(붙임)

전자거래 안전성 강화 종합대책

2005. 9.

금 융 감 독 원

차 례

Ⅰ 수립배경 및 추진경과

□ 수립배경

o 세계 최고수준의 인터넷 이용환경을 바탕으로 인터넷에 기반한 금융거래 및 상거래 규모가 급증하면서 전자거래는 국가경제의 한 축으로 성장

- 은행 전체 거래중 전자금융 비중 76%, 증권 전체 거래중 사이버 비중 60% 도달

- 전자상거래 규모도 지난해 314조원을 기록

o 그러나, 지난 5월 발생한 인터넷뱅킹 해킹사건은 전자금융, 전자상거래를 포함한 전자거래 전반에 대한 불신 초래 및 거래 위축 우려

- 따라서 금번 사건을 계기로 전자거래에 관한 종합적인 안전성 강화대책을 마련하여 국민들이 안심하고 이용할 수 있는 전자거래 기반 조성

□ 추진경과

o '05. 5. 10 : 국내최초 인터넷뱅킹 해킹사건 발생(6. 4 범인검거 발표)

o '05. 5. 26 : 인터넷뱅킹용 인증서관리 프로그램의 해킹 취약성 보도 (KBS, MBC)

o '05. 6. 10 : 경제정책조정회의에 전자거래 안전성 강화대책 추진 보고

o '05. 6. 20 : 관계부처 합동 Task Force 구성(정통부, 산자부, 금감위, 금감원, 한국정보보호진흥원/총 5차례 합동회의)

o '05. 7. 4 : 금감원 주관 금융권 공동 Task Force 구성(총 28회 협의)

Ⅱ 전자거래 현황 및 문제점

1. 전자거래 현황

□ 인터넷뱅킹 이용현황

o '05년 6월말 인터넷뱅킹 고객수는 2,290만명, 2/4분기 인터넷뱅킹 서비스 이용건수는 일평균 1,042만건으로 창구거래 수준에 육박

- 특히, PC를 이용한 인터넷뱅킹 비중이 97.5%로서 휴대전화, PDA 등 이동통신기기를 이용한 모바일뱅킹에 비해 높은 수준

□ 사이버증권 이용현황

o '05년 2/4분기 사이버증권 거래규모는 833조원으로 전체 증권거래 규모(1,389조)의 60% 차지

□ 전자상거래 이용현황

o '05년 2/4분기 월평균 전자상거래 사업체수는 3,856개, 2/4분기 거래액은 2조 4,749억원으로 전년동분기에 비해 35% 증가하는 등 매년 큰 폭으로 증가 추세

□ 전자거래사고 현황

(단위 : 건)

유 형	2002년	2003년	2004년	2005년 7월 현재	계
현금/신용 카드복제	4(452)	6(66)	6(26)	-	16(544)
텔레뱅킹	-	1(10)	5(162)	5(186)	11(358)
인터넷뱅킹	1(71)	-	1(3)	2(67)	4(141)
합 계	5(523)	7(76)	12(191)	7(253)	31(1,043)

