[카드부문]

전자금융거래 보안 종합대책

2005. 9.

금 융 감 독 원

차 례

Ⅰ. 개 요

□ 최근 발생한 인터넷뱅킹 해킹사고와 관련하여 전자금융거래 사고 예방을 위하여 인터넷카드서비스, ARS서비스 등 전자금융 업무와 공인인증서 발급체계 개선 등 전자금융거래 안전성 강화를 위한 개선방안을 마련하고자 함

□ **종합대책 검토시 기본원칙**

o **금융회사는 전자금융거래를 수행하는 개인PC를 최대한 보호**

o **개인은 금융회사에서 제공하는 보안수단을 강제로 중단하거나 삭제 금지**

o **타 금융사의 정보유출 사고가 발생하더라도 금융사고가 연결되지 않도록 입력, 기록, 저장정보를 구분·관리**

□ **의무, 권고사항**으로 구분하여 개선방안 마련

구 분	내 용
의 무	감독기관 행정적 제재 또는 조치가 가능한 사항으로 금융회사가 반드시 따라야 하는 사항
권 고	금융회사가 따르도록 최대한 노력해야 하며, 경영실태평가 등에 반영 사항

Ⅱ. 추진경과 및 활동내역

□ 카드부문 T/F팀 구성·운영 (7. 4 ~)

o '05. 6. 10 경제정책 조정회의에서 인터넷뱅킹 해킹사고에 대한 후속조치 방안으로 관계기관 T/F 구성

- 정통부, 산자부, 금감위, KISA 등 관계기관 공동 T/F

o 전자금융거래 실태조사 및 종합대책 T/F 팀 구성(7. 4)

- 총 19명(은행, 증권, 보험, 카드 금융회사 직원 14명)

* T/F 참여카드사 : 비씨카드, 삼성카드 각 1명

o 전자금융 업무 파악, 문제점 도출, 개선방안 마련

- 인터넷카드서비스, ARS서비스, 전자상거래시 카드결제 등 업무 현황, 이용절차 및 시스템 구성 등 업무 파악

o 보안 솔루션 점검 및 적용방안 마련

- 보안제품 특성 및 보안수준 분석

- 카드사 특성을 고려한 보안제품 적용시 문제점 분석

□ 전자금융거래 업무현황 자료 제출 요구(7. 15)

o 전자금융거래 매체 및 업무별 보안관리 현황 자료 요구

□ 카드부문 보안실무자 1차 회의 개최

○ 일 자 : 2005. 8. 5(목)

○ 참가사 : 비씨카드 등 8개사 8명(전업계, 국민카드, 외환카드)

□ 카드부문 보안실무자 2차 회의 개최

○ 일 자 : 2005. 8. 11(목)

○ 참가사 : 비씨카드 등 18개사 20명(전업계 및 은행계 카드사)

□ 전자금융거래 업무현황 추가 자료 제출 요구(8. 18)

○ 고객정보 변경현황, SMS이용 현황 등 자료 제출 요청

□ 카드부문 보안강화 종합대책 최종(안) 마련(8. 22)

