로 인해 보험계약자들은 그들의 보험료를 낮추기 위해 다양한 요구를 하게 될 것이다. 예를 들어 현재는 개인상해보험에서 모든 종류의 리스크가 하나의 약관에 포함되어 있지만 사물인터넷을 통해 개인 행동에 대한 다양한 정보를 수집할 수 있다면 보험사는 개개인에 대한 맞춤형 보험상품을 개발할 수 있게 될 것이다. 이러한 제품의 차별화는 고객 만족도를 더욱 증가시켜 줄 것으로 예상된다.

상업의 경우 화물 컨테이너나 운송 차량에 센서를 부착하여 도난, 파손 등의 정보를 수집함으로써 보험사들은 운송보험을 개선할 수 있을 것으로 기대된다. 다양한 정보를 이용하여 보험사들은 자산위험을 보다 정확하게 평가할 수 있으며 따라서 보험료 책정도 보다 명확해질 수 있다.

라. 투자 및 자산관리(Investment and wealth management)

금융기관은 사물인터넷으로부터 수집한 고객정보(행동, 선호도, 위치정보 등)를 이용하여 투자결정과 자산할당 등에 활용할 수 있다. 예를 들어 고객의 관심분야, 구매패턴 등을 더욱 면밀히 분석함으로써 고객의 자산관리 개선 및 투자제안에 도움이 될 것이다. 또한 기존의 설문조사 등을 통해 분석하였던 고객의 리스크 수용도를 사물인터넷 수집 정보를 프로그래밍화(POL-based)하여 분석함으로써 훨씬 정확한 결과 도출이 가능할 것이다.

또한 다양한 센서로부터 수집되는 실시간 정보를 이용하여 포트폴리오 관리를 자동화함

으로써 투자관리 운용사, 펀드, 가격산정 전략을 차별화 할 수 있을 것으로 보인다. 이러한 자동화된 기술을 이용하여 방대한 양의 데이터를 종합하여 트레이딩 기술에 융합함으로써 현재 인간이 수행하는 것보다 훨씬 빠르게 대응할 수 있다.

마. 상업용 부동산(Commercial real estate)

상업용 부동산에 실시간입찰(RTB) 시장이 출현함에 따라 전문가들은 다양한 시나리오를 구상할 수 있게 되었다. 이미 부동산을 검색하고 임대해주는 과정을 투명하게 제공해주는 서비스 관련 스타트업들이 출현하고 있으며, 빌딩의 에너지 및 보안 관련 데이터를 수집하는 센서, 엘리베이터 등 건물 주변 환경과 사람 간 상호작용에 관련된 데이터를 수집하는 센서 등을 활용하여 부동산의 가치를 더욱 정확하게 평가할 수 있을 것이다. 또한 투자자들에게 보다 투명한 가격을 제공함으로써 부동산 임대나 매매 시의 불화를 줄여줄 수 있을 것이다.

또한 거주자의 행동을 분석하고 건축 자재를 모니터링하여 얻은 데이터는 상업 및 주거용 건물을 디자인하고 건축할 때도 활용이 가능하다. 예를 들어 건설장비에 부착된 센서로부터 얻은 데이터는 건설회사가 프로젝트 진행 시 안전사고를 예방하는데 도움이 될 것이다.

바. 리스크 관리(Risk management)

사물인터넷은 금융회사의 다양한 잠재적인 리스크를 감소시키고 성과를 향상시키는 데 도움이 될 것이다. 예를 들어 금융회사 직원들의 스트레스 레벨, 이동패턴 등을 모니터링 함으로써 잠재적인 내부 부정행위를 예측하여 행위 리스크를 보다 잘 관리할 수 있다. 또한 가상 또는 현실 환경에서 다중요소(multi-factor) 인증을 사용함으로써 인증 도용을 방지할 수 있다. 예를 들어 소매상인은 카드를 이용하여 결제 처리 시 카드와 연관관계를 사전에 설정한 물리적 장비(스마트폰 등)가 근처에 있는지 여부를 검증함으로써 해당 고객이 정당한 사용자인지를 확인할 수 있다.

또한 포트폴리오 매니저들은 직원들이 스트레스를 받는 상황에서 그들이 어떻게 행동 하는지를 분석함으로써 삶의 질을 개선시킬 수 있다. 물론 직원들은 본인들이 감시당하는 것을 싫어하겠지만 해당 직원들이 고객정보 등 중요정보를 취급하는 업무를 담당하는 경우 이러한 감시가 가까운 미래에는 채용의 의무사항으로 반영될 수도 있을 것이다.

2. 보안 고려사항

스마트홈, 스마트카, 스마트의료 등 사물인터넷이 점차 보급되면서 기존 인터넷 상에서 존재하던 위협이 현실 세계로 전이되고 있다. 또한 PC, 모바일이 주 보호대상이었던 기존과는 달리 정보보호 패러다임의 변화로 가전, 자동차, 웨어러블 기기 등 주변의 모든 사물이 보호대상이 됨에 따라 자동차 해킹, 교통 제어 시스템 해킹과 같은 사물인터넷 상의 보안 사고는 인간의 생명까지 위협할 정도로 심각한 영향을 끼칠 수 있다.([표 1], [표 2])

[표 1] 사물인터넷 공격 및 위협사례	
유 형	공격 및 위협사례
악성코드 감염	<ul style="list-style-type: none"> • 2013년 말부터 2014년 초 Proofpoint는 10만 대 이상의 스마트 TV, 스마트 냉장고, 라우터 등의 Thingbots을 통해 총 750,000건의 피싱과 스팸 메일을 전 세계 개인과 기업에 발송되었음을 밝힘
	<ul style="list-style-type: none"> • 리눅스 달로즈 웹으로 PHP 취약점을 악용하여 보안용 IP 카메라, 셋톱박스, 무선랜카드 등 리눅스 OS를 사용하는 사물인터넷 기기 감염
데이터 및 기기 탈취	<ul style="list-style-type: none"> • 자동차를 해킹하여 디지털 콤파스, 휠 인코더, 관성 측정 유닛 등의 센서에 잘못된 정보를 삽입함으로써 급정거하거나 차선을 이탈 등 조작 시연(2013 블랙햇 컨퍼런스)
펌웨어, 운영체제	<ul style="list-style-type: none"> • Hack in the Box 보안컨퍼런스에서 무선 IP카메라의 펌웨어 변형공격 시연
권한 탈취, 불법 접근 및 정보유출	<ul style="list-style-type: none"> • 2012년 미국 데이터 암호화 및 인증 절차의 부재로 고속도로 교통표시판(VMS) 및 교통 제어 시스템 해킹
	<ul style="list-style-type: none"> • 2012년 OBD-II (자기진단장치)의 취약점 이용 차량 접속을 통해 BMW 차량 300대 이상 도난
	<ul style="list-style-type: none"> • 2013년 독일 리큐리티랩스(Recurity Labs) 해킹 실험을 통해 에틀링겐(Ettlingen) 도시의 전력 공급을 외부에서 무단으로 차단할 수 있음을 입증
	<ul style="list-style-type: none"> • SHODAN은 인증이 필요 없는 사물인터넷 디바이스와 서비스들의 정보를 매달 5억 개 이상 수집하여 검색 기능을 제공하는 서비스(2009년 서비스 시작, 백도어를 검색하기 때문에 어둠의 구글이라고 불림)로써 SHODAN을 이용하여 취약한 사물을 검색하면 디폴트 패스워드를 사용하고 있는 프린터, 서버, 시스템제어 장치들이 검색되어 아무런 인증절차 없이 사물인터넷 기기에 접속 가능

[표 2] 정보보호 패러다임의 변화

구분	정보보호 패러다임의 변화	
보호 대상	PC, 모바일	가전, 자동차, 의료기기 등 모든 사물(Things)
대상의 특성	고성능, 고가용성을 가지는 운영환경	고성능, 고가용성 + 초경량, 저전력
보안 주체	ISP, 보안 전문업체, 이용자	ISP, 보안 전문업체, 이용자 + 제조사, 서비스제공자
보호 방법	별도의 보안장비, S/W 구현 및 연동	별도의 보안장비, S/W 구현 및 연동 + 설계단계부터 사물 내 보안 내재화
피해 범위	정보유출, 금전피해	정보유출, 금전피해 + 시스템 정지, 생명 위협

자료 : 사물인터넷(IoT) 정보보호 로드맵, 미래창조부, 2014

사물인터넷 환경에서는 다양한 사물이 인터넷에 접속됨에 따라 기존 인터넷 환경에서 발생할 수 있는 모든 보안상 취약점들이 사물인터넷에서도 발생할 수 있다. 하지만 이러한 사물들은 자원이 제한적이고 저전력 통신 기술을 적용한 네트워크에서 구동되기 때문에 기존의 고성능 환경에서 동작하는 보안 대응기술을 사용하는데 많은 제약이 따르며, 신규 보안위협 또한 지속적으로 발생할 수 있다.

이와 같이 증가하는 보안위협 대비 대응 가능한 기술이 제한적인 사물인터넷 환경에서 금융회사가 안전하게 사물인터넷 서비스를 이용하기 위해서는 다양한 보안상 고려사항을 준수해야 한다.

우선 기존의 타 시스템들과 마찬가지로 사물인터넷도 기밀성(confidentiality), 무결성(integrity), 가용성(availability) 세 가지 요소는 가장 기본적인 보안 서비스로 요구된다. 따라서 금융회사들이 기존에 적용하고 있던 보안대책을 사물인터넷 환경의 서버, 네트워크, 정보보호시스템, 웹애플리케이션 및 모바일애플리케이션 등에도 동일하게 적용하여 동등한 보안수준을 유지해야 한다. [표 3]는 OWASP에서 공개한 IoT Top 10 취약점 및 대응방안을 정리한 것으로 대부분이 기존의 취약점 및 대응방안에서 크게 벗어나지 않는 것을 알 수 있다.

[표 3] OWASP IoT Top 10 취약점			
ID	취약점 명	설 명	대응방안
I1	취약한 웹 인터페이스 (Insecure Web Interface)	취약한 계정관리, SQL삽입, XSS 등 웹애플리케이션 취약점 존재	디폴트 계정 사용 금지, 암호찾기 절차 강화, SQL삽입 등 웹애플리케이션 취약점 제거
I2	불충분한 인증/권한 (Insufficient Authentication/ Authorization)	단순한 패스워드 사용, 쿠키재전송, 복호화 가능한 알고리즘을 이용한 패스워드 암호화 등을 통한 인증/권한 획득	패스워드 복잡도 강화, 단방향 암호알고리즘을 이용한 패스워드 암호화, 2팩터 인증 등 사용
I3	취약한 네트워크 서비스 (Insecure Network Services)	불필요한 서비스 포트 사용, 취약한 UDP 서비스 사용 등 네트워크 취약점 존재	필요한 포트만 접속을 허용하는 등 네트워크 취약점 제거
I4	전송암호화/무결성검증 취약 (Lack of Transport Encryption/ Integrity Verification)	중요정보의 평문전송, SSL/TLS의 잘못된 보안설정 등으로 인한 전송구간 중요정보 노출	통신구간은 안전한 보안설정이 이루어진 SSL/TLS 등을 이용하여 기밀성 보장
I5	프라이버시 문제 (Privacy Concerns)	I1~I4 취약점을 이용하여 개인정보 유출	불필요한 개인정보는 네트워크 구간에 전송하지 않고, 전송 시 반드시 암호화
I6	취약한 클라우드 인터페이스 (Insecure Cloud Interface)	I1~I4 취약점을 이용하여 클라우드 계정정보 탈취 또는 중요정보 유출	I1~I4 대응방안 준수
I7	취약한 모바일 인터페이스 (Insecure Mobile Interface)	I1~I4 취약점을 이용하여 모바일앱 계정정보 탈취 또는 중요정보 유출	I1~I4 대응방안 준수
I8	불충분한 보안 설정 가능성 (Insufficient Security Configurability)	사물인터넷 관련 서버, 네트워크 장비, 기기 등의 보안설정이 미흡하여 계정관리 취약, 보안감사 및 로깅 미실시	관리자와 일반사용자 계정을 분리 사용하고 강력한 계정관리 보안설정 준수. 보안감사 및 로깅을 활성화하고 이벤트 발생 시 관리자에게 통지
I9	취약한 소프트웨어/펌웨어 (Insecure Software/Firmware)	패치파일이 암호화되어 있지 않거나 민감정보를 포함, 업로드 전 검증과정을 거치지 않아 보안위협에 노출	사물인터넷 기기가 자동업데이트 기능을 제공하는지 확인, 패치파일에 대한 철저한 검증 등
I10	취약한 물리 보안 (Poor Physical Security)	USB 포트를 통한 기기 접근, 스토리지의 탈취 등	USB 포트 등 외부접근을 차단하고, 스토리지 탈취 시 데이터 리셋 등의 보호조치 마련

하지만 기본적인 보안 기능 외에도 사물인터넷 환경의 장치들은 운용환경 특성상 [표 4]에 명시된 별도의 보안 기능을 고려해야 한다. 사물인터넷 환경에서는 경량화 된 보안 솔루션이

필요하며, 수 많은 사물들을 인간이 직접 관리하기 힘들기 때문에 분산되고 자동화된 보안 관리 기능이 있어야 한다. 이 때 높은 보안 수준을 요구하는 경우 알고리즘 복잡도가 높아지게 되며, 필요한 연산량 역시 알고리즘 복잡도에 비례해서 증가하게 된다. 따라서 보호 하고자 하는 정보의 가치에 따라서 보안 수준은 다르게 적용되어야 한다.

[표 4] 사물인터넷을 위한 보안 기능

사물인터넷 보안 기능	보안 기능에 대한 설명
사물인터넷 장치를 위한 보안 부팅 지원	<ul style="list-style-type: none"> • 사물인터넷 상에서 동작하는 각 장치들이 안전한 보안 연산 환경을 보장하기 위해서는 처음 스위치가 켜 졌을 때 펌웨어에 대한 인증값을 검증하여 무결성을 확인할 수 있는 보안부팅(secure booting) 기술이 필요 • 이를 위해서는 운영체제 외적으로 별도의 장치에 의해서 전자서명과 같은 암호학적 연산이 동작될 수 있어야 함
경량 암호 및 분산된 자발적 보안 설정 지원	<ul style="list-style-type: none"> • 프라이버시 보호 및 암호화 방식은 단순하고 작은 장치에서도 적용 가능한 경량 암호화(lightweight encryption) 솔루션이 필요함 • 최소 260억 개 이상의 사물들이 네트워크에 연결되기 때문에 보안 관리자에 의해서 모든 사물들에 대한 보안 파라미터를 적절하게 관리하는 것은 불가능 • 따라서 관리자가 없이도 자발적으로 인증 및 보안을 위한 설정이 이루어지도록 해야 함
사물들 간의 가상 사설망 설정 및 관리 지원	<ul style="list-style-type: none"> • 공공 네트워크를 통해서 중요한 데이터를 전송하는 경우에는 사물들 간에 가상 사설망(virtual private network)을 설정하고 해제하는 것이 가능해야 함 • 또한 각 장치들에 할당된 제한된 대역폭과 임베디드 장치의 간헐적 네트워크 연결 특징을 유지하면서 동시에 소프트웨어 업데이트와 보안 패치가 전달되는 메커니즘 또한 구성되어야 함
빅데이터 분석에 대한 프라이버시 보호 기능	<ul style="list-style-type: none"> • 사물인터넷 상으로 많은 센서로부터 수집된 정보는 빅데이터 분석이 적용되는데 이 때 프라이버시 보호 기능이 제공되어야 하며, 사물인터넷 데이터에 대해서도 적절한 프라이버시 보호 기능 및 익명화 기술이 적용될 수 있음
심층 패킷 정보감시 기능 지원	<ul style="list-style-type: none"> • 심층 패킷 정보감시(deep packet inspection, DPI)가 가능한 방화벽과 침입방지 시스템이 구성되어야 함 • 필요에 따라 특정 장치를 목적으로 하는 트래픽에 대한 DPI 솔루션이 적용되어야 함

자료 : 사물인터넷 시대의 사이버 물리 시스템 보안 기술 동향

또 한 가지 고려할 사항은 사물인터넷 환경에서 저전력, 저성능 기기에 동작 가능한 다양한 경량형 암호화 및 메시지 프로토콜이 개발되고 있지만 이러한 신규 알고리즘 및 프로토콜은

기존의 검증된 기술들과는 달리 잠재적인 취약점을 포함하고 있을 수 있다. 예를 들어 많은 금융회사들이 도입하고 있는 비콘의 경우 원본 정보를 복제해 정보를 유출하는 클로닝(Cloning)이나 네트워크 통신 관련 정보를 속여 통신 흐름을 왜곡시키는 스푸핑(Spoofing) 등 다양한 보안상 취약점이 존재한다. 따라서 무조건적인 신기술 도입보다는 충분한 기술검증 및 보안대책 마련이 선행되어야 할 것이다.

