안전한 전자금융 구현을 위한 금융감독 방향

2013.7.18.

IT감독국 IT보안팀장 정 기 영

금융감독원

목 차

2013년 도
금융IT 감독 · 검사 업무 방향

대내외 금융IT 감독 환경 변화

전자금융 거래 증가	IT리스크 증가	소비자보호 강화필요	IT감독 · 검사 수요증대
거래규모 증가	IT보안사고 발생	금융거래정보 보호강화	선제적 감독 검사 강화
거래 수단 다양화	신규 보안위협 증가	장차법 시행 ('13.4월)	기획 · 테마 검사 강화

IT·전자금융 부문에 대한 감독·검사 강화

전자금융 안전성 제고 및 이용자 보호

금융IT 감독 강화

- IT지배구조 정착
- 신기술 전자금융 감독강화
- 온라인 결제 보안 강화

사이버테러 선제 대응

- 전자금융사기 예방서비스 실시
- 사고 예방중심 감독
- 보안취약점 관리·감독 강화

소비자 보호 강화

- 장애인 편의성 제고
- IT감독 정책 소통 강화
- 소비자 보안 의식 제고

IT검사 품질 제고

- 보안테마 검사 실시
- 효율적 검사 지원 (선택과 집중)
- 검사 역량 강화

II 주요 금융IT 보안 이슈 및 감독방향

1. 사이버테러 대응강화 및 종합대책 마련
2. 전자금융사기 예방서비스 전면 시행
3. 공인인증서 제도의 문제점에 대한 개선방안 마련
4. 인증방법평가위원회 운영 활성화
5. 전문 인력 및 예산 확충
6. 장애인 전자금융서비스 편의성 증대
7. 스마트폰 금융 안전대책 마련
8. 윈도우 XP지원 종료에 따른 대응방안
9. 금융권 전자금융관련 위기상황 연락체계 개선

1. 사이버테러 대응강화 및 종합대책 마련(1)

가. 사고 개요

3.20 사고개요

◆ '13.3.20(목) 5개 금융회사의 영업점 **단말기(PC) 및 자동화 기기(ATM)** 들이 **악성코드에 감염**되어 영업점 거래가 중단

복 구

◆ 사고당일 인터넷 뱅킹 및 창구영업을 재개 하였으며, 이후 영업점 PC 및 ATM도 모두 복구 완료

사고원인

◆ 공격자가 **조직적, 장기적으로 보안이 취약한 서버 및 단말기를 공격**하여 사용권한을 탈취하고 악성코드를 PC 및 자동화기기에 유포하여 장애를 발생시킨 **지능형지속위협(APT) 공격의 형태**

1. 사이버테러 대응강화 및 종합대책 마련(2)

나. 사고이전 보안강화 대책

1 금융회사 IT 보안강화 종합대책(2011) 마련

➢ 정보보호최고책임자(CISO) 지정 제도 도입, 보안 인력 및 예산 확충, IT보안 인프라 강화

2 IT보안 실태에 대한 테마검사 실시

➢ 은행·증권·보험·비은행을 대상으로 외부전문가와 합동으로 보안실태 점검

3 2013년 2월 이후 사이버테러 대응강화 조치 내용

➢ 금융전산 위기경보 조치

- 북한 핵실험에 따른 금융전산 위기경보 **"관심"** 단계 발령(2.12 17:00) 및 **위기관리 활동 강화 요청**(3.8)

➢ **DMZ구간 내** 전 서버에 대한 **취약점 분석 및 보안 관제 실시** 지도

➢ 은행·비은행·보험 **CIO 대상** 사이버테러 대응 강화 지도

1. 사이버테러 대응강화 및 종합대책 마련(3)

다. 사고이후 조치내용

1 **금융위와「금융전산위기관리협의회」 및「금융전산위기상황대응반 」구성**

◆ 위기경보수준을"관심"에서 "주의"로 격상(3.20 15:30)

2 **금감원 「자체비상대책반 」 가동(3.20)**

◆ IT담당 부원장보를 반장으로 24시간 비상대책반 구성·운영

3 **IT검사역을 현장에 투입(3.20)**

◆ 사고발생 금융회사에 즉시 IT검사역을 투입하여 사고원인 및 복구조치 점검

4 **보안대책 이행 철저 및 업데이트 서버에 대한 악성코드 감염여부 점검 지도**

5 **고객피해 발생현황 파악 및 피해 발생사실 확인시 피해보상대책 방안강구 지도**

6 **휴일 및 급여일(25일) 대비 비상근무 유지 지도(3.22)**

1. 사이버테러 대응강화 및 종합대책 마련(4)