○ 카드부문 종합 대책 최종(안)에 대한 세부 내역 및 추진 일정 확정

Ⅲ. 인 터 넷

1. 이용 신청

□ 현 황

○ 개 요

- 신용카드회원이 신용카드사에서 제공하는 사용내역 조회, 현금서비스 및 카드론 신청 등 인터넷을 이용한 전자금융거래를 하기 위한 가입 절차

○ 가입 절차

① 카드사(은행) 홈페이지 접속하여 회원가입 선택

② 개인신상정보(성명, 주민번호 등) 입력

③ 소지한 카드정보(카드번호, 카드비밀번호, 유효기한, CVC) 입력

* 인터넷뱅킹과 카드부문이 통합된 경우, 공인인증서 발급 절차 선행

④ ID/PW 발급 후 인터넷 회원 가입 완료

○ 본인 확인 방법

공통사항	추가 입력 사항
- 카드번호 - 카드비밀번호 - 유효기한 - CVC(카드뒷면에 인자된 3자리 검증값) - 주민번호	- 공인인증서

□ 문 제 점

ㅇ **대면에 의한 본인확인 절차 없이 가입이 가능하여 카드 정보를 이용한 제3자의 부정 가입 가능**

- 대면에 의한 별도 가입신청 절차 없이 기 발급 받은 신용카드의 카드번호, 카드비밀번호를 필수입력항목으로 사용하고 있어 제3자의 부정가입 가능

  또한, 일부 카드사의 경우 카드비밀번호조차도 입력받지 않아 상대적으로 정보 도용에 의한 부정 가입 용이

ㅇ **키보드 해킹에 의한 정보 유출**

- 키보드 해킹프로그램에 의하여 로그인 ID 및 비밀번호 유출 가능

  또한, 가입을 위하여 입력하는 정보 및 개인 신용정보 유출 가능

□ 대 책

ㅇ **인터넷 회원 가입시 본인확인 절차 강화**

- 카드번호, 카드비밀번호, 유효기한을 필수입력 항목으로 지정**[의무, 2005. 12월]**

- 공인인증서에 의한 본인 확인 과정 추가[권고]

*** 공인인증서를 이용할 경우에는 공인인증서 소유자와 인터넷 고객의 동일인 여부를 반드시 확인**

ㅇ **인터넷 회원 가입 여부 SMS 통보[권고]**

- 정보 도용에 의한 부정 가입 방지를 위하여 신용카드 발급시 신청서에 기재한 휴대폰 번호로 인터넷 회원 가입현황을 SMS 문자전송

ㅇ **키보드 보안 및 해킹방지 프로그램 설치[의무, 2005. 12월]**

- 해킹에 의한 입력 정보유출 방지를 위하여 키보드해킹 방지 및 개인 PC 방화벽 설치 의무화 실시

※ 붙임1 "PC용 보안프로그램 개선 방안" 참조

<참고자료 : 보안프로그램 설치 현황>

- 전업카드사중 3개 카드사(LG, 삼성, BC) 키보드 해킹방지 프로그램 제공

- 전업카드사중 1개 카드사(삼성카드) 개인용 방화벽 제공

2. 카드 발급 신청

□ 현 황

○ 개 요

- 카드사 인터넷 회원으로 가입 후 홈페이지에 로그인 "카드신청"화면을 선택하여 신규 카드 발급 신청

○ 신청 절차

① 온라인으로 개인정보를 입력하여 카드 신청서 작성
② 신청 자격 심사
③ 카드 발급 및 배송
④ 카드 수령 전 회원가입 신청서상에 인수 서명 및 신용정보 활용 동의서 작성
⑤ ARS 또는 홈페이지에 접속하여 카드 비밀번호 등록

○ 본인 확인

공통사항	추가 입력 사항
- 상담원에 의한 신청내용 확인 - 발급심사시 신분증 발급일자 확인(주민등록증(행자부), 운전면허증(경찰청)) - 카드 인도시 신분증 확인(신용정보 활용 동의서 등 필요서류에 본인 서명)	

□ 문 제 점

○ 고객 입력 자료를 토대로 제출 서류의 진위 여부를 확인하고 전화로 1차 자격심사

○ 카드 인도시 대면 확인 및 신청서에 인수 서명 및 정보활용 동의서를 작성하는 대면에 의한 확인 절차가 있어 부정 발급 위험성 적음

□ 대 책

○ 본인확인 절차 강화[권고]

