최근의 보안이슈 및 금융IT 감독방향

2013. 12. 12

IT감독국
김윤진 부국장

목 차

Ⅰ 개요

1 전자금융거래 현황

2 IT보안 및 감독 강화 필요성 증대

1. 전자금융거래 현황

가. 인터넷뱅킹(2013년 9월말 기준)

◆ **은행** : 인터넷뱅킹 등록고객수는 전분기말 대비 **2.0% 증가한 9,347만명**

◆ 3/4분기중 인터넷뱅킹 일평균 이용금액은 **33조 4,790억원**으로 전분기대비 **0.4% 증가**

나. 모바일뱅킹(2013년 9월말 기준)

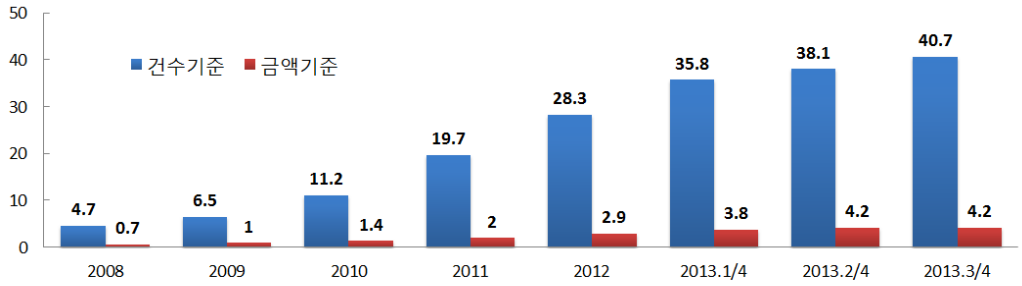
◆ 전체 모바일뱅킹 등록고객수는 전분기말 대비 **6.2% 증가**한 **4,706만명**

- **스마트폰** 기반 모바일뱅킹 등록고객수는 전분기말 대비 **8.9% 증가**한 **3,411만명**

◆ 3/4분기중 모바일뱅킹 일평균 이용건수 및 이용금액은 **2,230만건**, **1조 4,192억원**으로 전분기 대비 각각 **8.5%**, **1.8% 증가**

- **스마트폰** 기반 모바일뱅킹 일평균 이용건수 및 이용금액은 전분기말 대비 각각 **9.4%**, **1.5% 증가**한 **2,224만건**, **1조 3,723억원**

전체 인터넷뱅킹 중 모바일뱅킹 비중



•자료출처 : 한국은행
※본 조사에서 인터넷뱅킹은 모바일뱅킹을 포함하고 있음

<참고> 전자금융거래의 확산에 따른 영향

가. 비대면 거래 꾸준히 증가

◆ 스마트폰, 자동화기기(CD・ATM), 텔레뱅킹 등을 이용한 전자금융거래의 빠른 확산으로 지점 창구거래 비중이 지속적으로 감소

구분	입출금 및 자금이체 거래 기준	
	비대면 거래	대면 거래
2011.9월중	86.5%	13.5%
2012.9월중	87.8%	12.2%
2013.9월중	88.4%	11.6%

<자료:한국은행>

나. 금융회사 영업점 전략에도 영향

◆ '12년말 은행 점포 7,698개(출장소 포함) 중 10% 이상이 마이너스 실적을 거둔 것으로 조사(헤럴드경제, '13.8.21)

◆ 국내 은행들이 내년 상반기까지 총 79개의 영업점을 감축(198개 폐쇄, 88개 축소 또는 이전, 119개 신설) 할 계획(서울경제, '13.10.31)

2. IT보안 및 감독 강화 필요성 증대

다양한 서비스 출현

NFC

스마트폰 뱅킹

전자금융사기 지속 발생

◆피싱 피해 현황
- 피해 접수건수 : **43,208**건
- 피해 규모 : **4,534**억원
('06~'13.8월말 기준, 사이버경찰청)

◆파밍 피해 현황
- 피해 접수건수 : **1,553**건
- 피해액 : **80억26백만원**
('13.1~8월말 기준, 사이버경찰청)

◆신종금융사기 피해 현황
- 피해 접수건수 : **112**건
- 피해액 : **6억95백만원**
('13.6~7월말 기준, 사이버경찰청)

보안위협 증가

APT

보안취약점

◆ 전자금융서비스 확대 및 보안위협 증가에 따라 금융회사의 금융IT보안 역량제고 필요

➔ 안전한 금융서비스 제공을 위한 금융IT감독 역할 증대

II 최근의 보안 이슈

1. 금융전산 보안 강화 종합대책 추진
2. 전자금융사기 예방서비스 전면 시행
3. 금융권 전자금융관련 위기상황 대응 체계 개선
4. 윈도우 XP 지원종료에 따른 대응
5. 금융회사 IT 및 보안인력 확충 추진
6. 스마트폰 금융 안전대책 이행