주 : ( )내는 백만원

2. 전자거래 보안 실태 및 문제점

□ 보안프로그램

o 국내 해킹방지프로그램 제조업체들의 자체적인 해킹프로그램 수집·분석 능력에 한계

o 특히, 상용 키로거프로그램(키보드 입력내용 원격파악기능)에 대해서는 보안프로그램에서 일반적으로 탐지 곤란

□ 공인인증서 관리체계

o 위·변조 신분증에 의한 인증서 발급 및 해킹을 통해 입수한 신상정보로 타인에 의한 재발급 가능

o 대부분의 경우 공인인증서를 PC 자체에 보관하고 있으나, PC 해킹 시 절취가능성이 존재하며, 현행 1024비트 암호체계 미흡

□ 전자금융

o 인터넷뱅킹시 사용되는 현행 보안카드는 경우의 수가 30~35개로 적기 때문에 해킹을 통해 일부 번호 유출시 안전성 확보 곤란

o 텔레뱅킹의 경우 전화도청을 통한 금융사고 가능성 상존

□ 전자상거래

o 전자상거래시 신용카드 정보, 은행 계좌정보 등의 정보보호장치 미흡

o 전자상거래 카드결제시 공인인증서 또는 카드사 제공 인증시스템(ISP, 안심클릭)이 사용되나 카드사 제공 인증시스템의 본인확인절차 미흡

Ⅲ 전자거래 안전성 강화 대책

1. 기 본 방 향

□ 전자거래에 관한 종합적인 안정성 강화 방안을 마련하여 국민이 안심하고 거래할 수 있는 전자거래기반 조성

o 정보보호업체, 관련부처와 공동으로 해킹프로그램에 대한 수집·분석 체계를 강화하고, 정보의 공동 활용을 통한 보안프로그램의 성능 향상

o 인터넷뱅킹, 사이버증권·보험, 전자상거래 등 전자거래 분야 시스템에 대한 보안성을 강화하고, 이용자의 보안카드 비밀번호 보안성을 강화

o 공인인증서 발급·재발급 과정에서 본인 신원 확인 절차를 강화하고, 인증서 보관·관리상의 보안장치를 추가하여 해킹으로부터 공인인증서를 보호

□ 일반국민의 전자거래 이용시 불편과 부담을 최소화 하면서, 전자거래 전반의 이용 활성화를 위한 정책 추진

2. 해킹방지 부문

< 문 제 점 >

o 인터넷 뱅킹에 설치되는 국내 해킹 방지프로그램들이 신규 발생하는 해킹프로그램 대응에 한계가 있음

o 상용 키로거프로그램(키보드 입력내용 원격파악기능)에 대해서는 보안프로그램에서 일반적으로 탐지하지 않음

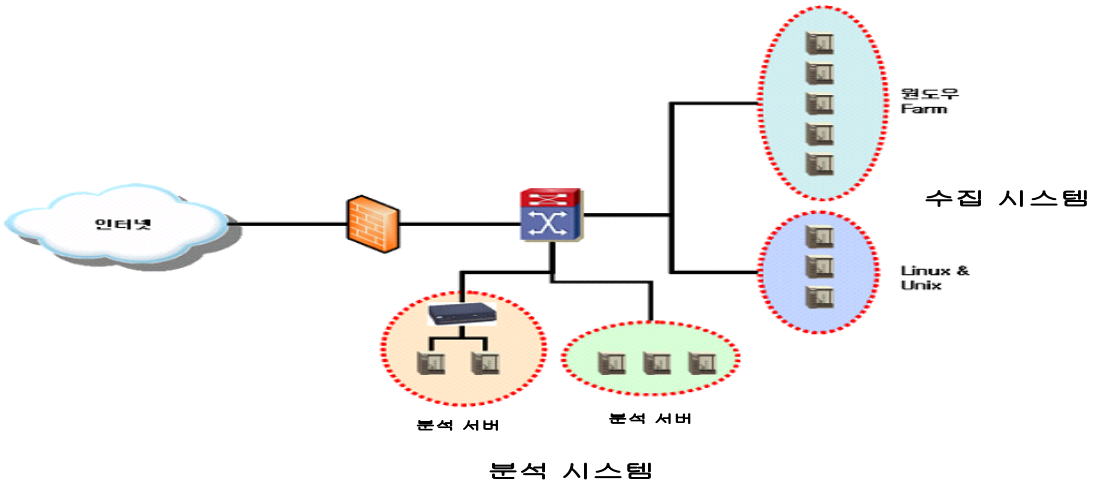
o 애플리케이션 영역에 대한 키보드 보안 프로그램의 한계

□ 해킹프로그램 자동 수집·분석 체계 강화['05.9]

o 한국정보보호진흥원, 백신업체가 합동으로 시중에 유포되고 있는 신규 해킹 프로그램에 대한 광범위한 수집·분석 시스템 구축

- 한국정보보호진흥원에서 운영하고 있는 기존 정보수집 시스템(허니넷) 확대 구축

< 해킹 프로그램 수집·분석 환경 구축 >



- 수집·분석된 해킹프로그램을 백신업체 및 금융감독원 등과 공유, 해킹 방지프로그램 테스트 및 대응능력 개선

□ 상용 키로그프로그램 백신 탐지[‘05.12]