마지막으로 사물인터넷에 사용되는 센서 등 저전력, 저성능 기기의 특성상 기존의 PC, 모바일 등에 사용되던 보안솔루션 적용이 어렵고 운영 중인 단말의 보안 업데이트가 어려운 장치들이 존재하며, 이런 장치로 인해 전체 시스템의 보안 수준이 떨어질 우려가 있다. 따라서 기존에는 단말에 각종 보안프로그램 등 고도의 보안솔루션을 설치하여 보안성을 향상시켰지만, 사물인터넷 환경에서는 보안솔루션에 의존하지 않고 보안성을 강화할 수 있는 방안도 동시에 강구해야 될 것이다. 따라서 사물인터넷 환경에서 금융회사는 금융사기, 해킹 등 다양한 보안위협으로부터 자산을 보호하기 위해 거래시점부터의 사고 방지에 집중하던 기존 사고 관리 접근 방식과 더불어 통합보안관제시스템 및 이상행위탐지시스템 등 사고 감시 모니터링에도 보다 많은 관심을 기울일 것으로 예상된다.

V. 결론

사물인터넷 기술이 우리 생활에 널리 보급됨에 따라 금융회사 또한 사물인터넷에 대한 관심이 지속적으로 증가하고 있다. 아직까지는 비콘 기술을 활용한 영업점 안내 서비스, 보험회사의 UBI 상품 위주로 금융분야 적용사례가 많지 않지만, 가까운 미래에는 사물인터넷이 금융분야로 확산되어 금융회사를 이용하는 고객들의 생활에 자연스럽게 동화될 것으로 많은 전문가들은 예측하고 있다.

현재 글로벌 선진국 및 기업들이 새로운 수익창출의 신성장 원동력이 될 것으로 전망되는 다양한 플랫폼을 개발하여 사물인터넷 시장의 주도권을 잡기 위해 노력하고 있으며, 모바일, 하드웨어, 빅데이터, 클라우드 컴퓨팅, 인공지능 등 타 IT기술과 융합하여 빠르게 발전하고 있다. 따라서 금융회사는 향후 사물인터넷으로의 서비스가 이전되는 환경에 대비하여 사물인터넷 생태계를 예의주시하여야 할 것이다. 앞으로 금융회사는 단독으로 글로벌 금융시장에서 경쟁우위를 점하기가 점점 힘들어질 것으로 판단되며, 따라서 사물인터넷 관련 기업 뿐만 아니라 제조업, 운송업, 농업, 부동산 등 사물인터넷 생태계 내 다양한 분야와 전략적 제휴를 맺고 고객의 니즈를 만족시킬 수 있는 신규 사업을 창출해나갈 것으로 예상된다.

이와 더불어 증가하는 보안위협 대비 대응 가능한 기술이 제한적인 사물인터넷 환경에서 금융회사가 안전하게 사물인터넷 서비스를 이용하기 위해서는 다양한 보안상 고려사항을 준수해야 할 것이다. 특히 저전력, 저성능 기반 사물인터넷 환경에서 개발되는 신규 알고리즘 및 프로토콜은 기존의 검증된 기술들과는 달리 잠재적인 취약점을 포함하고 있을 수 있다. 따라서 무조건적인 신기술 도입보다는 충분한 기술검증 및 보안대책 마련이 선행되어야 할 것이다. 또한 사물인터넷 환경에서 금융회사는 금융사기, 해킹 등 다양한 보안위협으로부터 자산을 보호하기 위해 거래시점부터의 사고 방지에 집중하던 기존 사고 관리 접근 방식과 더불어 통합보안관제시스템 및 이상행위탐지시스템 등 사고 감시 모니터링에도 많은 투자가 이루어져야 할 것이다.

〈참고문헌〉

- [1] Gartner, “In 2020, 25 Billion Connected ‘Things’ Will Be in Use”, 2014
- [2] IDC, “The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things”, 2014
- [3] Accenture, “The Bank of Things? How the Internet of Things will transform Financial Services”, 2014
- [4] Deloitte University Press, “The derivative effect ? How financial services can make IoT technology pay off”, 2015
- [5] 미래창조부, “사물인터넷(IoT) 정보보호 로드맵”, 2014
- [6] 김영식, “사물인터넷 시대의 사이버 물리 시스템 보안 기술 동향”, 2015
- [7] 김기영, “oneM2M 사물인터넷 서비스 플랫폼 표준화 동향”, 2014
- [8] 김재호, 윤재석, 최성찬, 류민우, “IoT 플랫폼 개발 동향 및 발전방향”, 2013
- [9] 최환석, 이우섭, “사물인터넷 플랫폼 기술 및 국제 표준화 동향”, 2015
- [10] 김종현, “주간 금융경제동향”, 우리금융경영연구소
- [11] http://onem2m.org/Press/20140807-oneM2M_press_release_on_candidate_release.pdf
- [12] Allseen Alliance, <https://allseenalliance.org/about>
- [13] <http://postscapes.com>
- [14] <http://mattturck.com/2016/03/28/2016-iot-landscape/>
- [15] <https://www.owsap.org>

금융회사의 보안서비스 제공 현황 및 활용방안

한 승 우*

I. 서론	57
II. 보안서비스 제공 현황	58
1. 로그인 보안	58
2. 계좌 보안	63
3. 이체 보안	66
4. 보안통지	72
III. 보안서비스별 주요 이용자	78
IV. 결론	80

* 금융보안원 보안연구부 보안기술연구팀 (e-mail : swhan@fsec.or.kr)

요 약

최근 스마트폰을 이용한 전자금융서비스의 발전과 함께 보안 위협이 증가하고 있다. 이에 금융회사에서는 이용자가 안전한 전자금융서비스를 이용할 수 있도록 보안서비스를 제공하고 있다. 금융회사 보안서비스는 전자금융거래 이용 절차에 따라 4가지로 구분할 수 있다.

첫째, 로그인 보안은 비인가자의 접근을 막고, 피싱 사이트를 구별 할 수 있도록 피싱 방지, 해외 IP차단 등의 서비스를 제공한다. 둘째, 계좌 보안은 전자금융 거래 기능을 제한하여 이용자의 계좌를 보호하기 위한 것으로 보안계좌, 계좌 숨기기 등의 서비스가 있다. 셋째, 이체 보안은 이체 거래 시 추가 인증 등을 통해 본인확인 절차를 강화하는 것으로 단말기지정, 추가인증 등이 서비스가 있다. 마지막으로 보안통지는 중요 변동사항이 발생되었을 때 이용자에게 즉시 알려줌으로써, 사고 발생 시 신속한 대처를 할 수 있도록 도와주는 서비스이며, 이외에도 다양한 보안서비스를 제공하고 있다.

이에 본 고에서는 다양한 전자금융거래 사고 위협으로부터 이용자 보호를 위해 금융회사에서 제공되는 보안서비스의 특징에 대해 소개한다. 각 보안서비스 특징을 통해 적합한 이용자를 분류하고, 금융회사에서 활용할 수 있는 방안에 대해 제시하고자 한다.

I. 서론

전자금융서비스를 보다 안전하게 이용할 수 있도록 금융회사는 이용자에게 다양한 보안 서비스를 제공하고 있다. 일부 보안서비스는 의무화함으로써 인증 절차가 추가되는 등 이용자의 편의성을 저해시킨다는 의견이 있으나¹⁾ 의무화 시행 전·후 1개월을 비교하면 전자금융사기 피해가 건수기준으로 52% 감소하는 효과²⁾가 나타났다.

스마트폰 보급은 스마트뱅킹 이용자가 급증하는 이용환경 변화에 많은 영향을 줄 뿐만 아니라 높은 보안성과 편리함을 주는 수단이기도 하다. 하지만 스마트폰 이용자를 대상으로 하는 위협이 지속적으로 증가하고, 공격 기술이 고도화되고 있다. 금융이용자를 보호하기 위해 금융회사의 노력도 중요하지만 무엇보다도 이용자 스스로가 금융회사에서 제공하는 보안서비스를 적극 이용함으로써 사고 예방의 노력이 필요하다.

본 고에서는 금융회사에서 제공하고 있는 보안서비스를 전자금융거래 이용 절차인 로그인 보안, 계좌 보안, 이체 보안, 보안통지(기타) 4가지로 분류하여 소개한다. 각 보안서비스 특징을 통해 주요 이용자를 분류하고, 금융회사에서 활용할 수 있는 방안에 대해 제시하고자 한다.

1) 정대용, 이경복, 박태형, "전자금융사기 예방서비스의 개선방안에 관한 연구: 2013년 전자금융사기 피해사례분석을 중심으로", 2014.12.

2) 금융감독원, "「전자금융사기 예방서비스」의 안정적 정착(2013.11.5.)" 보도자료 참고

II. 보안서비스 제공 현황

1. 로그인 보안

로그인 보안은 이용자가 피싱 사이트를 구별할 수 있도록 기능을 제공하여 비인가자의 로그인 위협으로부터 이용자를 안전하게 보호하는 것으로, 피싱 방지(개인화), 해외 IP차단, 그래픽 인증, 안심로그인, 지문인증, 예외기기 로그인 알림, 해외IP 로그인 알림, 로그인 2채널 인증 등의 서비스가 있다.

예를 들어 피싱 방지(개인화) 서비스의 경우 [그림 1]과 같이 피싱 사이트와 정상 사이트를 구별 할 수 있다. 이용자가 피싱 사이트에 접속 시 사전에 설정한 문자 'ABC'와 스마일 이미지를 확인 할 수 없다.

[그림 1] 피싱 방지(개인화) 서비스 이용의 예



가. 피싱 방지(개인화)

[특 징]

- 본인확인용 아이콘 및 문자열 확인을 통한 피싱 방지
- 로그인 후 이용자 본인이 사전에 설정한 아이콘 및 문자열을 확인하여 피싱 사이트를 구별하는 방식

[기대 효과]

- 이용자의 설정에 따라 정상 사이트와 피싱 사이트를 구별할 수 있으므로 피싱 피해 방지 가능

[제공 방법]

- (서비스 신청) 인터넷/스마트뱅킹을 통해 아이콘 선택 및 문자 입력
- (서비스 이용) 인터넷/스마트뱅킹 로그인 후 아이콘 선택 및 문자 확인

나. 해외 IP 차단

[특 징]

- 해외 IP 주소(인터넷 주소)로 접속하는 경우 인터넷/스마트뱅킹 접속 차단 또는 이용 가능한 서비스를 제한
 - ※ 일반적으로 한국인터넷진흥원에 등록되지 않은 IP를 해외 IP로 판단하며, 금융회사별로 상이할 수 있음
- 계좌 조회 및 이체 등 모든 인터넷/스마트뱅킹 서비스가 차단되며, 금융회사에 따라 일부 비중요 서비스에 한해 허용

[기대 효과]

- 해외에서(또는 해외를 경유하여) 시도되는 접속 또는 부정거래를 차단

[제공 방법]

- (서비스 신청) 인터넷/스마트뱅킹을 통해 서비스 신청
- (서비스 해지) 이용자가 직접 영업점에 방문하여 해지

다. 그래픽 인증

[특 징]

- 비밀번호와 같이 입력하는 방식이 아닌, 그래픽 아이콘을 조합하여 인증
- 1차 로그인 후, 순서가 매번 바뀌는 아이콘들 중에서 사전에 설정한 4개 아이콘을 조합하여 추가 인증

※ 그래픽 인증 시 아이콘 개수는 금융사 별로 상이할 수 있음

[기대 효과]

- 인터넷 뱅킹 이용 시 그래픽 인증을 지원하지 않거나, 아이콘 보기 중 이용자가 설정한 아이콘이 존재하지 않는 경우, 이용자는 피싱 사이트로 판단 가능
- 최근 비밀번호 방식이 10자리 내외의 특수문자/대·소문자/숫자의 조합을 요구하는 반면, 4개의 아이콘만을 기억하면 되므로 이용 편의성 증대

[제공 방법]

- (서비스 신청) 인터넷 뱅킹을 통해, 서비스 신청 및 인증 시 사용할 4개의 아이콘을 등록
- (서비스 이용) 인터넷 뱅킹 이용 시 1차 로그인 후, 기등록한 4개 아이콘을 순서대로 조합하여 추가 인증

라. 안심로그인

[특 징]

- 이용자가 인터넷뱅킹을 접속하는 PC의 IP 정보(지리적 정보)와 휴대폰 위치를 비교함으로써, 비인가/비정상 로그인을 차단하는 서비스
- PC 및 휴대폰의 위치가 다른 경우 SMS를 통해 이용자에게 통지하고, 이용자는 휴대폰에서 로그인 차단 및 로그아웃 처리 가능

[기대 효과]

- 이용자가 스마트폰을 소지하는 것만으로도 공인인증서 및 비밀번호 유출 등으로 인한 비인가된 로그인을 즉시 확인 및 차단 가능

[제공 방법]

- (서비스 신청) 인터넷뱅킹 및 별도 사이트(로그인 도용방지 서비스 등) 신청
 - (서비스 해지) 인터넷뱅킹 및 별도 사이트(로그인 도용방지 서비스 등) 해지
- ※ 자체 서비스가 아닌, 통신사 및 외부 업체와의 협력을 통해 제공하는 서비스로 외부 별도 사이트(<http://idsafe.kr>)에서도 서비스 신청/해지 가능

마. 지문인증

[특 징]

- 스마트폰에 등록된 지문을 통해 스마트뱅킹 서비스 이용 시 지문 인증 적용
- 지문 인식 기능이 제공되는 스마트폰에서 스마트뱅킹 로그인, 이체 및 모바일통장 출금 서비스를 위한 본인인증에 활용

[기대 효과]

- 기존의 비밀번호 입력 방식에 비해 지문을 터치함으로써 이용 편의성 제공
- 공인인증서 및 비밀번호에 비해 유출 등의 위협으로부터 비교적 안전

[제공 방법]

- (서비스 신청) 스마트뱅킹 앱을 통해 신청 및 별도 통합 인증앱 설치 후 지문 등록
- (서비스 해지) 스마트뱅킹을 통해 지문 등록 해지

바. 예외기기 로그인 알림

[특 징]

- 평소에 인터넷뱅킹을 사용하지 않던 PC에서 로그인 시도 시 즉시 이용자에게 SMS로 알리는 서비스
- PC 교체, 공공장소의 PC 사용으로 인해 새로운 PC에서 인터넷뱅킹 로그인 시도 시 SMS로 통지
- PC 구분에는 유·무선 통신카드 고유번호 등을 활용

[기대 효과]

- 비인간된 로그인 시도 시 이용자는 수신된 SMS를 통해 즉시 확인할 수 있으며, 추가 피해 예방을 위한 대응 가능

[제공 방법]

- (서비스 신청) 인터넷/스마트뱅킹 및 영업점 방문을 통해 신청
- (서비스 해지) 영업점 방문을 통해 본인확인 후 해지

사. 해외 IP 로그인 알림

[특 징]

- 해외 IP(인터넷 주소)로 로그인한 사실이 있는 경우, 향후 국내 IP로 로그인 시 해외 IP 접속 사실을 팝업으로 이용자에게 알리는 서비스
※ 한국인터넷진흥원에 등록되지 않은 IP는 해외 IP로 판단
- 국내에서 로그인을 하더라도 글로벌 및 외국계 기업의 IP인 경우 해외 IP로 인식될 수 있음

[기대 효과]

- 해외에서의 비인가된 접속 사실을 팝업을 통해 이용자가 확인 할 수 있으며, 추가 피해 예방을 위한 대응 가능

[제공 방법]

- (서비스 신청/해지) 별도 신청/해지 없이 모든 인터넷뱅킹 이용자에게 적용

아. 로그인 2채널인증

[특 징]

- 인터넷뱅킹 로그인 시 공인인증서 또는 ID/PASSWORD 인증 후 ARS 전화를 통해 추가 인증하는 서비스
- ARS 전화를 수신하여 안내에 따라 전화기에 인증번호를 입력하는 방식
- (관련 대책) 금융감독원 「전자금융사기 예방서비스(2012.09)」

[기대 효과]

- 비인가된 로그인 시도 시 추가인증을 위한 ARS 전화가 이용자에게 수신됨으로 즉시 확인하고 차단 가능

[제공 방법]

- (서비스 신청) 인터넷뱅킹을 통해 신청(영업점 방문 신청 불가)
- (서비스 해지) 인터넷뱅킹을 통해 해지

[표 1] 로그인 보안 서비스 요약

서비스명	서비스 특징
피싱 방지(개인화)	본인확인용 아이콘 및 문자열을 통한 피싱 사이트 구별
해외 IP차단	해외 IP주소로 접속 시 차단
그래픽 인증	비밀번호 대신 그래픽 아이콘을 조합하여 인증
안심로그인	인터넷뱅킹 이용PC와 휴대폰 위치를 비교하여 로그인을 허용
지문인증	스마트폰에 등록된 지문으로 로그인, 이체 등에 본인인증으로 활용
예외기기로그인알림	평소 이용되지 않는 PC에서 로그인 시 이용자에게 알림
해외IP 로그인 알림	해외IP 접속 사실이 있는 경우, 이용자에게 알림
로그인 2채널인증	로그인 시 ARS 전화로 추가 인증

2. 계좌 보안

계좌 보안은 전자금융 거래 기능을 일부 제한하여 이용자의 계좌를 보호하기 위한 것으로, 비밀번호 변경, 보안계좌, 계좌 숨기기, 특정계좌 조회금지, 계좌안심 서비스 등이 있다.