- 온라인 신청시 공인인증서를 추가로 제출하게 하여 본인확인을 강화하고 제출 서류의 진위 여부, 본인 여부에 대한 확인 철저

3. 정보조회/ 수정

□ 현 황

○ 개 요

- 인터넷을 통하여 기 등록된 고객 주소, 전화번호, 결제계좌 등의 개인정보를 조회 또는 변경

○ 본인 확인

공통사항	추가 입력 사항
- 로그인 ID - 로그인 패스워드	- 공인인증서

□ 문 제 점

○ 중요 개인정보 변경에 대한 본인확인 절차 취약

- 대출시 입금되는 결제계좌, 금융거래 사실의 통지 수단인 전화번호 등 중요 개인정보 변경에 대한 본인확인 절차 취약

  특히, 결제계좌의 변경은 현금서비스 신청 등 대출 계좌로 이용되고 있어 부정 발급된 계좌로 대출금을 이체 시키는 사고 발생 위험

○ 개인 정보 유출 위험

- 로그인 ID, PW만을 이용하여 본인 인증후 모든 개인정보에 접근이 가능하여 개인정보 유출사고 발생 가능

  동 유출 정보를 이용, 타 금융회사에 접근하여 금융사고 발생 가능

□ 대 책

○ 인터넷을 이용하여 결제계좌 변경시 본인확인 절차 강화 [의무, 2006. 6월]

- 결제계좌 변경시 다음중 하나이상을 선택하여 인증강화
  ① 공인인증서
  ② 카드번호 및 카드비밀번호 또는 CVC값
  ③ ISP 또는 안심클릭
  ④ 기 결제계좌 재 확인

○ 주요정보를 '*' 처리 내지 로그인 절차 강화[의무, 2005. 12월]

- 전화번호, 주소 등은 비대면거래에서 개인을 인증하기 위하여 사용되는 주요 정보로 일부내용을 '*' 처리 내지 로그인 절차를 강화하여 정보에 대한 접근 및 변경 강화

예) 휴대폰 번호 보호 및 관리
  ○ 개인전화 번호(직장, 집, 휴대폰)를 개인정보 조회시 끝 4자리를 '*'로 처리

ㅇ **중요 개인정보 변경시 휴대폰 SMS 통지 및 번호관리 강화[권고]**

- 사용자 주요정보 변경 및 SMS 통지서비스 해지 내역을 실시간으로 SMS을 통하여 고객에게 통지함으로서 불법 개인정보 변경에 의한 금융사고 방지

또한, SMS 발송시 주요정보로 활용되는 휴대폰 전화번호 변경에 대한 절차 강화

예) 개인 휴대폰 SMS번호 변경시 본인 인증 방법
- 기존 전화번호 끝 4자리(개인정보 화면에 기존 전화번호 일부자리를 '*'로 Display)
- 입력 전화번호 명의자와 카드 소지자간 본인 확인(이동통신사 연계)
- 공인인증서를 이용한 본인 인증후 변경 등

4. 금융서비스(현금서비스, 카드론 등)

□ 현 황

ㅇ 개 요

- 카드사 홈페이지에 접속하여 금융서비스를 신청하는 것으로 본인의 신용도에 따른 대출 한도 내에서 현금서비스, 카드론 등 대출을 신청하여 지정계좌*로 이체

* 이체 신청 계좌는 CD 공동망을 이용하여 대출 신청인 여부를 확인 후 동일인일 경우에만 이체

ㅇ 본인 확인

공통사항	추가 입력 사항
- 카드번호 - 카드비밀번호 - 유효기한 - CVC	- 결제비밀번호(안심클릭, ISP) - 공인인증서 - 보안카드번호

ㅇ 은행 이체와 카드 대출 신청 비교

은행 이체계좌 지정	카드사 대출 입금 계좌 지정
1. 계좌 정보 및 이체정보 입력 2. 계좌 비밀번호 확인 3. 입금 계좌입력(CD 공동망 이용 계좌 확인) 4. 일회용비밀번호 확인(대면 확인 후 발급) 5. 공인인증서 제출(인터넷 뱅킹, ARS는 대면 확인 후 발급된 이체 비밀번호 입력)	1. 카드정보 및 대출 신청 정보 입력 2. 카드 비밀번호 확인 3. 입금 계좌입력(CD 공동망 이용 입금 계좌 확인)

□ 문 제 점

o 카드정보 유출에 따른 현금서비스 이체 사고 위험

- 카드 결제대금 납부 및 기 대출시 이체계좌 등 기 거래 본인 계좌가 아닌 신규 계좌로 자금이체가 가능하여 유출된 카드정보를 이용한 금융사고 발생 위험