o 백신업체에서 소송을 우려하여 해킹 악용소지가 있으나 탐지하지 않고 있는 상용 키로그프로그램에 대해서도 탐지하여 이용자에게 삭제 선택권 부여

※ 상용 키로그프로그램 : 키보드 입력 내용을 원격에서 파악하는 기능을 가진 프로그램으로 시중에서 합법적으로 판매됨

□ 키보드 보안 프로그램 기능 개선[‘05.12]

o 인터넷 뱅킹 전과정에 대한 보안 체계 구축을 위하여 키보드 입력으로부터 애플리케이션으로 넘어가는 부분까지 암호화 추진

□ 전자금융 이용자 정보보호수칙 작성 및 홍보[‘05. 10]

o 전자금융이용자 정보보호 수칙을 제정하여 인터넷뱅킹, 사이버증권 등 인터넷사이트 접속시 Pop-up창 형태로 홍보

3. 전자금융 부문

□ 신분증 위·변조여부 확인 강화

< 문 제 점 >

o 위조기술 발달에 따라 주민등록증, 운전면허증의 위·변조 확인 애로

o 본인확인절차 강화를 위한 현장교육 실시

- 전자금융 신규가입 업무를 담당하는 창구직원에 대하여 실명확인증표 식별방법 등에 대한 주기적 교육 실시
- 주민등록증 홀로그램, 사진, 성명 등 수정 흔적 확인 및 ARS1382·인터넷진위확인 서비스 등을 통한 확인 강화

※ 행정자치부와 연계하여 사진 또는 지문에 의한 신분증 위·변조 확인 강화 추진 예정

□ 인터넷뱅킹/텔레뱅킹

< 문 제 점 >

o 보안카드 비밀번호 경우의 수 부족(30~35개)
o 입력정보에 대한 해킹공격 및 도청 취약
o 중요 거래정보 고객통지 및 정보관리 미흡

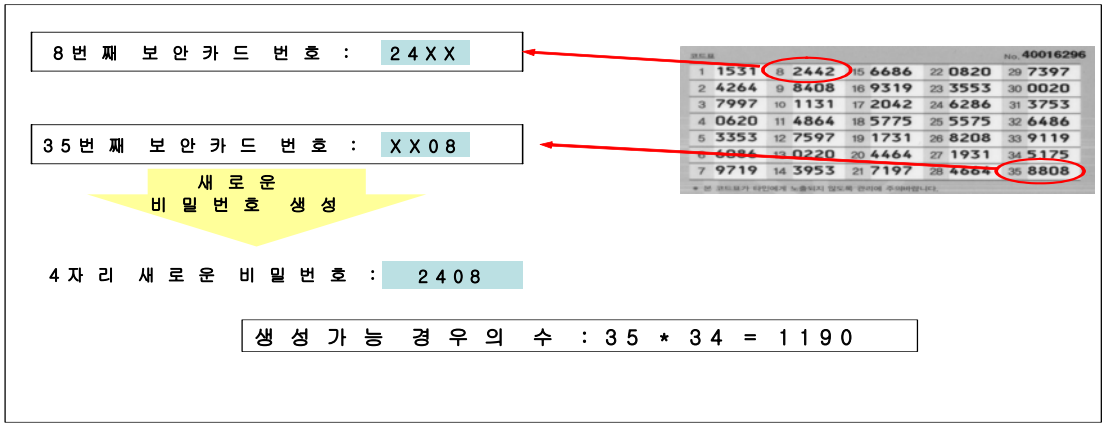
o PC용 보안프로그램 설치 의무화 등 해킹방지 기능 강화

- 전자금융거래시 개인 PC에 보안프로그램(키보드해킹방지, 개인방화벽) 제공 의무화[기조치, '05.7]
- 금융부문 해킹대응을 위한 전담조직 구축 검토[금융감독원, '05.12]

o 보안카드 유효비밀번호 확대['06. 3]