예를 들어 보안계좌 서비스는 [그림 2]와 같이 인터넷/스마트뱅킹 이용 시 계좌 정보가 노출되지 않을 뿐만 아니라 창구거래, CD/ATM을 제외한 전자금융거래 서비스를 이용하지 못한다.

[그림 2] 보안계좌 서비스 이용의 예(설정 전/후 비교)

http://fsecbank.com		http://fsecbank.com	
(일반) 1234-567890	1,000,000원	(일반) 1234-567890	1,000,000원
(적금) 0429-123456	100,000,000원	(적금) 0429-123456	100,000,000원
(보안) 0987-654321	100,000,000원		

〈 보안계좌 설정 전 〉

〈 보안계좌 설정 후 〉

가. 비밀번호 변경

[특 징]

- 영업점에 직접 방문하지 않고, 인터넷 뱅킹을 통해 계좌 비밀번호 변경이 가능한 서비스
- 비밀번호 유출이 의심되는 등 비밀번호 변경이 필요할 때 신속히 변경함으로써 추가 피해 방지

[기대 효과]

- 피싱 등을 통해 계좌 비밀번호 유출 시, 이용자가 계좌 비밀번호를 변경함으로써 즉각적인 대응 가능

[제공 방법]

- (서비스 이용) 인터넷 뱅킹을 통해 이용자가 직접 변경

나. 보안 계좌

[특 징]

- 중요 계좌에 대한 전자금융거래를 차단하는 서비스
 - ※ 전자금융거래 예 : 인터넷뱅킹, 텔레뱅킹, 스마트뱅킹, 콜센터 등을 통한 조회, 이체 및 출금 등
- 보안 계좌에 대해서는 영업점 방문을 통한 창구(대면) 거래, CD/ATM 등만 이용 가능
- (관련 대책) 금융감독원 전자거래 안전성 강화 대책

[기대 효과]

- 전자금융거래상에 계좌가 조회되지 않도록 하여 계좌를 보호할 수 있으며, 전자금융 거래를 차단하여 보안 위협으로부터 이용자 보호 가능

[제공 방법]

- (서비스 신청) 인터넷/스마트뱅킹을 통해 서비스 신청
- (서비스 해지) 이용자가 직접 영업점에 방문하여 해지

다. 계좌 숨기기

[특 징]

- 인터넷/스마트뱅킹 계좌조회 시 일부 계좌를 화면상에 보이지 않도록 숨겨주며, 직접 계좌번호를 입력해야만 이용 가능한 서비스
- 보안 계좌와 달리 전자금융거래가 차단되지 않고, 계좌 숨김/해제가 자유로움
※ 단, 계좌가 1개인 경우 서비스 이용 불가

[기대 효과]

- 인터넷뱅킹 공유, 공공장소 등에서 계좌조회 시 불필요한 계좌가 나타나지 않도록 하여 계좌를 보호함

[제공 방법]

- (서비스 신청) 인터넷/스마트뱅킹을 통해 서비스 신청
- (서비스 해지) 인터넷/스마트뱅킹을 통해 서비스 해지

라. 특정계좌 조회금지

[특 징]

- 타인의 계좌조회를 방지하고, 철저한 계좌정보 보호를 위해 등록된 계좌의 조회를 금지하는 서비스
- 인터넷뱅킹 사이트 등을 통한 간편서비스, 폰뱅킹, 결제원 ARS를 통한 계좌조회가 금지되어 조회가 불가능해짐

[기대 효과]

- 계좌번호, 계좌 비밀번호만으로 이용 가능한 계좌의 간편 조회를 방지함

[제공 방법]

- (서비스 신청) 인터넷뱅킹을 통해 서비스 신청
- (서비스 해지) 인터넷뱅킹을 통해 서비스 해지

마. 계좌안심서비스

[특 징]

- 서비스 신청 시 계좌관리점 이외 지점거래가 제한되는 서비스
- 빠른조회 서비스에 등록되어져 있는 경우 4가지 거래제한 항목(자동화기기/선택제한 사항없음/텔레뱅킹/텔레뱅킹_자동화기기) 선택만 가능
 - ※ 단, '선택제한사항없음'을 선택하면 계좌관리점 이외 지점 거래만 제한됨

[기대 효과]

- 금융거래 이용 장소가 계좌관리점으로 한정함으로써 위험 노출을 최소화할 수 있음

[제공 방법]

- (서비스 신청) 인터넷뱅킹을 통해 서비스 신청
- (서비스 해지) 계좌관리점 방문을 통해 서비스 해지

[표 2]

계좌 보안 서비스 요약

서비스명	서비스 특징
비밀번호 변경	계좌 비밀번호를 변경
보안계좌	중요 계좌에 대한 전자금융거래 일부를 차단
계좌 숨기기	일부 계좌를 보이지 않도록 숨김
특정계좌 조회금지	특정계좌에 대한 계좌조회 금지
계좌안심서비스	계좌관리점 이외 지점거래를 제한

3. 이체 보안

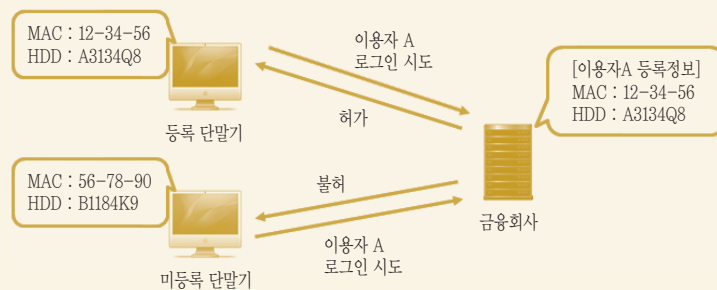
이체 보안은 금융위원회 및 금융감독원의 대책인 「전자금융사기 예방서비스(2012.9)」에 의해 시행된 것으로 이체 거래 시 추가 인증 등으로 본인확인 절차를 강화하는 것으로 단말기

지정, 추가인증, 입금계좌지정, 지연이체, 모바일 승인, 앱 인증, 이체시간지정, 1회용 비밀번호 등이 있다.

예를 들어 단말기 지정 서비스의 경우 [그림 3]과 같이 사전에 등록된 단말기에서 로그인, 이체 거래 등이 발생할 수 있도록 이용가능한 단말기를 제한하는 서비스이다. 지정되지 않은 단말기에서는 추가 인증을 요구하거나 이용을 제한한다.

[그림 3]

단말기 지정 서비스 이용의 예



가. 단말기 지정

[특 징]

- 이용자가 사전에 지정한 단말기(PC, 스마트폰 등)에서만 인터넷/스마트뱅킹 허용
- 미지정 단말에서는 계좌 조회 등 일부 서비스만 이용 가능하며, 추가 인증(ARS, SMS등) 시 모든 서비스 이용 가능
 - ※ 금융회사 별로 미지정 단말에서의 이용 가능 서비스는 상이할 수 있음
- 이용 단말의 지정여부 확인에는 단말의 유·무선 통신카드 고유번호 등을 사용
- (관련 대책) 금융감독원「전자금융사기 예방서비스(2012.09)」

[기대 효과]

- 지정단말기 이외에서 발생하는 부정거래를 차단함으로써 이용자 보호 가능

[제공 방법]

- (서비스 신청) 지정을 원하는 단말에서 로그인 후, 단말 지정 신청(단말 정보 수집 및 등록)
- (서비스 해지) 지정된 단말이 1대일 경우, 이용자가 직접 영업점에 방문하여 해지
※ 지정 단말이 2대 이상인 경우 최종 1대를 제외하고 인터넷 뱅킹을 통해 해지 가능

나. 추가인증

[특 징]

- 중요 금융거래 시 ARS 및 SMS 등으로 추가 본인인증을 수행하는 서비스
※ 중요 금융거래 예 : 고액 이체, 공인인증서 (재)발급 및 타기관 인증서 등록 등
- 추가 인증에는 이용자가 사전 등록한 전화번호가 사용되며, 금융회사에서 제시한 인증번호를 입력하여 승인하는 방식
- (관련 대책) 금융감독원 「전자금융사기 예방서비스(2012.09)」

[기대 효과]

- 부정거래 시도 시 이용자에게 추가인증이 시도되어 정상거래 아닐 경우 이용자가 즉시 확인하여 차단 가능

[제공 방법]

- (서비스 신청) 인터넷/스마트뱅킹 및 영업점 방문을 통해 서비스 신청
※ 일반적으로 2개 이상의 전화번호 등록 요구
- (서비스 이용) ARS 인증 전화 미수신 또는 일정시간 이상 SMS 인증번호 미입력 시 거래 취소

다. 입금계좌지정

[특 징]

- 이용자가 지정한 계좌로만 이체(입금) 가능하도록 기능을 제한하는 서비스
- 미지정 계좌로의 입금은 사전 설정한 이체한도금액 내에서만 가능하며, 이체한도금액을 초과한 경우 계좌 및 공인인증서 비밀번호 등이 일치하더라도 이체 차단

- (관련 대책) 금융감독원 「신(新)입금계좌지정제(2014.12)」

[기대 효과]

- 입금계좌가 제한됨에 따라 부정거래 및 이용자의 착오송금으로 인한 피해 방지

[제공 방법]

- (서비스 신청) 인터넷/스마트뱅킹, ATM, 영업점을 통해서 입금계좌지정 등록 및 미지정 계좌 이체한도 설정
- (서비스 해지) 이용자가 직접 영업점에 방문하여 해지

라. 지연이체

[특 징]

- 계좌이체 거래 시 거래지시 시점부터 일정시간 경과 후 이체되는 서비스
- 이용자가 설정한 지연시간(최소 지연시간 이상) 이후 거래가 처리되며, 지연시간 전까지 거래 취소 가능
 - ※ 보통 최소 지연시간은 3시간이며, 금융회사별 최소 지연시간 및 취소 가능 시간은 상이할 수 있음
- 사전 설정한 이체한도금액 내에서 즉시 처리 가능하도록 예외설정 가능

[기대 효과]

- 부정거래 및 이용자의 착오송금 등이 발생하더라도 지연시간내에 거래 취소가 가능하여 피해 예방 가능

[제공 방법]

- (서비스 신청) 인터넷/스마트뱅킹 및 영업점 방문을 통해 신청
- (서비스 해지) 이용자가 직접 영업점에 방문하여 해지

마. 모바일 승인

[특 징]

- 중요 금융거래 시 전용 스마트폰 앱을 통해 추가 승인을 수행
- 앱으로 수신된 모바일 승인 요청 정보를 확인 후, 앱 내에서 승인 여부 결정
- (관련 대책) 금융감독원 「전자금융사기 예방서비스(2012.09)」

[기대 효과]

- 부정거래 시도 시 모바일 앱을 통해 승인 요청이 전달되며, 정상거래가 아닐 경우 이용자가 즉시 확인하여 차단 가능

[제공 방법]

- (서비스 신청) 인터넷/스마트뱅킹 및 영업점 방문을 통해 서비스 신청

바. 앱 인증

[특 징]

- 중요 금융거래 시 전용 스마트폰 앱에서 생성된 인증번호를 입력하여 추가 인증을 수행
- ARS 및 SMS를 통해 인증번호를 수신하는 것이 아니라, 스마트폰 앱에서 생성된 인증번호를 입력하는 방식
- (관련 대책) 금융감독원 「전자금융사기 예방서비스(2012.09)」

[기대 효과]

- 부정거래 시도 시 모바일 앱을 통해 인증 요청이 전달되며, 정상 거래가 아닐 경우 이용자가 즉시 확인하여 차단 가능

[제공 방법]

- (서비스 신청) 본인 명의 휴대폰을 이용할 경우 인터넷뱅킹 및 영업점 방문을 통해서 가입 가능하며, 타인 명의 휴대폰인 경우 영업점 방문을 통해서만 신청 가능
- (서비스 해지) 인터넷뱅킹 및 영업점 방문을 통해 해지

사. 이체시간 지정

[특 징]

- 이체 가능 시간대를 지정하고, 해당 시간을 제외한 시간대에는 이체를 차단하는 서비스
- 요일 및 시간 단위로 이체 가능 시간 지정

[기대 효과]

- 전자금융사기 취약시간대(주말 및 심야 시간 등)에 출금 및 이체를 차단하여 이용자 피해 예방

[제공 방법]

- (서비스 신청) 인터넷뱅킹 및 영업점 방문을 통해 신청 및 시간 지정
- (서비스 해지) 인터넷뱅킹 및 영업점 방문을 통해 해지

아. 1회용 비밀번호

[특 징]

- 인터넷/스마트뱅킹을 통해 공인인증서 (재)발급 및 타기관 공인인증서 등록 시 1회용 비밀번호를 통해 추가 인증하는 서비스
- ARS 등을 통한 추가인증이 어려운 경우, 영업점에 방문하여 1회용 비밀번호를 발급 및 인증하는 방식으로 1회용 비밀번호는 일정기간 동안만 유효
- (관련 대책) 금융감독원 「전자금융사기 예방서비스(2012.09)」

[기대 효과]

- 계좌정보, 보안카드 및 OTP 탈취를 통한 비인가된 공인인증서 (재)발급 및 타기관 공인인증서 등록 시도 시 1회용 비밀번호를 요구하여 비인가 접근 차단 가능

[제공 방법]

- (서비스 신청) 영업점에 방문하여 신청 및 1회용 비밀번호 발급
- (서비스 이용) 일정기간 동안 사용하지 않을 경우, 비밀번호 폐기

[표 3]

이체 보안 서비스 요약

서비스명	서비스 특징
단말기지정	사전에 지정한 단말기에서만 서비스 허용
추가인증	중요 금융거래 시 ARS 및 SMS 등 추가 본인인증 수행
입금계좌지정	지정한 계좌로만 이체가 가능하도록 제한
지연이체	이체 거래 시 일정시간 경과 후 이체
모바일 승인	스마트폰 앱을 통한 승인 및 본인인증
앱 인증	스마트폰 앱에서 생성된 인증번호를 입력하여 본인인증 수행
이체시간지정	이체 시간대를 지정하고, 지정 이외의 시간에는 이체를 차단
1회용 비밀번호	공인인증서 재발급 및 타기관 공인인증서 등록 시 1회용 비밀번호 추가 요구

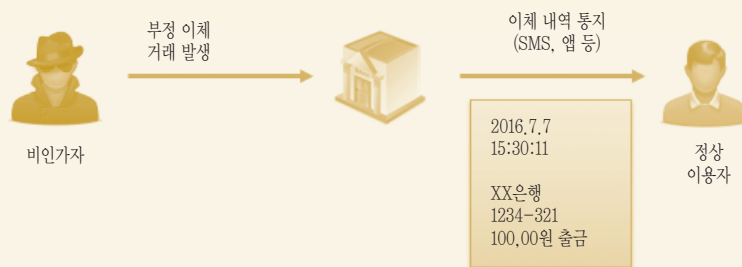
4. 보안통지

보안통지는 중요 변동사항(이체, 공인인증서 (재)발급 등)을 알리거나 보안매체 (보안카드, OTP 등) 이용 시 보안 강화를 제공하는 특징이 있으며, OTP(일반형), 스마트 OTP, 알림 서비스, 서비스 잠금 설정, Safe보안카드, 폰뱅킹 SMS인증, 이용전화번호 지정, 보안SMS 서비스 등이 있다.

예를 들어 알림서비스는 발생하는 모든 거래내역을 이용자에게 알려주는 것으로 [그림 4]와 같이 비인가자가 부정 이체를 발생시킨 경우, 정상 이용자에게 이체 내역을 문자메시지, 앱 푸시 등으로 알림으로써 즉각적인 인지와 금융정보 변경 등의 대처가 가능하도록 도와준다.