- 은행계 카드사중 일부는 타인에게 대출금 이체시 은행의 이체 프로세스와 동일하게 운영(일회용 비밀번호, 공인인증서)하지 않아 금융사고 발생 위험

o 입력정보에 대한 해킹공격에 취약

- 개인 PC용 방화벽, 키보드 해킹방지 프로그램을 제공하지 않는 경우 해킹 툴을 이용한 공격에 무방비

- 또한, 개인 PC용 방화벽, 키보드 해킹방지 프로그램에서 모든 해킹 프로그램을 방어할 수 없으며, 새로운 해킹 기법에 대한 대응 곤란

□ 대 책

o 신규 계좌로 대출금 이체시 본인확인 절차 강화[의무, 2006. 6월]

- 카드사와 기 거래계좌가 아닌 신규계좌로 대출금을 이체하는 경우에는 공인 인증서 또는 콜센타를 통한 본인 확인

- 또한, 타인 계좌(자행, 타행 포함)로 이체시에는 반드시 은행의 이체 절차와 동일하게 보안카드 및 공인인증서 사용

*** 공인인증서를 이용할 경우에는 공인인증서 소유자와 인터넷 고객의 동일인 여부를 반드시 확인**

o 키보드 보안 및 해킹방지 프로그램 설치[의무, 2005. 12월]

- 안전한 전자금융거래 보장 및 고객정보 보호를 위하여 고객 PC에 키보드 보안 및 해킹방지 프로그램 제공

5. 기 타(분실, 사고 접수, 해제 등)

□ 현 황

ㅇ 개 요

- 카드회원이 본인의 카드를 분실 또는 도난시 부정사용 예방을 위하여 동 카드의 거래 중지를 카드사 홈페이지에 접속하여 신고 또는 해제 가능

ㅇ 신고 절차

① 카드사 홈페이지 접속
② 사고신고 화면 선택
③ 사고카드 선택 및 사유 입력
④ 사고 및 분실 신고 완료
⑤ 부정사용 여부 확인

ㅇ 사고신고 해제 방법

① 객장을 방문하여 대면에 의해 사고 해제
② 콜센타를 통하여 본인확인 후 해제

ㅇ 본인 확인

공통사항	추가 입력 사항
- 로그인 ID - 로그인 패스워드	

□ 문 제 점

ㅇ 사고신고 해제시 본인확인 절차 미흡

- 영업점이 적은 전업계카드사의 경우 주로 콜센타를 이용하여 사고 해제 신청 업무를 처리하고 있어 비대면에 의한 본인 확인에 따른 리스크 발생

□ 대 책

ㅇ 비대면 사고 해제 신청시 본인 확인 절차 강화[의무, 2006. 6월]

- 인터넷을 통한 사고 및 분실 해제시 카드번호, 카드비밀번호, CVC, 주민번호, 공인인증서를 제출하도록 절차 강화

- 콜센타에 의한 본인확인시 카드신청서상 기록한 정보를 이용하여 본인확인을 강화하고 FAX등을 통한 고객 본인 신분증 추가 징구

ㅇ 사고 해제 내역 SMS서비스 및 유선 통지[의무, 2005. 12월]

- 해제시에는 사고 신고시 사용된 전화번호내지(휴대폰 전화번호 사고 신고시 등록) 사전에 등록된 전화를 이용하여 사고신고 해제 내역을 반드시 SMS 내지 유선 통지

Ⅳ. ARS

1. 이용 신청

□ 현 황

○ 개 요

- 각 카드사에서 제공하는 ARS전용번호를 이용하여 사용내역 조회, 현금서비스 신청, 분실 신고 등을 이용

- 신용카드를 소지하고 있는 고객이면 누구나 별도의 가입절차 없이 이용 가능

  * 은행계 카드사는 텔레뱅킹 가입절차와 동일

○ 본인 확인

공통사항	추가 입력 사항
- 카드번호(주민번호) - 카드비밀번호 - CVC(카드뒷면에 인자된 3자리 검증값)	

□ 문 제 점

○ 본인확인 항목에 대한 오류횟수 통합 관리 미흡

- 비밀번호, CVC값 등 카드사에서 본인 확인 수단으로 이용하고 있는 정보의 입력 오류횟수가 각 채널별(ARS, 인터넷, CD/ATM 등)로 관리되고 있어 실질적인 오류 허용 횟수가 증가하여 사고 발생 위험