- 단기적으로 현행 보안카드의 비밀번호 입력방식을 개선하여 보안카드 유효비밀번호 숫자를 확대(현행 35개를 약 1천개로 확대)

※ 보안카드의 2개 비밀번호를 제시하여 첫 번째는 앞 2자리, 두 번째에는 뒤 2자리를 입력토록 개선



o 일회용 비밀번호 생성기(OTP:One Time Password) 도입['06.12]

- 금융거래시마다 새로운 비밀번호를 발생시키는 일회용비밀번호 생성기를 도입하여 보안카드를 OTP로 전환

- 하나의 OTP 생성기로 다수의 금융기관과 거래가 가능하도록 통합인증체계를 구축하여 사용자 편의성 제고 및 중복투자 방지

※통합인증체계 관리·운영을 위한 센터 구축 검토

o 보안수준별 거래한도 차등 적용['06. 12]

- 인터넷뱅킹 및 텔레뱅킹 고객의 보안등급을 3등급으로 구분하고 보안등급 수준에 따라 거래한도 차등 적용

○ 보안등급

거래이용수단	보 안 등 급
OTP발생기	1 등 급
HSM 방식 공인인증서 + 보안카드	
보안카드 + 휴대폰 SMS(거래내역통보)	2 등 급
보안카드	3 등 급

※ HSM(Hardware Security Module) : 공인인증서 복사방지를 위해 사용하는 보안성이 강화된 스마트카드, USB 저장장치

○ 보안등급별 거래한도 (단위:천만원)

구 분			기존 한도	보 안 등 급		
				1등급	2등급	3등급
인터넷 뱅킹	개인	1회	10	10	5	1
		1일	50	50	25	5
	법인[주)]	1회	50	50		
		1일	500	500		
텔레뱅킹	개인	1회	5	5	2	1
		1일	25	25	10	5
	법인	1회	10	10	2	1
		1일	50	50	10	5

주) 기업법인은 한도를 그대로 적용하되 1등급 보안수준 의무화

o 보안계좌 신설 및 고객서면동의 강화

- 조회·이체 등 모든 비대면 전자금융거래를 허용하지 않는 보안계좌의 신설 및 전자금융 서비스별(인터넷뱅킹, 텔레뱅킹, 모바일뱅킹 등) 선택항목란을 추가하여 고객 서면 동의 강화

o 전자금융업무별 비밀번호 오류횟수 통합관리['05.12]

- 인터넷뱅킹, 텔레뱅킹 등 전자금융업무별 비밀번호 오류횟수를 통합 관리하여 비밀번호 관리 강화

※ 계좌비밀번호 오류횟수가 각각 5회로 지정되어 통합관리가 되지 않을 경우 인터넷뱅킹, 텔레뱅킹, ARS, CD/ATM 등 최대 30회 정도 확인 위험 발생

o 인터넷을 이용한 빠른조회 서비스 폐지['05.12]

- 포털 등 인터넷 웹사이트에서 은행 동의 없이 금융계좌조회 서비스 제공으로 인한 금융거래정보(계좌번호, 계좌비밀번호 등) 유출 방지 및 고객 금융정보 관리 강화

※ 대부분 포털 등 인터넷 사이트에서는 이용자에게 보안프로그램을 제공하고 있지 않아 금융거래정보의 유출 위험성 존재

※ 인터넷 웹사이트에서 제공(자체서버에 고객 금융거래정보 저장)하는 계좌이체서비스에 대해서도 차단

o 텔레뱅킹 도청방지 시스템 구축 유도

- 전화 다이얼 톤 도청에 의한 텔레뱅킹 거래정보 유출을 차단할 수 있는 방지 시스템 적용을 적극 유도

o 착신금지전화, 선불폰, 선불카드 폰 등에 의한 텔레뱅킹 제한

- 공중전화 등 발신자 추적이 불가능한 전화 및 소유주가 불분명한 전화에 의한 텔레뱅킹 거래를 제한

- 고객이 지정하는 전화번호에 의해서만 텔레뱅킹이 가능한 지정전화번호제도 도입과 사고추적이 곤란한 국제전화 등에 의한 텔레뱅킹 제한은 각 금융회사가 자율적으로 결정

o 고객정보관리 강화 및 중요거래사항에 대한 통지 활성화['05.12]

