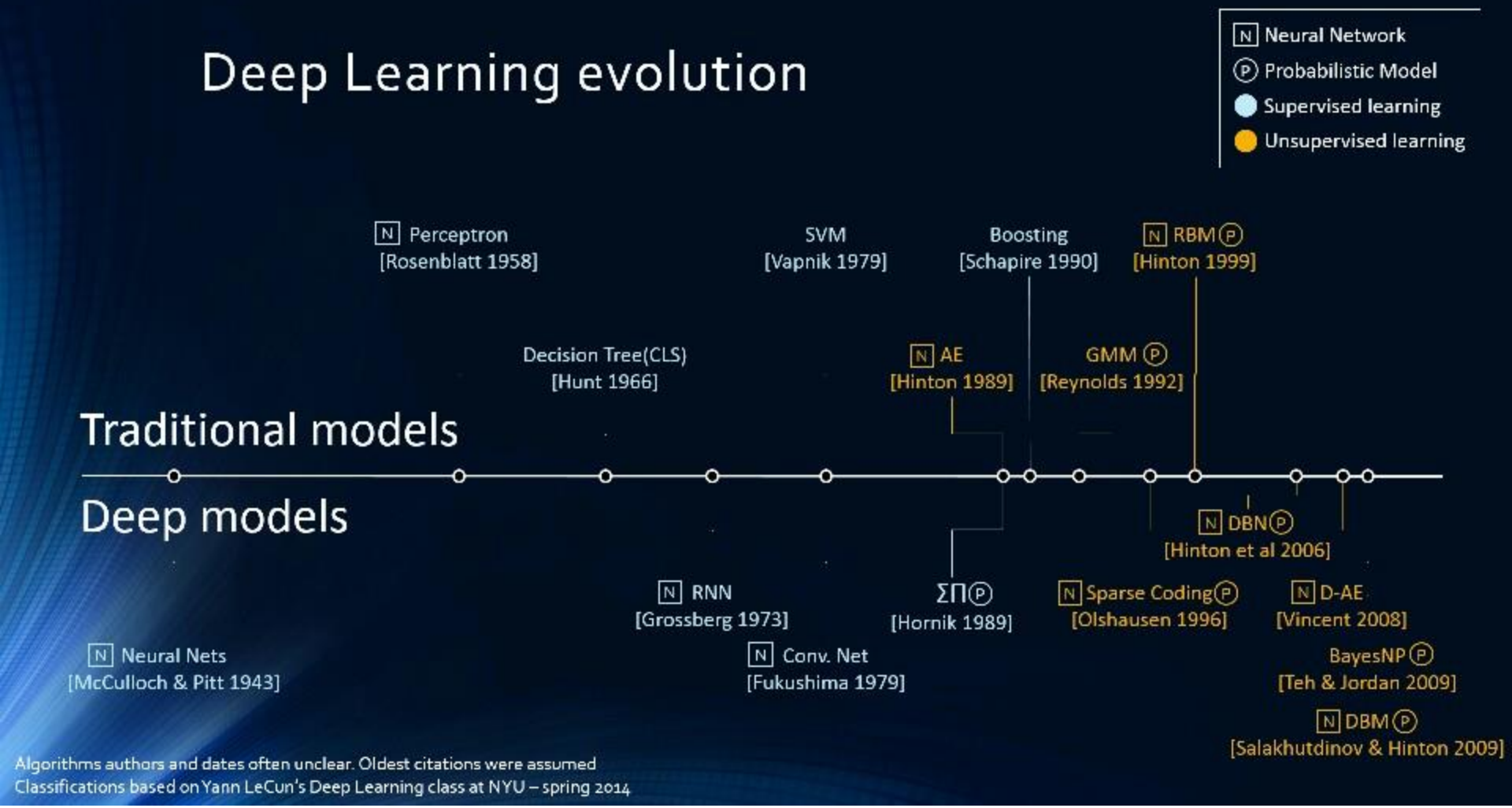


"Financial Security" – Now and Future

('Security' – Now and Future, Regulation & Business & Risk)

2016.8.18 Jason, M

Contents

AGENDA

P2P 이체

삼성페이

Password Stress

지문/홍채

공인인증서 고찰
금융회사의 아이티 능력 – 디비설계/로직분석력 보유?
데이터기반 보안 필요? - 비용/편익? 이게 다일까?
대고객접점 - 기기우선 - 삼성페이 P2P - 대적할 방법은?
1년이상 장기 미이용고객 인터넷 회원정보
신용정보 이용조회 시스템
이메일 보안
CAPTCHA, BF Attack

소송 시 고객 패소 원인/비율

SMS인증

MBP

전용회선

보안프로그램

망분리

1. Electronic Financial Transaction Business & Risk Management & Regulations

MBP

Moderate

적당히 나쁜 사람(Moderately Bad Person·MBP)' - 김화진 서울대 교수
- 자본주의 경제에 참여하는 평균적인 부정적 인간형을 MBP로 규정
- MBP들이 잘못 행동하는 것을 근절하기 위해 모든 곳에 폐쇄회로TV를 설치해 감시할 필요는 없다
- MBP들은 근본적으로는 선량하고 소심한 사람들

법학에는 '평균인' '선량한 관리자의 주의의무' '건전한 상식' 등의 개념이 판단 기준으로 사용

http://mnews.joins.com/article/20453128

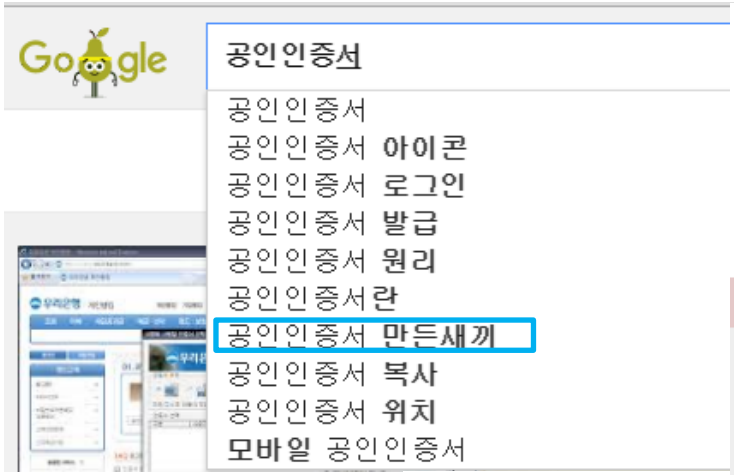
Q : 안전하게 하는것만이 정답인가?

"적당히 나쁜 사람은 자신이 크게 선하지 못하다는 것을 알지만 철저하게 나쁜 사람은 자신이 괜찮다고 생각한다
(A moderately bad man knows he is not very good: a thoroughly bad man thinks he is all right)."
기독교 사상가 C.S. 루이스

. 구글의 종전 슬로건 '사악해지지 말자(Don't be evil)'에도 이윤 추구 과정에서 누군가에게 나쁜(bad) 짓을 할 가능성이 높음은 부인할 수 없지만 최소한 사악(evil)해지지는 않도록 노력하자는 **내적 갈등**

http://mnews.joins.com/article/20453128

*...M M(Manager) Level Risk



최근 스미싱·피싱·파밍 등 전자금융사기 수법의 진화에 따라 공인인증서 파일을 비롯한 개인정보의 유출이 급증하고 있습니다.

이에 따라 공인인증서 이용고객의 2차 피해를 예방하기 위해 공인인증서 이용 안전성 강화의 일환으로 **공인인증서 비밀번호 설정 규칙을 다음과 같이 강화**하오니, 불편하시더라도 양해하여 주시기 바랍니다. **(시행시기 : 2014년 9월말부터)**

비밀번호 설정 규칙 강화

(규칙1) 숫자, 영문, 특수문자 반드시 포함
※ 고객 혼선 방지를 위한 특수문자 4종(‘ ” ₩ |) 제외
※ 영문 대소문자 구분 기능 추가

(규칙2) 공인인증서 비밀번호 설정 시 **최소 자릿수 증가(8→10자리)**

[공지][완료] [개인정보ㄴ

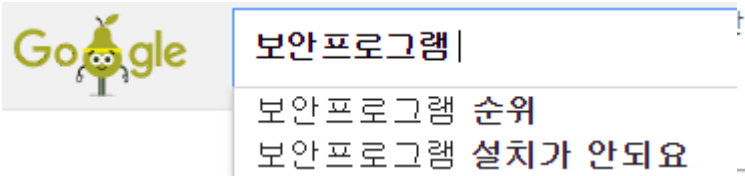
Lineage

리니지 고객님. 안녕하세요.

8월12일 정기점검 이후 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 따라
1년 이상 미이용(미접속)한 회원의 개인정보는 분리 저장·관리 됩니다.

'장기 미이용 계정'으로 전환이 되더라도 Plaync 아이디와 비밀번호로 로그인을 하시면
'장기 미이용 계정' 복귀 신청이 가능합니다.

안전한 개인정보보호와 건전한 게임문화 조정을 위해 항상 최선을 다하도록 하겠습니다.



M...* C Level Risk

Google 인터파크 해킹

전체 이미지 뉴스 동영상 지도 더보기 검색 도구

검색결과 약 467,000개 (0.39초)

[단독]인터파크 고객정보 1000여만건 유출...경찰, 해킹 혐의 수사 착수 ...
news.khan.co.kr/kh_news/khan_art_view.html?artid=201607251546001&code...
2016. 7. 25. - 경찰은 해킹 세력이 인터파크 직원에게 악성코드를 심은 e메일을 보내 해당 PC를 장악한 것으로 추정하고 있다. 전산망을 공유하는 회사에서는 ...

인터파크 해킹 관련 이미지 이미지 신고

인터파크 해킹에 대한 이미지 더보기

인터파크, 해킹당해 1000만 명 고객 정보 유출됐다 - 허핑턴포스트
www.huffingtonpost.kr/2016/07/26/story_n_11189998.html
2016. 7. 26. - 인터넷 쇼핑몰 인터파크가 해킹을 당해 1000여만명의 고객정보가 유출돼 경찰이 수사에 들어갔다. 인터파크는 2300여만명의 가입자를 보유한 ...

