핀테크 시대의 보안기술

금융보안원

유재필 (jpyoo@fsec.or.kr)

2015. 07. 08

목 차

Ⅰ 핀테크 정의 및 동향

Ⅱ 보안 패러다임 변화과 주요 기술

Ⅲ 결론

Ⅰ 핀테크 정의 및 동향

정의 및 발전단계

▶ (정의) Financial + Technique

- 금융서비스(결제, 송금, 투자, 대출 등)와 IT기술의 결합
- (舊)금융전산화→(現)'혁신 IT 기술적용', '소비자 중심 서비스'의 이미지

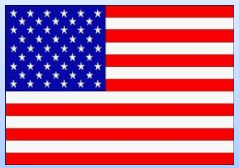
분야	정의	키워드
광의	• 금융서비스를 지원하는 모든 IT행위	• 서버단 전산화, • IT기술이 금융서비스를 지원 • SI 작업, 시스템 도입
협의	• 혁신IT기술을 금융서비스에 적용, 새로운 가치 창출	• IT기술이 사용자 서비스까지 확대 • IT기술에 금융서비스가 내재 • IT혁신 기술 도입

▶ (기폭제) 국내외 환경이 상이

- 해외 : 글로벌 금융위기→ 금융경쟁력 확보
- 국내 : 천송이 코트 논란→ 금융IT이용환경 개선→ 보안 문제?

참고 : 주요국 추진동향

▶ (미국) 창업기업, 혁신기술을 기반으로 하는 自生的 핀테크 산업기반



(특징) 혁신기술 중심, 타국에 비해 상대적으로 창업기업이 많음

(주도자) 서부*(실리콘벨리, 기술중심)와 동부**(뉴욕, 금융서비스 중심)로 이원화

(원동력) 혁신적 기술기반, 강력한 창업기반, 산업육성 규제기반

▶ (UK) 글로벌 금융리더십 탈환을 위해 정부가 적극 견인(民官 공동협력)

(특징) 계획도시 중심의 핀테크 산업 육성(런던의 테크시티)