- 고객 개인정보(SMS전화번호, 주민번호 등) 조회시 일부를 '*'처리 및 대면확인이 아닌 온라인상에서 이루어지는 입·출금계좌변경, 한도증액, 휴대폰 SMS번호변경 등 중요거래사항에 대한 고객통지 의무화

o 전자금융거래 이용자 보안의식 제고

- 전자금융거래시 보안 유의사항 작성 및 홍보/교육을 강화하여 이용자가 자체적인 보안수단을 강구하도록 유도

※ 금융회사 제공 보안프로그램 등을 고의 또는 자의로 실행하지 않는 경우 책임이 부과될 수 있음을 강조

□ 사이버증권/보험

< 문 제 점 >

o 사이버 증권/보험 거래시 해킹방지 프로그램 미제공
o 선물거래에 공인인증서 미적용
o 내부직원에 의한 비밀번호 유출 위험

o 사이버 증권/보험 거래시 개인 PC에 보안프로그램 제공 의무화['06. 6]

- 인터넷뱅킹과 동일한 수준의 보안프로그램 제공

o 선물거래 공인인증서 사용 의무화[‘06. 6]

- 사이버 증권 거래와 동일하게 공인인증서 사용

o 사이버 증권 보안카드 유효비밀번호 확대 및 일회용비밀번호 생성기 도입

- 인터넷뱅킹과 동일

o 사이버 증권거래 신규 신청시 최초 접속기한 설정[‘05.12]

- 전자금융 신청 후 접속기한을 설정하여 기한내 접속이 없을 경우 자동취소 처리

o 증권계좌 개설시 PIN PAD 도입 의무화[’06. 6]

- 은행과 동일하게 계좌개설, 거래전표 등에 비밀번호 기재를 금지하여 내부직원에 의한 비밀번호 유출 위험 제거

o 사이버 보험계약, 지급시 공인인증서 의무화[‘06.3]

- 전자서명이 어려운 경우 녹취, FAX발송 등 전자서명을 보완하고 전자보험거래 약관에 반영

o 사이버 보험금, 대출금 등의 지급신청시 이체계좌 및 한도 제한[‘05.12]

- 본인명의 유실적 계좌로만 이체 허용(1일 이체한도 1억 이내)

※ 단, 사전등록계좌, 콜센터 본인확인(신분증 FAX수신 등) 등은 예외허용

o 고객정보관리 강화 및 중요거래사항에 대한 통지 활성화[‘05.12]

- 인터넷뱅킹과 동일

□ 금융부문 해킹대응을 위한 전담조직 설립 검토[‘05.12]

o 일회용비밀번호 발생기 공통사용을 위한 통합인증센터 기능

o 국가 사이버안전센터, 한국정보보호진흥원 등으로부터 제공되는 해킹프로그램에 대한 적용, 테스트 및 대응방안 수립·시행

o 금융부문 정보보호제품 품질 검증(인증) 및 지속적인 품질관리

※ 미국의 경우 금융보안기술연구소(BITS)를 ‘96년부터 설립·운영중

□ 금융회사 IT보안조직·인력·예산

< 문 제 점 >

o 정보보호업무수행을 위한 관리 및 통제인력 부족
o 정보보호전담조직의 총괄적 통제력 부족
o 정보보호에 대한 투자 미흡

o 전자금융거래 보안업무수행을 위한 정보보호인력은 IT인력대비 3~5%이상으로 권고

※ 정보보호업무 수행직원은 책임있는 정규직원을 채용토록 권고

o 정보보호전담조직을 IT담당임원(CIO)직속의 독립된 별도조직으로 개편토록 권고

o 정보보호예산은 IT예산대비 최소 3~5%이상으로 권고

4. 전자상거래부문

< 문 제 점 >

o 전자상거래시 신용카드 정보, 은행 계좌정보 등의 보호장치 미흡
o 전자상거래 인증시스템(ISP, 안심클릭)의 본인확인절차 미흡

o 전자지불중계업체(PG사), VAN사에 대한 정보보호 강화['05.12]