Society
Level Risk

M(Manager)
Level Risk

C(CEO, CISO..)
Level Risk

BigPicture

법률(法 律)	Act
대통령령(大 統 領 令)	Presidential Decree
총리령(總 理 令)	Ordinance of the Prime Minister
부령(部 令)	Ordinance of the Ministry of (부처명)
시행령(施 行 令)	Enforcement Decree
시행규칙(施 行 規 則)	Enforcement Rule
조례(條 例)	Municipal Ordinance
규칙(規 則)	Municipal Rule

1. 법인의 목표 – 이익(사회의 수준) -> 사회(금융소비자의 피해) 발생 -> 법규제 강화 -> 보안관련 이슈 발생 -> 보안을 법의 영역으로 포함시킴 (2000년 초반 이후 15년) & 보안사고의 피해는 사회의 몫
2. 보안준수노력에 의한 소비자 피해(편의성) & 법인의 경쟁력 감소 공감 -> 자율보안체계로 전환노력
3. 금융 서비스 미래
   a. 글로벌 경쟁력 감소에 의한 소비자의 금융서비스 직구매 예상(~2020년) – 국제 경쟁력 확보 차원 검토필요
   b. 보안은 안전/위험의 이분법적 결정이 아닌 리스크(비용/편익)의 관점으로 판단할 필요
   c. 전통적 금융회사는 대응비용 (IT 및 신기술 분석 능력 낮음)이 매우 크게 작용하였음
   d. IT비용이 낮아지는 상황(PC, 모바일기기, 오픈소스, 클라우드컴퓨팅, AI, 블록체인, 가상화폐 등)과 IT기반 서비스로 전환되는 상황에서 수익>0 인 사업자가 등장할 가능성 커짐

(인가심사기준) 은행업감독규정상 **은행업 인가심사기준**을 기본적으로 적용
-인터넷전문은행 **도입취지**에 부합되도록 **다음 사항**을 인가심사시 **중점적으로 고려**

(1) **사업계획의 혁신성(Innovation)**

- **기존 금융관행**을 **혁신**하고 **새로운 서비스**를 **제공**할 수 있는지 여부
- **기존 은행시장**을 보다 **경쟁적으로 변화**시킬 수 있는지 여부

(2) **주주구성과 사업모델의 안정성(Stability)**

- **충분한 출자능력, 건전한 재무상태** 및 **사회적 신용**을 갖춘 **주주**로 **구성**되고 **지속가능한 사업모델**을 갖추었는지 여부

(3) **금융소비자 편익 증대(Consumer Convenience)**

- 다양한 **금융서비스**를 금융소비자에게 **더 낮은 비용이나 좋은 조건**으로 제공할 수 있는지 여부
- 소비자가 **점포 방문**을 **하지 않고도 편리**하게 금융서비스를 이용할 수 있는 **시스템 구축** 여부

(4) **국내 금융산업 발전 및 경쟁력 강화에 기여(Competitiveness)**

- 차별화된 금융기법, 고객별 맞춤형 서비스 제공 등을 통해 **금융산업 부가가치**를 **제고**시키고 **신규 일자리**를 많이 **창출**할 수 있는지 여부

(5) **해외진출 가능성(Global Expansion)**

- 국내 시장에서의 경쟁 뿐 아니라 아시아 등 **해외시장 진출**을 고려한 **사업계획과 실천능력**을 가지고 있는지 여부

출처 : IT. 금융 융합 및 신성장동력 창출을 위한인터넷전문은행 도입방안 `15.6 금융위원회

Digital Only – 경쟁의 대상은 글로벌
규제(대륙법 기반 – 현재사회에 후행) - 글로벌 경쟁력 확보 불가

Q : 글로벌 온라인 혁신을 위한 방향은?
- (예측) 규제 혁신 불가 (정부규제는 사회(기업)를 위한 Support 개념으로 전환필요)
- (현황) 후진적 규제에 따른 기업 내 모든 자원 소모(선순환 전환 불가)
- (현황) 국내외 경쟁력 확보 불가
- (환경) 글로벌 온라인 플랫폼이 국내 온/오프라인 장악 예상
- (기술) 디지털은 인공지능으로 빠르게 이동중(Automation)
- (전망) 기존 산업주체 변화 불가(디지털 리더 부재 – 지속가능 기업인재양성모델 부재)

Q : What is your World Best Competitiveness?

World Best Competitiveness for Financial Security is…
Secure Minimum Regulation and Make All Automation
(To AI Tech, for Security – Tech & Audit … etc)

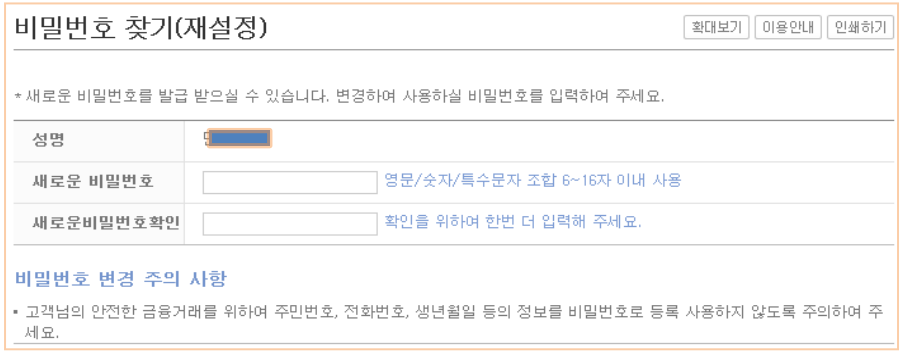
https://brunch.co.kr/@taeeonkoo/36

2. Case Study (실 규제영향 사례 중심)

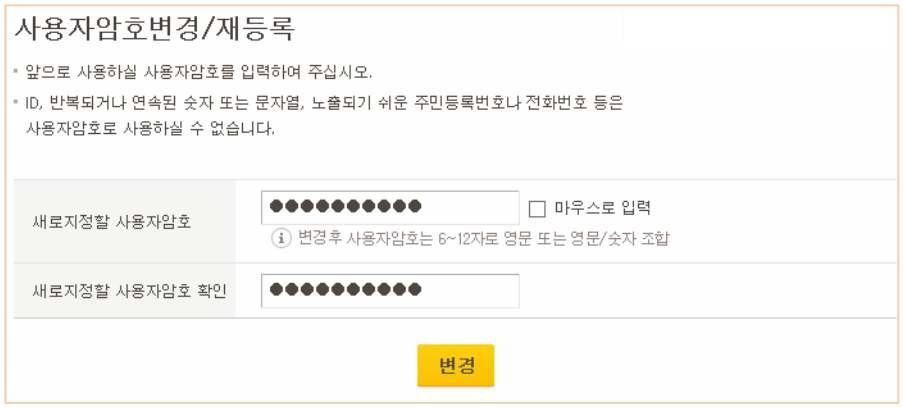
Case Study - 비밀번호

6~16자 영문/숫자/특수문자 조합
6~12자 영문 또는 영문/숫자 조합
8자리, 10자리 등
Q 정답은?