1. 금융전산 보안강화 종합대책 추진

가. 종합대책의 개요 및 특징

▣ **지난 3.20 농협·신한은행 등 금융전산 사고를 계기로 금융전산 보안 전반에 대한 실태점검 및 TF 운영을 통하여 종합적인 개선대책 마련(7.11)**

▣ **금번 종합대책의 특징**

- **(최근 동향)** 최근 사이버공격은 APT 공격 등 여러 금융회사에 동시 다발적·반복적으로 발생하고, 날로 대형화·지능화되는 추세
- **(중점 방향)** 이러한 상황을 감안하여 금번 대책에서는 금융보안 패러다임 전환**(타율→자율, 비용→투자)** 에 중점

〈 금융전산 보안강화 종합대책 주요 특징〉
①금융회사의 자율적 내부통제 강화를 위하여 CISO 전임제 도입, 보안조직 권한 강화, 취약점 점검제도 도입 등 제도적인 장치를 마련
②금융회사의 자율적 보안노력을 유도하기 위하여 IT 신기술 보안가이드 제공, 보안수준 자체평가 지원 등의 지원방안 마련
③금융회사의 적극적 전산보안 투자를 유도하기 위하여 업무망과 인터넷망 분리를 의무화하고 이상금융거래를 탐지하는 시스템 구축대상을 확대

1. 금융전산 보안강화 종합대책 추진(계속)

1. 금융전산 위기대응 체계 강화

금융전산 보안 컨트롤타워 역할 강화

- (현행)금융결제원, 코스콤, 금융보안연구원 등 금융보안관련 기관간 역할 중복
- (개선)금융전산 보안 협의회 설치

전금융권 공동 백업전용센터 구축

- (현행)전산센터, 재해복구센터 동시 파괴 시 중요 금융정보 영구손실 우려
- (개선)금융권 공동백업 전용센터 구축

침해사고 전담반 운영 등 위기대응 능력 강화

- 침해사고분석 전담 조직을 금융ISAC 내 설치
- APT공격 등에 대응한 훈련시나리오 보안, 단말기 긴급 복구체계 마련

보안관제 및 정보공유 전 금융권 확대

- 전자금융거래 제공 금융회사는 금융ISAC 모니터링 의무화
- 금융회사별 수집정보를 공유할 수 있는 체계 구축

1. 금융전산 보안강화 종합대책 추진(계속)

2. 금융회사의 전자금융기반시설 보안 강화

금융전산 망분리 의무화

- 전산센터 물리적 망분리 의무화(2014년까지)
- 본점, 영업점은 단계적 망분리 추진
- 망분리 가이드라인 배포

금융전산시설 내부통제 강화

- CEO 책임하에 취약점 점검 및 보완조치 이행철저
- 非금융 전산시스템도 취약점 점검 및 보안관제
- 전산시스템 접근 시 별도의 추가인증 적용 의무화
- 보안규정 위반시 내부 제재근거 마련

금융보안관리체계 인증제도 도입

- 정보보안 및 전자금융거래 업무특성 반영
- 일정 규모 이상 금융회사 인증 의무화
- 인증 금융회사에 인센티브 부여

1. 금융전산 보안강화 종합대책 추진(계속)

3. 금융회사의 보안 조직•인력 역량 강화

조직 및 인력 강화

CISO 역할·독립성 강화

- CISO-CIO 겸직 금지
- CISO 전임자 임기보장
- IT보안위원회 운영
- CISO 정책협의회 활성화

전산보안 인력 사기진작

- CEO 책임하 보안인력 사기진작 방안 마련 시행
- 정보보호 관련 훈·포상 추천
- 정보보안 담당자 면책근거 마련

금융보안 전문인력양성 및 교육강화

- 금융보안 전문교육과정 확대
- 임직원 보안교육 강화
- 금융정보보호 교육센터 운영

금융보안 전문인력 확보 방안
(출처 : ’ 11.5월, 금융보안연구원)

1. 금융전산 보안강화 종합대책 추진(계속)

4. 금융전산사고 예방활동 강화로 금융소비자 보호 도모

금융 이용자 보호 강화

- **이상금융거래 탐지시스템 구축 확대**
  - 카드사 위주 → 은행, 증권 등으로 확대
  - 이상금융거래 정보 공유체계 구축 권고
- **금융회사 사칭 불법사이트 접속 차단**
  - 인터넷사업자(ISP)를 통해 불법사이트 접속 차단(Black List 등록)
- **보안사고 예방교육 및 홍보 강화**
  - 전자금융서비스 이용신청 시 교육·홍보자료 배포
  - 전자금융보안사고 예방법 설명 화면노출