- 고객 비밀번호 보관을 금지하고, 계좌정보 등 업무상 필요한 금융정보는 암호화하여 보관

- 전자지불중개업체, VAN사에서 결재기능 수행시 신용카드 또는 은행 계좌정보 보호를 위해 개인 PC에 보안프로그램 제공 유도

※ VAN(Value Added Network)사 : 가맹점과 카드사간 카드결제 업무 대행
※ 전자지불중계업체(PG:Payment Gateway) : 온라인 쇼핑몰 업자를 위해 지급결제 업무 대행

- 카드사에서 결제기능 제공시 개인 PC에 보안프로그램 의무 설치

o 전자상거래 결제시 본인확인절차 강화

- 카드사 제공 인증시스템(안전결제, 안심클릭) 발급/재발급 절차 개선('05.12)

※ SMS, 공인인증서, 일회용 비밀번호, 조회불능 특수정보 입력 등 강화조치 의무화

- 신용카드 결재시 공인인증서 사용여부는 전자상거래 위축 및 이용자 불편 등을 고려하여 신용카드사가 자율적으로 결정

※ 국민, BC, 외환카드사의 경우 30만원 이상 공인인증서 사용 중

- 계좌이체를 통한 30만원 이상 전자상거래 결재시 공인인증서 사용 의무화('05.12)

※ 항공권 예약, 등록금, 원서접수 등 본인확인이 가능한 거래는 예외

o 신용카드 2008년까지 IC카드로의 전환 추진

- 계획수립시('03. 4) 정한 년도별 전환 목표 달성

5. 공인인증서 부문

< 문 제 점 >

o 공인인증서 온라인 재발급 시 신원확인 정보가 해킹에 취약
o PC에 저장된 공인인증서의 경우 해커에 의한 절취 가능

□ 공인인증서 재발급 시 온라인 신원확인 방법 강화('06. 3.)

o 타인에 의한 공인인증서 온라인 재발급을 방지하기 위해 인터넷뱅킹에서 사용하는 보안카드 입력방식 적용

- 보안카드의 비밀번호를 조합하여 비밀번호의 수를 기존 35개에서 약 1,000개 이상으로 확대

o 보안카드 미소지자가 공인인증서를 재발급 받고자 하는 경우에는 대면확인을 통하여 발급

□ 공인인증서의 보관·관리방법 개선

o 공인인증서 보관시 PC가 아닌 이동식 저장장치(USB 장치 등)를 이용토록 유도

- PC에 저장시 인증서비밀번호와 PC 고유정보를 조합하여 암호화함으로써 공인인증서 해킹 방지('06. 6)

o 고액 금융거래자는 안전성이 강화된 스마트카드 또는 USB장치 등을 이용토록 권고

□ 공인인증서 암호체계를 현행 1024비트에서 2048비트로 강화('06.6)

Ⅳ 추 진 일 정

해킹방지 부문 (정통부 · 금감원)

- o 해킹프로그램 자동 수집·분석 체계 강화 ····· '05. 9
- o 상용 키로그 프로그램 백신 탐지 ····· '05.12
- o 키보드 보안 프로그램 기능 개선 ····· '05.12
- o 전자금융 이용자 정보보호수칙 작성 및 홍보 ····· '05.10

전자금융 부문(인터넷뱅킹 · 텔레뱅킹 : 금감위 · 금감원)

- o PC용 보안프로그램 제공 의무화 ····· '06. 6
- o 보안카드 유효비밀번호 확대 ····· '06. 3
- o 일회용 비밀번호 생성기(OTP)도입 ····· '06.12
- o 인터넷뱅킹·텔레뱅킹 등 보안수준별 거래한도 차등 적용 ····· '06.12
- o 전자금융업무별 비밀번호 오류횟수 통합관리 ····· '05.12
- o 인터넷을 이용한 빠른조회 서비스 폐지 ····· '05.12
- o 고객정보관리강화 및 중요거래사항 통지 ····· '05.12
- o 선물거래시 공인인증서 사용 의무화 ····· '06. 6
- o 증권계좌개설시 PIN PAD 도입 의무화 ····· '06. 6
- o 금융부문 해킹대응을 위한 전담조직 설립 검토 ····· '05.12