[그림 4]

보안통지 서비스 이용의 예



가. OTP(일반형)

[특 징]

- 이체거래 인증 시 보안카드가 아닌, 일회용 비밀번호(OTP)를 사용
- 별도 화면 및 연산기능이 있는 단말(OTP 발생기)을 통해 1분마다 새로운 비밀번호 생성
 - ※ 금융회사 및 제조사마다 비밀번호 생성 주기 및 유효기간이 상이할 수 있음

[기대 효과]

- OTP는 일회용이기 때문에 유출 되더라도 재사용이 어려움
- 보안카드 대비 우수한 관리 편의성 및 보안성으로 금융 거래 시 보안사고 감소에 효과적

[제공 방법]

- (서비스 신청) 영업점 방문을 통해, OTP 서비스 신청 및 발생기 발급(유료) 후 사용
- (서비스 이용) 인증 필요 시, OTP 발생기에서 생성된 OTP 번호 입력

나. 스마트 OTP

[특 징]

- 일반 OTP와는 달리, 스마트폰 및 스마트 OTP 카드를 사용하여 OTP를 생성
- 스마트 OTP 기능이 탑재된 IC 카드를 스마트폰(NFC 탑재)과 접촉하면 OTP가 자동 입력되거나 앱 화면에 출력

[기대 효과]

- 이용자가 지정한 1개 스마트폰에서만 동작하기 때문에 스마트 OTP 카드 분실 시, 부정사용이 어려움
 - ※ 스마트폰 미지정형의 경우 다수 스마트폰에서 사용 가능
- 별도 OTP를 소지하지 않고, 스마트폰과 IC카드만을 사용하기 때문에 편의성 증대
- 향후 2채널 인증 및 기타 간편 결제에도 활용 가능

[제공 방법]

- (서비스 신청) 영업점 방문을 통해, 스마트 OTP 카드 발급 및 지정 스마트폰 등록 후, 관련 앱 설치 및 최초 1회 스마트OTP 카드에 스마트폰 등록(둘 간의 접촉)
- (서비스 이용) OTP 발생 필요시마다 스마트 OTP 카드와 스마트폰을 접촉하여 OTP 생성

다. 알림서비스

[특 징]

- 인터넷/스마트뱅킹 상에서 발생한 입·출금거래 내역을 SMS, FAX, 이메일, 별도 스마트폰 앱을 통해 이용자에게 통지
※ 금융회사별 서비스 이용료 및 통지 내역은 상이할 수 있음
- 알림 받는 방식에 따라서 거래 발생 즉시 또는 주기적(익일 통지 등)인 통지 기능을 제공하며, 이용자가 설정한 계좌, 최저 통지금액 등 일부 세부적인 통지 요건 등을 설정 가능
- (관련 대책) 금융감독원 「전자금융거래 안전성 강화 종합대책(2015.09)」

[기대 효과]

- 부정거래 발생 시 이체내역을 이용자에게 알림으로서 즉각적인 인지 및 추가 피해 방지를 위한 대처 가능

[제공 방법]

- (서비스 신청) 인터넷/스마트뱅킹을 통해 서비스 신청
- (서비스 해지) 인터넷/스마트뱅킹을 통해 서비스 해지

라. 서비스 잠금 설정

[특 징]

- 전자금융서비스 이용 시 로그인, 이체 등과 같은 일부 업무에 대해 이용자 스스로가 차단/허용을 자유롭게 설정할 수 있는 서비스
- 제공 방법 및 제공 기능 범위는 금융회사마다 차이가 있으며, 일반적으로 이체 허용 여부에 대한 제어 기능을 제공

[기대 효과]

- 업무 허용 여부를 이용자 스스로 설정할 수 있으므로, 각종 전자금융사고에 노출되는 시간을 최소한으로 줄여 사고 예방에 도움

[제공 방법]

- (서비스 신청) 영업점 또는 인터넷뱅킹 메뉴, 전용 스마트폰 앱을 설치하여 이용 신청
- (서비스 이용) 서비스 제공 방식에 따라 차이점이 존재함
 - (인터넷뱅킹) 로그인 후 해당 메뉴에서 기능 차단 및 허용이 가능하며, 기능을 허용 시키기 위해서는 2채널 인증 필요
 - (전용 앱) 로그인 없이 버튼을 통해 기능 차단 및 활성화 가능
 - ※ 차단 및 활성화 시 추가인증, 카드 태깅 등의 서비스별 차이점 존재
 - ※ 단말기를 등록하여 이용하는 것으로 해지 시 영업점 방문이 필요하며, 기기변경이 있을 경우 메뉴에서 변경 가능

마. Safe보안카드

[특 징]

- 인터넷/스마트뱅킹 화면에 표시되는 보안카드의 지시번호를 이용자 휴대폰으로 통지하여 해당되는 보안카드번호를 직접 화면에 입력하는 서비스

[기대 효과]

- 전자금융 사고에 노출되더라도 입력해야 할 보안카드번호와 지시번호를 알 수 없어 전자금융사기를 방지

[제공 방법]

- (서비스 신청) 인터넷/스마트뱅킹 또는 영업점에서 서비스 신청
- (서비스 해지) 인터넷/스마트뱅킹 또는 영업점에서 서비스 해지

바. 폰뱅킹 SMS인증

[특 징]

- 전자금융사기 피해 예방을 위해, 폰뱅킹 이체 거래시 이용자 휴대폰으로 전송되는 SMS의 6자리 인증번호를 입력하여 일치하는 경우에만 이체되는 서비스
- ※ 단, 폰뱅킹 거래 도중 SMS 인증을 할 수 없는 전화기(유선전화, 2G폰 등)에서는 서비스 이용이 제한

[기대 효과]

- 폰뱅킹을 이용하기 위해서는 이용자 휴대폰을 이용한 인증이 필요하므로 전자금융사기 피해 예방에 도움

[제공 방법]

- (서비스 신청) 폰뱅킹 또는 영업점 방문을 통해 서비스 신청
- (서비스 이용) 영업점 방문을 통해 서비스 해지

사. 이용전화번호지정

[특 징]

- 사전에 신고한 전화번호에서만 폰뱅킹을 이용할 수 있도록 하고, 그 외의 전화번호 및 발신번호가 없는 경우 폰뱅킹을 제한하는 서비스
- ※ 단, 조회 서비스는 이용 가능
- 휴대폰 번호 등을 포함하여 3개의 전화번호까지 지정 등록 가능하며, 해외, 사설교환기가 설치된 회사전화에서 이용 불가능

[기대 효과]

- 폰뱅킹 이용이 가능한 전화를 제한하여, 정보 유출로 인한 사기 위험 노출을 최소화

[제공 방법]

- (서비스 신청) 영업점 방문을 통해 서비스 신청
- (서비스 해지) 영업점 방문을 통해 서비스 해지

아. 보안SMS 서비스

[특 징]

- 인터넷뱅킹을 통한 중요변동사항 발생 시 은행에 등록된 이용자의 휴대폰으로 중요변동사항에 대해 SMS를 발송하는 서비스
- 중요변동사항은 공인인증서 발급/재발급, 입출금계좌변경, 인터넷/스마트뱅킹 출금거래, 보안용 휴대폰문자 통지서비스 신규/변경/해지 등이 해당

[기대 효과]

- 중요변동사항 발생 시 보안SMS를 수신함으로써 이용자가 즉시 확인하여 추가 피해 예방을 위한 조치 가능

[제공 방법]

- (서비스 신청) 인터넷/스마트뱅킹을 통해 서비스 신청
- (서비스 해지) 인터넷/스마트뱅킹을 통해 서비스 해지

[표 4] 보안통지 서비스 요약

서비스명	서비스 특징
OTP(일반형)	일회용 비밀번호를 생성
스마트 OTP	스마트 카드 등을 이용하여 일회용 비밀번호를 생성
알림서비스	입출금거래 내역을 이용자에게 즉시 통지
서비스 잠금 설정	로그인, 이체 등의 업무에 대해 차단/허용을 설정
Safe보안카드	보안카드번호의 지시번호를 휴대폰 문자로 통지
폰뱅킹 SMS인증	폰뱅킹 이체 거래 시 인증번호를 입력하여 인증
이용전화번호 지정	사전 등록된 전화번호에서만 폰뱅킹 서비스 이용 가능
보안SMS 서비스	중요 변동사항 발생 시 이용자 휴대폰으로 SMS를 발송

Ⅲ. 보안서비스별 주요 이용자

전자금융거래 이용 절차에 따라 구분된 각 보안서비스는 기능별 특징, 기대효과 등이 다르고, 모든 보안서비스를 이용하는 것이 보안성을 높이는데 도움을 줄 수 있지만 이용자의 편의성을 저해시킬 수 있다. 따라서 보안서비스의 특징과 이용자의 성향 등을 고려하여 선택적으로 이용할 필요가 있으며, [표 5]은 이러한 고려사항을 통해 주요 이용자를 분류하였다.

[표 5] 보안서비스별 주요 이용자 분류 결과		
서비스명		주요 이용자
로그인 보안	피싱 방지(개인화)	인터넷/스마트뱅킹 사용 빈도가 높은 이용자
	해외 IP차단	주로 국내에 거주하며, 해외여행/출장 빈도가 낮은 이용자
	그래픽 인증	새로운 비밀번호 입력방식의 서비스 이용에 거부감이 없는 이용자
	안심로그인	스마트폰을 항상 소지하고, 사용이 익숙한 이용자
	지문인증	지문을 이용하여 간편한 서비스 이용을 원하는 이용자
	예외기기로 로그인알림	한정된 이용 단말기 내에서만 이용하는 이용자
	로그인 2채널인증	로그인 보안을 강화하기를 원하는 이용자
계좌 보안	비밀번호 변경	주기적인 비밀번호 변경을 원하는 이용자
	보안계좌	특정 계좌에 대한 전자금융거래 차단을 원하는 이용자
	계좌 숨기기	계좌정보 노출을 꺼리고, 계좌번호를 암기하고 있는 이용자
	특정계좌 조회금지	간편서비스(폰뱅킹 등)를 이용한 계좌 조회 이용을 원치 않는 이용자
	계좌안심서비스	계좌관리점 방문이 잦거나 방문 이용에 불편함이 없는 이용자

서비스명		주요 이용자
이체 보안	단말기지정	주로 국내에 거주하며, 한정된 이용 단말기 내에서 이용하는 이용자
	추가인증	주로 국내에 거주하며, 고정적인 단말기 이용이 어려운 이용 이용자
	입금계좌지정	특정 입금계좌에 한해 고액 이체 빈도가 높은 이용자
	지연이체	즉시 이체 및 출금을 요구하지 않는 이용자
	모바일 승인	스마트폰 사용이 익숙한 이용자
	앱 인증	스마트폰 사용이 익숙한 이용자
	이체시간지정	이용 시간대가 일정한 이용자
	1회용비밀번호	법인명의 휴대폰 이용 등 추가인증이 어려운 이용자
보안 통지	OTP(일반형)	고액 이체 빈도가 높은 이용자
	스마트 OTP	스마트폰을 이용하며, 고액 이체 빈도가 높은 이용자
	알림서비스	입출금내역을 실시간으로 통보 받기를 원하는 이용자
	서비스 잠금 설정	전자금융서비스 이용 채널 또는 기능 제어를 원하는 이용자
	Safe보안카드	OTP보다 보안카드 이용을 선호하는 이용자
	폰뱅킹 SMS인증	폰뱅킹 서비스 이용 빈도가 높은 이용자
	이용전화번호 지정	고정적인 전화를 이용한 폰뱅킹 서비스 이용 빈도가 높은 이용자
	보안SMS 서비스	중요 변동사항에 대해 통지 받기를 원하는 이용자

IV. 결론

이용자는 금융회사에서 제공하는 보안서비스의 특징과 기대효과를 살펴보고, 이용자 성향에 알맞은 보안서비스를 선택하여, 이용자 스스로를 보호하기 위해 적극적인 노력이 필요하다. 물론 전자금융서비스를 제공하는 금융회사에서도 이용자 보호를 위한 지속적인 노력이 필요하므로, 본 고를 통해 할 수 있는 방안을 제시하고자 한다.

첫째, 이용자 보호를 위해 다양한 보안서비스 도입 여부를 검토하는데 활용할 수 있다. 인터넷뱅킹 중심에서 스마트뱅킹으로 이용자 환경이 변화함에 따라, 이용자 편의성 등을 고려한 신규 보안서비스가 지속적으로 등장하고 있다. 특히 피싱 방지(개인화), 스마트 OTP, 서비스 잠금 설정 등의 서비스 도입이 확대되고 있는 추세이며, 스마트폰을 활용한 신규 보안서비스가 지속적으로 등장할 것으로 예상됨에 따라 금융회사에서 미제공중인 보안서비스 현황 파악에 도움일 될 것으로 보인다.

둘째, 주요 이용자 별 맞춤형 서비스를 권장하는데 이용될 수 있다. 카드사에는 이용자의 소비 형태에 맞게 카드를 추천하는 서비스인 ‘내게 맞는 카드 찾기’라는 것이 제공된다. 이체 거래를 제공하는 금융회사에서도 이와 유사하게 이용자의 이용 성향, 환경 등을 고려한 맞춤형 서비스를 제공하여, 이용자에게 적극적인 보안서비스 이용을 권장 할 수 있다.

마지막으로 이용자 편의성을 고려한 정보 제공에 활용 할 수 있다. 대부분 ‘보안센터’를 통해 보안서비스를 대한 정보를 안내하고 있지만, 일부 보안서비스는 안내되지 않거나 별도의 메뉴에서 제공되는 등 이용자 편의성이 고려되지 않았다. 한눈에 어떠한 보안 서비스들을 제공하는 알고, 해당 보안서비스의 기능과 효과를 안내한다면 이용자들은 보다 적극적으로 보안서비스를 이용할 수 있을 것이라고 기대된다.

Trend

- 싱가포르의 핀테크 추진 현황
- NIST, 블록암호 운영방식에 관한 권고
- 타이젠 소개 및 특징 조사

싱가포르의 핀테크 추진 현황

유재필, 이준우*

1. 개요	84
2. 핀테크 정책	85
3. 핀테크 추진기구	87
4. 요약 및 시사점	91
5. 참고	93
6. 참고자료	98

* 금융보안원 융합보안부 핀테크보안팀 (e-mail : jpyoo@fsec.or.kr, leejunwoo@fsec.or.kr)

1 개요

핵심요약

- ◎ 싱가포르를 자국을 아시아 금융서비스 허브로 육성한다는 목표아래 국가차원의 핀테크전략을 수립하고 전담기구를 마련하여 추진 중
- ◎ 전통적인 아시아 금융 강국의 이점을 살려 10여 년 전부터 금융IT융합 활성화 정책을 지속적으로 마련해왔으며,
- ◎ 최근에는 정부차원의 대규모 자금투자프로그램 준비와 더불어 ‘정부핀테크전담부처 (FTIG)’, ‘핀테크오피스’, ‘핀테크 컨소시엄’ 등 정부 및 민간 분야 전담기구를 통해 핀테크 활성화를 지원 중

□ 배경

- 미국, 영국 등 북미·유럽에 편중되어 있던 핀테크 열기가 전 세계로 확대되면서 한국, 싱가포르, 일본, 홍콩, 호주 등 아시아 주요 국가들은 적극적으로 국가차원의 핀테크 활성화를 추진
- 이에 아시아 금융 강국인 싱가포르의 핀테크 활성화 주요정책들을 조사, 검토하여 참고 자료로 활용하고자 함

□ 조사내용

- 싱가포르 핀테크 활성화 주요정책
 - 핀테크 관련 주요 정책 추진경과 및 현황
 - 주요 핀테크 추진 기구 (정부 및 민간)

2 핀테크 정책

- ◆ (과거) 전통적 금융강국인 싱가포르는 금융-IT기술 융합의 중요성을 예전부터 인식하여 국가차원의 전략을 개발·추진해왔으며,
- ◆ (현재) 최근에는 시장활성화를 위해 대규모 자금지원 프로그램을 마련

□ 과거('06~)

- 금융환경*에 ICT 혁신기술을 도입, 싱가포르를 아시아 금융IT허브로 육성하기 위한 전략을 '06년 수립

* 관련내용은 <참고1. 싱가포르 경제 및 비즈니스 환경> 참조

- 국가 미래 ICT 성장전략인 iN2015(Intelligent Nation 2015)*에서 국가 9대 성장동력 중 하나로 금융IT(핀테크)를 지정하고 추진방향을 설정

* 싱가포르 ICT주무부처인 IDA(Infocom development Authority of Singapore)에 의해 '06년도 수립된 '10년 후 미래성장 전략'으로 세부내용은 <참고 3 : iN2015 중 핀테크 관련 주요내용>참고

< 참고 : iN2015(Intelligent Nation 2015) 중 핀테크분야 관련내용 >

목표	건전한 규제와 최고의 인프라를 통해 아시아 핀테크 허브로 도약		
기대효과	금융서비스 경쟁력 향상, 혁신 서비스 발굴		
추진전략	'금융서비스 관문(gateway)' 육성	'ICT혁신센터' 육성	'차세대 결제인프라' 구축
세부전략	① 안전한 핀테크 비즈니스 환경 구축 ② 저비용, 고품질의 정보통신망 구축 ③ 금융-기술 간 협업체계 구축 및 강화 ④ 첨단 핀테크 서비스 도입 및 안착화 ⑤ 신규 금융서비스 지역시장 형성	① ICT기술혁신 촉진을 위해 금융서비스 특화 프로젝트 추진 ② 금융서비스 지원을 위한 ICT역량강화	① 혁신적 결제서비스 구축 및 도입촉진 ② 핵심 응용서비스 개발 및 도입촉진

□ 현재('14~'15)

- (14년) 스마트국가(Smart Nation)* 비전 선포에서 핀테크 창업기반 육성의 중요성을 강조

* 싱가포르의 리셴룽 총리가 '14년에 발표한 ICT기반 스마트국가로의 발전비전으로 관련내용은 <참고3 : 스마트 국가(Smart Nation) 관련 주요내용> 참조

< 참고 : 스마트국가(Smart Nation) >

- 사물인터넷, 빅데이터 등 ICT혁신기술을 활용하여 시민들 삶의 질을 개선하고 관련 산업을 육성하여 국가 미래먹거리를 창출하려는 비전 및 전략
- 리셴룽 총리가 직접 스마트국가 비전을 발표하고('14) 각 부처는 관련 인프라(Smart Nation Platform) 및 서비스 개발을 촉진