금융전산부문 감독 및 검사 강화

- **금융지주회사 및 IT자회사 감독 강화**
  - 지주사·자회사 검사시 소속 IT자회사 연계검사
  - 위·수탁 계약시 전산사고 책임 명확화
- **전산사고 빈번한 금융회사 집중관리**
  - 사고원인 분석 및 조치 완료시까지 이행계획 집중 점검·관리
  - 금융전산 사고시 홈페이지 공시방안검토
- **업무정지 등 제재기준 마련**
  - 안전조치 의무 위반시 위법·부당행위의 경중에 따른 세부 제재부과 기준 마련

<참고> 전자금융감독규정 개정 주요내용 ('13.12.3)

가. 취약점 분석 · 평가

◆ **연 1회 이상(홈페이지에 대해서는 6개월에 1회 이상) 취약점 분석 · 평가 실시**

(대상기관) 총자산 2조원이고 상시 종업원 수 300명 이상 금융회사
(평가방법) CISO 및 내·외부 전문가로 자체 전담반을 구성하거나, 외부 전문기관에 위탁

◆ **간이 취약점 분석 평가**

(대상기관) 총자산 2조원, 상시 종업원 수 300명 미만 금융회사 또는 전자금융업자
(의무완화) 분석·평가 내용의 완화(감독원장 마련) 및 자체 전담반 구성 의무 면제

나. 침해사고대응기관 지정 및 업무범위

◆ **침해사고대응기관 : 금융결제원, 코스콤**

① 정보수집·전파를 위한 정보공유체계 구축
② 침해사고 예보·경보 발령내용의 전파
③ 침해사고의 확산방지를 위한 필요조치

◆ **금융회사는 침해사고대응기관의 장에게 침해사고 훈련(연 1회 이상) 결과를 제출해야 함**

<참고> 전자금융감독규정 개정 주요내용 ('13.12.3)

다. 임직원 정보보호 교육계획 수립 · 시행

◆ **CISO는 매년 의무교육시간 등 정보보호 교육계획을 수립 · 시행하여야 함**

임원 : 3시간 이상(CISO는 6시간 이상), **직원** : 6시간 이상, **IT 담당 직원** : 9시간 이상, **IT보안 담당 직원** : 12시간 이상

라. 정보보호 위원회 운영

◆ **금융회사 내에 정보기술보안사항을 심의 · 의결하기 위해 설치 · 운영**

CISO(위원회의 장) 주관 하에 준법감시인, 정보보호업무 관련 부서장 등으로 구성

마. 보안규정 위반에 따른 내부 처벌근거 마련 의무화

◆ **CEO는 정보보안 관련법규를 위반한 임직원에 대해 이를 제재하기 위한 내부 절차를 수립하여야 함**

<참고> 전자금융감독규정 개정 주요내용 ('13.12.3)

바. 정보처리시스템 접근통제 강화

◆ **정보처리시스템의 운영체제 계정으로 로그인할 경우, 추가인증절차 의무화**

- 계정의 사용권한, 접근 기록, 작업 내용 등 상시 모니터링 체계 구축

사. 금융전산 망분리 의무화

◆ **전산실 내 정보처리시스템 및 직접 접속 단말기에 대해서 외부통신망으로부터 물리적으로 분리(2014년말까지)**

◆ **내부 업무용 시스템은 외부통신망과 분리 · 차단 및 접속 금지(은행 15년말, 기타 16년말)**

아. 국외 사이버몰 결제업무에 대한 전자금융업 등록요건 완화

◆ **국외에서 주로 영업하는 국외 사이버몰에서 전자상거래 결제 업무를 대행하는 전자지급결제대행업자(PG)의 등록요건 완화**

- 해외 계열사의 인력, 전산시설 등 포함하여 인적, 물적 요건 등 등록요건 충족여부 판단
- 국내에서 발생하는 거래관련 민원처리 등을 위한 최소한의 인력 (전산업무 종사경력 1명 포함 3인)을 의무화

2. 전자금융사기 예방서비스 전면시행

가. 전자금융사기 예방시스템 개요

◆ **개요**

사기범이 **고객정보**(계좌번호, 계좌비밀번호, 보안카드번호 등)를 **획득**한 후 **고객명의의 공인인증서를 발급**받아 금융자산을 편취해가는 **사기수법을 예방**하기 위한 시스템

◆ **다음의 경우 추가적인 본인확인 필요**

①공인인증서를 발급/재발급 받거나 타기관에서 발급한 공인인증서를 등록하고자 하는 경우

①인터넷뱅킹을 이용하여 300만원 이상(1일 누적 기준) 이체하는 경우

◆ **시행 시기 : '13. 9. 26(목)**

◆ **대상자 : 개인 인터넷뱅킹거래 고객**

<본인확인 방법>

2. 전자금융사기 예방서비스 전면시행(계속)