(주도자) 금융권이 주도하여 개발 및 투자, 정부는 컨트롤타워 역할

(원동력) 정부 및 금융권의 강력한 추진의지

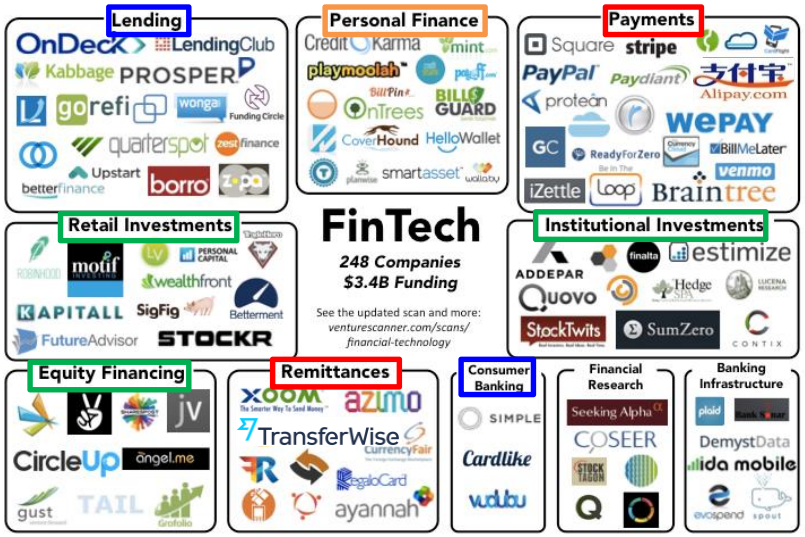
▶ (중국) 국영은행에 대한 대안금융을 통해 금융서비스 경쟁력 제고

(특징) BAT(Baidu, Alibaba, Tencent)를 중심으로 인터넷 기반 종합 금융서비스 제공

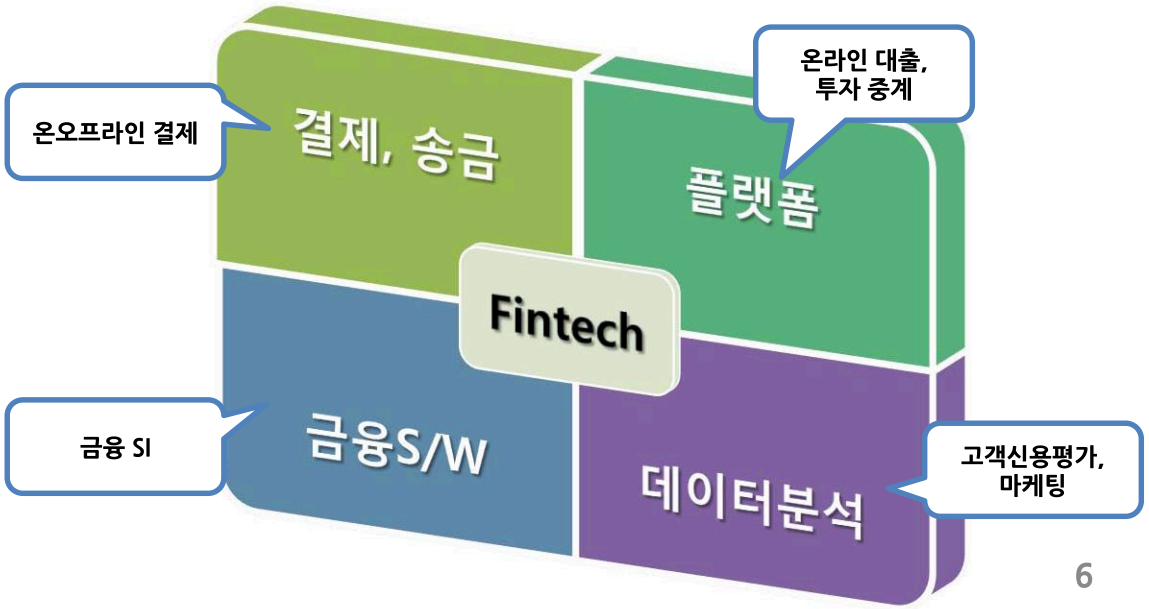
(주도자) 대형 IT업체(민간) 주도, 정부는 先산업, 後규제로 경쟁유도

(원동력) 거대소비 시장, 정부의 추진의지(IT산업활성, 금융경쟁촉발)

주요 서비스 분야



▶ 서비스 별 (미국 Venture Scanner)



▶ 적용 영역별 (영국 무역청)