- (15년) FSTI(Financial Sector Technology & Innovation) 계획수립을 통해 핀테크분야에 향후 5년간 2억 2500만 싱가포르 달러(한화 약 1,900억원) 투자 예정

< 참고 : 스마트국가(Smart Nation) >

- (목적) 핀테크 활성화를 위한 정부차원의 자금지원 프로그램
- (추진기관) MAS(Monetary Authority of Singapore*)
 - * 싱가포르 금융주무부서로 한국은행+금융위와 유사한 형태
- (지원금액) 2억 2500만 싱가포르 달러 (향후 5년간)
- (지원분야) 정보보호, 결제, 머신러닝, 클라우드, 인증, 생체인식, 블록체인 등
- (지원조건)
 1. (혁신센터) 금융사가 R&D센터나 혁신연구실을 싱가포르에 설립 할 경우
 2. (기관 프로젝트) 성장성, 경쟁력이 있는 창의적 서비스를 개발 할 경우
 3. (산업 프로젝트) 타산업 간의 융합이 필요한 프로젝트를 추진할 경우

3 핀테크 추진기구

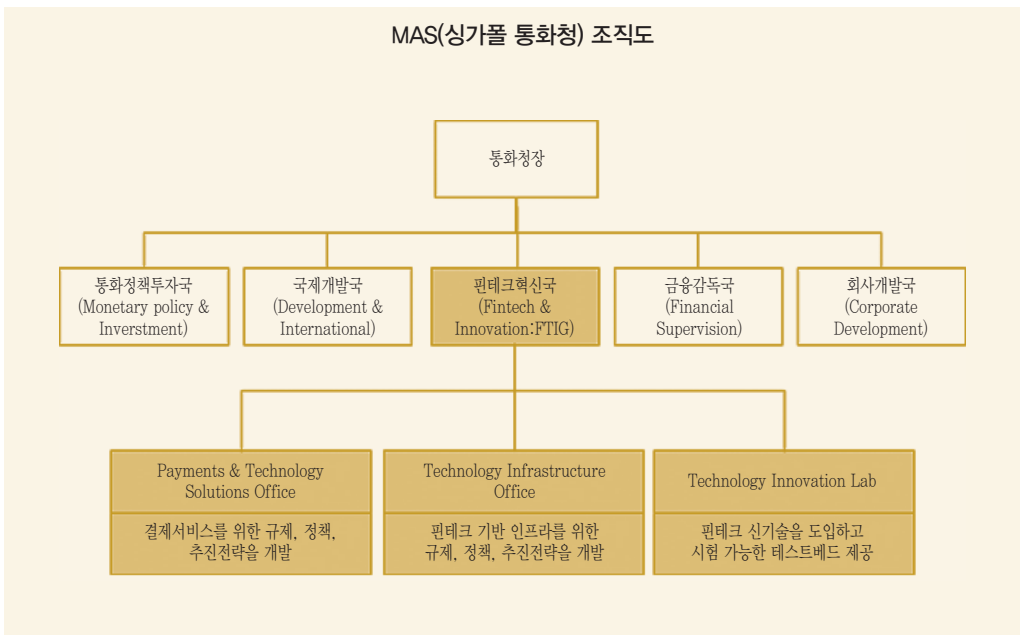
□ 개요

- 정부 핀테크 정책의 효율적 추진을 위해 민·관의 추진기구가 활동
 - 정부전담부처(FTIG), 윈스톱지원창구(Fintech Office), 산업계 결속단체(핀테크 컨소시움) 등이 대표적

싱가포르 핀테크 추진 전담조직 비교			
분야	규제, 정책	창업, 멘토링	산업계 결속, 이익대변
명칭	FTIG (FinTech Innovation Group)	핀테크 오피스 (Fintech Office)	핀테크 컨소시움 (Fintech Consortium)
형태	정부부처(정부)	가상조직(정부운영)	포럼(민간)
국내유사조직	부처(금융위, 미래부 등) 內 핀테크 유관부서	핀테크 지원센터	핀테크협회, 핀테크포럼
설립일	2015.07	2016.05	2015.
주요사업	<ul style="list-style-type: none"> • OpenAPI 지원 • 생태계 구축 • 규제 개선 • 정책 개발 • 규제 샌드박스 운영 (Regulatory Sandbox) 	<ul style="list-style-type: none"> • 창업 지원 • 멘토링 지원 • 자금 지원 • 기타 (컨설팅, 교육, 인증, 장비지원 등) 	<ul style="list-style-type: none"> • 정보공유 • 홍보 • 사업 컨설팅

□ FTIG (Fintech Innovation Group)

- (배경) 핀테크 활성화 사업 추진 시 합리적인 규제관리, 효율적인 추진전략 개발 필요
- (조직) 국내 금융정책기구(금융위+한국은행)와 유사한 역할을 하는 MAS(싱가폴 통화청) 내에 ‘국(局)’규모의 조직(FTIG)을 두고 산하에 3개 팀운영을 통해 핀테크관련 규제, 정책 등을 기획 및 조정
 - (결제 및 기술솔루션 팀 : Payments & Technology Solutions Office) ‘빠르고’, ‘편리하며’, ‘안전한’ 결제서비스를 위한 정책개발
 - (기술인프라 팀 : Technology Infrastructure Office) 클라우드, 빅데이터, 블록체인 등 핀테크 서비스 기반 인프라에 대한 정책개발
 - (기술혁신 팀 : Technology Innovation Lab) 핀테크 신기술을 도입하고 이를 시험할 수 있는 규제 샌드박스 제공



○ (관련사업) '6대 기술주제'*를 중심으로 규제, 정책, 기술 관련 전략기획 수립 및 핀테크 생태계 활성화 지원

* 6대 기술주제 : 모바일 결제, 인증(생체), 블록체인(분산장부), 클라우드, 빅데이터, 머신러닝

- (규제) 결제서비스, 핀테크인프라 관련 정책 및 추진전략을 개발하고 동시에 규제개선 추진

- (생태계 구축) 핀테크 이해관계자*로 구성된 핀테크 생태계 구축

* 핀테크 기업, IT기업, 금융사, 투자자, 연구기관, 교육기관, 정부기관, 전문가 등

- (OpenAPI 지원) 기존 금융사의 IT자원을 핀테크 기업의 서비스로 쉽게 연결할 수 있는 'OPEN API 서비스' 제공

- (규제 샌드박스 운영) 새로운 서비스를 안전하고 통제된 환경에서 시험·검증할 수 있는 규제 샌드박스(Regulatory Sandbox)* 운영

* 혁신적 기술이 포함된 핀테크 서비스에 대해 기존규제를 적용하지 않고 자유롭게 신규서비스의 가능성을 시험, 검증하는 방식

□ 핀테크 오피스(Fintech Office)

○ (배경) 분산되어 있던 정부차원의 핀테크 지원프로그램들을 정부기관 간 유기적 협력을 통해 원스톱으로 지원할 필요

○ (조직) MAS와 NRF(국가연구재단) 주관 하에 다수의 정부기관*이 협력한 가상조직으로 창업부터 제후까지 핀테크 관련업무를 원스톱으로 지원

* 경제개발청(Economic Development Board:EDB), 정보통신 투자공사(Infocomm Investments Pte Ltd :IIPD), 생산표준청(Spring singapore:Spring), 정보통신 미디어 개발청(IMDA)

○ (관련사업) 각 정부기관별 특화된 전문분야를 세부적으로 지원

- 창업자금지원, 멘토링, 저작권보호, 교육, 인증, 장비구입지원 등

싱가포르 핀테크 추진 전담조직 비교		
추진 사업	상세내용	산업계
ACE 스타트업	<ul style="list-style-type: none"> • 평가 후 창업자금 지원 • 사업초기 멘토링 제도 지원 	생산표준청 (Spring)
TECS (Technology Enterprise Commercialisation Scheme)	<ul style="list-style-type: none"> • 사업초기 자금지원으로 저작권 보호 	생산표준청 (Spring)
CDG-TI (Capabilities Development Grant Technology Innovation)	<ul style="list-style-type: none"> • 컨설팅, 교육, 인증, 장비구입 등 자금 지원 	정보통신 미디어개발청 (IMDA)
TIS (Technology Incubation Scheme)	<ul style="list-style-type: none"> • 투자자금 지원 • 멘토링 제도 지원 	국가연구재단 (NRF)

□ 핀테크 컨소시엄(Fintech Consortium)

- (배경) 핀테크업계 간 결속 및 이익대변 필요
- (조직) 핀테크업계 민간단체로 구성되어 업계 상호간 정보공유, 사업운영 컨설팅 등을 제공
- (핀테크 관련 추진사업) 3대 핀테크 플랫폼 제공을 통해 핀테크 생태계 활성화를 지원
 - (온라인 핀테크 지원 플랫폼) 온라인 포털을 통해 ‘금융분석툴’, ‘연구자료’, ‘아웃소싱’, ‘제휴’ 관련 정보 제공
 - (오프라인 핀테크 지원 플랫폼) 오프라인 세미나, 토론회 개최 등을 통해 싱가포르 핀테크 커뮤니티 유대관계 활성화
 - (인큐베이션 플랫폼) 핀테크 관련연구수행, 자문, 투자지원 등을 수행

4 요약 및 시사점

□ 요약

- 싱가포르는 입지적 조건, 비즈니스 편의환경을 바탕으로 싱가포르를 아시아 핀테크 허브로 육성하려는 계획을 지속적으로 추진해 오
 - 최근의 글로벌 핀테크 붐과 더불어 싱가포르는 대규모 투자계획을 마련하고 전담조직을 구성하여 정부차원에서 핀테크 활성화를 지원
- 규제개선보다는, ‘자금 및 조직 지원’*을 통한 시장활성화의 측면이 강하며 특히 ‘핀테크 오피스’라는 범부처 핀테크 활성화 기구를 운영
 - * 최근 핀테크 분야에 1,900억원 규모의 투자계획을 확정하였으며, 관련 업무를 전담하는 정부조직을 ‘국’규모로 구성하여 운영
 - 부처별 산재해 있는 핀테크 지원프로그램 창구의 일원화를 통해 고객편의를 향상시키고 업무 간 시너지 증대를 추구하여,
 - 창업자금지원부터 멘토링, 저작권보호, 교육, 인증, 장비구입지원 등의 업무 지원 가능

□ 시사점

- 국내도 싱가포르의 사례처럼 범부처 차원의 지원체계 마련할 필요
 - ‘핀테크지원센터’와 같이 기 활성화된 핀테크관련 윈스톱 지원체계를 범부처 지원이 가능한 형태로 확대하여,
 - 기술개발, 창업지원, 자금지원, 규제개선, 서비스창출, 제휴활성화 등이 상호 유기적으로 연계되고 더욱 확대되도록 지원할 필요 있음
 - 또한 정부차원의 관련분야 업무조직을 체계화, 세분화 및 격상시켜 업무집중도를 향상시키고 정책추진이 탄력 받을 수 있는 방안 검토
- 글로벌 진출을 위해 더욱 적극적인 목표 및 전략 수립 필요
 - 싱가포르는 지리적 위치, 발달된 금융서비스를 장점으로 자국을 아시아의 핀테크 허브로 육성한다는 계획을 수립하고 있음

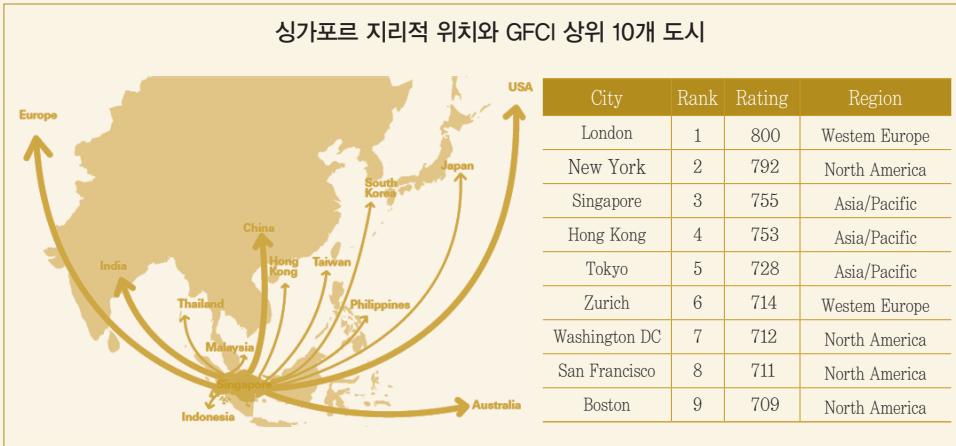
-
- 우리도 좁은 국내시장의 한계를 극복하고 핀테크 시장가치의 효용성을 극대화하기 위해서는, 판로개척은 물론 우리나라 핀테크 시장을 글로벌 플레이그라운드로 한 단계 업그레이드 할 필요
 - 이 과정에서 세계 최고 수준의 ICT 인프라 및 보유기술, 높은 교육수준 및 기술적응력의 적극 활용 필요

5 참고

〈 참고1 : 싱가포르 경제 및 비즈니스 환경 〉

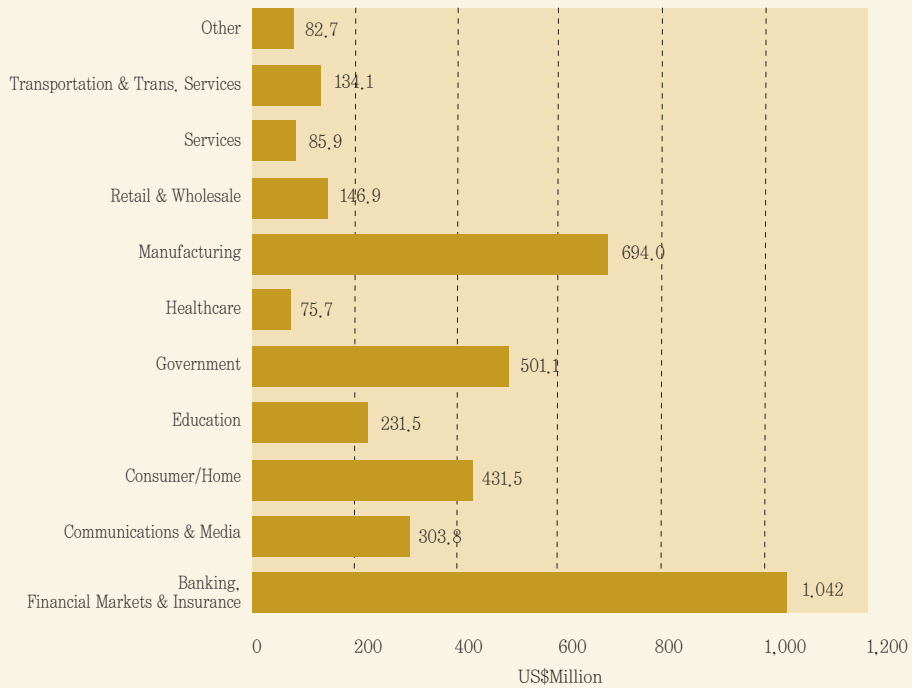
- 아시아의 입구인 지리적 요인으로 금융산업과 물류산업이 발달
 - (지리적 요인) 인도, 중국, 아시아 주요국과 인접하고 아시아 입구의 역할을 하여 전통적으로 물류산업이 발달
 - (금융산업) 200개의 글로벌 금융사를 유치하여 높은 수준의 국제금융 경쟁력을 지님
- ※ 싱가포르는 Z/Yen 그룹에서 실시하는 국제금융센터 지수(Global Financial Centres Index : GFCI)에서 세계 3위, 아시아 1위 기록(2016년)

싱가포르 지리적 위치와 GFCI 상위 10개 도시



- 싱가포르의 시장가치는 약 6천억원 수준으로 투자는 대규모, 다양한 채널로 형성
 - (시장) 싱가포르 핀테크 시장 크기는 약 8억불 (한화로 약 6천억원)으로 추산되고, 고용 인원은 7,000 여명 수준
 - (투자규모) 싱가포르의 핀테크 투자규모는 타산업 ICT 투자에 비해 절대적으로 우위(10억불)
 - (민간투자) 정부의 투자 뿐만 아니라, 민간에서도 핀테크환경을 위해 투자
- ※ 싱가포르 정부기관 MAS(통화청)은 핀테크예산으로 2억 2500만 싱가포르 달러 투자 예정, 글로벌 은행 DMS는 핀테크 생태계 구축을 위해 7백만불 투자(2015.)