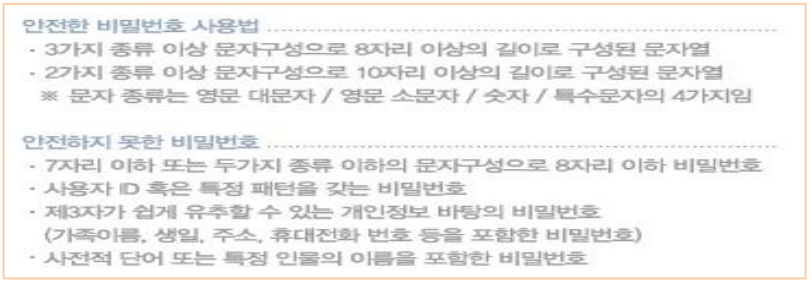
S 은행 6~16



K 은행 6~12

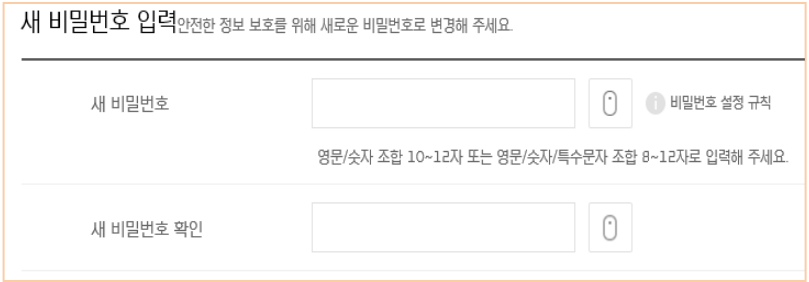


S 카드 8~



S 카드 8~20

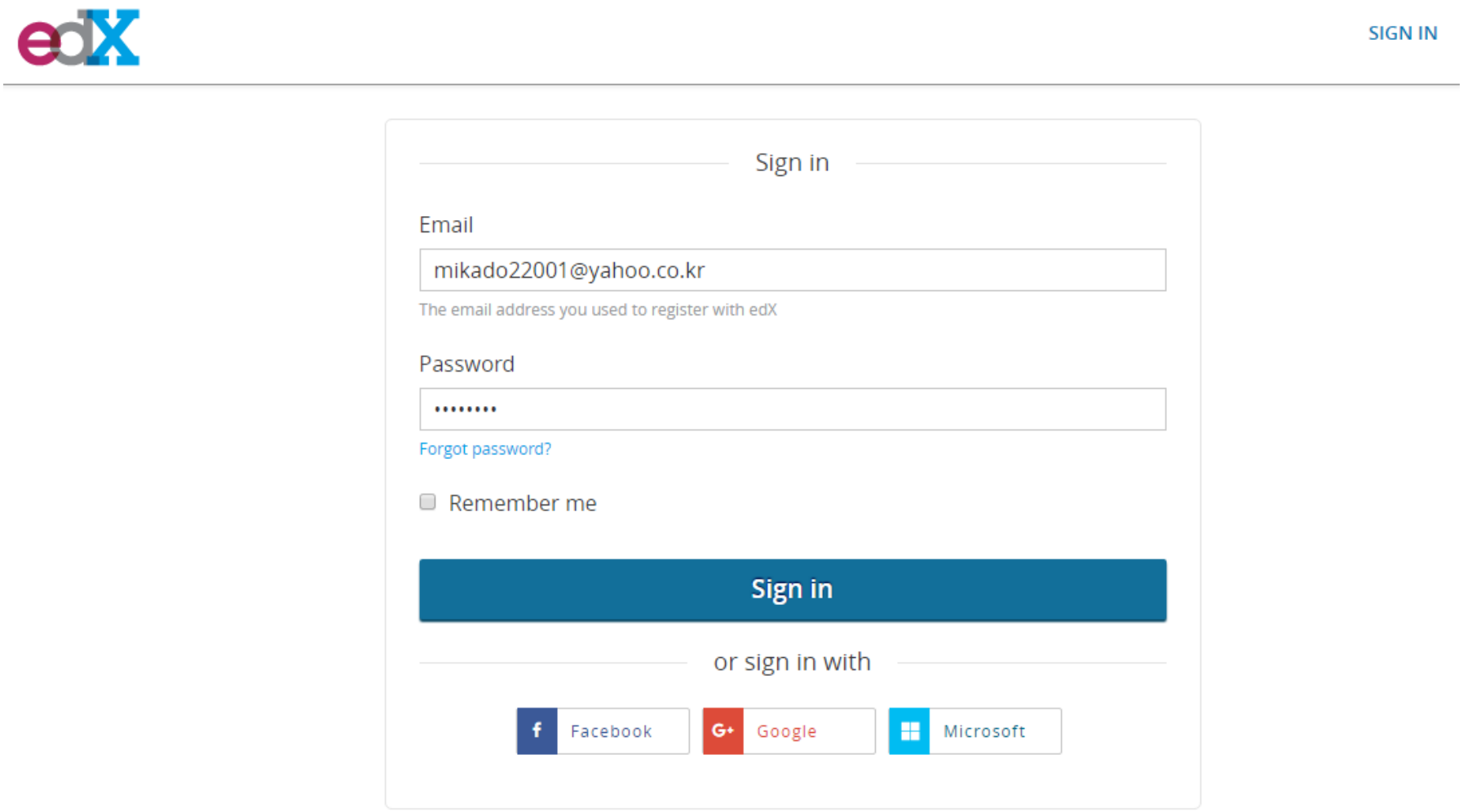
H 카드 8~12



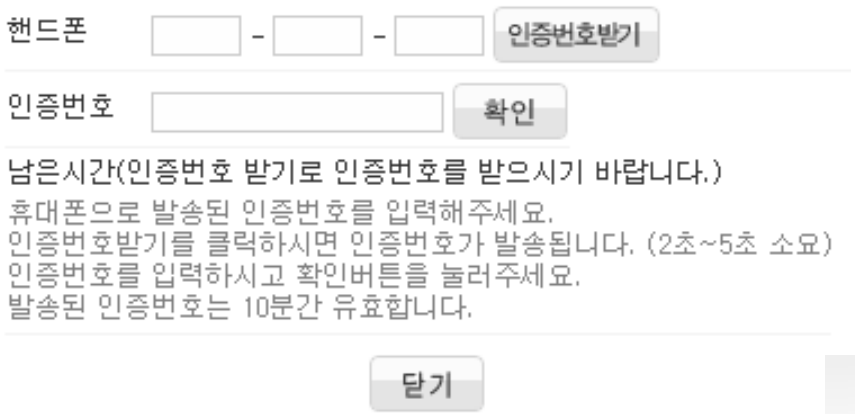
패스워드 이용행태 관련 – 보안위협 분석

	ID 공유(재사용)	PW 공유(재사용)	ID/PW공유(재사용)
2010.2 Trusteer 보고서	65% (온라인뱅킹 계정포함)	73% (온라인뱅킹 계정포함)	47% (온라인뱅킹 계정포함)
2011.6 Troyhunt 보고서	-	92% (소니 시스템 간) 67% (소니와 타 사이트 간)	-
2011.9 Paypal 보고서	-	60%	-
2012.7 Troyhunt 보고서	-	59% (소니와 야후 간)	-
2012.9 CSID 자료	-	61% (미국인 대상) 76% (미국인 대상, 18~24세)	-
2013.4 Ofcom 자료	-	55% (영국인 대상)	-

http://passwordresearch.com/stats/statindex.html


edX
SIGN IN
Sign in
Email
mikado22001@yahoo.co.kr
The email address you used to register with edX
Password
••••••••
Forgot password?
Remember me
Sign in
or sign in with
Facebook
Google
Microsoft

Case Study - SNS or 휴대폰인증로그인



Case Study - 보안프로그램

보안 프로그램

1) 키보드보안
2) 개인방화벽
3) 공인인증서 보안프로그램
4) 정보수집 프로그램

필수 or 선택

VS

강력한 개인화 분석 시스템
Powered by IT

필수 설치 프로그램

통합 설치

프로그램명	기능	설치현황
통합 보안프로그램 (nProtect Online Security)	- 개인방화벽 : 해킹 툴 및 바이러스를 검사하고 치료해 주는 프로그램 - 키보드 보안 : 키보드 및 가상 키패드로 입력되는 정보를 보호해 주는 프로그램	설치함
공인인증서 보안프로그램 (AnySign for PC)	- 공인인증서 : 본인 인증 및 입력되는 정보를 보호해 주는 프로그램	설치함

선택 설치 프로그램

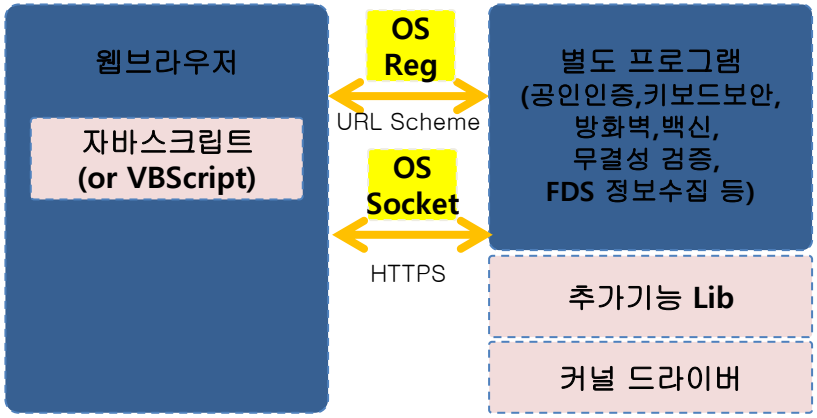
프로그램명	기능	설치현황
전자금융거래 보안프로그램 (IPinside)	- PC정보보호 : 안전한 온라인 거래를 위해 정상적인 접속 여부를 검증해 주는 프로그램	설치

통합 설치 대상 프로그램

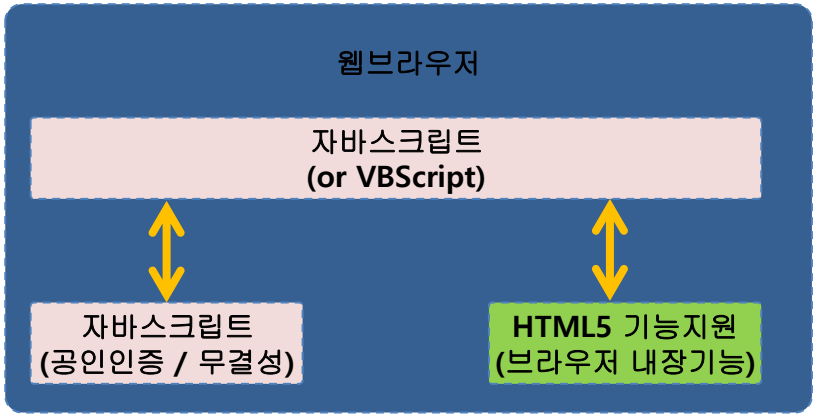
구분	프로그램명	프로그램안내
필수	공인인증서 보안프로그램 Wizvera Delfino	공인인증서 로그인과 거래내역에 대한 전자서명을 위한 프로그램입니다. 자세히보기
필수	개인PC방화벽 프로그램 AhnLab Safe Transaction	인가되지 않은 접근을 차단하고 해킹 툴 및 바이러스를 검색하고 치료해주는 프로그램 입니다. 자세히보기
필수	키보드보안 프로그램 TouchEnKey	계좌번호/비밀번호와 같은 금융정보 및 개인정보를 보호하는 가상 키보드 보안 프로그램입니다. 크롬, 파이어폭스, 오페라 사용자의 경우에는 [브라우저확장기능설치]를 우선 실행하시기 바랍니다. 자세히보기

(Non-ActiveX / HTML5) 실행 및 동작방식 변화

(연동방식-변경1)사전 설치형(EXE)의 경우 연동



(연동방식-변경2)HTML5 또는 자바스크립트 방식



※ HTML5을 지원하는 상위버전 브라우저에서는 HTML5기능을 호출하여 이용하고, 이외의 하위버전 브라우저에서는 자바스크립트로 해당기능을 구현하여 제공

주요 보안위협 비교 (공인인증서 전자서명 관련) (1/2)

구 분	[ActiveX 형태] 기존 보안기능 제공 형태 (ActiveX 등 플러그인 이용)	[A-TYPE] 플러그인 연동부분만 제거 (ActiveX 인터페이스삭제)	[B-TYPE] 자바스크립트로 중요기능 구현 (HTML5 표준기술 일부 이용)	[C-TYPE] HTML5 표준기능 활용 (자바스크립트는 연동수준 활용)
			하위버전 브라우저인 경우 (HTML5 미지원)	상위버전 브라우저인 경우 (HTML5 일부지원)
	플러그인 (ActiveX 등) 형태	14년 말까지 전자상거래 결제 시 적용가능형태 (플러그인만 이용하지 않으면 됨, '14.10.7 미래부/금융위 회의결과)		
		금감원 : 보안성심의 대상 아님(신규서비스 아님)		
(T1) 사용자 UI	웹 브라우저 + 별도 S/W에서 제공 가능	웹 브라우저 + 별도 S/W에서 제공 가능	[-] 웹 브라우저 + HTML/JS (난독화/무결성 검토)	[-] 웹 브라우저 + HTML5 (자바스크립트 연동)
(T2) 서명기능 연동	자바스크립트 (COM 인터페이스 호출)	자바스크립트 + [-] URL Scheme, 웹소켓, HTTPS 등	자바스크립트 (스크립트간 호출)	자바스크립트
(T3) 서명/암호 연산	별도 S/W(실행화일 형태) 이용	별도 S/W에서 기능 제공	[-] 자바스크립트 (난독화/무결성 검토)	-

주요 보안위협 비교 (공인인증서 전자서명 관련) (2/2)

구 분	[ActiveX 형태] 기존 보안기능 제공 형태 (ActiveX 등 플러그인 이용)	[A-TYPE] 플러그인 연동부분만 제거 (ActiveX 인터페이스삭제)	[B-TYPE] 자바스크립트로 중요기능 구현 (HTML5 표준기술 일부 이용)	[C-TYPE] HTML5 표준기능 활용 (자바스크립트는 연동수준 활용)
			하위버전 브라우저인 경우 (HTML5 미지원)	상위버전 브라우저인 경우 (HTML5 일부지원)
	플러그인 (ActiveX 등) 형태	14년 말까지 전자상거래 결제 시 적용가능형태 (플러그인만 이용하지 않으면 됨, '14.10.7 미래부/금융위 회의결과)		
		금감원 : 보안성심의 대상 아님(신규서비스 아님)		
(T4) 저장위치 (암호화 되어있음)	단순 File	단순 File	브라우저 내부(로컬스토리지), -접근성 검토 필요-	브라우저 내부(로컬스토리지), -접근성 검토 필요-
	-	[+] S/W HSM (Optional)	-	-
	H/W HSM	H/W HSM	[-] -	[-] -
	모바일 기기(USIM/등)	모바일 기기(USIM/등)	모바일 기기(USIM/등)	모바일 기기(USIM/등)
(T5) 기타 (입력보안)	키보드보안, 가상키패드	키보드보안, 가상키패드	[-] 가상키패드 (자바스크립트 구현)	[-] 가상키패드 (자바스크립트 구현)
(T6) 기타 (보안서비스 형태)	-	[+] 항상 일부 보안기능이 동작 가능한 형태임 [-] 업체별 보안프로그램이 항상 실행(중복?)	-	-

자동로그인 기능

제목	전자금융거래 App의 자동 로그인 등의 기능 적용 가능 여부에 대한 회신
처리구분	완료
소관부서	IT금융정보보호단
등록자	IT금융정보보호단
회신일	2016-06-23
첨부파일	
요청대상 행위	□ 스마트폰앱에서 이용자의 금융기관 계정정보(ID/PW)를 이용자 단말기에 저장하여, 멀티로그인, 자동로그인, 로그인 세션 유지 기능 제공이 가능한지 여부
판단	□ 멀티로그인, 자동로그인, 로그인 세션 유지 기능은 전자금융거래법 및 관련 규정에서 이를 직접적으로 제한하지 않으므로 제공 가능할 것으로 판단됩 니다.
판단이유	□ '스마트폰 전자금융서비스 안전대책'은 과거 스마트폰 보급에 따른 잠재적 보안위협에 대응하기 위해 시 행되었으나 (' 10.1.7.), 현재 금융위·금감원에 등록 되어 있지 않은 행정지도 * 입니다. * '14.12.30. 금융혁신위원회 제5차 회의에서 금융위ž금감원에 등록되어 있지 않은 행정지도 등은 일괄 폐지 ◦ 따라서 요청하신 사안은 금융 회사가 자율적으로 결정하여 운영할 수 있는 사안입니 다. □ 다만, 금융기관 계정정보(ID/PW)를 이용자의 단말기에 저장하는 경우 저 장된 인증정보의 탈취를 통한 보안사고가 발생하지 않도록 주의해 주 시기 바랍니다.