□ 대 책

○ 주요 정보의 입력 오류 횟수 통합관리[의무, 2005. 12월]

- 주요정보(비밀번호, CVC값)의 오류횟수가 각 채널별로 분리 운영되고 있는 오류 횟수를 통합 관리하여 각 금융회사에서 정한 일정 횟수를 초과시 사용 정지

2. 카드 발급 신청

□ 현 황

○ 개 요

- ARS만을 이용하여 카드발급 신청은 불가능하면 ARS를 통하여 카드 발급을 신청하여도 상담원으로 연결되어 상담원에 의한 본인 확인 후 카드 발급 신청 접수

○ 본인 확인

공통사항	추가 입력 사항
- 상담원에 의한 카드 입회신청서 상의 기본 정보 확인 - 발급심사시 신분증 발급일자 확인(주민등록증(행자부), 운전면허증(경찰청)) - 카드 인도시 신분증 확인(신용정보 활용 동의서 등 필요서류에 본인 서명)	

□ 문 제 점

○ 위조 신분증에 의한 카드 발급 신청 가능

- 최근 신분증을 위조한 금융사고가 증가하고 있으며 동 위조 신분증을 이용한 카드 발급이 가능하여 고객 피해 발생 위험

□ 대 책

○ 카드 인도시 추가 본인 확인 수단 강구[권고]

- 신분증 재확인 또는 재직자의 경우 사원증, 의료보험증 등 2차적인 본인 확인 서류를 이용하여 확인한 이후 카드를 인도하도록 카드전달 업체와의 계약 내용에 포함

3. 정보조회/ 수정

□ 현 황

○ 개 요

- 카드 발급 회원은 카드사에서 제공하는 ARS전용번호로 전화 후 청구금액, 한도 조회 등 카드거래 관련 내역 조회

○ 본인 확인

공통사항	추가 입력 사항
- 주민번호 또는 카드번호 - 카드 비밀번호 또는 이용자 번호(폰뱅킹 비밀번호) 입력	

□ 문 제 점

○ 조회 서비스에 의한 고객 금융 거래정보 유출 가능

- ARS 이용시 본인 확인을 위하여 입력되는 주민번호, 카드번호, 카드 비밀번호는 타인에게 유출되기 쉬울 뿐만 아니라 카드정보 보유자는 누구나 금융정보 조회 가능

□ 대 책

○ 개인정보 유출에 대한 고객 주의 홍보 강화[권고]

- 카드정보 유출로 인한 금융정보 추가 유출 가능성 및 위험성에 대하여 대 고객 홍보를 강화하여 카드비밀번호, 폰 뱅킹 비밀번호 관리 강화

4. 금융서비스(현금서비스, 카드론 등)

□ 현 황

○ 개 요

- 카드소지자중 대출이 필요한 경우 카드사 ARS 전용 전화를 이용하여 본인의 신용도에 따른 대출 한도 내에서 현금서비스, 카드론 등 대출을 신청하여 지정계좌로 이체

○ 절 차

① 카드사 ARS 전용번호로 전화 연결
② 카드번호, 주민번호, 카드비밀번호 입력
③ 금융 서비스 이용메뉴로 접속하여 대출 신청
※ 카드사의 현금서비스 및 카드론은 전체 매출에서 ARS 이용 매출 비중이 상대적으로 높음

○ 본인 확인

공통사항	추가 입력 사항
- 카드번호 - CVC값 - 카드비밀번호	

○ 은행 이체와 카드 대출 신청 비교

은행 이체계좌 지정	카드사 대출 입금 계좌 지정
1. 계좌 정보 및 이체정보 입력 2. 계좌 비밀번호 확인 3. 입금 계좌입력(CD 공동망 이용 계좌 확인) 4. 일회용비밀번호 확인(대면 확인 후 발급) 5. 폰뱅킹 비밀번호(이체비밀번호)	1. 카드정보 및 대출 신청 정보 입력 2. 카드 비밀번호 확인 3. 입금 계좌입력(CD 공동망 이용 입금 계좌 확인)