싱가포르 각 분야 별 ICT 투자 현황



○ 생태계, 법률 등 핀테크기업 운영하기 위한 환경 지원

- (핀테크 생태계) 핀테크기업, 투자자, 인큐베이터 등 다양한 이해관계자들이 핀테크 생태계를 구성
- (법률) 저작권 보호 등의 법률을 통해 창업을 지원하는 환경 조성

※ 저작권보호에 관한 법률이 강력하여 핀란드에 이어 세계에서 가장 저작권보호가 잘되는 국가로 선정

싱가포르의 핀테크 생태계



〈 참고2 : 스마트국가(Smart Nation) 관련 주요내용 〉

□ 목표 및 추진방향

- (목표) ICT 기술과 인프라를 바탕으로 더 나은 공공서비스를 제공, 시민들의 삶의 질 개선, 비즈니스 업무의 효율성 증진
- (추진방향) 14년 스마트 국가(Smart Nation) 비전 발표, 이후 스마트 국가 플랫폼(Smart Nation Platform:SNP) 구축 및 각 분야 별로 세부사업 추진

□ 추진경과

- (스마트 국가 비전) 스마트 교통(Smart Mobility), 스마트 생활(Smart Living), 협력체제, 생태계 등의 내용을 포함하는 ICT 발전방향으로 스마트 국가 비전을 발표

스마트 국가 비전

- 총리실에서 업무를 조정하며 정부 전 부처가 협력
- 싱가포르 총리 리셴룽이 직접 발표 ('14.11.24)

- (스마트플랫폼 구축) 정부기관 데이터를 공유할 수 있게 연결, 수집, 응용의 3단계에 걸쳐 플랫폼 구축

스마트플랫폼 구축

- (연결) 광역인터넷망과 무선인터넷망 확대로 빠른 통신망 구축
- (수집) 필요한 정보를 생성·공유할 수 있는 운영시스템 구축
- (응용) 네트워크와 데이터 플랫폼을 공유하는 테스트 베드운영

〈 참고 3 : iN2015 중 핀테크 관련 주요내용 〉

□ 개요

- (목표) 싱가포르를 국가 ICT 성장 전략 종합계획 인 iN2015(Intelligent Nation 2015)에서 국가 9대 성장동력 중 하나로 핀테크를 지정하고, 핀테크분야 추진 방향을 설정
- (주요내용) 싱가포르를 아시아 핀테크 허브로 육성한다는 목표하에 ‘금융서비스 관문 육성’, ‘ICT 혁신센터 육성’, ‘차세대 결제인프라 구축’을 3대 추진전략으로 설정하고 분야별 추진방안과 연계 전략프로그램을 제시

□ 상세내용

- (금융서비스 관문 육성) 사이버 침해사고 없이 안전하고 편리하게 금융서비스를 제공할 수 있도록 아래 5가지 추진전략 제안
 - ① (안전한 핀테크 비즈니스 환경 구축)
 - － 아시아 금융 서비스 관문으로서 ‘보안’, ‘개인정보’, ‘인증’의 중요성 강조
 - － 상기 요소의 구체적인 추진을 위해 NTF와 연계
 - ② (저비용, 고품질의 정보 통신망 구축)
 - － 초고속 광대역 유무선 네트워크를 구축하고 싱가포르와 해외간 연결망 확대
 - ③ (금융-기술 간 협업체계 구축 및 강화)
 - － 산업계와 타기관 협업 유도, 산업계와 연계된 학위 및 인턴십 개발, 금융-기술 융합 전문가 육성으로 금융-기술 간 협업체계 구축
 - ④ (첨단 핀테크 서비스 도입 및 안착화)
 - － 해외 첨단 핀테크 서비스 유치를 위해, 사업연속성 및 재난방지 능력을 강화 하고 국내외 기업 간 전략적 제휴 촉진
 - ⑤ (신규 금융서비스 지역시장 형성)
 - － 기술 표준화, 금융시스템 통합 등으로 타국가와 금융시장연결을 주도하여 신규 금융서비스를 적용할 수 있는 지역시장 형성

- (ICT혁신센터 육성) ICT를 통해 금융서비스를 혁신할 수 있도록 아래 2가지 추진 전략 제안
 - ① (ICT기술혁신 촉진을 위해 금융서비스 특화 프로젝트 추진)
 - 기업의 R&D기관 투자 활성화, R&D를 통한 상품화 촉진 등으로 산업계와 R&D기관 간 생태계 구축
 - ② (금융서비스 지원을 위한 ICT 역량 강화)
 - 금융사, 연구기관, ICT기업 간의 협력 촉진으로 금융서비스에 적용가능한 신기술 개발
- (차세대 결제인프라 구축) 신기술을 활용하여 기존과 다른 방법으로 편리한 금융 서비스를 제공할 수 있도록 아래 2가지 추진전략 제안
 - ① (혁신적 결제서비스 구축 및 도입 촉진)
 - 다양한 산업의 기술융합 장려, 개방형 표준 기술 권고 등으로 혁신적인 결제 서비스 구축 및 도입 촉진
 - ② (핵심 응용서비스 개발 및 도입 촉진)
 - 온라인 청구서 서비스, 통합 결제 서비스 등의 편리한 서비스 개발 및 도입을 촉진하는 생태계 조성

6 참고자료

- 1) 싱가포르 통화청(MAS), <http://www.mas.gov.sg>
- 2) 싱가포르 정보통신개발청(IDA), <http://www.ida.gov.sg>
- 3) 핀테크 컨소시움, <http://singaporefintech.com>
- 4) Leveraging Infocomm To Ensure Singapore's Prospects in the Financial Markets
- Report by the iN2015 Financial Services Sub-committee- ,IDA, 2006
- 5) Releasing the iN2015 Vision ,IDA, 2010
- 6) Smart nation Platform, IDA, 2014.6.
- 7) MAS Paves the Way for Fintech Innovation with SGD 225 Million Scheme,
RAJAH & TANN, 2015.7.
- 8) The Singapore Fintech Consortium Promises to Help Turn Singapore Into a
Global Fintech Hub, Fintechnews Singapore, 2015.11.
- 9) 금융허브 싱가포르 새 목표는 '핀테크 허브', 중앙일보, 2016.4.26.
- 10) MAS Establishes FinTech Office, Announces Upcoming Public Consultation on
Regulatory Sandbox, and Organises Singapore FinTech Festival, RAJAH & TANN,
2016.5.

NIST, 「블록암호 운영방식에 관한 권고 - 형태보존 암호화 (Format-Preserving Encryption, FPE) 방법」 소개

이 근 영*

1. 개요	100
2. 블록암호(Block Cipher)	101
3. 형태보존 암호(Format-Preserving Encryption)	104
4. 형태보존 암호화 방식 - FF1과 FF3	106
5. 시사점	108
6. [참 조] 현대 블록암호 운용 방식(mode)	109

* 금융보안원 보안연구부 보안기술연구팀 (e-mail : kylee@fsec.or.kr)

1 개요

- 미국 국립표준기술연구소인 NIST¹⁾에서 컴퓨터 보안 표준 SP(Special Publication) 800-38G ‘블록암호(Block Cipher) 운영 방식에 관한 권고 - 형태보존 암호화 (Format-Preserving Encryption) 방법’²⁾을 제정(2016.3.29.)함에 따라,
- 본 보고서에서는 NIST의 SP 800-38G에서 기술하는 내용을 기반으로 블록암호인 형태보존 암호화의 개념과 그에 관한 2가지 방식의 기술 및 특징에 대해 요약 · 소개함

1) 미국 상무부 국립표준기술국(National Institute of Standards and Technology)으로 권고 및 협력체제 구축 활동을 함

2) NIST Special Publication(SP) 800-38G, Recommendation for Block Cipher Modes of operation : Methods for format-Preserving Encryption
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38G.pdf>

2 블록암호(Block Cipher)

- (개념) 기밀성이 필요한 정보를 정해진 블록 단위로 암호화 하는 대칭키 암호 시스템으로 n -bit 평문 블록을 암호화하거나 n -bit 암호문 블록을 복호화하며, 암호화 알고리즘은 k 비트 키를 사용

※ 스트림 암호(Stream Cipher)는 블록암호와 달리 데이터의 흐름(스트림)을 순차적으로 처리하며, 비트 단위로 암호화/복호화가 이루어짐



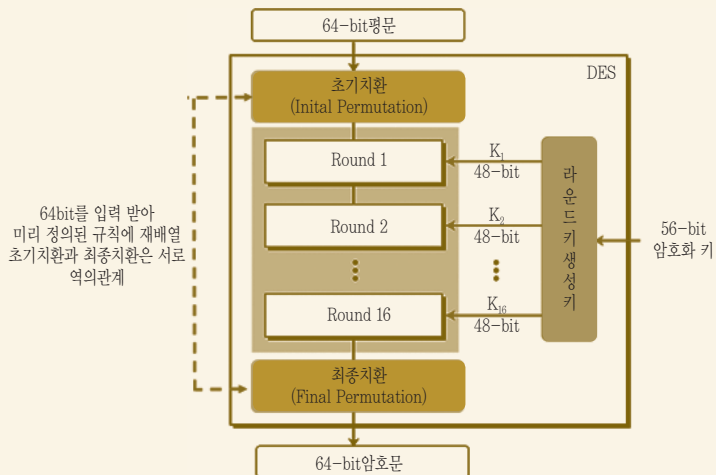
- (구조) 현대 블록암호는 샤논이 제안한 형태³⁾와 기타 구성 요소의 복합적인 합성 암호 (Product Cipher)의 형태를 가지며, ①Feistel 구조와 ②SPN 구조 등이 존재

블록 암호 구조	
구분	내용
Feistel 구조	<ul style="list-style-type: none"> • 암호화 과정에 역함수가 필요 없다는 장점 • 구현 시 스왑(Swap)단계 때문에 연산량이 많이 소요되며 암호에 사용되는 라운드 함수를 안전하게 설계해야 하는 단점 • 대표적으로 3DES(Data Encryption Standard)가 사용됨

3) 샤논은 미국의 수학 및 암호학자이며 “Communication Theory of Security Systems” 논문에서 안전한 암호 설계를 위한 혼돈(Confusion)과 확산(Diffusion)*의 성질에 대해 발표함(1949년)

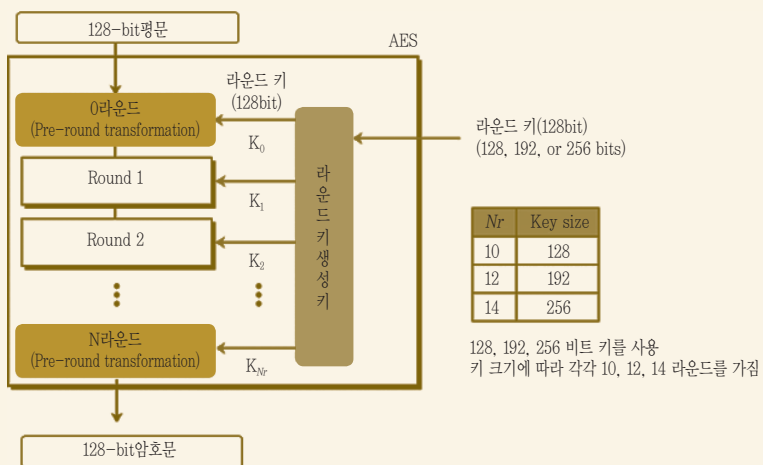
* 혼돈은 암호문과 키(key) 사이의 관계를 숨기는 것이며, 확산은 암호문과 평문 사이의 관계를 숨기는 것임

DES의 일반적인 암호화 구조



- 중간 비트의 이동없이 암호화화가 가능하여 Feistel구조에 비해 효율적으로 설계 가능
- 암호화 과정에서 역함수가 필요하도록 설계되어야 한다는 단점
- 대표적으로 AES(Advanced Encryption Standard)가 상용됨

SPN구조



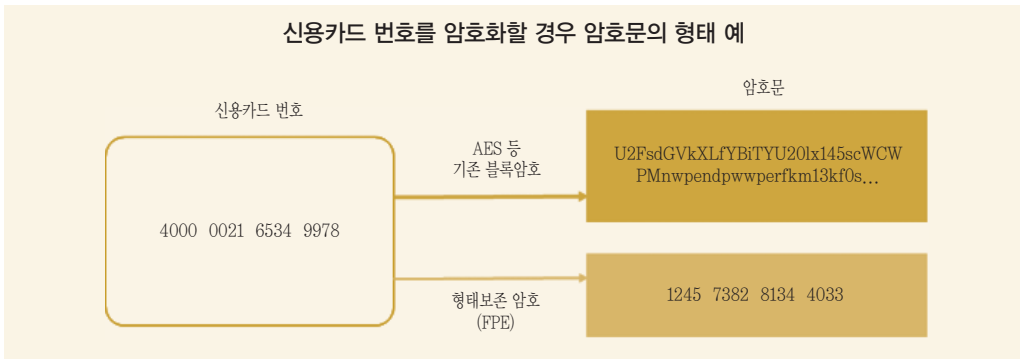
- (현대 블록암호 운용 방식(mode)*) 암호화하려는 정보가 블록의 길이보다 길 경우, 가변 길이의 데이터를 암호화하기 위해 ①ECB(Electronic CodeBook mode, 전자 코드북 방식), ②CBC(Cipher Block Chaining mode, 암호 블록 체인 방식), ③CFB(Output-FeedBack mode, 출력 피드백 방식), ④OFB(Cipher-FeedBack mode, 암호 피드백 방식), ⑤CTR(CounTeR mode, 카운터 방식)과 같은 블록암호 알고리즘 운영 방식을 사용

* MODE는 평문을 암호화하기 위해 블록암호 알고리즘을 반복하여 사용하여 긴 평문 전부를 암호화할 필요가 있는데, 이와 같이 반복하는 방법을 블록암호의 모드(mode)라고 함

※ 상세 내용은 '[참조] 현대 블록암호 운용 방식(mode)' 참고

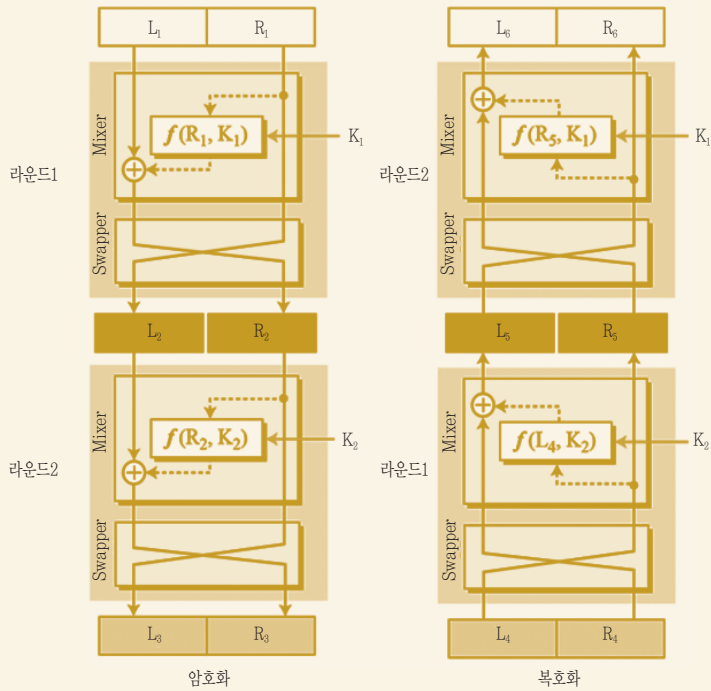
3 형태보존 암호(Format-Preserving Encryption, FPE)

- (개념) 블록암호에 기반하여 특정한 형태의 평문의 값을 동일한 형태의 값으로 변환하는 암호 알고리즘



- (특징) ①트윅(Tweak)을 사용하며 ②Feistel 구조의 암호화 방식을 기반으로 ③기존 암호화 방식의 대체 및 보완의 역할
 - (트윅(Tweak)) 형태보존 암호에서 기밀성을 제공하기 위해 정형화된 데이터에 추가적인 입력정보임. 트윅은 꼭 비밀로 보호되어야 하는 요소는 아니며, 암호화 함수 모두를 결정하기 때문에 키의 변화 가능한 부분으로 간주됨
 - (Feistel 구조) 암호화 방식이 특정 계산 함수*의 반복으로 이루어지는 블록암호의 Feistel구조에 기반 함
 - * 각 과정에 사용되는 함수를 라운드 함수(round function)라고 하며, FF1에서는 10라운드, FF3에서는 8 라운드를 발생
 - (기존 암호화 방식의 대체 및 보완) 일반적인 암호 알고리즘은 비트열을 비트열로 변환하지만 신용카드번호나 주민등록번호, 사회보장번호(Social Security Number, SSN) 등과 같이 비트열이 아닌 특정한 형태의 데이터를 가진 경우 원본 데이터의 값을 동일한 형태로 변환하여 기존 암호화 방식의 대체 기술

두개의 라운드를 갖는 Feistel 구조 및 동작과정의 예



- 두개의 라운드 키 K_1 , K_2 가 존재하며, 키는 암호화와 복호화에서 역순으로 사용됨
- 두개의 믹서는 서로 역관계이고 스와퍼는 서로 역관계이므로 암호화 알고리즘과 복호화 알고리즘은 서로 역관계임
- $L_4=L_3$ 와 $R_4=R_3$ 을 만족(전송 도중 암호문은 변하지 않음) 한다는 가정 하에 $L_6=L_1$ 와 $R_6=R_1$ 임을 증명할 수 있음