나. 세부내용

① 이용자가 대상 거래를 수행할 PC를 미리 지정하는 경우

→ 이용자는 **다음의 방법* 중 한 가지**를 택해 **본인의 PC를 거래이용 PC로 지정**

ⓐ 휴대폰문자(SMS) 인증

ⓑ 2채널 인증(인터넷뱅킹 이용 중인 PC채널 외에 유선전화 등 다른 채널을 통해 인증)

ⓒ 영업점 방문(1회용 비밀번호를 발급받아 인증)

② 이용자PC를 미리 지정하지 않는 경우

→ **공인인증서 (재)발급 또는 타행 발급 공인인증서 등록시:** 상기 ⓐ, ⓑ, ⓒ의 방법으로 본인인증 후 (재)발급 또는 등록

→ **인터넷뱅킹을 통해 300만원 이상 이체시:** 상기 ⓐ, ⓑ의 방법으로 추가적인 본인인증을 거친 후 이체 가능(본인이 희망하는 경우 SMS사후통지로 변경 가능)

<참고> 신종 금융사기수법 개요

가. 메모리해킹 개요(자료 : 사이버경찰청)

◆ **(수법 개요) 정상적인 계좌이체 종료 후, 보안강화 팝업창이 뜨면서 보안카드번호 앞.뒤 2자리 입력 요구 → 일정시간 경과 후 범행계좌로 이체**

① 사용자PC가 악성코드에 감염됨

② 금융정보 유출

③④ 정상적으로 인터넷뱅킹 종료

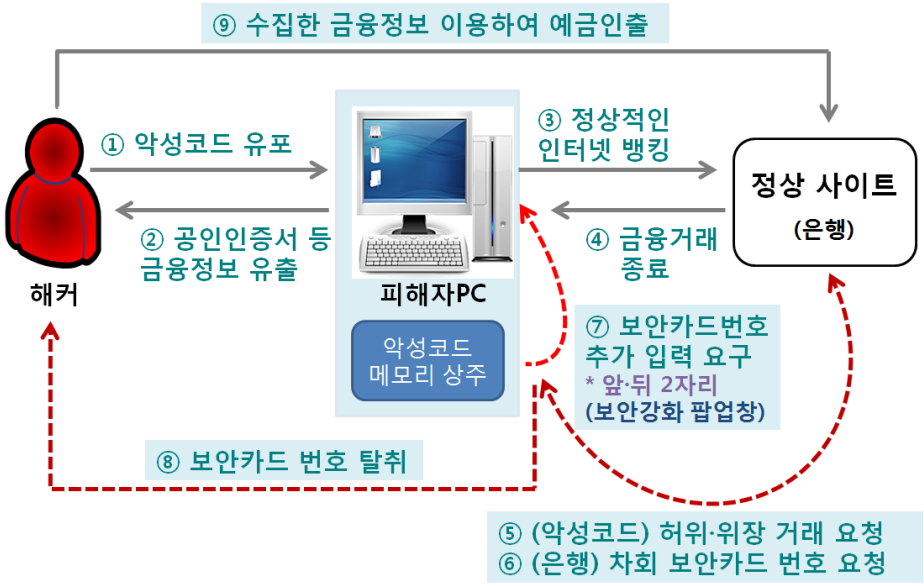
⑤ 사용자PC 메모리에 상주한 악성코드가 은행을 상대로 허위.위장 거래 요청

⑥ 은행 사이트에서는 정상 요청으로 오인하고 다시 보안카드번호 요청

⑦ 악성코드 작동으로 피해자 PC상에서 보안카드 번호 입력 요구(보안강화 팝업창)

⑧ 보안카드 번호 탈취 후 거래 중단

⑨ 수집한 금융정보를 이용하여 예금 부당 인출



<참고> 신종 금융사기수법 개요 (계속)

나. 금융권 조치내용

① **비정상 종료 거래에 대해 본인확인 강화**
* 보안카드 비밀번호 입력을 요구하였으나 요구한 **비밀번호가 입력되지 않고 거래가 종료**된 후, 다음 거래가 다른 PC에서 이루어질 경우에는 **본인확인을 강화**