일회용비밀번호(OTP) 생략 문의

질의 요지	▫ '16.4.19. 변경 예고한 「전자금융감독규정」이 시행된 이후, 일회용 비밀번호를 사용하지 않는 '간편뱅킹 서비스'를 제공하는 것이 가능한지 질의 ○ '간편뱅킹 서비스'는 고객이 직접 사전에 지정한 단말기(PC, 스마트기기 등)를 통해 전자금융사고의 발생 가능성이 낮은 안전한 거래(본인계좌이체 등)를 하는 경우에 한해 일회용 비밀번호 입력을 생략하고 통장 비밀번호 입력만으로 거래할 수 있도록 하는 서비스임
회답	▫ 전자자금이체시 보안카드를 포함한 일회용 비밀번호 적용 의무를 폐지하는 내용의 「전자금융감독규정('16.4.19. 변경예고)」이 시행되면 전자자금이체시 일회용 비밀번호를 생략하는 것이 가능합니다. ○ 아울러, 전자금융거래에 있어서 「전자금융감독규정」 제37조에 따라 안전하다고 판단되는 인증방법을 사용하는 것이 가능합니다.
이유	▫ 「전자금융거래법」 제21조는 전자금융거래의 안전성 및 신뢰성을 확보하는 것을 전제로 특정 기술 또는 서비스의 사용을 강제하지 않는 '기술중립성 원칙'을 명확히 하고 있으며, 「전자금융감독규정」 제37조도 전자금융거래에 있어 특정한 인증수단을 한정하고 있지 않으므로 금융회사 또는 전자금융업자는 자신의 판단과 책임 하에 적절한 인증수단을 선택하여 사용할 수 있습니다.

신규 인증방법 적용의 건

비조치의견서 (☐비조치 ☐조치 ☑기타)

요청대상 행위	☐ 인터넷/스마트뱅킹을 통한 전자자금이체 거래시 NH안심보안카드*를 인증방법으로 사용할 경우, * NH안심보안카드를 스마트폰에 접촉하여 본인임을 인증하고, 이체 거래시 보안카드번호를 입력하는 2단계 인증절차를 수행 ◦ 동 인증방법이 전자금융감독규정 제37조에서 정한 안전한 인증방법에 해당하는지 여부
판단	☐ 금융회사는 전자금융거래에 사용되는 인증방법을 자율적으로 선택하여 사용할 수 있습니다. ◦ 다만, 개정 법규의 취지에 따라 금융회사 자체적으로 보안 및 인증방법에 대한 안전성을 확보해야 하오니 이 점 유념하시기 바랍니다.
판단이유	☐ 전자금융거래법 제21조 제3항 및 전자금융감독규정 제37조의 내용을 고려*할 때 금융회사는 전자금융거래에 사용되는 인증방법을 자율적으로 선택할 수 있습니다. * 특정 기술 또는 서비스의 사용을 강제하지 않는 '기술 중립성 원칙'이 도입됨에 따라 경쟁촉진적인 인증기술 사용을 위해 전자금융거래시 공인인증서 등을 사용하도록 한 의무를 폐지(금융위원회 고시 제2015-7호)

※ **비조치의견서의 효력**(「법령해석 및 비조치의견서 업무처리에 관한 운영규칙」 제6조의2, 제11조제1항 · 제2항 참조)

1. 금융감독원장은 해당 행위가 법령등에 위반되지 않는다는 비조치의견서를 회신하는 경우 해당 행위에 대해서는 사후에 회신내용의 취지에 부합하지 않는 법적 조치를 취하지 않습니다.
2. 그러나 다음의 어느 하나에 해당하는 경우에는 금융감독원장이 이미 회신한 비조치의견서의 내용과 다른 법적 조치를 취할 수 있습니다.

가. 신청인이 요청서에 기재한 내용 또는 제출한 자료의 내용이 사실과 다른 경우

나. 신청인이 중요한 자료를 제출하지 아니한 사실이 발견된 경우

다. 신청인이 요청서에 기재한 내용과 상이한 행위를 한 경우

라. 관련 법령등이 변경된 경우

마. 판단의 기초가 되는 사실관계의 변동, 그 밖의 사정변경으로 인하여 기존의 의견을 유지할 수 없는 특별한 사유가 있는 경우

3. 금융감독원장이 일정 요건 충족을 조건으로 제재 등 조치를 취하지 않겠다는 조건부 비조치의견서를 회신하였으나 신청인이 해당 조건을 충족하지 못한 경우에는 금융감독원장은 이미 회신한 비조치의견서의 내용과 다른 법적 조치를 취할 수 있습니다.

Case Study - SMS 인증 – 이용금지 권고

DRAFT NIST Special Publication 800-63B
Digital Authentication Guideline
Authentication and Lifecycle Management
Paul A. Grassi
Elaine M. Newton
Ray A. Perlner
Andrew R. Regenscheid
William E. Burr
James L. Fenton
Justin P. Richer
COMPUTER SECURITY
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

DRAFT NIST Special Publication 800-63B
Digital Authentication Guideline
Authentication and Lifecycle Management
Paul A. Grassi
Applied Cybersecurity Division
Information Technology Laboratory

Requirement	AAL 1	AAL 2	AAL 3
Permitted authenticator types	Memorized Secret Look-up Secret Out of Band SF OTP Device MF OTP Device SF Cryptographic Device MF Software Cryptographic Authenticator MF Cryptographic Device	MF OTP Device MF Software Cryptographic Authenticator MF Cryptographic Device or memorized secret plus: Look-up Secret Out of Band SF OTP Device SF Cryptographic Device	MF OTP Device MF Cryptographic Device SF Cryptographic Device plus Memorized Secret
FIPS 140 verification	Level 1 (Government agency verifiers)	Level 1 (Government agency authenticators and verifiers)	Level 2 overall (MF authenticators) Level 1 overall (verifiers and SF Crypto Devices) Level 3 physical security (all authenticators)
Assertions	Bearer or proof of possession	Bearer or proof of possession	Proof of possession only
Reauthentication	30 days	12 hours or 30 minutes inactivity; may use one authentication factor	12 hours or 15 minutes inactivity; shall use both authentication factors
Security Controls	[SP 800-53] Low Baseline (or equivalent)	[SP 800-53] Moderate Baseline (or equivalent)	[SP 800-53] High Baseline (or equivalent)
Records Retention	Not required	7 years, 6 months	10 years, 6 months

5.1.3.2. Out of Band Verifiers

Out of band verifiers SHALL generate a random authentication secret with at least 20 bits of entropy using an approved random number generator. They then optionally signal the device containing the subscriber's authenticator to indicate readiness to authenticate.

Due to the risk that SMS messages may be intercepted or redirected, implementers of new systems SHOULD carefully consider alternative authenticators. If the out of band verification is to be made using a SMS message on a public mobile telephone network, the verifier SHALL verify that the pre-registered telephone number being used is actually associated with a mobile network and not with a VoIP (or other software-based) service. It then sends the SMS message to the pre-registered telephone number. Changing the pre-registered telephone number SHALL NOT be possible without two-factor authentication at the time of the change. **OOB using SMS is deprecated**, and may no longer be allowed in future releases of this guidance.

(전화번호에 의존한 2factor이므로 미사용 권고)

https://pages.nist.gov/800-63-3/sp800-63b.html

Case Study - SMS 인증 – 이용금지 권고

Memorized Secrets

Look-up Secrets

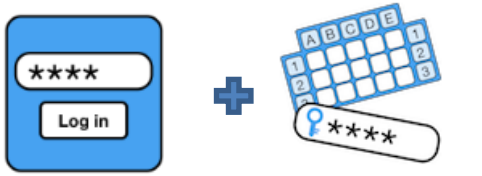
Out of Band : SMS

Single Factor OTP Device

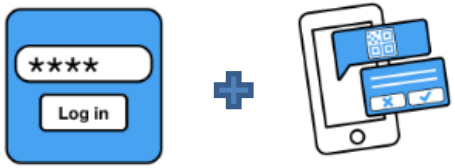
Single Factor Cryptographic Devices

Multi-Factor
Cryptographic **Software**

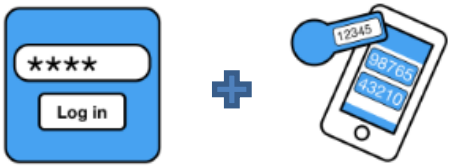
cryptographic **key is stored on disk or some other "soft" media** that requires activation through a second factor of authentication



Memorized Secrets Look-up Secrets
(카드인증과 유사)



Memorized Secrets Out of Band
(휴대폰 인증과 유사)



Memorized Secrets Single Factor
OTP Device

Multi-Factor OTP Devices
(예시 : PW입력 OTP기기)

A multi-factor (MF) OTP device hardware device generates one-time passwords for use in authentication and requires activation through a second factor of authentication.

Multi-Factor Cryptographic **Devices**
(예시 : 지문+FIDO)

A multi-factor cryptographic device is a **hardware device that contains a protected cryptographic key** that requires activation through a second authentication factor

다양한 비대면확인 방식 허용
('15.5월 개선방안 발표, 금년 12월중 유권해석 변경을 통해 **적용 예정)**

* ① 신분증 사본 온라인 제출, ② 영상통화, ③ 현금카드 등 전달 시 확인
④ 기존계좌 활용 ("4가지 방식에 준하는 방식"도 적용 가능)

출처 : IT. 금융 융합 및 신성장동력 창출을 위한인터넷전문은행 도입방안 `15.6 금융위원회

다양한 비대면확인 방식 허용 ???

전자금융감독규정

[시행 2016.6.30.] [금융위원회고시 제2016-24호, 2016.6.30., 일부개정]

제1장 총칙

제3조(전자금융보조업자의 범위) 법 제2조제5호에서 "금융위원회가 정하는 자"라 함은 다음 각 호의 어느 하나에 해당하는 자를 말한다.

1. 정보처리시스템을 통하여 「여신전문금융업법」 상 신용카드업자의 신용카드 승인 및 결제 그 밖의 자금정산에 관한 업무를 지원하는 사업자
2. 정보처리시스템을 통하여 은행업을 영위하는 자의 자금인출업무, 환업무 및 그 밖의 업무를 지원하는 사업자
3. 전자금융업무와 관련된 정보처리시스템을 해당 금융회사 또는 전자금융업자를 위하여 운영하는 사업자
4. 제1호 부터 제3호의 사업자와 제휴, 위탁 또는 외부주문(이하 "외부주문등"이라 한다)에 관한 계약을 체결하고 정보처리시스템을 운영하는 사업자

제5장 전자금융업무의 감독

제60조(외부주문등에 대한 기준) ① 금융회사 또는 전자금융업자는 전자금융거래를 위한 외부주문등의 경우에는 다음 각 호의 사항을 준수하여야 한다.