II 보안 패러다임 변화와 주요 기술

국내 핀테크 보안 요구사항

▶ 금융보안 환경변화에 대한 대응방향을 의미

① 이용자 편의 증대

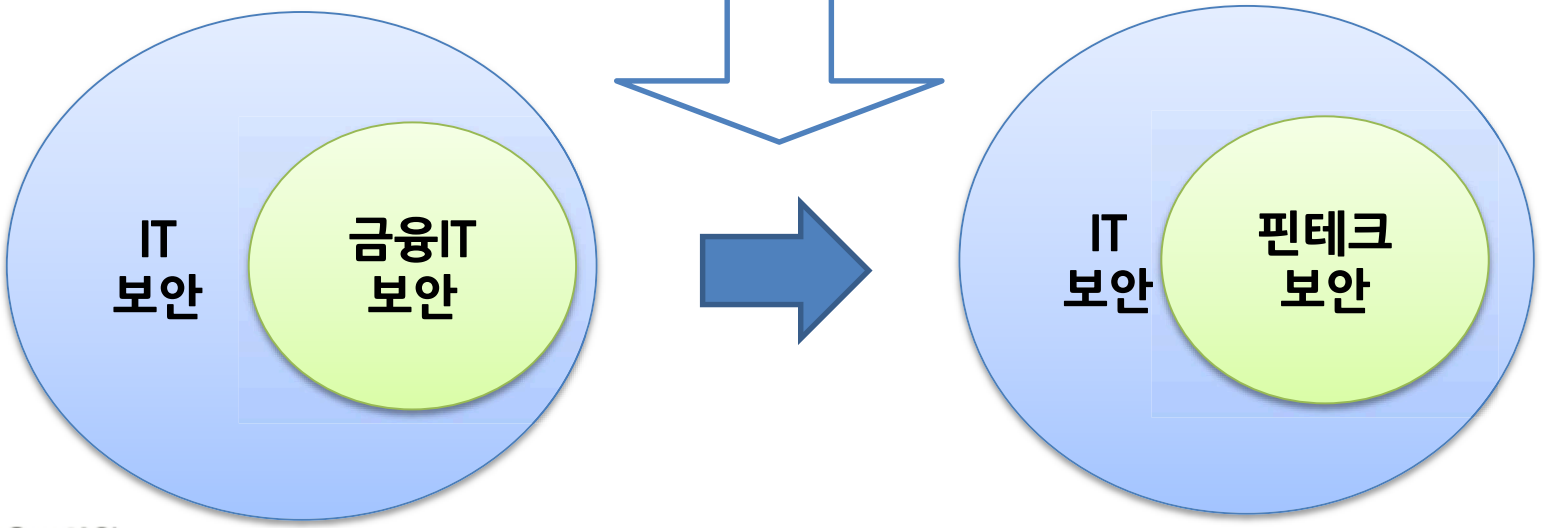
- 간편중심 결제환경, 온라인 플랫폼 화

② 글로벌 표준 지향

- 액티브X, 공인인증서 대체방안 마련

③ 비즈니스적 관점의 보안접근(Risk Management)