전자상거래 부문(산자부 · 금감원)

- o PG사, VAN사에 대한 정보보호 강화 ····· '05.12
- o 전자상거래 결제시 본인확인절차 강화 ····· '05.12

공인인증서 부문(정통부)

- o 재발급 시 온라인 신원확인 방법 강화 ····· '06. 3
- o 공인인증서의 보관·관리방법 개선 ····· '06. 6
- o 공인인증서 암호체계 강화 ····· '06. 6

< 참 고 >

전자금융거래 안전성 강화 종합대책 요약표

[공통부문]

구 분	의무사항[시행시기*]	권고사항
해킹대응	◦전자금융거래시 PC용 보안 프로그램 의무제공['06.6]	◦전자금융 이용자 정보보호 수칙 작성 및 홍보
	◦PC용 보안프로그램 기능강화['05.12]	
	◦금융부문 해킹대응 전담조직설립 검토	
일회용비밀번호 보안강화	◦보안카드 비밀번호 분할입력에 의한 유효비밀번호 확대['06.3]	
	◦일회용비밀번호(OTP) 발생기 도입 ['06.12]	
	◦OTP 통합인증센터 구축검토['05.12]	
공인인증서	◦보관방법개선 -공인인증서 PC저장시 비밀번호와 PC고유정보로 암호화 보관	◦이동식 저장매체 이용 ◦보안성이 강화된 USB, 스마트카드 등(HSM) 사용
	◦인증서 재발급시 본인확인 강화 -보안카드 S/N(3자리) 추가입력['05.12] -일회용비밀번호발생기(OTP) 입력['06.12]	
	◦타행/타기관 발급 공인인증서 등록절차 강화['05.12]	
정보보안 인력·조직·예산		◦정보보호인력을 IT인력대비 3~5%이상 유지
		◦정보보호전담조직을 CIO 직속의 독립된 별도조직으로 개편하여, 총괄적 통제체제 구축
		◦정보보호예산은 IT예산대비 3~5%이상 유지

*해당하는 월말까지 구축완료

[은행부문]

구 분	의무사항[시행시기]	권고사항
전자금융거래 신규가입	◦본인확인절차 강화 교육['05.10] -영업점 직원 현장교육실시 ※행자부와 사진·지문에 의한 신분확인 강화 추진 예정	
	◦보안계좌신설, 서면동의강화['06.3] -전자금융허용하지 않는 보안계좌신설 -전자금융관련 고객 서면동의 강화	
인터넷뱅킹, 텔레뱅킹 등 전자금융거래	◦보안수준별 거래한도 설정['06.12] -보안수준(3등급 분류)에 따른 인터넷뱅킹, 텔레뱅킹 등 거래한도설정	◦선불폰, 선불카드폰 등에 대한 텔레뱅킹 거래제한
	◦중요거래 휴대폰SMS통지 활성화['05.12] -중요거래사항(공인인증서 재발급, 한도증액 등)에 대한 고객통지 의무	◦텔레뱅킹 도청방지 시스템 구축 적극권고
	◦보안카드 지시번호 및 비밀번호 오류횟수 매체별 통합관리['05.12]	◦피싱예방 및 신고방법 홍보
	◦인터넷뱅킹 빠른조회서비스 폐지['05.11]	
전자지불	◦30만원 이상 온라인 계좌이체시 공인인증서 의무 사용['05.12]	◦VAN사업자 업무위탁시 내부통제 및 보안심사 강화
자동화기기	◦자동화기기 무매체거래 이체, 출금시 전용비밀번호 또는 보안카드 의무사용['05.12]	◦자동화기기 보안강화 -공공장소, VAN자동화기기 좌우차단시설 확대설치 등
	◦자동화기기 보안강화 -점내기기까지 암호화 확대 적용['06.6]	