1. 외부주문등에 의한 정보처리시스템의 개발업무에 사용되는 업무장소 및 전산설비는 내부 업무용과 분리하여 설치·운영
2. 금융회사와 이용자 간 암호화정보 해독 및 원장 등 중요 데이터 변경 금지
3. 계좌번호, 비밀번호 등 이용자 금융정보 무단보관 및 유출 금지
4. 접근매체 위·변조, 해킹, 개인정보유출 등에 대비한 보안대책 수립
5. 금융회사와 전자금융보조업자 간의 접속은 전용회선을 사용
6. 정보처리시스템 장애 등 서비스 중단에 대비한 비상대책 수립
7. 외부주문등의 입찰·계약·수행·완료 등 각 단계별로 금융감독원장이 정하는 보안관리방안을 따를 것
8. 업무지속성을 위한 중요 전산자료의 백업(backup)자료 보존 및 백업설비 확보 등 백업대책 수립
9. 정보관리의 취약점을 최소화하고 보안유지를 위한 내부통제방안을 수립·운용하고, 통제는 제8조제1항제2호의 조직에서 수행

전자금융거래법

[시행 2016.1.27.] [법률 제13929호, 2016.1.27., 일부개정]

제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

4. "전자금융업자"라 함은 제28조의 규정에 따라 허가를 받거나 등록을 한 자(금융회사는 제외한다)를 말한다.
5. "전자금융보조업자"라 함은 금융회사 또는 전자금융업자를 위하여 전자금융거래를 보조하거나 그 일부를 대행하는 업무를 행하는 자 또는 결제중계시스템의 운영자로서 「금융위원회의 설치 등에 관한 법률」 제3조에 따른 금융위원회(이하 "금융위원회"라 한다)가 정하는 자를 말한다.

[전자금융] 전자금융보조업자 범위

1. 금융회사의 전화인증 업무를 위탁하여 수행하는 경우 전자금융보조업자 해당 여부

1. 금융회사의 전화인증 업무를 위탁하여 수행하는 경우 전자금융보조업자 해당 여부

ㅇ 전자금융거래법상 전자금융보조업자는 금융회사 또는 전자금융업자를 위하여 전자금융거래를 보조하거나 그 일부를 대행하는 업무를 행하는 자 또는 결제중계시스템의 운영자로서 금융위원회가 정하는 자를 의미합니다.(동법 제2조 제5호)

ㅇ 금융회사의 전자금융거래시 추가인증 수단 중 하나인 전화인증 업무를 수행하고 있다면, 이는 전자금융보조업자의 요건인 금융회사를 위하여 전자금융거래를 보조하는 것으로 판단됩니다.

관련법령 : 전자금융거래법제2조(정의)
작성부서 : 금융위원회 사무처 금융서비스국 전자금융과, 02-2156-9496

검사 · 제재개혁 추진성과

2016. 4. 8.

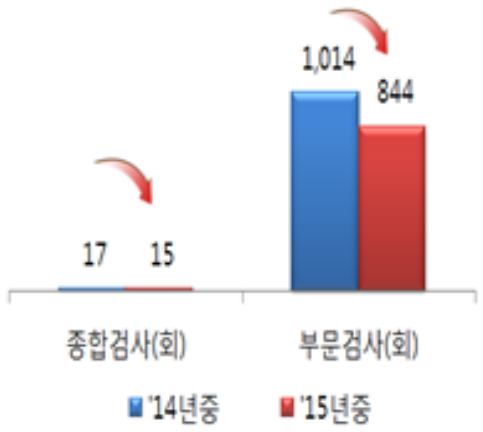
금 융 감 독 원

□ 신분제재 보다는 **기관 위주의 제재를 강화**하여 실시하되, 신규 업무 진출 제한문제를 개선하는 등 **기관제재의 실효성·합리성 제고** 추진

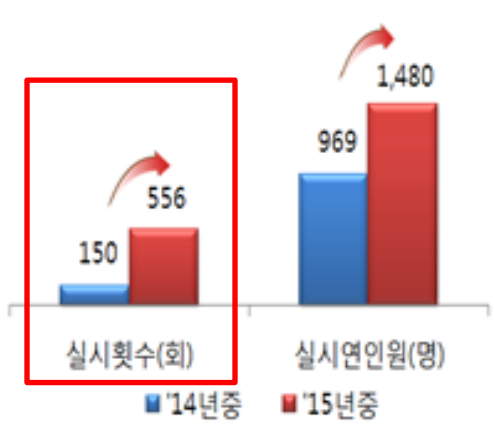
○ 금융지주·보험·저축은행·카드·신용정보회사가 **제재 받은 경우** 적용되는 **신규사업 진출 제한기간을 합리적으로 조정***('15.9월)

* (종전) 기관경고 이상 : 3년간 → (조정후) 기관경고 : 1년간, 시정명령·영업정지 이상 : 3년간

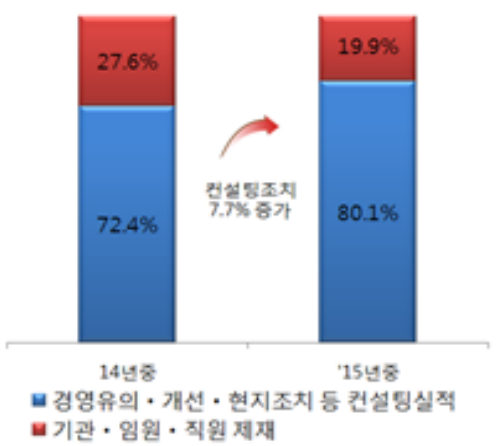
현장검사 축소



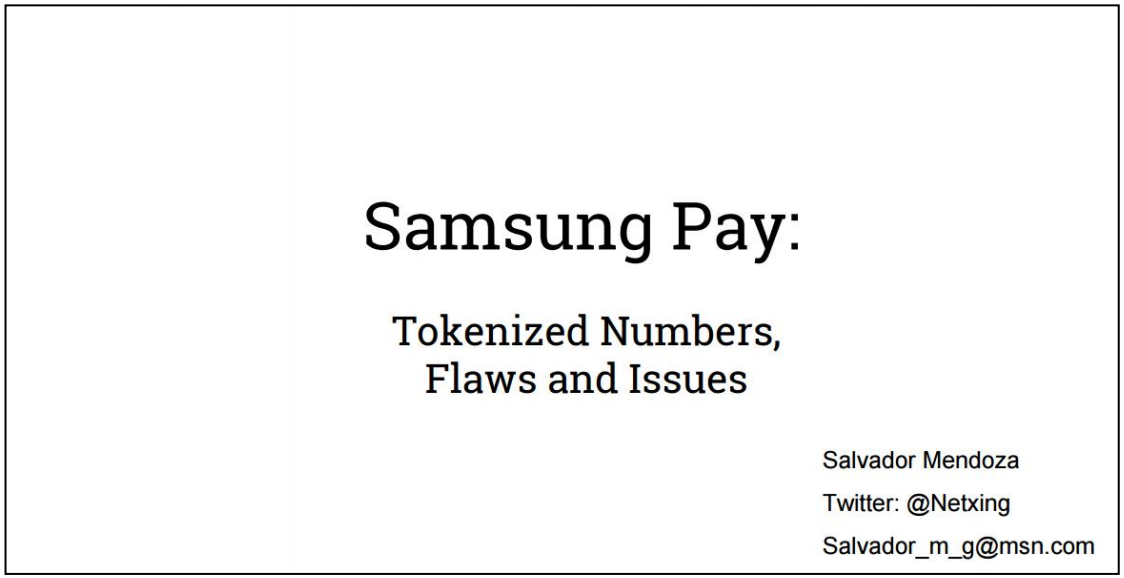
조사출장 확대

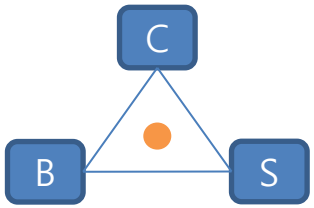


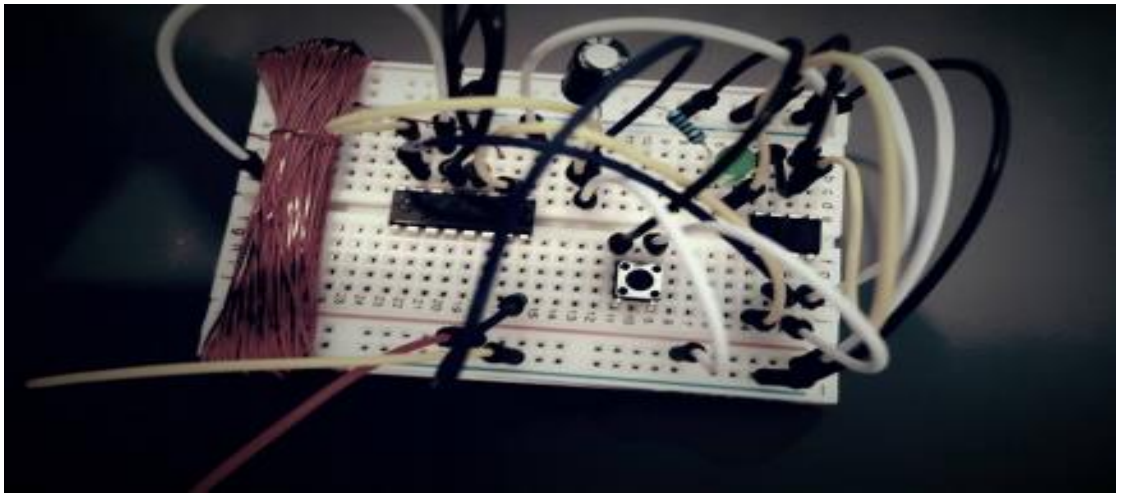
컨설팅 조치 증가

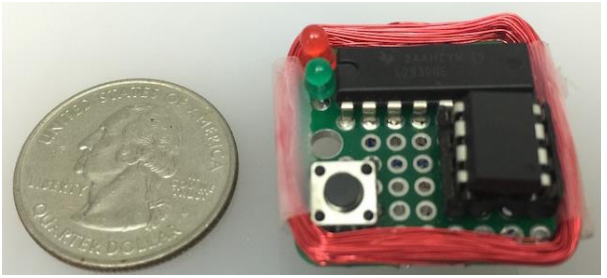


https://www.fsc.go.kr/downManager?bbsid=BBS0030&no=96097









https://samy.pl/magspoof/

https://www.blackhat.com/docs/us-16/materials/us-16-Mendoza-Samsung-Pay-Tokenized-Numbers-Flaws-And-Issues.pdf
https://www.blackhat.com/docs/us-16/materials/us-16-Mendoza-Samsung-Pay-Tokenized-Numbers-Flaws-And-Issues-wp.pdf