② **악성코드 제거를 위한 백신프로그램 업데이트 및 배포**

③ **의심거래 발견시 고객에게 SMS 통지 및 보안카드 재발급 유도**

④ **신종 전자금융사기로 인한 피해를 예방하기 위해 이메일, 팝업창 등을 통해 소비자 유의사항을 안내**

다. 금융소비자 당부내용

① 인터넷뱅킹래 중 보안카드 비밀번호 등의 입력을 요구하는 **팝업화면**이 뜨는 경우 **정보를 입력하지 말고** 거래 금융회사에 문의

② 인터넷뱅킹 **거래가 비정상 종료되는** 경우 거래 금융회사에 문의

③ PC백신프로그램을 항상 최신버젼으로 유지하고 **악성코드 탐지 및 제거를 생활화**

④ 무료 다운로드 등 출처가 **불분명한 파일**은 다운로드 금지

⑤ OTP·보안토큰 등 **안전성이 높은 보안매체 사용**

⑥ 예금인출 사고시 즉시 해당 **금융회사 및 경찰청(☎112)에 신고**하고 **사기계좌의 지급정지를 요청**

3. 금융권 전자금융관련 위기상황 대응체계 개선

가. 개요

◆ **전자금융사고 발생에 보다 신속하게 대응하기 위해 금융감독원과 금융회사간 신속한 비상연락체계 구축이 필요**

- 기존 유선 및 이 메일을 통한 연락으로는 신속한 상황전파 및 대응에 한계

나. 전자금융사고 대응시스템 주요 개선내용

◆ **위기상황 대응요구서 작성 및 요청 기능(금감원)**

- 위기상황 발생 시 위기상황 전파 및 금융회사 대응현황 파악을 위한 위기상황 대응요구서 요청기능

◆ **위기상황 대응요구서 조회 및 대응보고서 작성 기능(금융회사)**

- 위기상황대응요구서를 조회하여 이에 대한 위기상황대응보고서를 작성·제출

◆ **전자금융사고대응 담당업무 설정(금융회사)**

- 담당 업무별(CIO, CISO, 문서책임자, 정보보호책임자 등) 사용자 지정

3. 금융권 전자금융관련 위기상황 대응체계 개선(계속)

다. 향후 대책

◆ **전자금융사고대응시스템 개선사항 안내 및 담당자 등록 협조요청**

- 사용자별 담당업무 지정 및 SMS수신을 위한 연락처를 최신상태로 갱신

◆ **향후 긴급 상황 발생시 동 전파체계를 이용한 위기상황 전파 실시 예정**

- 비상연락망을 통한 문자메시지 전송 및 위기상황대응요구서를 통한 상황 전파를 동시실시

4. 윈도우XP 지원종료에 따른 대응

가. 개요

◆ **MS사가 ’14.4.8부로 PC운영체제인 윈도우 XP에 대한 지원 종료 발표**

- 윈도우 XP의 안전한 전자금융서비스 제공에 한계가 발행할 것으로 예상

*** ’13.5월 기준 금융회사 전체 단말기 78만대 중 65.6만대(약 84.1%)가 윈도우 XP이하 버전 사용 중이고 CD/ATM의 경우 전체 8만대 중 7.8만대(약 97.6%)가 해당**

나. 문제점

◆ **윈도우 XP지원 종료시 보안패치가 이루어지지 않아 악의적인 공격에 상대적으로 취약**

- 윈도우 XP는 상위버전에 비해 악성코드 감염률이 2배 가량 높고 신 버전의 IE설치가 불가하여 웹 페이지를 통한 악성코드 유포에 취약

◆ **문제 해결에 대한 기술 지원이 중단되어**

- 윈도우 XP관련 장애 등 문제발생시 금융회사가 자체 해결 해야하는 문제점

4. 윈도우XP 지원종료에 따른 대응(계속)