- 기술, 정책의 조화를 통한 피해최소화, 이익 극대화



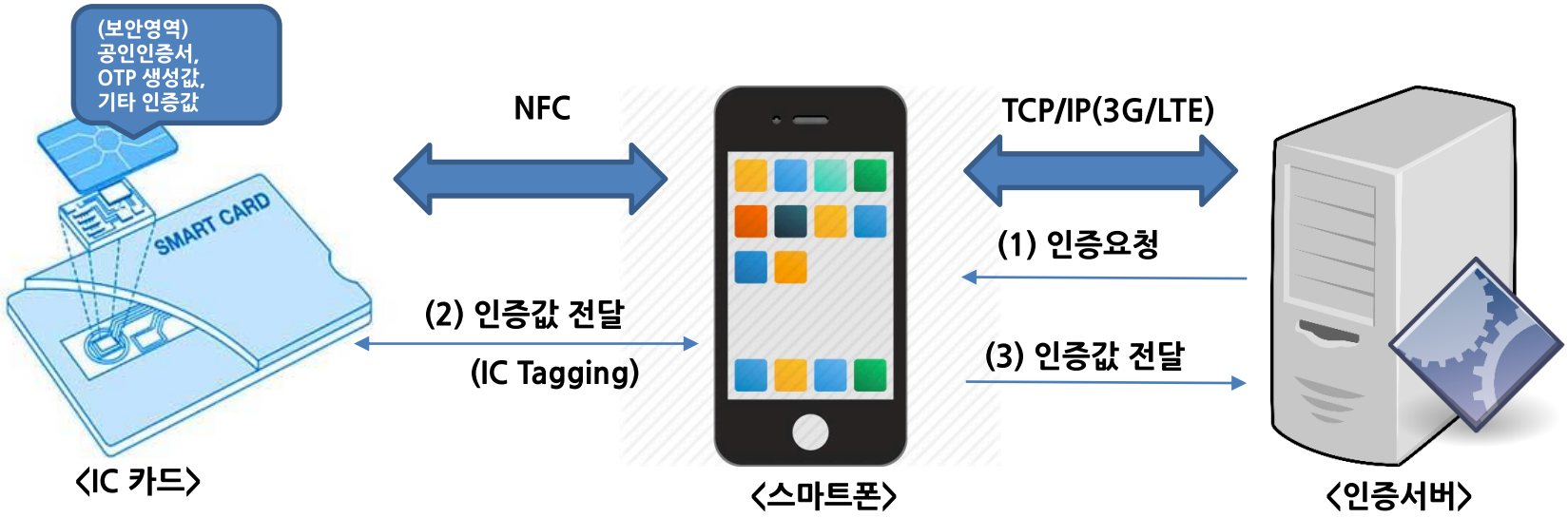
핀테크 보안 서비스 분야별 핵심고려 사항

구분		결제	뱅킹	투자/대출
비보안	통신	NFC(결제정보전달) BLE(결제인증) MST(결제정보전달)	NFC(본인인증)	
	생체인식	지문, 정맥, 음성 , 필기, 얼굴 등		→
	S/W		OPEN API 금융 SI (인터넷전문은행)	
	데이터분석	빅데이터(마케팅, 부정거래감시)		빅데이터(신용평가) 빅데이터(투자정보분석)
보안	인증	IC Tagging 생체인증 규격(FIDO 등)		→ →
	데이터보호	TEE(단말) 토큰화(네트워크)	→ →	
	모니터링	FDS(고도화)	FDS(구축)	FDS(구축)

IC Tagging

▶ IC카드 內 인증정보를 스마트폰을 통해 서버에 전달하여 인증처리

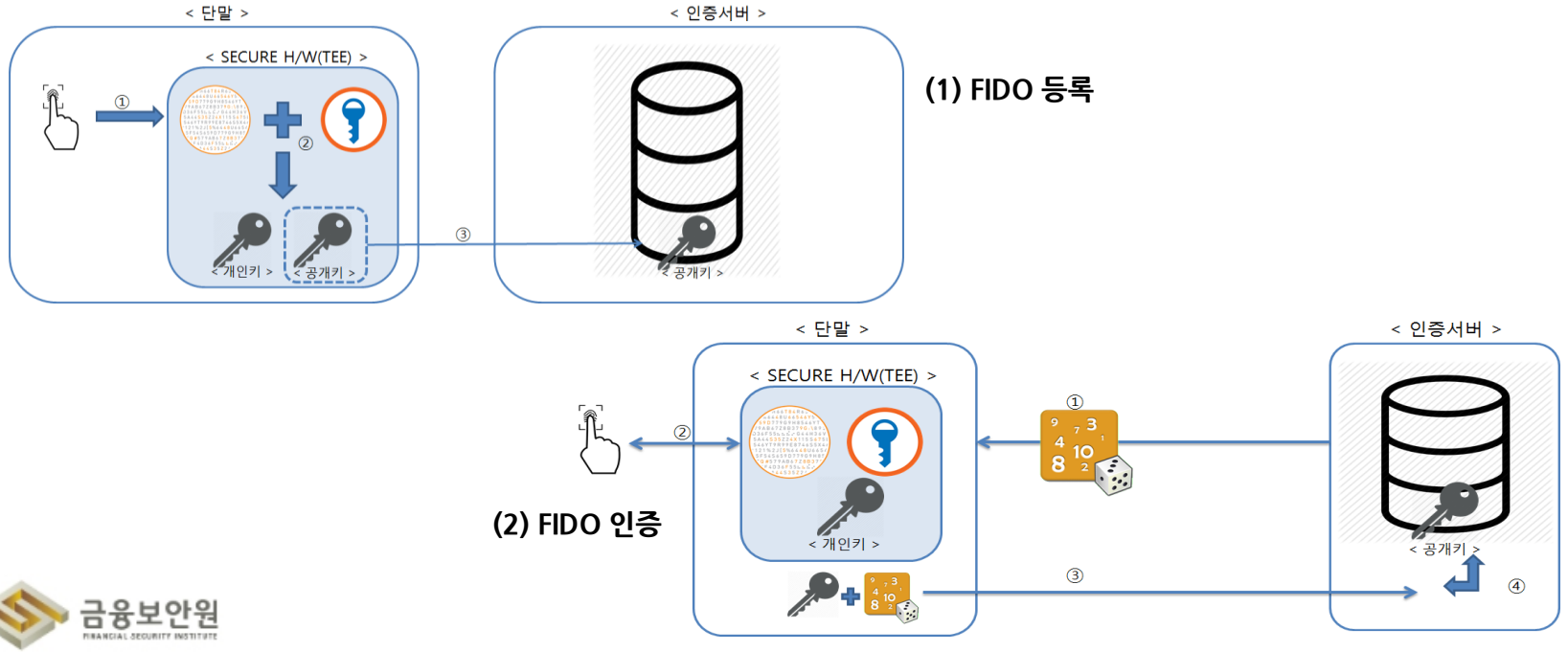
- (기능) IC카드(정보저장), 스마트폰(정보전달)
- (특징) 소유기반, 비설치형(모바일 기반)
- (구분) 기존카드 호환형(후불교통카드), 신규 발급형(Applet)
- (적용) 공인인증서, OTP