라. 향후 대책

사이버테러 방지를 위한 조치 방안

전산장애 발생 금융회사에 대해 사고검사 실시

◆3.27(수)부터 **사고 원인 및 법규 위반** 여부 등에 대해 검사 실시

IT보안 실태 테마검사 및 IT모범규준 이행 실태점검 실시

◆(검사대상) 은행, 증권, 카드, 보험 등

◆(중점 검사/점검 사항)

–(보안실태) IT보안 내부통제 체계, IT보안 시스템 취약점, 개인정보보호 준수여부

–(모범규준) CISO 임명, IT보안 인력 및 예산의 비율준수 여부, 취약점 점검 및 정보기술 계획 수립, 침해사고 대응책 마련

금융전산 보안 강화 대책 마련

◆IT보안 실태 테마검사 및 IT모범규준 이행 실태점검 결과 등을 기반으로 **금융전산 보안 대책** 마련 예정

2. 전자금융사기 예방서비스 전면 시행(1)

가. 전자금융사기 예방서비스 개요

▣ (현재)공인인증서 재발급 또는 자금이체 시 **보안카드 또는 OTP**만으로 본인여부를 확인

▣ (향후)공인인증서 재발급 또는 자금이체 시 이용할 단말기(PC)를 금융회사에 등록하여 **지정된 단말기**를 이용하거나

- 미지정 단말기에서는 기존의 보안카드 또는 OTP 등의 본인확인 이외에 **추가 인증(휴대폰문자 또는 전화 인증 등)** 실시

※ 300만원 이상 자금이체 시 동 서비스를 이용하지 않는 고객에 대해서는 휴대폰 문자 메시지로 이체사실을 통지

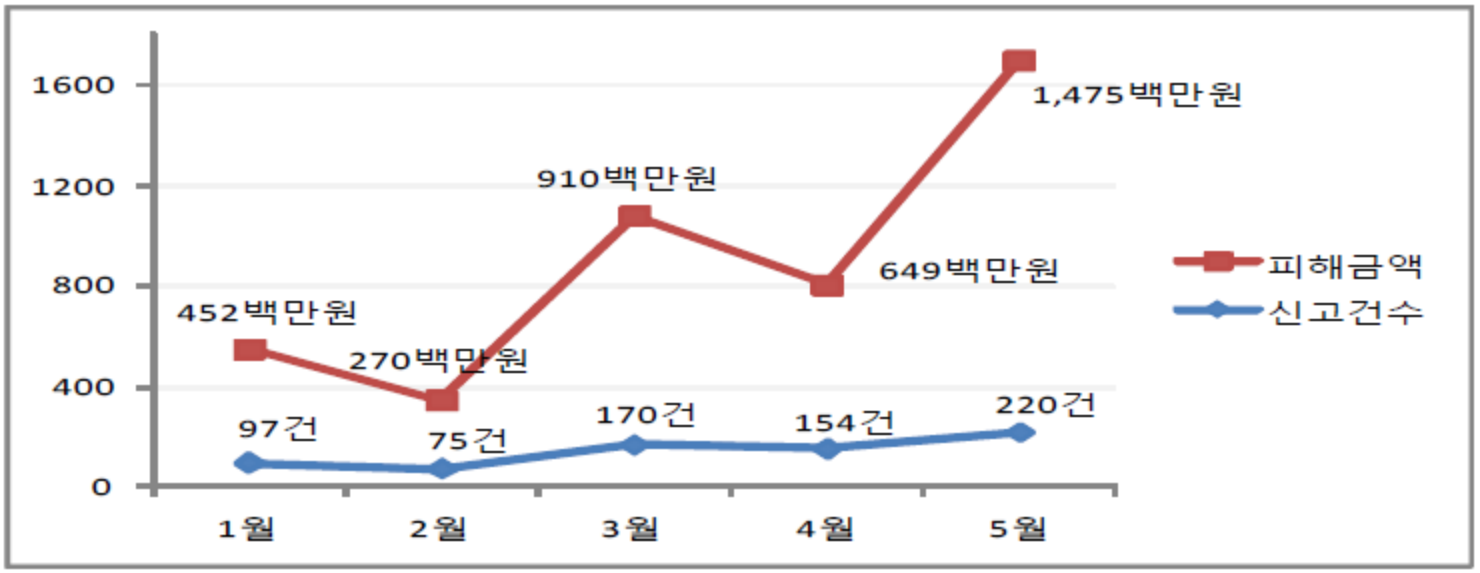
〈참고〉 파밍 공격 피해 현황

◆ 전체적인 전자금융사기 피해는 감소

('11년 8,244건 / 1,019억원 → '12년 5,709건 / 595억원)