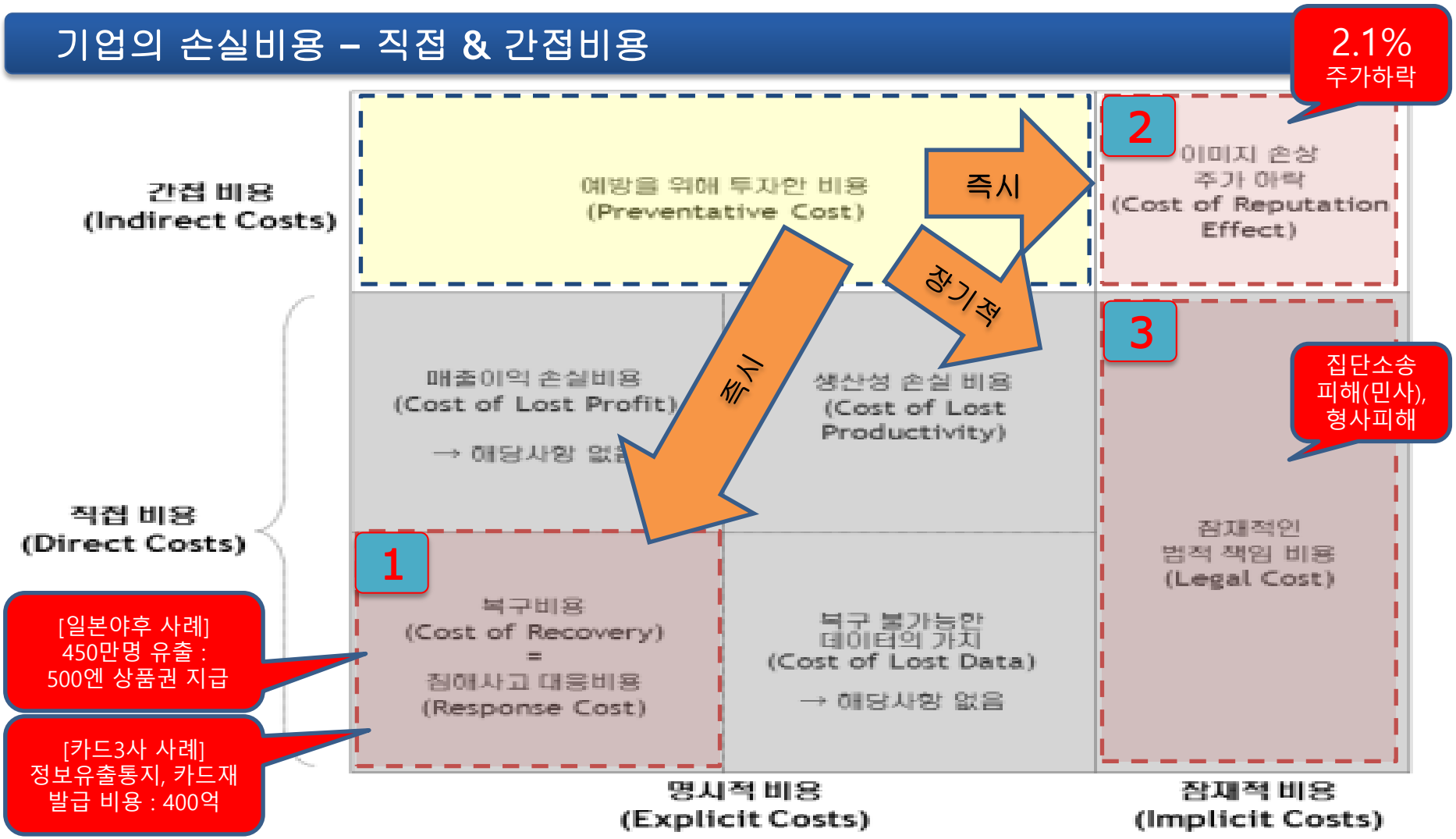
Black Hat Sound Bytes

- Samsung Pay has some levels of security, but it is a fact that could be a target for malicious attacks.
- Samsung Pay has some limitations in the tokenization process which could affect customers' security.
- Finally, tokens generated by Samsung Pay could be used in another hardware.

Salvador Mendoza (@Netxing)

https://www.blackhat.com/docs/us-16/materials/us-16-Mendoza-Samsung-Pay-Tokenized-Numbers-Flaws-And-Issues.pdf
https://www.blackhat.com/docs/us-16/materials/us-16-Mendoza-Samsung-Pay-Tokenized-Numbers-Flaws-And-Issues-wp.pdf

기업의 손실비용 – 직접 & 간접비용



※ 출처 : 개인정보 유/노출 사고로 인한 기업의 손실비용 추정 (2009.8, 정보보호학회지, 제19권 제4호) 논문 등 인용

기업의 손실비용 1 침해사고 대응비용 (카드3사 사례 : 400억 이상)

정보유출 카드3사, 재발급·통지비용만 400억원 넘어

hphong@wowtv.co.kr 홍헌표 기자

기사 소셜댓글 입력 : 2014-02-04 08:47

◎ 정보유출 카드3사 재발급 등 부수비용

	KB국민카드	롯데카드	NH농협카드
재발급비용	115억원	75억원	62억원
우편비용	87억원	12억원	50억원
SMS서비스	추가예상	추가예상	추가예상
콜센터 운영	7억원	12억원	추정 어려움
인프라 증설	-	5억원	-
합계	209억원+α	104억원+α	112억원+α

(자료 : 전자공시시스템 및 각 사)

기업의 손실비용 2 침해사고 에 따른 주가하락 (- 2.1%)

✓ 개인정보유출이 알려진 상장기업은 이틀내 상장가치의 2.1% 하락

(The Global Rise of a Duty to Disclose Information Security Breaches, 2004, Ethan Preston & Paul Turner, pp. 457~491)

기업의 손실비용 3 개인정보 유출사건 및 형사처분 결과

업 체	발생일시	원인	피해규모	유출정보	처분결과
LG전자	2006년 9월	과실/해킹	3,600	사진, 자기소개서, 연구실적	법령 시행전
옥션	2008년 1월	해킹	1,081만	성명, 주민등록번호, 주소 등	법령 시행전
현대캐피탈	2011년 4월	해킹	175만	성명, 주민등록번호, 연락처 등	불기소 (혐의없음)
SK컴즈	2011년 7월	해킹	3,500만	아이디, 비밀번호(암호화), 성명, 주민등록번호(암호화), 연락처 등	불기소 (혐의없음)
넥슨	2011년 11월	해킹	1,320만	아이디, 비밀번호(암호화), 주민등록번호(암호화) 등	불기소 (증거불충분)
EBS	2012년 5월	해킹	422만	아이디, 비밀번호, 성명, 주민등록번호 등	불기소 (혐의없음)
KT	2012년 7월	해킹	870만	성명, 주민등록번호, 전화번호, 단말기명 등	불기소 (혐의없음)

출처 : 경찰청, 서울지방경찰청 수사결과 발표

※ 출처 : "개인정보 보호조치 위반 사건 수사의 문제점과 대책(Violation of Privacy Protection Issues and Measures of Investigation), 2013.9" 논문 인용

Case Study - [침해] 손실비용

(`14년기준)	임직원수	총이익	인당영업이익	점포수
신한은행	14,602	1조400억	7114만원	895
국민은행	21,568	6천700억	3106만원	1157
하나은행	9,339	5천700억	6103만원	
외환은행	7,926	4천억원	5047만원	

http://www.yonhapnews.co.kr/economy/2014/07/25/0301000000AKR20140725200200002.HTML

(영업이익, 억원)

구분	계열사	2014년	2015년	구분	계열사	2014년	2015년	구분	계열사	2014년	2015년
증권	KB투자증권	214	476	보험	KB생명	60	183	카드	KB국민카드	2,745	2,849
	하나금융투자	625	1,106		하나생명	69	220		하나카드	76	254
	신한금융투자	913	1,942		신한생명	681	883		신한카드	5,078	5,215
	총계	1,752	3,524		총계	810	1,286		총계	7,899	8,318

Kb투자 458명, 하나금융투자 1642명　　하나생명 151명 신한생명 1430명

주요 VAN사 3년 간 실적 비교

141명　229명　152명　150명　181명 (단위 : 억 원, %)

	스마트로			한국정보통신			나이스정보통신			KIS정보통신			케이에스넷		
	2013	2014	2015	2013	2014	2015	2013	2014	2015	2013	2014	2015	2013	2014	2015
매출액	1,410	1,414	1,524	2,057	2,261	2,688	2,007	2,255	2,639	1,300	1,694	1,904	1,501	1,636	1,719
영업이익	125	133	240	245	250	315	203	212	342	161	171	195	215	254	264
영업이익률	8.87	9.41	15.75	11.91	11.06	11.72	10.11	9.40	12.96	12.38	10.09	10.24	14.32	15.53	15.36

자료 : 금융감독원 전자공시시스템

http://www.thebell.co.kr/front/photo_view.asp?img_fn=20160518010003316000202221.jpg&imgdir=20160518&width:1332

기업의 손실비용 – 정보보호 투자 VS 침해사고 인과관계

- ✓ 정보보호 투자와 침해사고의 인과관계를 분석
  - "정보보호 투자 => 침해사고 감소" : 인과관계 없음
  - "침해사고가 많은 기업 => 정보보호 투자를 증가" : 데이터에 의해 입증
- ✓ 정보보호에 매우 민감하기 때문에 다른 업종에 비해 과감한 사전적인 투자를 수행하는 것으로 인식되고 있는 금융업의 경우, 침해사고의 발생에 따라 사후적 정보보호 투자를 수행하고 있는 대표적인 업종임

정확한 보안위협 분석후 정보보호 투자필요

[경찰이 늘어나면 범죄가 줄어들 것인지를 분석]

=> 지역별로 범죄발생 건수와 경찰의 수 및 그 지역의 특성을 나타내는 정보 를 수집

=> 즉 경찰의 숫자 가 많을수록 오히려 범죄가 늘어나는 것으로 결론 도출됨

OLS(Ordinary Least Square, 최소 자승법) > 0

[상식에 어긋나는 왜 이러 한 결과가 나타나는가?]

=>사실은 경찰이 많을수록 범죄가 늘어나는 것이 아니라 범죄가 많은 지역에 경찰을 많이 투입하였기 때문

※ 출처 : "정보보호 투자와 침해사고의 인과관계에 대한 실증분석(Information Security Investment and Security Breach: Empirical Study on the Reverse Causality), 2013.10" 신일순, 장원창, 박희영 인하대학교논문 인용

기업의 손실비용 3 판결의 변화 시작!

SK컴즈 정보유출 사건 : **재판부의 기술적 부분 정확한 이해 및 입증자료가 판결 좌우**
사고 발생 : 2011년 네이트와 싸이월드 회원 3500만명(34,954,887명)의 개인정보 유출사고

관련 소송 20여건 가운데 모두 해킹 피해자들인 원고 측이 패소 (2012년 4월 대구지법을 제외)

판결법원	대구지법 김천지원 구미시법원	서울중앙지법 (민사32부) 서창원, 조수진, 이승일	서울 중앙지법	대구지법 (민사12부) 김현환, 이성, 전명환	서울 서부지법 김성곤,김기춘,강인혜
사건번호	2011가소17384	2011가합90257 손해배상(기)		2012나9865위자료 (2011가소17384의항소심)	2013가합3052
선고일자	2012.04.26	2012.11.23	2013.02.15	2014.02.13	2014.04.17
원고수			2,882명		1215명
청구액	300만원	50만원		300만원	30만원
배상액수	100만원	기각	20만원 (위자료)	100만원 (위자료)	기각
이용자 측 소송대리인	법무법인 유능 유능종변호사	법무법인 대륙아주 담당변호사 김형우		법무법인 유능 담당변호사 남광진 외 1인	법무법인 법여울 담당변호사 김병진
SK컴즈 측 소송대리인		전원열,김진환,이준희,이언석 ,지성호		소송대리인 변호사 황영목 외 5인	소송대리인 변호사 전원열
㈜이스트소프트 측 소송대리인		법무법인 지후 담당변호사 마명원			

기업의 손실비용 3 판결의 변화 시작!