생체인증(FIDO： Fast IDentity Online)

▶ 사용자의 고유한 신체구조 및 행위에 기반하여 인증하는 방식

- (구분) 생체기반(지문, 홍채, 정맥, 심박), 행위기반(서명, 걸음걸이 외)
- (특징) 비설치형, 사용자 편의 대폭 개선
- (보안) 유노출의 위험성(불변의 정보)
- (규격) FIDO(비대칭키 구조) vs 서버 분산 저장

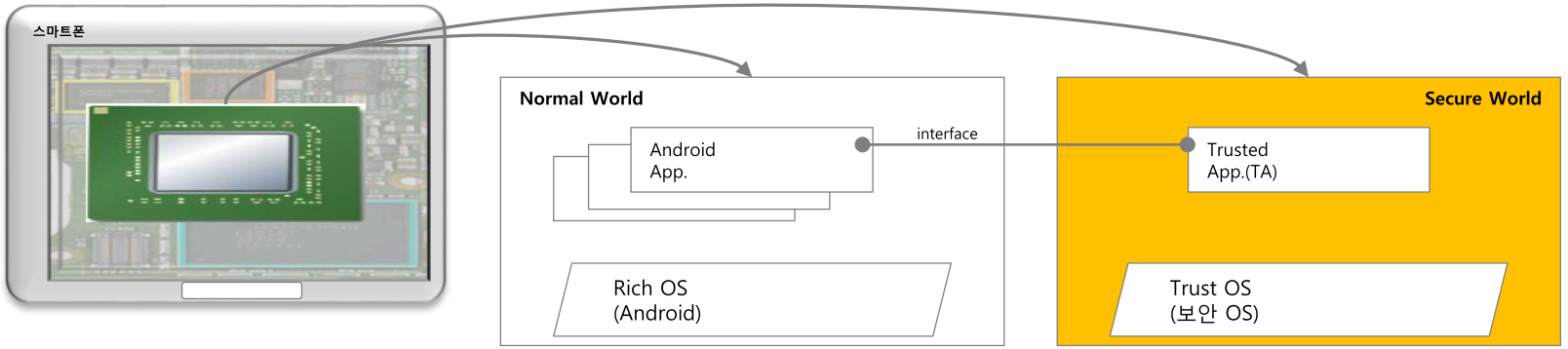


TEE (Trust Execution Environment)

▶ 모바일 AP를 Normal영역(일반응용)과 Secure 영역(보안응용)으로 구분

- CPU내 SE(Secure Element)인 TZ를 기반으로 하는 Secure OS, 앱 운영 환경
- (적용) 스마트폰 단독 OTP, 생체인증 기기등으로 활용
- (이슈) 인프라 보급(지원 단말) 이 관건, 제조사 의존적