◆ 그러나, 파밍 등 신종금융사기 건은 증가 추세

('13.1월 97건 / 4.5억원 → 5월 220건 14.8억원)



< 파밍 신고 건수 및 총 피해금액 현황 ('13. 1~5월) >

2. 전자금융사기 예방서비스 전면 시행(2)

나. 향후 계획

’13년 9.26 부터
전면 시행 예정

☑ 전자금융사기 예방서비스 전면시행 전
대국민 홍보를 강화하기 위하여
TV, 라디오 등 다양한 매체를 통한 홍보 실시 예정

☑ 전면시행에 차질이 발생하지 않도록
금융회사의 철저한 준비 필요

3. 공인인증서 제도의 문제점에 대한 개선방안 마련

추진방향

◆ 공인인증서 사용 실태를 고려할 때 대안 없이 폐지하는 경우 많은 부작용 예상

◆ 금융위 「전자금융인증체계 개선방안」용역 후 대응책을 마련할 계획

◆ 「인증방법평가위원회」운영을 통하여 공인인증서 이외의 다양한 인증기술 도입 유도

4. 인증방법평가위원회 운영 활성화

설치 배경

◆ 국무총리실 주관 T/F는 공인인증서 대체 인증방법에 관한 **「전자금융거래 시 인증방법에 대한 가이드라인」**을 발표('10.5.31)

◆ 동 가이드라인의「인증방법평가위원회」를 금감원내 설치('10.9.20)