다. 금융회사 유의사항

◆ **윈도우 XP 이하 운영체제를 상위 버전 운영체제로 전환**

- 윈도우 XP이하 단말기는 **'14.4.8**일 이전까지, 서버(윈도우 서버 2003)는 **'15.7.13**일까지 전환을 완료

◆ **운영체제 전환 이행계획 수립**

- 자체 운영체제 전환 계획을 수립하여 전환 실시

◆ **보안대책 및 비상 대응계획 수립**

- 운영체제 전환에 따른 프로그램 에러나 취약점으로 장애 또는 보안사고의 발생에 대비하여 대응계획 및 보안대책을 수립·운영

◆ **운영체제 미 전환 및 대응 소홀에 대한 책임 강화**

5. 금융회사 IT 및 보안인력 확충 추진

관련 규정

◆ 정보기술 부문 사고 방지 및 안전성 확보를 위해 IT인력을 전체인력의 5%, 보안인력을 IT인력의 5% 이상 확보토록 권고

미이행시 규제

◆ 이를 달성하지 못한 경우 홈페이지에 그 사유를 공시하도록 함으로써 인력 확보를 유도

향후 계획

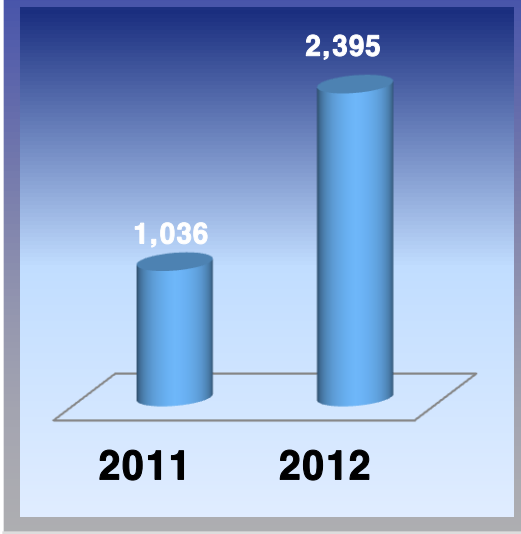
◆ 현행 권고 기준 충족 지도

◆ 인력 확충 방안 협조 요청

6. 스마트폰 금융 안전대책 이행

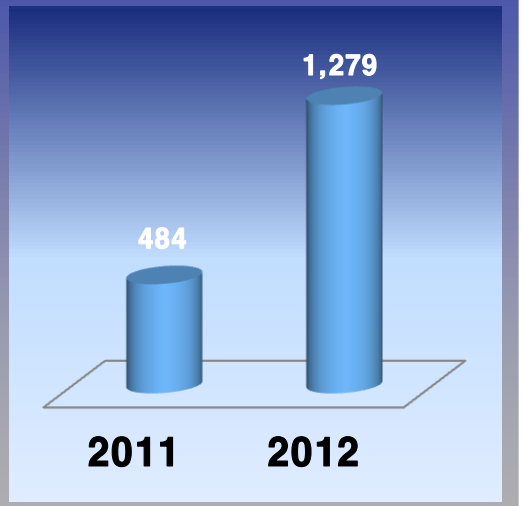
◆ 스마트폰 금융 이용자의 급증으로 스마트폰에 대한 다양한 보안위협 제기

스마트폰 뱅킹 등록 고객 수
(단위 : 만명)



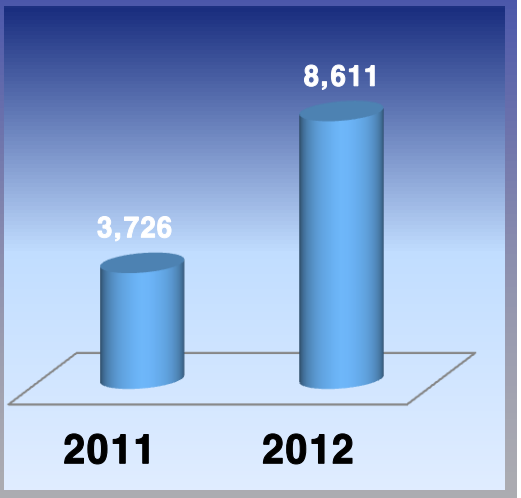
▲ 131.3% up

모바일뱅킹서비스 이용 건수
(단위 : 건)



▲ 116.4% up

일평균 모바일뱅킹 이용 금액
(단위 : 억원)



▲ 131.1% up

6. 스마트폰 금융 안전대책 이행(계속)

가. 스마트폰 금융 안전대책 실태점검개요

점검기간	◆ (현장점검)'12.11.12 ~ 12.06 (3주간) * 현장점검에서 제외된 회사는 서면점검 수행
점검대상	◆ 스마트 폰 전자금융 앱을 제공하는 금융회사
중점검사	◆ 「스마트폰 전자금융서비스 안전대책」 및 「스마트폰 앱 위 · 변조 방지대책」 등에 대한 이행여부를 중점점검

나. 결과조치 및 향후계획

◆ 미준수 금융회사에 대해서는 이행계획서 징구
◆ 점검결과 주요 미흡사항에 대한 유의사항 통보
◆ 현장 및 자체점검 결과시 징구 이행계획서에 대한 서면점검 실시 중 ('13.11.22~'14.2.21)

<참고1> 스마트폰 전자금융서비스 안전대책(2010.1)

보안위협	보안 대책
전자금융거래 서비스	▶ 다단계 가입자확인을 통해 전자금융서비스 가입 절차 강화 * 1단계 확인(ID.비밀번호 등)→2단계 확인(일회용비밀번호 등)→3단계 확인(공인인증서 등) 이용고객에 대한 보안유의사항 안내 후 가입 허용 (고객 홍보 강화) ▶ 로그인시 사용자 인증강화(공인인증서, OTP) ▶ PC 인터넷뱅킹 거래인증방법 및 자금이체한도 적용 ▶ 멀티로그인(Multi-Login) 제한, 스마트폰 지정제 도입
기술적 침해대응	▶ 금융거래정보의 종단간(End-to-End) 암호화 ▶ 입력정보 보호대책 적용, 중요정보를 스마트폰에 저장 금지 ▶ 악성코드 예방대책 적용 (지속적인 패턴 업데이트) ▶ 전자서명 등을 이용한 부인방지 적용 ▶ 금융거래기록 보관 범위 확대
취약점 모니터링, 고객정보 보호	▶ 잠재적인 취약점에 대한 모니터링 강화 ▶ 신규 발견된 취약점에 대한 즉각적인 보안대책 적용 ▶ 고객정보보호 캠페인 지속 추진 ▶ 정보보호전문가 양성을 위한 교육 프로그램 확충