- TZ (지문정보, 마스터 키 등 핵심 Credential 저장)
- TEE (TZ를 기반으로 하는 Secure OS, 앱 운용 환경),
- TUI (입출력 보호), TA(Secure World에 올라가는 앱)



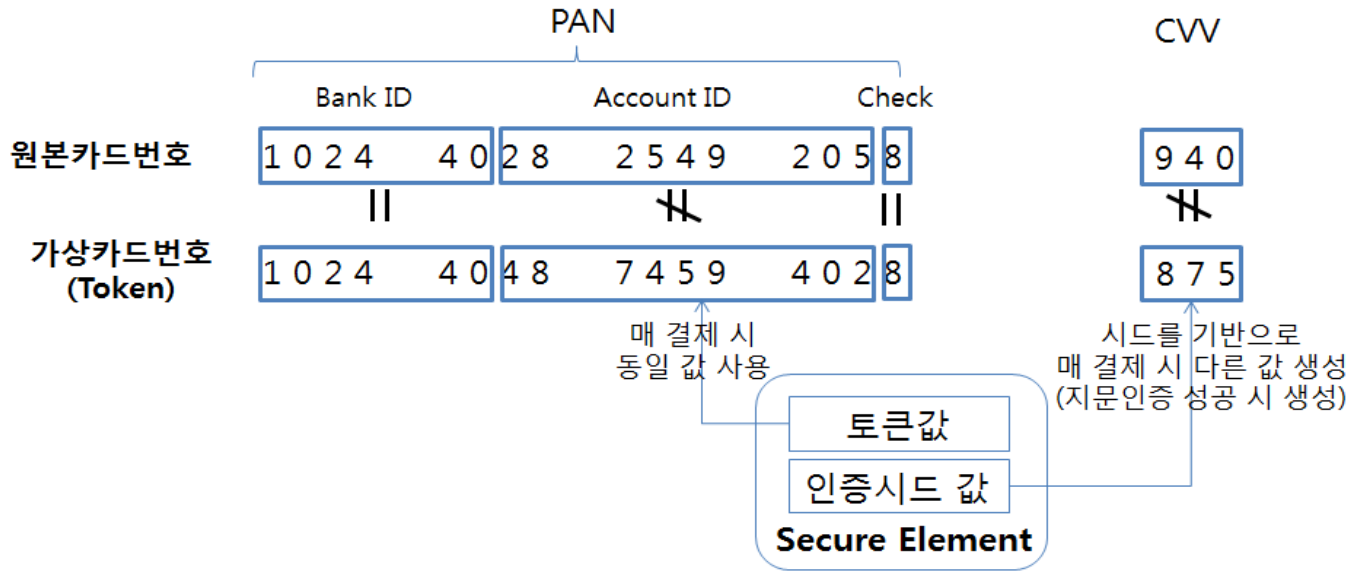
o (입출력 값 보호) 결제 비밀번호, 계좌번호, 송금액 등을 TEE 환경에서 구동함으로써 입력 값 탈취 방지 및 화면 캡쳐 방지 가능

o (거래내역 무결성 제공) 보안영역의 암호화 키 등을 이용하여 암호화 처리하여 금융사 서버까지 거래내역 무결성 제공

토큰화 (Tokenization)