[증권부문]

구 분	의무사항[시행시기*]	권고사항
온라인 트레이딩 등 전자금융거래 이용 및 절차	◦PIN PAD 도입['06.6]	◦중요거래 휴대폰SMS통지 활성화
	◦전자금융거래 신청후 최초 접속기한 설정 (신청일 익일부터 5영업일이내)['05.12]	◦전자금융 서비스간 동시 접속 및 동일 서비스 동시접속 제한
	◦최근접속기록 고객 알림['05.12]	◦비밀번호 자동설정 기능 제한
	◦접속 매체별 사고등록 통합관리['05.12]	
	◦주문대리인 설정시 이체·대체거래는 제한['05.10]	
	◦보안카드 지시번호 및 비밀번호 오류횟수 매체별 통합관리['05.12]	
	◦이체/대체 거래시 공인인증서 및 일회용 비밀번호(보안카드 포함) 의무적용['05.12]	
	◦선물거래시 공인인증서 도입['06.6]	
ARS서비스 이용	◦공중전화, 착신금지 전화에서 거래제한 ['05.12]	◦도청방지시스템 구축 권고 ◦자금이체·대체 거래 제한
기 타	◦증권카드의 IC카드 전환['08.12]	

[보험부문]

구 분	의무사항[시행시기]	권고사항
전자금융거래 신규가입	◦본인확인절차 강화 교육['05.10] -영업점 직원 현장교육실시 ◦인터넷을 통한 신규가입시 본인확인 강화 (공인인증서, 신용카드정보 등 이용)['05.12]	
사이버보험 등 전자금융거래	◦비밀번호, 보험가입·해지 등 중요거래 사항 고객 휴대폰SMS통지['05.12]	◦고객정보 관리강화 및 중요 거래에 대한 통지 활성화
	◦고객정보 변경시 본인확인강화 등['05.12] -중요 개인정보 일부를 '*' 처리 -신규가입과 동일한 수준으로 본인확인	
	◦보험가입 등 전자서명시 공인인증서 실시간 유효성체크(OCSP) 적용['05.12] -전자서명이 어려운 경우 녹취, FAX 등으로 보완하고, 전자보험거래 약관에 반영	
	◦보험금, 대출금 등의 지급신청시 본인확인 강화['05.12] -타인명의 및 무실적 계좌로 이체제한 -1일 이체한도(1억 이내) 제한	
ARS서비스 이용	◦공중전화, 착신금지 전화에서 거래제한 ['06.6]	

[카드부문]

구 분	의무사항[시행시기]	권고사항
전자금융거래 신규가입	◦인터넷을 통한 회원가입시 본인확인 강화 (신용카드정보 등 확인강화)['05.12]	
전자상거래 등 전자금융거래	◦안심결제, 안전결제 재발급시 본인확인 강화['06.6] -공인인증서, SMS인증, 일회용비밀번호 등 추가 확인	◦카드 인도시 추가 본인확인 수단 강구(2차적 본인확인 서류)
	◦인터넷을 이용한 결제계좌 변경시 본인확인강화['06.6] -공인인증서, 카드비밀번호 등 추가 확인	◦개인정보유출에 대한 고객 주의 홍보 강화
	◦고객정보 변경시 본인확인강화['05.12] -중요 개인정보 일부를 '*' 처리 -신규가입과 동일한 수준으로 본인확인 -비밀번호 오류횟수 통합관리	◦전자상거래에서 공인인증서는 카드사 자율결정
	◦전자상거래시 카드사 제공 결제시스템 사용 의무화['06.6]	◦VAN사와 카드사간 보안강화 시행 계획 마련
	◦카드 매출전표에 유효기간 인자 금지 ['05.12]	
	◦신규계좌로 대출금이체 및 사고해제시 본인확인 강화['06.6] -공인인증서, 콜센터 등을 통한 본인확인 -사고해제 내역 통지(SMS 또는 유선)	
ARS서비스 이용		◦도청방지시스템 구축 권고