□ 문 제 점

○ 카드정보 유출에 따른 현금서비스 이체 사고 위험

- 카드 결제대금 납부 및 기 대출시 이체계좌 등 기 거래 본인 계좌가 아닌 신규 계좌로 자금이체가 가능하여 유출된 카드정보를 이용한 금융사고 발생 위험

- 은행계 카드사중 일부는 타인에게 대출금 이체시 은행의 이체 프로세스와 동일하게 운영(일회용 비밀번호, 폰뱅킹 비밀번호)하지 않아 금융사고 발생 위험

○ 도청에 의한 정보 유출 위험

- 고객의 카드번호, 주민번호, 카드비밀번호 등 주요 정보가 전화 도청에 의하여 유출 위험

□ 대 책

○ 신규 계좌로 대출금 이체시 본인확인 절차 강화[의무, 2006. 6월]

- 기 거래 본인 계좌가 아닌 신규 계좌로 대출금을 이체하는 경우에는 보안카드 내지 콜센타를 통한 본인 확인

- 또한, 타인 계좌(자행, 타행 포함)로 이체시에는 반드시 은행의 이체 절차와 동일하게 보안카드 및 텔레뱅킹비밀번호 사용

ㅇ **ARS 도청 방지 시스템 구축[권고]**

- 전화 다이얼 톤에 의한 금융거래정보 유출위험을 차단할 수 있는 도청방지 솔루션 적용

- 해당 보안 시스템에 대한 성능 검증이 진행중이나 각 카드사의 ARS 시스템에 도입을 권고

5. 기 타(분실, 사고 접수, 해제 등)

□ 현 황

ㅇ 개 요

- 카드회원이 본인의 카드를 분실 또는 도난시 부정사용 예방을 위하여 동 카드의 거래 중지를 카드사 ARS전용 번호로 전화하여 신고 또는 해제 가능

ㅇ 본인 확인

공통사항	추가 입력 사항
- 주민번호 또는 카드번호 - 카드 비밀번호 또는 이용자 번호(폰뱅킹 비밀번호)	

□ 문 제 점

ㅇ **사고신고 해지시 본인확인 절차 미흡**

- 영업점이 적은 전업계 카드사의 경우 주로 콜센타를 이용하여 사고 해제 신청 업무를 처리하고 있어 비대면에 의한 본인 확인에 따른 리스크 발생

□ 대 책

ㅇ **비대면 사고 해제 신청시 본인 확인 절차 강화[의무, 2006. 6월]**

- 콜센타에 의한 본인확인시 최초 카드신청시 고객 제출 정보를 이용한 본인확인을 강화하고, FAX등을 통한 고객 본인 신분증 추가 징구, 영업점 방문에 의한 대면확인 내지 인터넷을 이용(공인인증서 이용)한 사고 해제를 권유

ㅇ **사고 해제 내역 SMS서비스 및 유선 통지[의무, 2005. 12월]**

- 해제시에는 사고 신고시 사용된 전화번호내지(휴대폰 전화번호 사고 신고시 등록) 사전에 등록된 전화를 이용하여 사고신고 해제 내역을 반드시 SMS 내지 유선 통지

Ⅴ. 자동화기기(CD/ATM)

1. 금융서비스 및 조회(현금서비스, 카드론 등)

□ 현 황

○ 개 요

- 카드소지자가 은행 또는 24시간 현금서비스 CD/ATM 기기를 이용하여 본인의 신용도에 따른 대출 한도 내에서 현금 인출 및 한도 조회 가능

- CD/ATM 을 이용하여 신청가능한 현금서비스 한도는 1회 70만원, 1일 200만원등으로 제한하여 운영

○ 본인 확인

공통사항	추가 입력 사항
- 카드 실물 - 카드비밀번호	

□ 문 제 점

○ 카드 도난 및 비밀번호 유출시 부정 사용

- 신용카드의 도난 및 비밀번호 유출로 인하여 현금서비스를 통한 부정사용으로 인한 고객 피해 가능

□ 대 책

○ 카드 및 비밀번호 보호에 대한 고객 홍보 강화[권고]