▶ 결제 시 가상의 카드번호를 이용하여 정보 유노출에 대응하는 기술

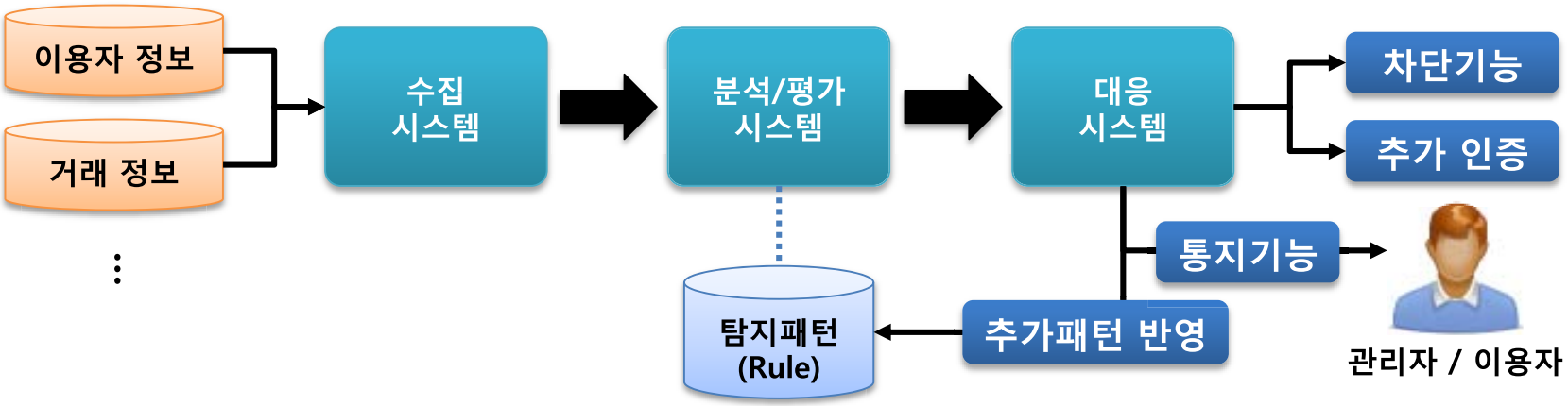
- 매 거래 시 1회용 검증값으로 거래를 검증
- 검증값 생성위치 : 로컬 VS 서버(HCE)
- 삼성페이, 애플페이 등 모바일 월렛형 결제 서비스에 활용



FDS (Fraud Detection System)

▶ 구성 요소와 주요 기능

- 다양하게 수집된 정보를 종합적으로 분석, 이상금융거래 유무를 판별
- 4가지 기능 (정보 수집, 분석 및 탐지, 대응, 관리/운영 및 감사)으로 구성
- 기술적 문제가 아니라 운영의 문제로 접근 필요
- 시장이슈 : 정보공유체계



Ⅲ 결론

이용자 편의 개선

▶ 기존 (거래 보안수준을 높이기 위해 결제, 뱅킹 서비스등에 설치형 S/W사용)

구분		용도
인증	공인인증서	사용자 인증, 전자서명(부인방지)
클라이언트 보안	키보드 보안	키보드 입력 중요데이터 암호화 및 위/변조 방지
	백신	악성코드 검색 치료
	방화벽	실시간 해킹차단