4 형태보존 암호화 방식 – FF1과 FF3

- (분류) NIST에서는 다수의 형태보존 암호화 방식 후보 중, FF1, FF2, FF3*을 표준안 드래프트로 선택, SP-38G에서 Feistel 구조를 사용하며 3DES(TDEA) 기반 암호화 방식의 형태 보존 방법으로 FF1과 FF3을 요약 및 명시

* FF1, FF2, FF3는 블록암호를 사용하는 Feistel 구조 기반의 형태보존 암호로 NIST에 각각 FFX [Radix], VAES3, BPS라는 이름으로 제출됨

- (암복호화 함수) 블록암호화(FF1과 FF3)를 위한 주어진 키 = K, 평문 = X, 트윅 = T일 때 형태보존 암복호화 함수는 아래와 같음

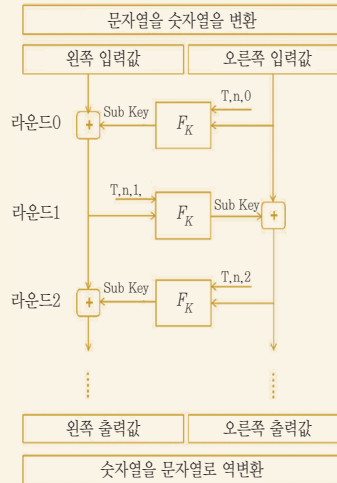
형태보존 암복호화 함수

- 암호화 함수
 - $FF1_Encrypt(K, T, X)$
 - $FF3_Encrypt(K, T, X)$
- 복호화 함수
 - $FF1_Decrypt(K, T, FF1_Encrypt(K, T, X)) = X$
 - $FF3_Decrypt(K, T, FF3_Encrypt(K, T, X)) = X$

- (FF1과 FF3 형태보존 암호화 방식 특징) FF1(또는 FFX [Radix]) 형태보존 암호와 FF3 (또는 BPS) 형태보존 암호의 특징은 아래와 같음

구분	내 용
FF1	<ul style="list-style-type: none"> • 평문 Character String을 아래 그림과 같은 방식으로 암호화하여 평문과 형태가 동일한 암호문 Character String을 정의된 Radix 내의 문자로 출력(형태가 보존됨) • 입력 값 평문/암호문(알파벳, 숫자, 비트열 등), 비밀키 K, 트윅(tweak) T 사용 • 길이와 radix를 사용하여 스트링 포맷 유지 • 입력의 최대 길이는 $2^{32} - 1$ 이지만 형태보존 암호의 특성상 주로 짧은 길이의 암호화에 이용 • 안전성을 F함수의 블록암호나 해쉬함수에 의존 • 트윅의 길이는 유연성을 가짐 • Feistel 라운드 수는 10회

FF1 암호화 과정 및 동작과정의 예



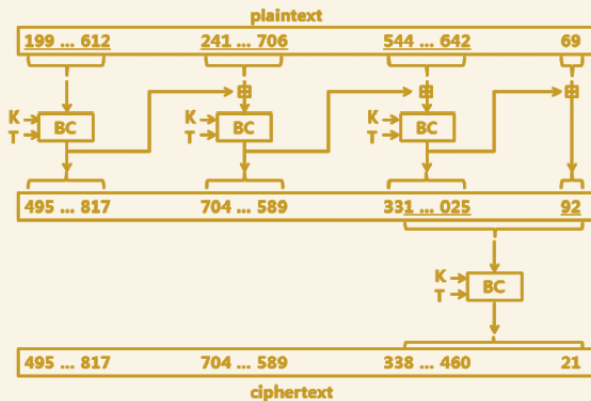
- 1) 숫자, 영문 대소문자, 특수문자 등이 포함된 평문 문자열을 $\{0, 1, 2, \dots, \text{radix}-1\}$ 내의 일련의 숫자열로 변환하는 인코딩
- 2) 인코딩된 데이터가 maximally balanced feistel 방법으로 형태 보존 암호화를 위한 왼쪽 입력값과 오른쪽 입력값으로 구분
- 3-1) 짝수 라운드 : 오른쪽 입력값이 트위, 라운드수, 오른쪽 입력값 길이와 함께 F함수의 입력으로 사용되어 서브키 생성
- 3-2) 홀수 라운드 : 왼쪽 입력값이 트위, 라운드수, 왼쪽 입력값 길이와 함께 F함수의 입력으로 사용되어 서브키 생성
- 4-1) 짝수 라운드 : 왼쪽 입력값과 서브키를 더한 값을 그 다음 라운드의 왼쪽 입력값으로 설정하고, 오른쪽 입력값은 그 다음의 오른쪽 입력값으로 그대로 설정
- 4-2) 홀수 라운드 : 오른쪽 입력값과 서브키를 더한 값을 그 다음 라운드의 오른쪽 입력값으로 설정하고, 왼쪽 입력값은 그 다음 라운드의 왼쪽 입력값으로 그대로 설정
- 5) 3) 과 4)의 과정을 10라운드 반복
- 6) 마지막 라운드 결과 값인 왼쪽 출력값과 오른쪽 출력값을 원래 평문을 구성하는 문자의 집합으로 변환하는 디코딩

자료 : 'ETRI, 블록암호에 기반한 FFX(radix)형태보존암호알고리즘의 성능비교, 한국통신학회' 재구성

- 내부함수 초기 벡터 값이 0인 CBC 모드와 매우 유사하며 트위 입력값에 카운터를 결합함
- 키 K, 평문 X, 트위 T를 가지며, 평문은 임의의 문자 Chars로 구성되고 평문의 길이는 $n = |X|$ 임
- 암호화되는 입력의 길이를 확장하기 위하여 Operationg Mode를 이용
- 형태보존 암호화 응용프로그램에서 충분히 사용할 수 있는 최대 2^{16} 블록까지 입력 값으로 사용 가능함
- Feistel 라운드 수는 8회 권장됨(FF1의 10라운드에 비해 처리 성능이 높음)

FF3 암호화 과정의 예 :

블록함수를 통해 세자리 십진수 평문을 암호화 하는 과정



자료 : 'ETRI, BPS 형태보존암호성능분석, 한국통신학회' 재구성

5 시사점

- 형태보존 암호화 방법인 FF1과 FF3의 암호화 구현은 NIST 암호화 알고리즘 검증 프로그램*을 참조하여 블록암호 운영방식에 관한 권고에 대한 준수 테스트가 가능함

* National Institute of Standards and Technology, Cryptographic Algorithm Validation Program (CAVP)

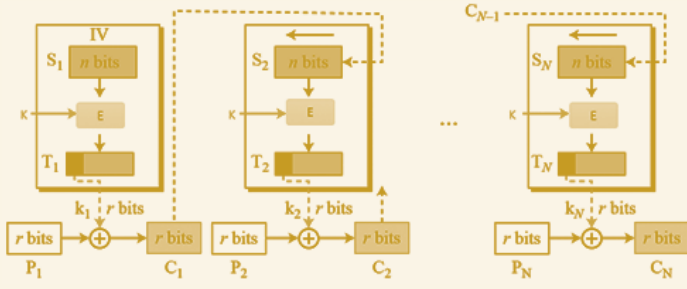
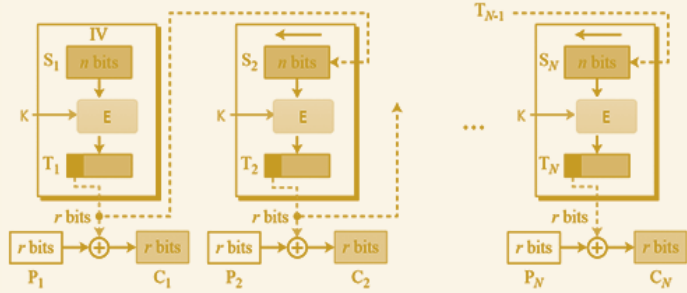
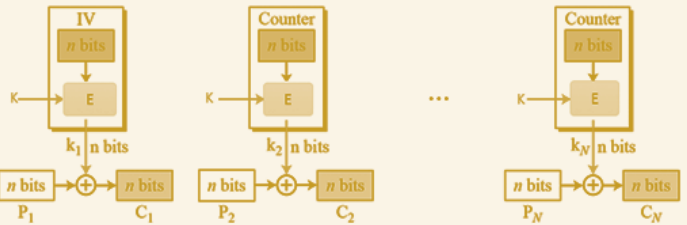
- 형태보존 암호 기법을 이용하면 평문 데이터와 같은 형태(길이, 형식)의 암호문이 생성되므로 속도가 빠르며 암호화로 인한 추가적인 저장공간과 DB의 스키마 변경이 필요 없는 장점을 지님

- 다만, 금융정보 보안이나 DB 암호화 분야에 활용 전 형태보존암호 알고리즘에 대한 취약성 및 안전성 검증*에 대해서 지속적인 연구 및 관심이 필요함

* 국가기관의 암호알고리즘에 대한 검증필암호모듈(KCMVP), 보안적합성 검증 등 보안성 검토 활용

6 [참조] 현대 블록암호 운용 방식(mode)

MODE	내 용
ECB	<ul style="list-style-type: none"> 한 블록의 평문은 한 블록의 암호문으로 암호화 됨 장점 : 간단, 고속, 병렬처리 가능 단점 : 평문 속의 반복이 암호문에 반영, 재생공격 가능 <p> E : Encryption D : Decryption P_i : Plaintext block i C_i : Ciphertext block i K : Secret Key </p> <p> 암호화 : $C_i = E_K(P_i)$ 복호화 : $P_i = D_K(C_i)$ </p>
CBC	<ul style="list-style-type: none"> 한 평문 블록이 암호화 되기 이전에 바로 앞 평문 블록의 암호문과 XOR되며 초기 벡터(IV) 사용 장점 : 평문의 반복은 암호문에 반영되지 않음 단점 : 비트 단위 에러가 있는 암호문 복호화 시 하나의 블록 전체와 다음 블록의 대응하는 비트에 에러가 발생 <p> E : Encryption D : Decryption P_i : Plaintext block i C_i : Ciphertext block i K : Secret Key IV : Initial Vector(C_0) </p> <p> 암호화 : $C_0 = IV, C_i = E_K(P_i \oplus C_{i-1})$ 복호화 : $C_0 = IV, P_i = D_K(C_i) \oplus C_{i-1}$ </p>
CFB	<ul style="list-style-type: none"> 평문과 암호문을 블록암호를 이용하여 암복호화하지 않고, n비트 쉬프트 레지스터의 값 S를 블록암호로 이용하여 암복호화 장점 : 블록 단위보다 작은 단위로 암호화 진행하며, 비트단위의 에러가 있는 암호문 복호화 시 평문의 대응하는 같은 위치에서 한 비트 오류 발생 단점 : 작은 블록 사이즈에 대해 블록암호의 암호화 알고리즘을 적용하기 때문에 CBC나 ECB에 비해 데이터 처리 효율성이 낮음 <p> E : Encryption D : Decryption P_i : Plaintext block i C_i : Ciphertext block i K : Secret Key IV : Initial Vector(S_i) T_i : Temporary register </p>

	 <p> $\text{암호화} : C_i = P_i \oplus \text{SelectLeftr}\{EK[\text{ShiftLeftr}(S_{i-1}) \mid C_{i-1}]\}$ $\text{복호화} : P_i = C_i \oplus \text{SelectLeftr}\{EK[\text{ShiftLeftr}(S_{i-1}) \mid C_{i-1}]\}$ </p>
OFB	<ul style="list-style-type: none"> CFB와 유사하나, 모든 암호문 블록의 각 비트는 이전 암호문 블록의 비트들과 독립적임 장점 : 암호문 블록 전송 도중 오류 발생시, 다음 블록의 비트에 영향을 주지 않음 단점 : 암호문이 임의로 변조 된다면 수신자가 복호화하는 평문에 영향을 줌 <p> <i>E</i> : Encryption <i>D</i> : Decryption <i>P_i</i> : Plaintext block <i>i</i> <i>C_i</i> : Ciphertext block <i>i</i> <i>K</i> : Secret Key <i>IV</i> : Initial Vector(<i>S₁</i>) <i>S_i</i> : Shift register <i>T_i</i> : Temporary register </p>  <p>OFB 모드의 암호화</p>
CTR	<ul style="list-style-type: none"> CTR이 암호화되며 모든 평문 블록마다 CTR은 다름 장점 : 패딩이 필요 없으며, 비트 단위의 에러가 있는 암호문을 복호화하면 평문의 대응하는 비트만 에러 발생 단점 : 능동적 공격자가 암호문 블록의 비트를 반전시키면 대응하는 평문 블록의 비트가 반전됨 <p> <i>E</i> : Encryption <i>P_i</i> : Plaintext block <i>i</i> <i>C_i</i> : Ciphertext block <i>i</i> <i>IV</i> : Initialization Vector <i>K</i> : Secret Key <i>K_i</i> : Encryption key <i>i</i> </p>  <p> $\text{암호화} : C_i = P_i \oplus E_K(\text{Counter}), \text{복호화} : P_i = C_i \oplus E_K(\text{Counter})$ </p>

타이젠(Tizen) 소개 및 특징 조사

조 현 호*

1. 개요	112
2. 타이젠 소개	113
3. 타이젠 구조 및 특징	114
4. 타이젠 보안	117
5. 결론	119

* 금융보안원 침해대응부 침해위협조사팀 (e-mail : hhcho@fsec.or.kr)

1 개요

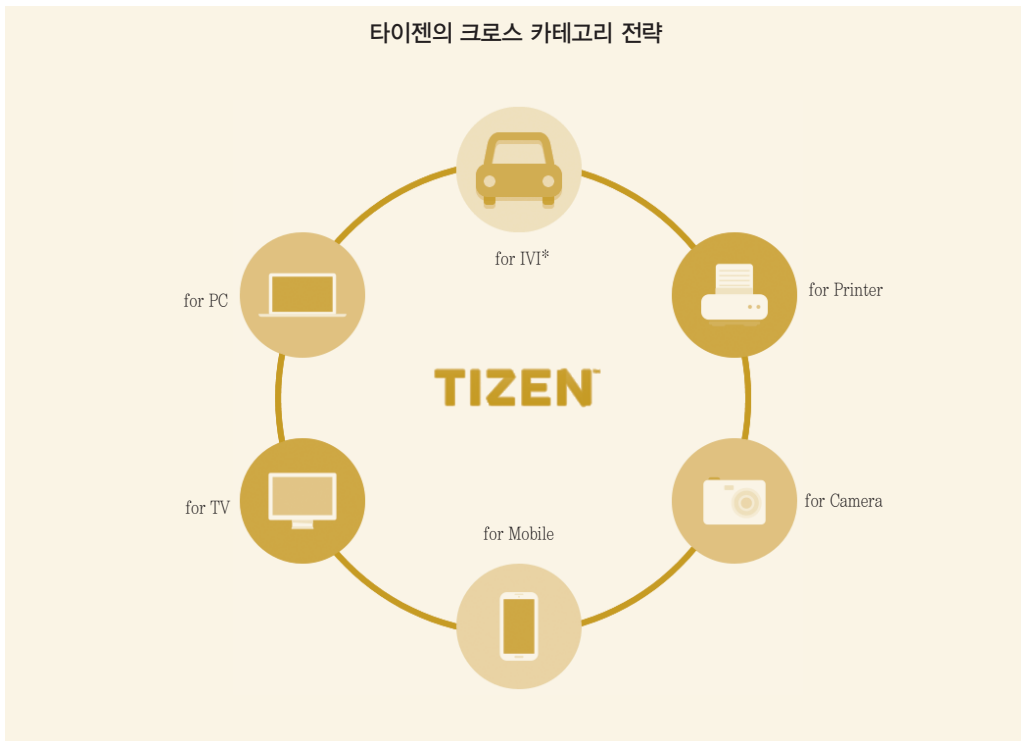
- 스마트폰, 스마트 워치 등 타이젠 운영체제를 탑재한 기기가 점차 출시되면서, 운영체제 점유율이 지속적으로 확대가 될 것으로 예상됨
- 본 보고서에서는 타이젠에 대해 소개하고, 특징 및 보안 기능에 대해 조사

2 타이젠 소개

- 타이젠은 리눅스 기반의 오픈소스 모바일 플랫폼인 LiMo*가 전신이며 삼성전자, 인텔, SK텔레콤, 도코모 등 제조사, 통신사가 공동으로 개발한 오픈소스 플랫폼

* LiMo : 리눅스 모바일(Linux Mobile)의 약자로 리눅스 기반의 모바일 폰 및 휴대용 기기를 위한 플랫폼으로 리모 재단(LiMo Foundation)에서 개발

- 2015년 9월 15일 타이젠 3.0이 공개되었으며, 스마트폰, 스마트워치, 카메라, 스마트TV 등 다양한 기기에 적용하는 것을 목표로 함



* in-vehicle infotainment(차량용 인포테인먼트) : 차 안에서 인터넷 검색, 영화, 게임, 네비게이션 등 다양한 엔터테인먼트 서비스를 제공하는 장치