<참고2> 스마트폰 앱 위·변조 보안대책(2012.6)

보안위협	보안 대책
기기 임의개조	① 폰 임의개조* 탐지 및 차단 * 탈옥(아이폰), 루팅(안드로인드폰)
앱 위·변조	② 전자금융앱 위·변조 탐지 및 차단
	③ 앱자체 보호(난독화, 안티디버깅, 무결성체크 등)
악성프로그램 감염	④ 백신프로그램 제공
입력·전송 정보 절취 또는 위·변조	⑤ 가상 보안키패드 제공
	⑥ 통신 암호화
	⑦ 확장형 E2E* 적용 * End-to-End : 금융거래정보가 입력되는 폰의 키패드 부터 금융회사의 서버까지 정보를 암호화

Ⅲ 금융IT 감독 방향

1 금융IT감독 강화

2 전자금융사고에 대한 선제적 대응

3 전자금융 소비자보호 강화

4 IT검사품질 제고

IT감독 업무 추진 방향

전자금융 안전성 제고 및 이용자 보호

금융IT감독 강화

- 전자금융거래의 본인 확인방법 다양화 추진
- 신기술기반 전자금융 거래서비스 감독강화
- IT감독협력체계 구축
- 전자금융업자에 대한 감독·검사 강화

전자금융사고 선제적 대응

- IT보안 강화대책 이행 여부 점검
- 전자금융사기 예방 서비스 이행상황 모니터링

전자금융 소비자보호 강화

- 장애인대상 전자금융 서비스 편의성 제고
- IT 감독 정책에 대한 소통 활성화
- 소비자 보안의식 제고를 위한 홍보강화

IT검사 품질 제고

- 보안 취약 부문에 대한 테마 검사 실시
- 효율적인 IT검사지원
- IT검사 역량 강화
- 금융지주사 소속 IT자회사 연계검사 실시

1. 금융IT감독 강화

가. 전자금융거래의 본인 확인방법 다양화 추진

인증방법평가위원회 구성('10.9월)

신규인증방법

인증방법평가기관 지정(4개사)

* 금융보안연구원, 한국시스템보증,
한국정보통신기술협회, 금융결제원

☞ 「인증방법평가위원회」운영을 통해 **공인인증서 이외의 다양한 인증방법 도입을 유도**

1. 금융IT감독 강화(계속)

나. 신기술기반 전자금융서비스 감독강화


NFC


스마트폰 뱅킹


모바일 직불카드

신기술 기반 다양한 전자금융서비스

- 스마트폰 뱅킹에 우려되는 위협요소 사전 모니터링 및 대응방안 마련
  * SMS문자 탈취, 메모리해킹 등 신·변종 전자금융사기
  - **스마트폰 금융 안전대책 이행실태 서면점검('13.11.22~'14.2.21)**
- 모바일 직불카드 등 새로운 매체를 이용한 전자금융거래서비스의 안전대책 마련

1. 금융IT감독 강화(계속)

다. IT감독협력체계 구축

해킹에 대한 협력체계 강화

◆ **한국인터넷진흥원(KISA)**과의 **업무협조체제 강화**

▪ 피싱·파밍 등 전자금융사기와 관련된 침해사고 사전예방 및 공동대응체계 구축

◆ 금융권·금융IT보안업체 실무자 등이 참여하는 **가칭「금융IT보안 연구회」 구성·운영**

1. 금융IT감독 강화(계속)

라. 전자금융업자 대한 감독 · 검사 강화

INITECH 이비카드 AUCTION ebay쇼핑 이베이 코리아 LG U+ 브이피(주) money 한국스마트카드 Korea Smart Card KG MOBILIANS Webcash

소비자보호

- 전자금융업자의 사고예방, 법규준수 유도를 위해 모니터링 강화
- 거래 유형·리스크 규모에 따른 검사 실시

2. 전자금융사고에 대한 선제적 대응

가. IT보안 강화대책 이행 여부 점검

◆ 취약점 분석 · 평가 현황, 금융전산 망분리 현황 등 금융권의 IT보안 강화대책 이행 여부를 점검

전자금융기반시설의 취약점·분석 평가

□ 정보기술부문 내부통제, 접근매체, 침해사고 대응조치 등을 연 1회이상 분석·평가 실시해야 함*

* 전자금융거래법 제21조의3('13.11.23일 시행)