운영 현황

◆ '10.10월 이후 현재까지 총 8회의 위원회가 개최되었으며 **총 2건의 인증방법 안전성 평가 완료**

◆ 다만, 현재까지 공인인증서를 대체하는 인증방법평가 이루어지지 않고 있으며, 평가 완료된 인증방법의 시장활용도 미미

조치 방안

◆ 인증방법 평가완료 시 관련사실을 금융회사 등에 통보

◆ 공인인증서 외 인증방법 도입 협조요청

5. 금융회사 IT 및 보안인력 확충 요청

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

〈참고〉 IT 및 보안인력 확충을 위한 협조 요청사항

금융연수원, 대학 등에 위탁교육 활성화

✓ 금융회사 IT 인력의 전문성 제고를 위하여 금융연수원, 국내 대학 보안관련학과 등에 위탁 교육 실시

✓ 금융연수원이 금융보안 담당자 과정을 개설하였으며, 국민은행은 고려대학교 정보보호 전문 대학원에 20명의 직원을 위탁교육 중

정보보호관련 학과에 대한 산학 연계 유도

✓ 금융권은 우수 IT 및 보안 인력을 유치하기 위하여 국내 대학과 산학 협조 강화

⇒금융권은 사회공헌 사업을 통해 회사 이미지를 제고하는 동시에 금융IT 보안에 필요한 인력 확보 가능

IT인력 및 정보보호 인력에 대한 우대책 시행

✓IT 전문 자격증 소지자 등 우수 IT인력에 대한 승진 및 포상 등 우대 정책 시행

6. 장애인 전자금융서비스 편의성 증대

「장애인차별금지법('13.4월)」 이행 강화

장애인에 대한
전자금융서비스 이용편의
제공 실태를 점검하고
조속한 법 이행을 독려

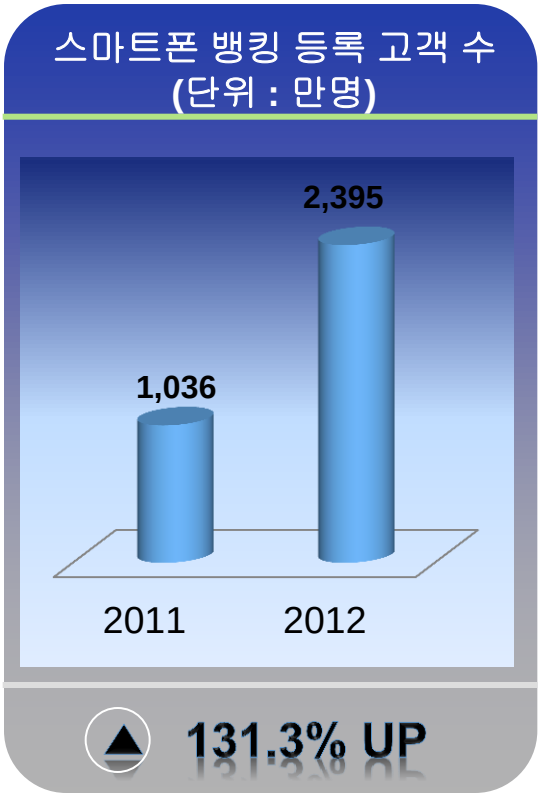
IT실태평가에 반영

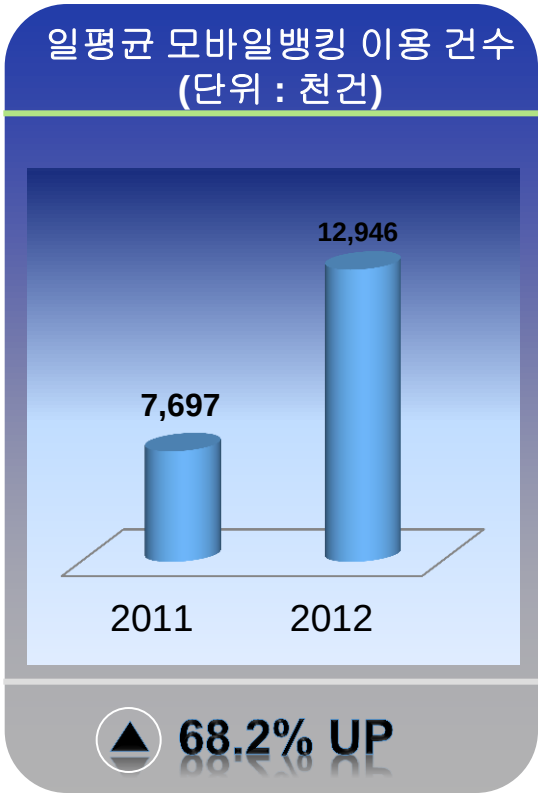
IT실태평가에
장애인 전자금융서비스
관련 평가항목을 추가
('13.2/4분기 중)

7. 스마트폰 금융 안전대책 마련(1)

◆ **스마트폰 금융 이용자의 급증으로 스마트폰에 대한 다양한 보안위협 제기**

(2013년 ¼분기 스마트폰 뱅킹 고객수 2,807만명, 모바일뱅킹 이용건수 18,935천건, 이용금액 1,264십억원)





7. 스마트폰 금융 안전대책 마련 (2)

◆ 스마트 폰 금융 보안 위협의 증가가 예상됨에 따라 스마트 폰 금융 안전대책 실태 점검

점검 기간	◆ (현장점검) '12.11.12 ~ 12.6 ◆ (서면점검) '13.2.19 ~ 4.30
점검 대상	◆ 스마트폰 전자금융앱을 제공하는 12개사 대상 ◆ 현장점검 제외 74개 금융회사
중점 검사	◆ 스마트폰 전자금융서비스 안전대책(2010.1) 및 스마트폰 앱 위·변조 방지대책(2012.6) 등에 대한 이행여부를 중점 점검

7. 스마트폰 금융 안전대책 마련 (3)

1. 점검결과

◆ **은행, 카드, 보험권역의** 안전대책 준수율은 **대체로 양호**(80% 이상)한 반면, **증권 및 저축은행 권역**의 준수율은 **저조**

◆ **스마트폰 금융보안 부문**의 **안전대책** 준수율은 **전반적**으로 **양호(95%)**한 반면, **앱 위·변조 방지** 부문의 준수율은 **미흡**한 수준

2. 결과 조치 및 향후 계획

◆ 현장점검 후 미 준수 금융회사에 대해서는 이행계획서 징구

◆ 현장 및 서면 점검결과 주요 미흡사항에 대한 유의사항 통보

◆ 2013년 하반기 중 현장점검 재 실시 예정

8. 윈도우 XP 지원종료에 따른 대응방안(1)