- 카드 분실시 해당 카드사에 즉시 신고하여 피해 예방, 자동화기기에서 뒷사람에 의하여 입력 비밀번호가 유출되지 않도록 주의 및 카드관련 주요정보 유출로 인한 사고 위험성에 대하여 대 고객 홍보 강화

* 자동화기기(CD/ATM)의 관리적/물리적/기술적 보안은 자동화기기 운영사(은행 및 전문업체)에서 담당

Ⅵ. 전자상거래

1. 공인인증서 발급

□ 현 황

○ 개 요

- 전자상거래이용시 신용카드 결제에 사용가능한 인증서는 범용 인증서*(유료)와 신용카드용 인증서**(무료) 가 있음

- 신용카드용 인증서는 공인인증기관(금융결제원, 코스콤)에서 대면 확인 후 발급한 공인인증서로 본인 확인 후 온라인으로 발급하고 있음

* 범용 인증서 : 인터넷 뱅킹 등 은행 및 금융결제원 제공 분야, 전자정부에서 제공하는 서비스, 기타 모든 전자거래

** 신용카드용 인증서 : 신용카드업무, 전자정부 민원서비스

○ 발급 절차(금융결제원 기준)

① 공인인증서 발급기관 홈페이지 접속 → "신용카드용 인증서 발급" 선택

② 주민등록번호 입력 → "인증서 발급" 선택 → 동일 공인인증기관에서 기 발행한 인증서 암호 입력

③ 주민등록번호, 이름, 영문이름 확인 → "신용카드용 인증서 발급" 선택

④ 인증서 저장매체(하드디스크, USB 등) 선택

⑤ 인증서 암호 입력 및 발급 확인

⑥ 최상위 인증기관 인증서 확인 및 발급 완료

< 카드용 공인인증서 발급 현황(7월말 기준) >

카드용 인증서 온라인 발급 기관	발급 수*	비 고
금융결제원	202,000	
코스콤	700	

* 출처 : 금융결제원, 코스콤(구 증권전산)

○ 본인확인 방법

공통사항	추가 입력 사항
해당 공인인증기관에서 발행한 공인인증서	주민등록번호 입력(금융결제원)

□ 문 제 점

○ 대면확인에 의한 인증서 발급 곤란

- 카드용 공인인증서 온라인 발급이 불가능하다면 카드사의 경우 대면확인 창구의 부족으로 공인인증서 발급 어려움

□ 대 책

○ 기 발급받은 공인인증서(범용, 은행거래용, 증권거래용)를 이용하여 카드용 인증서 발급

2. 공인인증서 사용

□ 현 황

ㅇ 개 요

- 우리원에서 추진하던 전자상거래에서 공인인증서 의무사용이 국무조정실 결정('04. 7월)에 의하여 '06. 9월 까지 유예되었으나

- 일부 카드사에서 30만원 이상 결제시 공인인증서를 적용하고 있으며 타 카드사에서도 공인인증서 적용*을 확대하고 있음

* 현재 공인인증서 적용을 일부 카드사(국민, BC, 외환)에서 자율적으로 시행하고 있으며 '05. 10월 전 카드사 적용 예정

□ 문 제 점

ㅇ 전자상거래에 카드 결제시 인증 수단 필요

- 분쟁조정위원회에서 전자상거래 결제시 카드사 제공 결제시스템(안심클릭, ISP)을 이용하여 발생한 사고는 카드사 책임이라고 결정*하여 안전한 전자상거래를 위한 인증수단 필요

* "제 3자가 타인의 신용카드 번호와 비밀번호 등을 도용, '안심클릭서비스'에 가입한 뒤 전자상거래를 통해 물품을 구입했다면 그 책임은 카드사에 있다"고 결정