금융전산 망분리

□ 업무망과 인터넷망의 분리 의무화*

* 망분리 가이드라인 '13.9.16일 배포

- 전산센터 : '14.12월까지 물리적 망분리 의무적으로 실시
- 본점 및 영업점 : 규모별로 단계적 망분리 추진, 망분리 방식은 선택가능

2. 전자금융사고에 대한 선제적 대응(계속)

나. 전자금융사기 예방서비스 이행상황 모니터링

□ 「전자금융사기 예방서비스」 전면 시행('13.9.26) 이후 **이행상황**을 **모니터링**하여 **문제점**에 대한 **대응 방안**을 **마련**

- 고객 스마트폰에 **악성앱**을 **설치**하거나, 고객의 부주의를 이용하여 **SMS 인증 정보**를 **탈취**하는 등 수법이 고도화지능화 되는 경향

- **휴대폰 SMS 인증 보안성 강화** 방안 마련

3. 전자금융 소비자 보호 강화

가. 장애인에 대한 전자금융서비스 편의성 증대

시각장애인 인터넷뱅킹

휠체어 고객 ATM

➡ 「장애인차별금지법」시행('13.4월) 이후 장애인에 대한 **전자금융서비스 이용편의 실태 조사**

- 인터넷뱅킹, 자동화기기 등에 대한 장애인 편의성 제공 미비 회사에 대해 법률 이행을 독려

3. 전자금융 소비자 보호 강화(계속)

나. 소비자의 보안의식 제고

대학생 금융보안캠프

- 금융소비자의 보안 인식 제고를 위해 금융보안연구원 등과 공동으로 **대학생 캠프, 금융정보보호 세미나 및 논문, 수기 공모전 개최**
- TV, 신문, 소셜미디어 등을 통해 전자금융 **소비자에 대한 홍보를 강화**

4. IT검사품질 제고

가. 보안 취약 부문에 대한 테마검사 실시

- 전자금융거래 이용현황, 본인 확인절차의 적정 여부 등 **'전자금융거래서비스 운영실태'에 대한 테마검사 실시**
- **IT내부통제 및 고객정보보호**에 대한 IT보안 실태 테마검사 실시

4. IT검사품질 제고(계속)

나. 전자금융거래 상시감시 강화

- IT감독국 검사지원팀의 **상시감시 활동 강화**로 IT리스크 요인 **사전 점검 및 적기 대응**
- 전자금융업자의 결제 불이행 예방을 위해 재무건전성, 영업실적 등 경영 **건전성 감시 강화**

4. IT검사품질 제고(계속)

다. 검사 역량 강화

새로운 서비스


NFC


스마트폰 뱅킹


직불결제

신종 보안위협


APT


악성코드


보안취약점

- 신기술 및 정보보안 등에 대한 외부 IT전문교육기관 연수를 실시하여 **검사 인력의 전문성을 강화**
- IT보안 실태 점검시 등에 **전문소프트웨어 및 외부전문인력을 활용**하는 등 IT검사 효율성을 제고

4. IT검사품질 제고(계속)

라. 금융지주사 소속 IT자회사에 대한 연계검사 실시

하나아이앤에스

MERITZ 메리츠금융정보

KB 데이타시스템

신한데이타시스템 SHINHAN DATA SYSTEM

DGB금융그룹 DGB데이터시스템

우리에프아이에스 WOORI FIS

BS BS정보시스템

- 금융지주사 소속 주력 금융회사에 대한 검사시 **지주사 소속 IT자회사**에 대해서도 **연계검사**를 실시

Ⅳ 맺음말

전자금융거래의 신뢰도 제고 및 리스크 최소화

금융당국

- 보안 컨트롤타워 역할강화
- 금융권 전체 보안 거버넌스 확립
- 금융회사 IT보안 역량 강화 및 보안 취약 요소 개선

금융회사

- 자체 보안 거버넌스 확립(보안 투자 및 인력 확보 등)
- IT 내부통제의 확립 및 보안 아웃소싱 관리 개선
- 보안시스템 설계 및 기술적 보호 조치 강화

금융소비자

- 개인정보는 스스로 보호한다는 인식 필요
- 보안 강화를 위해 다소 불편을 감내해야할 필요

IT산업계

- 새로운 보안위협에 대한 발빠른 대응 솔루션 개발
- IT 전문인력에 대한 집중양성
- 보안 기술 개발을 위한 투자 강화

안전한 전자금융 거래환경 조성 및 전자금융 소비자 보호

Thank You !