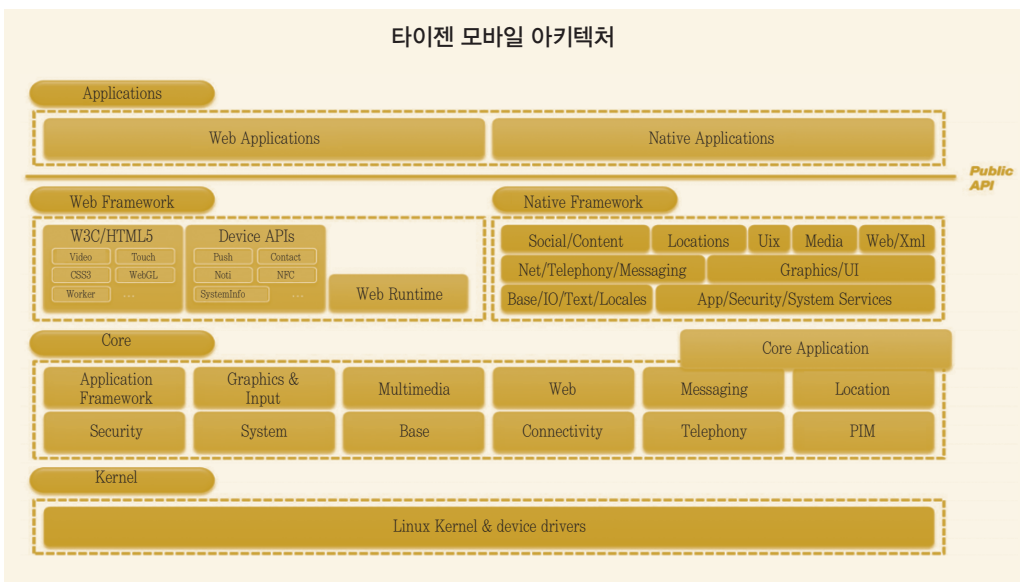
3 타이젠 구조 및 특징

- 타이젠은 누구나 프로젝트에 참여할 수 있는 오픈소스 플랫폼이며 아키텍처 및 구현 형태가 안드로이드와 유사함

타이젠, 안드로이드 환경 비교		
구분	타이젠	안드로이드
앱 개발 언어	HTML5/JS, C/C++	JAVA, C/C++
앱 배포 파일	웹 앱 : wgt 네이티브 앱 : tpk (권한, 코드 사이닝* 포함)	apk (권한, 코드 사이닝 포함)
샌드박스	UID, GID를 이용한 접근제한 커널 레벨의 Smack	UID, GID를 이용한 접근제한
커널	리눅스 커널	리눅스 커널
제조사	삼성, 인텔 등	구글

* Code Signing : 프로그램을 개발한 개인 또는 기업에서, 배포하는 프로그램이 본인의 것임을 증명하기 위한 수단

- 타이젠 아키텍처는 커널, 코어, 웹·네이티브 프레임워크, 어플리케이션으로 이루어져 있음



〈커널〉

- 타이젠 아키텍처의 가장 하위 단으로 리눅스 커널 및 각종 디바이스 드라이버로 구성되어 있음

〈코어〉

- 웹 프레임워크와 네이티브 프레임워크에서 공통적으로 사용하는 기능을 제공하며, 그래픽, 멀티미디어, 웹, 보안 등 다양한 오픈소스로 구성
- 서드파티 개발자에게는 공개되지 않아 제조사 및 타이젠 플랫폼 개발자만 Core API를 직접 사용할 수 있음

〈웹 프레임워크〉

- HTML 5 API, 비디오, 오디오 등 W3C 및 다양한 표준화 단체에서 정의한 표준을 제공하고, 표준에서 제공하지 못하는 부분을 채우기 위해 블루투스, NFC 등 디바이스 API 제공

〈네이티브 프레임워크〉

- 기존의 바다 플랫폼과 호환을 위해 구성되어 있으며, 네이티브 어플리케이션 개발을 위한 그래픽, UI, 입출력, 메시징 등 다양한 API 제공

〈어플리케이션〉

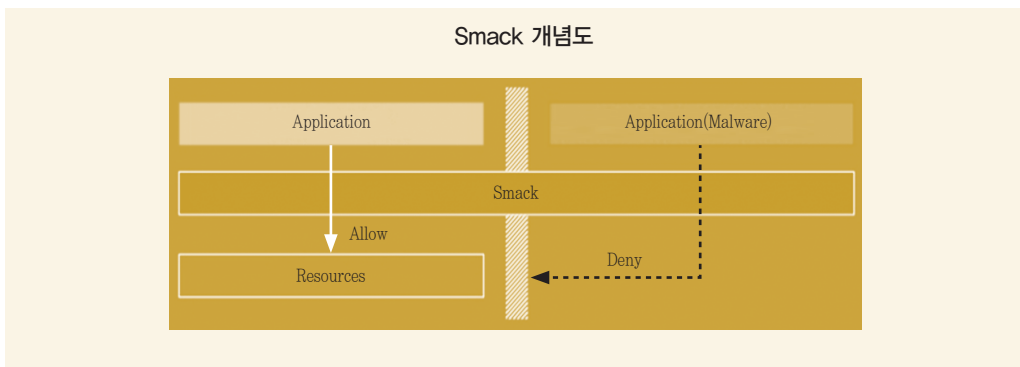
- HTML5 기반의 웹 어플리케이션 뿐만 아니라, C++ 기반의 네이티브 어플리케이션 형태로 개발 가능
- 웹 어플리케이션
 - (구조) wgt 확장자 구조, HTML, CSS, Javascript, config.xml 를 포함하고 있음
 - (특징) ① (쉬운 개발 및 높은 이식성) 개발이 상대적으로 쉬워 진입장벽이 낮고, 다른 기기나 플랫폼으로 이식성이 높음
 - ② (디바이스 API 지원) 웹 프레임워크에서 제공하는 디바이스 API를 이용하여 하드웨어 제어 가능
 - ③ (패키지 형태 배포) 웹 어플리케이션이지만 패키지 형태(wgt)로 배포가 가능하기 때문에, 타이젠 스토어에 등록 및 판매 가능

- 네이티브 어플리케이션

- (구조) tpk 확장자 구조, 바이너리, 리소스, manifest.xml 을 포함하고 있음
- (특징) 기존 바다 플랫폼을 지원하기 때문에, 변환 도구를 이용하여 어플리케이션 변환(바다 -> 타이젠) 가능

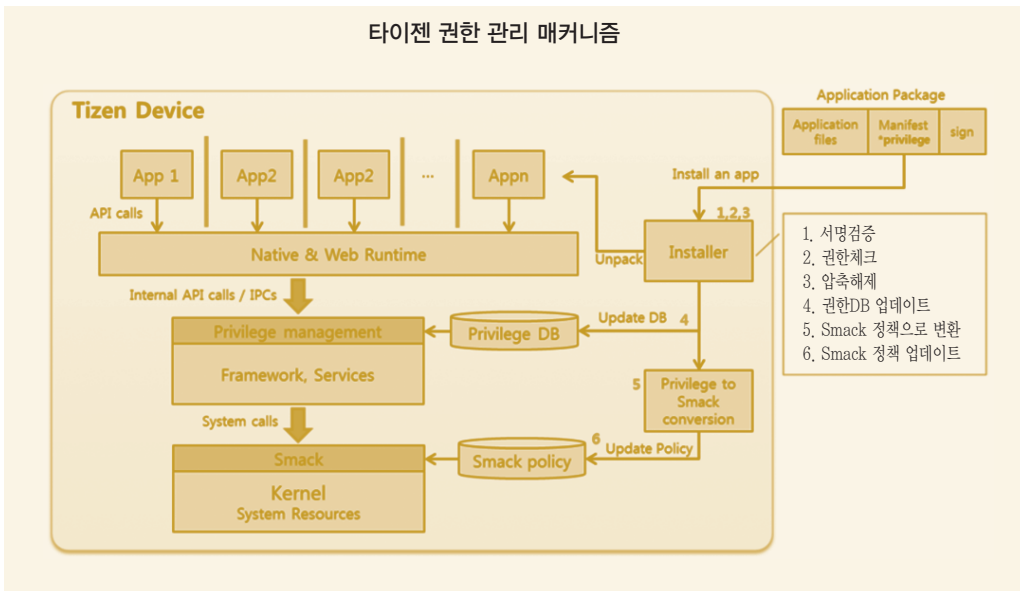
4 타이젠 보안

- (non-root applications) 구동되는 어플리케이션이 단일 유저권한으로 동작하고, 대부분의 daemon 또한 root 권한으로 동작하지 않음
 - 어플리케이션 취약점으로 인한 관리자 권한 획득 가능성 최소화
- (application sandboxing) 리눅스 커널 단에서 인가되지 않은 데이터 및 프로세스의 접근을 제어하는 Smack(Simplified Mandatory Access Control Kernel)을 적용
 - 스맥 룰(Smack-Rule)은 주체(프로세스), 접근대상(리소스), 액세스 타입(읽기, 쓰기, 실행 등)으로 구성되어 있으며, 주체가 접근대상에 대한 액세스 타입이 Smack 정책에 기록되어 접근 제어 기능 수행



- (Content Security Framework) Anti-Virus 솔루션을 내장하여 보안 관련 기능을 API 형태로 제공
 - 데이터, 어플리케이션의 악성 행위를 탐지하거나, 악성 URL 탐지 및 차단 등 기능 수행
- (Privilege) 어플리케이션이 사용하는 권한이 manifest.xml(네이티브 어플리케이션), config.xml(웹 어플리케이션)파일에 정의됨
 - ※ 안드로이드의 AndroidManifest.xml에 어플리케이션의 퍼미션을 정의하는 것과 유사한 형태

타이젠 권한 관리 매커니즘



- (보안 취약점) 타이젠 관련 보안 취약점은 2012년 IVI(in-vehicle infotainment) 기기와 관련된 정보노출 취약점이 공개되었고, 이후 추가적인 취약점 공개는 없으나 최근 스마트폰, 스마트워치 이용자 증가로 취약점 공개가 활성화 될 것으로 예상됨

취약 수준	Medium	CVE-ID	CVE-2012-6459
내용	Connman 은 임베디드 장비에서 인터넷 접속을 관리하기 위한 데몬으로, 오프라인 모드 (offline mode)가 "ON"으로 설정되어도, Bluetooth 서비스를 중단하지 않는다. 공격자가 취약점을 이용해 Bluetooth 패킷을 통해 중요 정보를 획득할 수 있다.		
영향을 받는 버전	Connman 1.3	관련 링크	http://www.cvedetails.com/cve/CVE-2012-6459/

5 결론

- 타이젠 운영체제는 아직 국내 점유율은 높지 않지만, 위치뱅킹 등 일부 디바이스를 대상으로 서비스가 출시되어, 이용자는 타이젠 기반의 금융서비스를 이용하고 있음
- 타이젠 운영체제는 안드로이드와 구조가 유사하여, 안드로이드에서 발생 했던 보안 위협이 타이젠에서 동일하게 발생하거나, 알려지지 않은 신규 위협이 추가로 발생할 수 있기 때문에 이에 대한 지속적인 연구 필요

전자금융과 금융보안 관련 전문가 기고 안내

전자금융과 금융보안 관련 기술·제도·정책 등의 연구 자료를 제공하기 위해 간행물 형태로 금융회사, 금융당국 및 유관기관에 배포하고 있습니다. 해당 간행물을 통해 금융권의 현안, 논평, 시사점 등 다양한 사안에 대해 공유하고 발전방향 등을 함께 모색하고자 전문가 기고를 안내하오니 여러분의 많은 참여 부탁드립니다.

1 모집분야

- 전자금융 및 금융보안 관련 현안사항(정책 및 기술) 및 시사점 등

〈 전자금융 및 금융보안 관련 연구(안) 예시 〉	
분야	전자금융 및 금융보안 관련 연구(안) 예시
보안 정책·관리	국내외 전자금융과 금융보안 관련 법률 및 제도 개선방안, 자율규제 방안 등
인증·암호기술	전자금융 신 인증기술 연구, 금융부문 암호기술 보안성 연구 등
서비스·응용SW 보안	스마트 결제 서비스 보안 기술, 금융 SW 시큐어 코딩 방안 등
모니터링·네트워크 보안	금융사 APT 대응 방안, 이상거래탐지시스템 기술 연구, 금융회사 망분리 방안 등
스마트 기기·차세대 보안	스마트 단말 보안 강화 기술, 금융부문 빅데이터 분석 기술, 금융권 클라우드 보안 등

2 기고신청

- (제출 항목) ① 기고자명 및 소속(기관 및 부서명), ② 원고제목, ③ 목차, ④ 요약내용(A4 1매 이내)
※ 선정 이후 작성해야 할 원고분량은 A4용지 15~20매 내외(폰트 12 등)입니다.

- (제출 시기) 상 시

- (제출처) 금융보안원 보안연구부 보안기술연구팀

e-Mail : research@fsec.or.kr Tel : 02-3495-9723

3 기타

- 수록된 원고에 대해서는 금융보안원의 지급기준에 따라 소정의 원고료 지급
- 선정된 주제에 대해 접수 후 2주 이내 별도 안내
※ 기고신청 건은 선정되지 않을 수 있습니다.

전자금융과 금융보안

발 행 2016년 7월

발 행 인 허 창 언

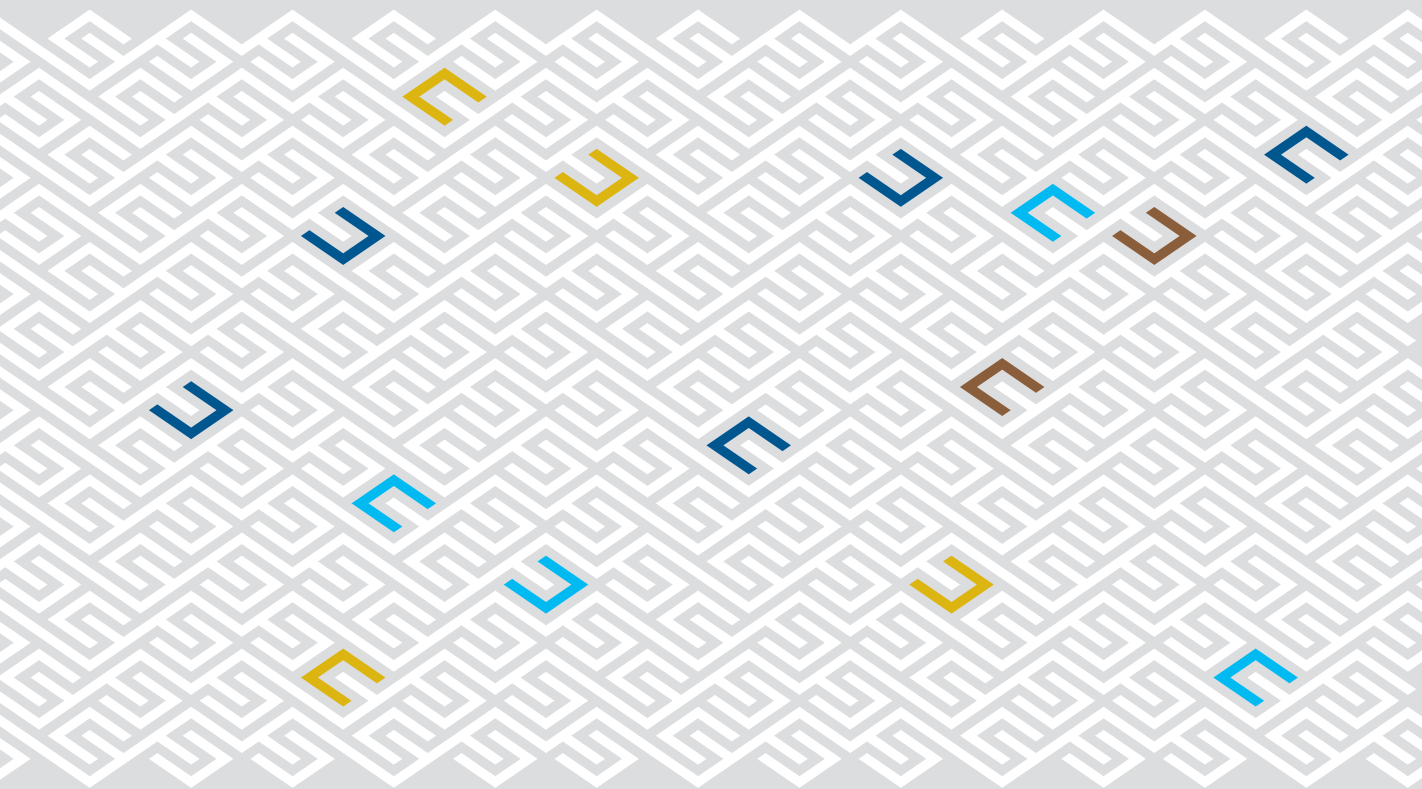
발 행 처 금융보안원

주 소 경기도 용인시 수지구 대지로 132

(비매품)

본 문서의 내용은 금융보안원의 서면 동의 없이 무단전재를 금합니다.

본 문서에 수록된 내용은 고지없이 변경될 수 있습니다.



금융보안원
FINANCIAL SECURITY INSTITUTE

전자금융과 금융보안 | 제5호