▶ 문제점

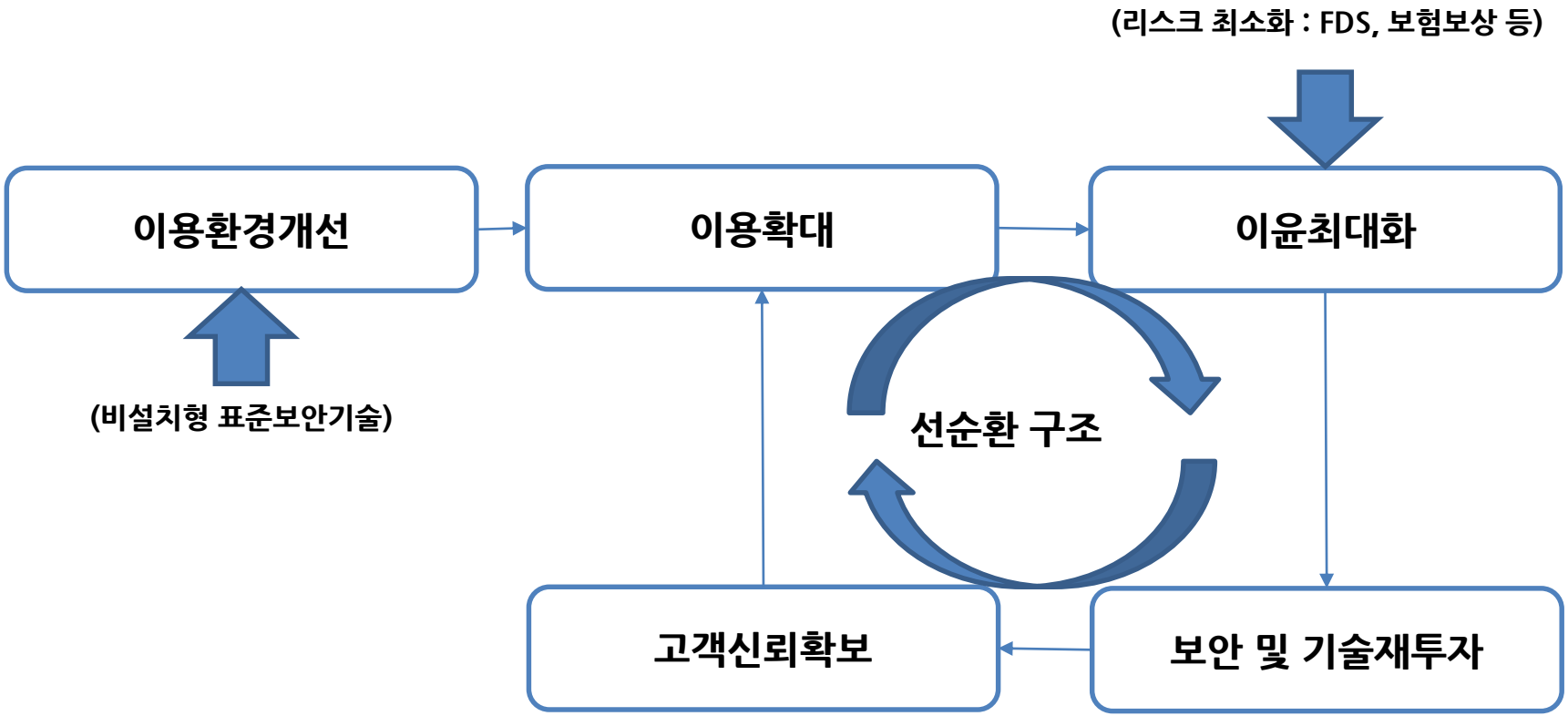
- 플러그인 형식으로 구현되어 결제편의 저하(정보초기화, 충돌, 모바일 미 대응)
- 해킹 기법의 고도화, 지능화로 보안 S/W우회 가능성 높아짐

▶ 해결방안

- 편의 인증(바이오 등) 도입
- 정책적 보안으로 피해 최소화(이체 및 결제한도)
- 서버단 보안솔루션(FDS)으로 약해진 사용자단 보안 기술 보완

보안에 대한 시각 변화

▶ 보안의 시각 : 방어 → 관리를 포함하도록 확장 필요



결론 및 시사점

▶ (전망) 금융IT 융합으로 금융보안 패러다임의 근본적 변화 발생

- 사전보안(사용자)에서 사후보안(서버)으로 보안의 패러다임이 이동

- 인증기술의 다양화, 기술의 중립화가 활발

▶ (방향) 보안은 기본이자 필수, 편의를 위해 희생하는 것이 아니라 효과적으로 강화하기 위해 방법의 전환이 필요

- (결제) 간소화 사전인증 + 강력한 FDS 운영 + 필요 시 추가인증

- (뱅킹) 간소화 사전인증 + FDS + 피해최소화 송금정책*

* 최소 송금자 상대자, 큰 규모의 거래액등에 대해 추가인증, 지연이체, 거래액에 상한선 등을 도입

- (사용자 선택) 보안 방식 및 절차 관련 사용자에게 선택권 부여, 사용자는 전자금융거래 시 보안위협을 충분 시 인지하고 이용

감사합니다

Q&A