1. 현황

◆ 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

2. 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

8. 윈도우 XP 지원종료에 따른 대응방안(2)

3. 금융회사 유의사항

◆ 윈도우 XP 이하 운영체제를 상위 버전 운영체제로 전환

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

9. 금융권 전자금융관련 위기상황 대응체계 개선(1)

1. 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

2. 전자금융사고 대응시스템 주요 개선내용

◆ 위기상황 대응요구서 작성 및 요청 기능(금감원)

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

◆ 위기상황 대응요구서 조회 및 대응보고서 작성 기능

- 위기상황대응요구서를 조회하여 이에 대한 위기상황대응보고서를 작성·제출

◆ 전자금융사고대응 담당업무 설정

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

9. 금융권 전자금융관련 위기상황 연락체계 개선(2)

3. 향후 계획

◆ 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

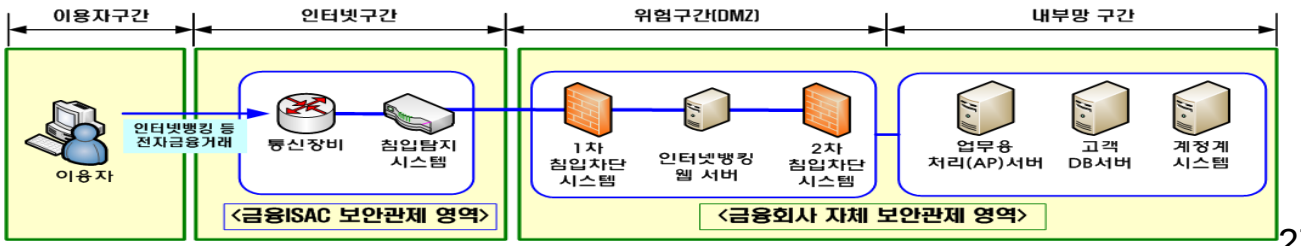
Ⅲ 금융전산 보안 강화 종합대책

1. 금융전산 위기대응 체계 강화
2. 금융회사 전자금융기반시설 보안 강화
3. 금융회사의 보안조직 및 인력 역량 강화
4. 금융 이용자 보호 및 감독 강화
5. 금융회사의 자율적 보안노력 지원

1. 금융전산 위기대응 체계 강화

금융전산 보안 컨트롤타워 역할 강화	▪ (현행)금융결제원, 코스콤, 금융보안연구원 등 금융보안관련 기관간 역할 중복 ▪ (개선)금융전산 보안 협의회 신설
금융권 공동 백업전용센터 구축	▪ (현행)전산센터, 재해복구센터 동시 파괴 시 중요 금융정보 영구손실 우려 ▪ (개선)금융권 공동백업 전용센터 구축
침해사고 대응전담반 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

* <참고> 금융권 침해대응 모니터링 체계



2. 금융회사의 전자금융기반시설 보안 강화

금융전산 망분리 의무화

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

해킹 경로 차단

금융전산시설 내부통제 강화

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

시설 보안 강화

금융보안관리체계 인증제도 도입

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

평준화된 보안수준 향상

3. 금융회사의 보안조직, 인력 역량 강화

보안역량 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)

4. 금융 이용자 보호 및 감독 강화

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·홍보 자료 배포
  - 전자금융보안사고 예방법 설명 화면 노출

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 공시방안 검토
- **6개월 업무정지 등 제재기준 마련**
  - 안전조치 의무 위반시 위법·부당행위의 경중에 따른 세부 제재부과 기준 마련

5. 금융회사의 자율적 보안노력 지원

자율적 보안 강화

☑ IT 신기술 접목 전자금융거래의 보안가이드 제공

- 새로운 IT기술과 전자적 장치를 활용한 전자금융 거래의 안전성 확보 유도

☑ 중소형 금융회사 보안 지원체계 마련

- 금융보안 전문기관 등을 통해 중·소형 금융회사에 대한 취약점 점검, 보안수준 진단 등을 지원

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 보호 한다는 인식필요
- 보안 강화를 위해서는 다소 불편을 감내할 필요

안전한 전자금융 거래환경 조성 및 전자금융 소비자 보호

Thank You !