개인정보유출-정신적 손해에 대한 위자료	2012나9865 동일 할 듯	-		해킹사고로 원고가 입은 정신적 손해를 배상할 의무 인정	-
최소수집의무 위반	2012나9865 동일 할 듯	위반없음		위반없음	-
공개용 알집 사용	2012나9865 동일 할 듯	**###위반없음###** (인과없음)		공개용 알집을 사용하는 것을 방지하지 않은 잘못은 해킹사고 발생 사이에 상당인과 관계 인정	**###위반없음###** (인과없음)
(침입탐지 등) 비정상트래픽 탐지 (보호조치 의무위반)	2012나9865 동일 할 듯	**###위반없음###** (단지 설치하여 운영하고 있어서&해커가 대단해서!)		대용량 개인정보(10G)의 유출 탐지와 방지를 위한 기술적 · 관리적 보호조치의무 위반 (침입탐지시스템 수준 지나치게 완화)	**###위반없음###** (단지 설치하여 운영하고 있어서&해커가 대단해서!)
DB서버 관리자 PC/게이트웨이 서버에 FTP 허용	2012나9865 동일 할 듯	- (FTP부분은 언급없음)		필요없는 FTP 서비스 이용 가능하도록 한 부분은 유출에 기여하였다고 인정	**###위반없음###** (법령상 의무가 아니어서)
관리자 PC 자동로그아웃기능 미설정	2012나9865 동일 할 듯	-		위반없음 (인과불충분)	위반없음 (인과불충분)
접근제어 미비	2012나9865 동일 할 듯	위반없음 (단순 현 기업 정책으로만으로 문제없음으로 결론내고 있음) 공인인증서 등 추가적인 인증수단은 관련성 없음		위반없음 (충분한 권한이 있는 DB기술팀 소속 PC)	-
MD5 이용	2012나9865 동일 할 듯	**###위반없음###** 일방향암호화 하고 있음 (MD5 이용한 증거가 없음?) = 모호한 부분임 =		개인정보를 안전한 방법으로 저장할 의무를 위반하였다고 봄이 타당 (MD5는 그 보안 강도가 다른 해시함수에 비해 낮음, 다만 손해배상범위와 크게 상관없음)	**###위반없음###** 암호화기술의 사용과 관련한 기술적 · 관리적 보호조치를 위반한 것으로 인정하기에 부족
기타	-	정보보호 관리체계 – 불인정 사후조치 주의의무 – 불인정 백신소프트웨어 – 시만텍 제품설치 망분리 조치 위반 – 당시 필수정책이 아님 사후조치 부분 - 이슈없음		-	-

사건 및 판례 분석 – 보이스 피싱(시티은행), 파밍(농협), 텔레뱅킹(농협) 등

보이스피싱 웹사이트피싱

2014.5 "전자금융거래법상 '이용자의 중과실'의 판단기준" 논문

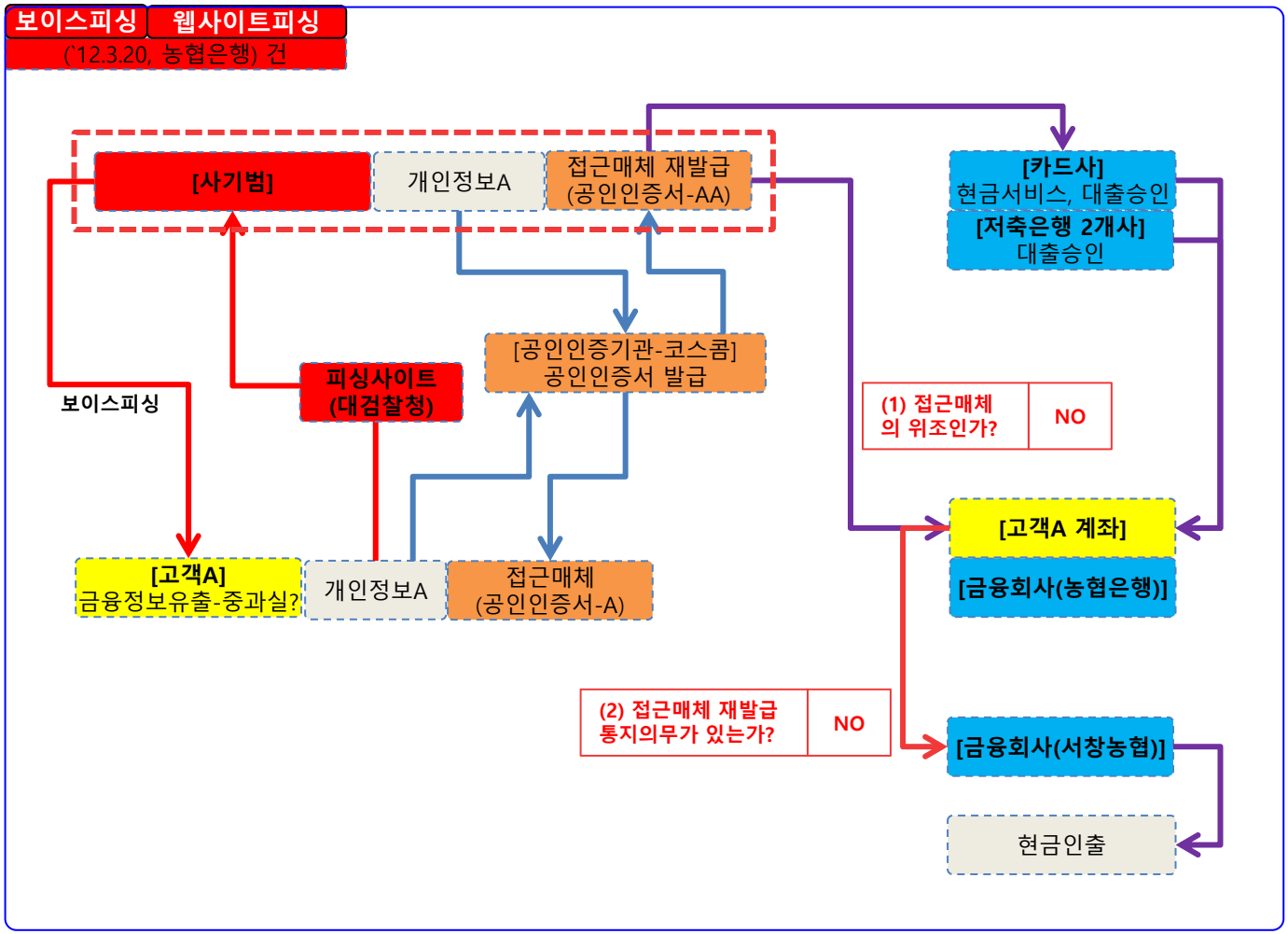
[접근매체, 고객의 중과실 해석]
금융거래정보 유출
(최초는 접근매체 유출아님,
즉 이용자의 중과실이 아님)

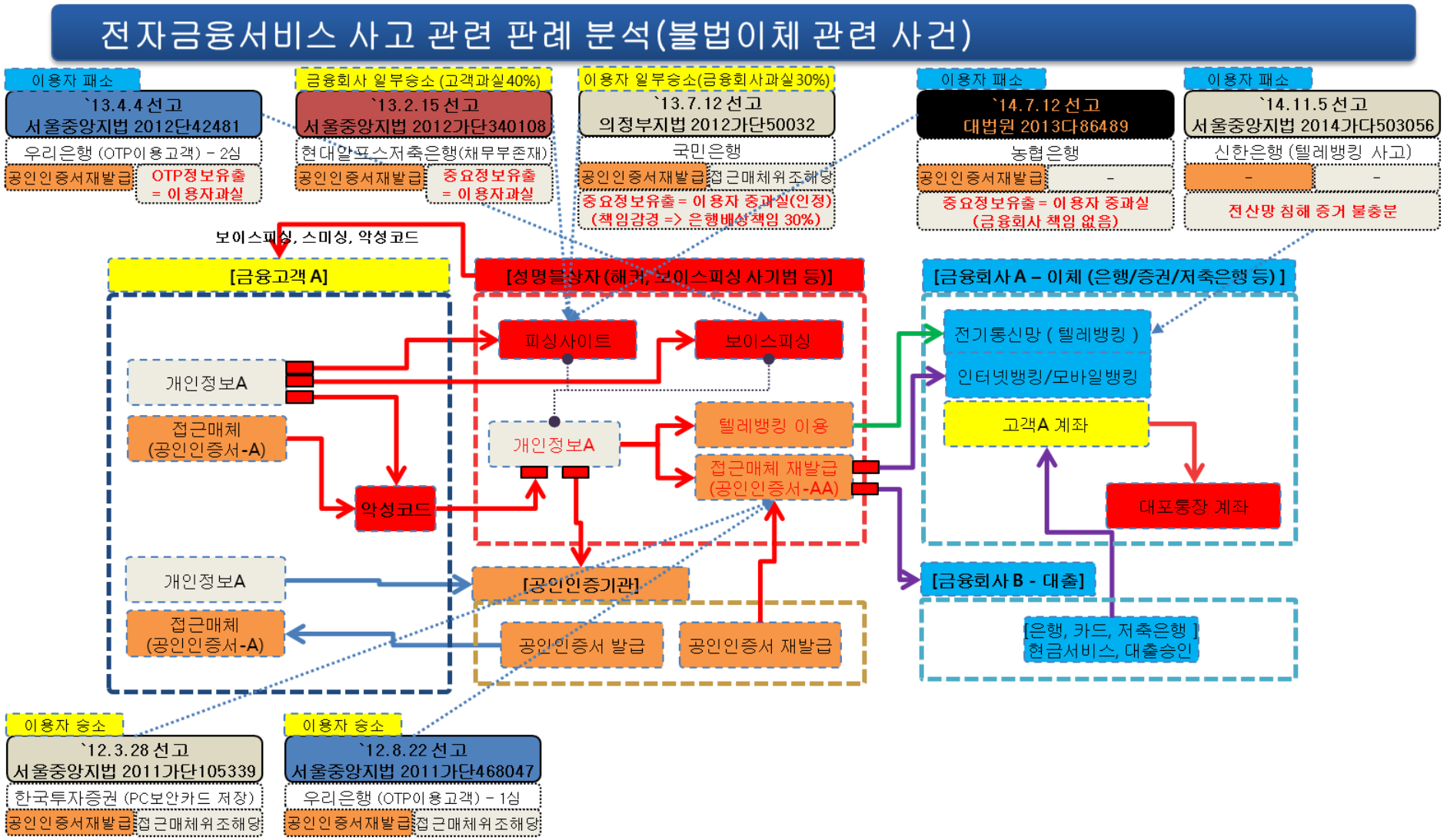
[전자금융거래법] 금융기관은 접근매체의 위변조로 발생한 사고의 책임있음, 이용자의 고의 또는 중과실이 있는경우 책임의 제한 또는 면제 가능

[금융회사]	[고객]
접근매체의 위변조?	금융정보유출-중과실?
위조, 변조 아님 정식 발급된것임	

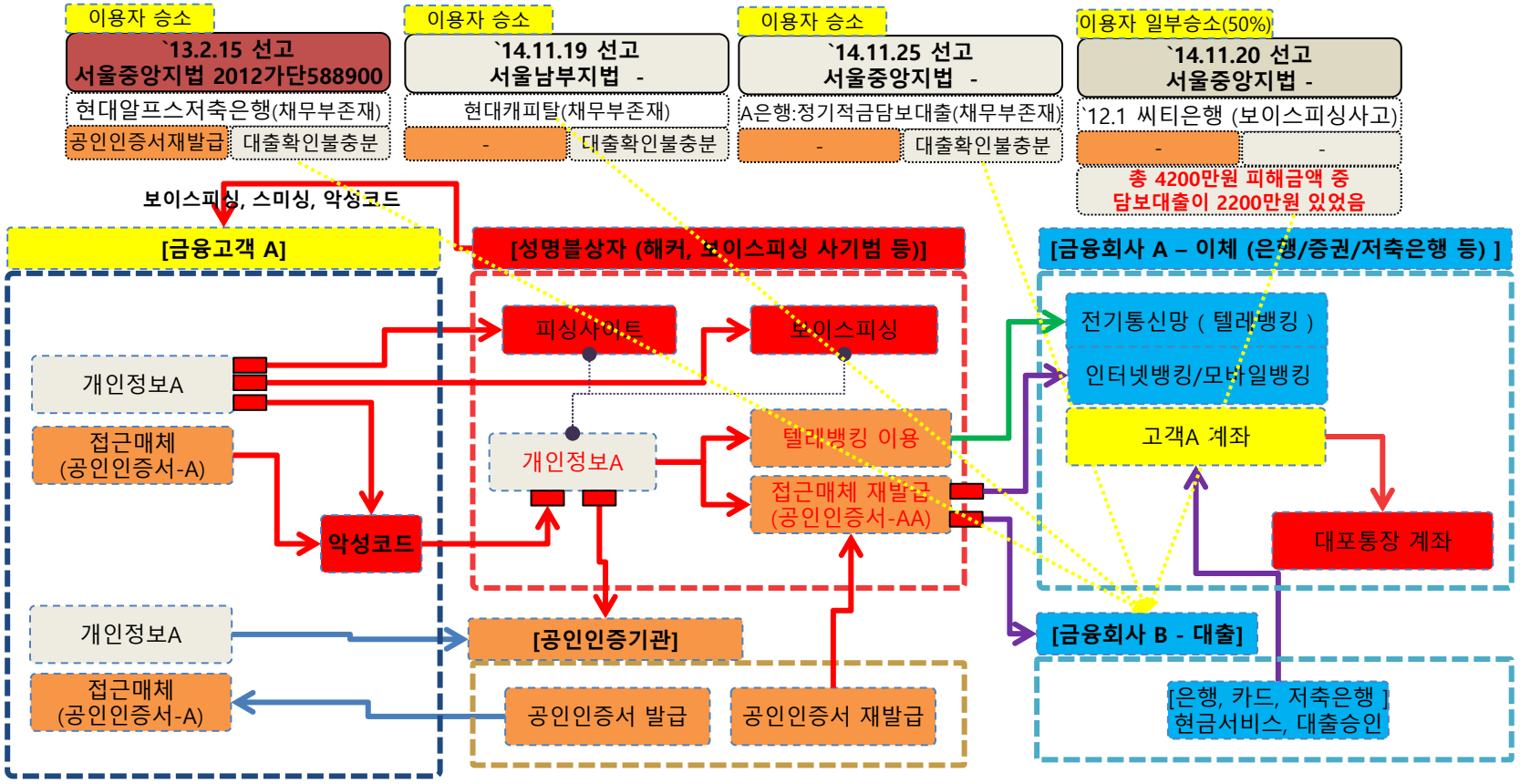
위변조로 봤는지 판례 확인필요

보이스피싱 웹사이트피싱
('12.3.20, 농협은행) 건




전자금융서비스 사고 관련 판례 분석(불법이체 관련 사건)
이용자 패소
`13.4.4 선고
서울중앙지법 2012단42481
우리은행 (OTP이용고객) - 2심
공인인증서재발급
OTP정보유출 = 이용자과실
금융회사 일부승소 (고객과실40%)
`13.2.15 선고
서울중앙지법 2012가단340108
현대알프스저축은행(채무부존재)
공인인증서재발급
중요정보유출 = 이용자과실
이용자 일부승소(금융회사과실30%)
`13.7.12 선고
의정부지법 2012가단50032
국민은행
공인인증서재발급
접근매체위조해당
중요정보유출 = 이용자 중과실(인정)
(책임감경 => 은행배상책임 30%)
이용자 패소
`14.7.12 선고
대법원 2013다86489
농협은행
공인인증서재발급
-
중요정보유출 = 이용자 중과실
(금융회사 책임 없음)
이용자 패소
`14.11.5 선고
서울중앙지법 2014가다503056
신한은행 (텔레뱅킹 사고)
-
-
전산망 침해 증거 불충분
보이스피싱, 스미싱, 악성코드
[금융고객 A]
[성명불상자 (해커, 보이스피싱 사기범 등)]
[금융회사 A – 이체 (은행/증권/저축은행 등)]
피싱사이트
보이스피싱
개인정보A
접근매체
(공인인증서-A)
악성코드
개인정보A
텔레뱅킹 이용
접근매체 재발급
(공인인증서-AA)
전기통신망 (텔레뱅킹)
인터넷뱅킹/모바일뱅킹
고객A 계좌
대포통장 계좌
개인정보A
접근매체
(공인인증서-A)
[공인인증기관]
공인인증서 발급
공인인증서 재발급
[금융회사 B - 대출]
[은행, 카드, 저축은행]
현금서비스, 대출승인
이용자 승소
`12.3.28 선고
서울중앙지법 2011가단105339
한국투자증권 (PC보안카드 저장)
공인인증서재발급
접근매체위조해당
이용자 승소
`12.8.22 선고
서울중앙지법 2011가단468047
우리은행 (OTP이용고객) - 1심
공인인증서재발급
접근매체위조해당

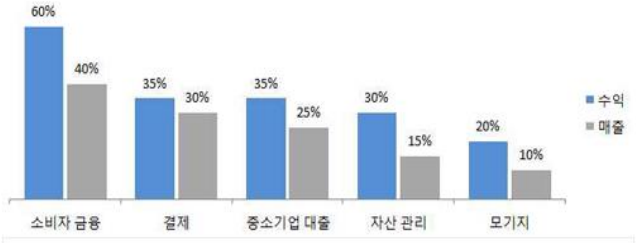
전자금융서비스 사고 관련 판례 분석 (대출관련 사건)



Insight & ForeSight

The Fight for the Customer

McKinsey Global Banking Annual Review 2015



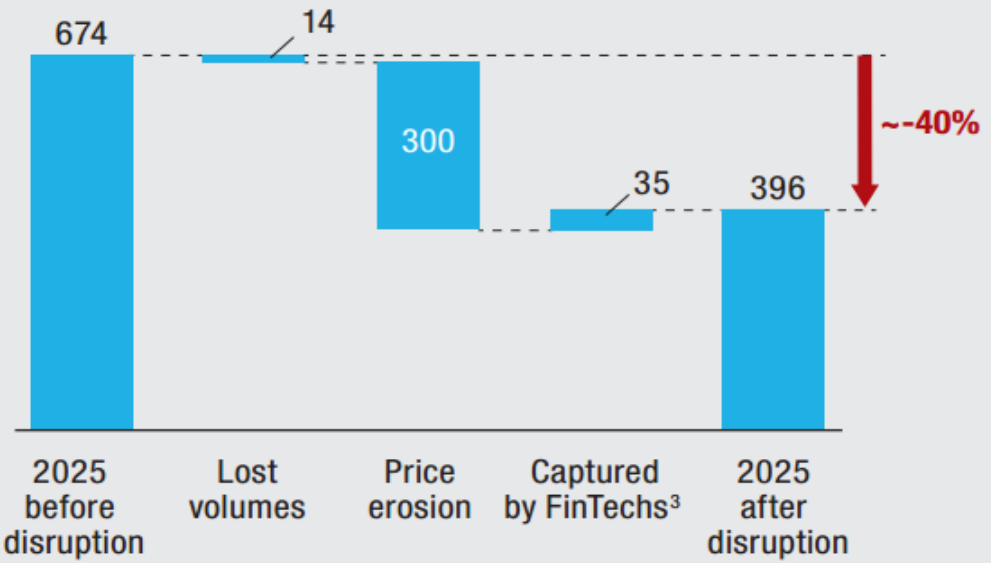
Esimated impact of FinTech disruption on five retail businesses, 2025

	Δ Profit[1] Percent	Δ Revenue[1] Percent
Consumer finance	-60	-40
Payments	-35	-30
SME lending	-35	-25
Wealth management[2]	-30	-15
Mortgages	-20	-10

Sample analysis

Disruption in consumer finance revenues

$ billion



[1] Compared to 2025 projections without the impact of Fintech and digital attackers; profit numbers include the impact of savings on operating costs as a result of digital; revenues are after risk cost, profits are after tax; figures are rounded.

[2] Excluding deposits

[3] Includes currently unbanked segments

Source: McKinsey Panorama

4. 미래금융 Biz 대응방안

초연결 사회에서의 금융의 미래와 보안 (금융의 위기 & IT/Security의 기회)

Technology

디지털 혁명

정치/경제/사회/문화 적인 다층적, 복합적
시대정신의 변화
(동일한 서비스를 상이한 기술기반으로 제공 가능)

인텔리젼스 혁명

데이터분석 & 인공지능 : 금융IT의 핵심화
(사회의 각 분야에서 인간의 노동을 대체하고 있음)

Hyper Connected Society

Business

세계화 (Globalization)

금융비지니스 변화 (직접금융 – Direct Finance)

(경쟁) Zero Cost IT기술활용

Risk Management : Big Data, Zero Cost
IoT, IoE : all Connected ...

Why not Security : Timing

금융 혁명 (Finance Revolution : 다이렉트 금융)

– The Future of Financial Security (금융보안의 미래) –
"Intelligence Security" : "(Big) Data Analysis & Risk Management"

The Integrity of Finance : 가상화폐의 미래, 수수료의 의미, 크라우드 펀딩

[참고1] FN's 40 leaders in fintech

1. 은행과 금융 서비스 회사들은 지금보다 더 **소비자의 선택**이 중심이 돼서 운영될 것
2. 미래 은행들은 **모바일 기기**로 옮겨갈 것
3. 시스템의 도움으로 항상 빈틈없이 **실시간**으로 고객의 잘못된 재정 운영을 멈추게 하고 올바른 선택을 할 수 있도록 돕게 될 것
4. 강력한 **알고리즘**으로 은행 **데이타**의 동향을 감시하게 될 것
5. 은행들은 고객 신분 정보 브로커가 될 가능성이 있음.
   고객정보분석과 행태를 추적관리하여 **새로운 유용한 정보를 창조하고 전달**하는 업무 수행
6. 은행들은 플랫폼으로 대체 될 것
   고객,금융상품,서비스를 분석, **고객 정보를 가공**하는 기술을 지향하는 플랫폼 회사로 변신
7. 금융 계정은 오픈 금융 생태계에서 모든 거래에서 유일한 신분증 역할을 수행하게 될 것
   하나의 계정으로 모든 거래를 하게 됨
8. 블럭체인(block chain) 기술이 널리 사용될 것.
   위험 또한 분산 되겠지만 새로운 문제가 대두될 것
9. 금융 거래가 **Social Network Platform**을 이용하는 추세가 확산될 것
10. 자본 조달 방식이 social network platform에 의해서 은행 중계가 사라지고
    투자자가 **직접 금융 소비자에게 자본을 제공**하는 것이 일반화 될 것

http://thetally.efinancialnews.com/2014/06/fintech-focus/

감사합니다

(facebook.com/sangshik, mikado22001@yahoo.co.kr)