□ 대 책

ㅇ 전자상거래에서 공인인증서 사용여부 자율적 결정

- 전자상거래에서 신용카드 결제시 사용자 인증 강화의 필요성이 인정되는 경우 공인인증서 사용여부는 각 카드사에서 자율적으로 결정

*** 공인인증서를 이용할 경우에는 공인인증서 소유자와 인터넷 고객의 동일인 여부를 반드시 확인**

ㅇ 향후 공인인증서 사용 의무화 및 적용 금액 하향 검토

- 국무조정실 결정에 따라 '06. 9월 이후 전자상거래에서 공인인증서 사용 의무화 재논의

- 아울러, 카드용 공인인증서 발급 현황 및 전자상거래에 미치는 영향 등을 분석하여 공인인증서 사용 결제 금액을 단계적으로 하향 조정 검토

3. 카드사 제공 결제시스템(안심클릭, ISP) 발급

□ 현 황

○ 개 요

- 전자상거래시 카드정보(카드번호, 유효기간, 비밀번호2자리)를 입력하지 않고 사전에 등록한 비밀번호를 이용하여 결제할 수 있는 카드사 제공 결제시스템은 안심클릭*과 ISP**(Internet Secure Payment, 안전결제) 시스템이 있음

* 안심클릭 : Visa사에서 제공하는 결제시스템

** ISP : 국민카드와 비씨카드 주도로 KVP(한국버추얼페이먼트)에서 제공하는 결제시스템

○ 발급 절차(안심클릭 기준)

① 카드사 홈페이지 접속 → "안심클릭 발급" 신청
② 카드번호 입력
③ 주민번호, CVC값, 카드비밀번호 2자리 입력
④ 약관 동의 → 안심클릭 비밀번호(영숫자조합 6~8자리), 안심클릭 비밀번호 확인 입력 → 개인 확인 메세지 입력
⑤ 안심클릭 등록 완료
⑥ 안심클릭 발급 결과 SMS 전송(SMS 신청 고객)

○ 본인확인 방법

안심클릭	ISP(안전결제)
카드번호 CVC 카드비밀번호 2자리 주민번호	카드번호 카드비밀번호 CVC

□ 문 제 점

○ 비대면 본인확인에 따른 부정 발급 가능

- 전자상거래 결제시 사용하는 카드사 제공 결제시스템(안심클릭, ISP)의 발급이 비대면으로만 이루어지고 있어 카드정보 노출로 인한 부정발급이 가능하며, 이를 이용한 부정사용 위험

□ 대 책

○ 재발급 절차 보완[의무, 2006. 6월]

- 카드정보(카드번호, 유호기간, 비밀번호, 주민번호, CVC) 유출로 인한 결제시스템(ISP, 안심클릭)의 부정발급/재발급을 방지하기 위하여 기존 발급 방식에 T/F팀에서 권고하는 보안방안(1 ~ 4안)을 카드사가 자율적으로 선택

< 재발급 절차 보완을 위한 방안 >

안 건	내 용
1안) SMS인증후 발급/재발급 내용 SMS 전송	○ SMS를 이용하여 인증번호를 발급받아 인증값을 입력하여 발급/재발급시 인증하고 발급/재발급 여부를 SMS로 통지
2안) 공인인증서 인증후 발급	○ 기 발급(은행, 증권, 카드) 받은 공인인증서를 이용하여 발급/재발급시 인증
3안) 일회용 비밀번호(평면카드 포함)로 인증후 발급	○ 대면 확인 후 발급한 일회용 비밀번호(평면카드 포함)를 이용하여 발급/재발급시 인증
4안) Web 등 에서 조회 불가 정보 입력	○ 결제 계좌번호 일부 자리, 주민번호 뒷자리 등 Web 등에서 조회가 불가능한 정보를 입력하여 발급/재발급시 인증

4. 카드사 제공 결제시스템(안심클릭, ISP) 사용

□ 현 황

○ 개 요

- 전자상거래시 신용카드 결제를 위하여 카드정보 입력의 불편함 및 정보유출 방지를 위하여 카드사에서는 카드사 제공 결제시스템을 사용하도록 권고하고 있으며 다수의 쇼핑몰에서 카드사 결제시스템을 이용

- 다만, 티켓발급, 대학 입학원서 대금 납부, 공과금 납부, 보험료 납부 등의 업무에서는 카드번호 입력 방식에 의한 결제 허용

○ 본인확인 방법

안심클릭	ISP(안전결제)
카드번호 안심클릭 비밀번호	ISP 비밀번호

□ 문 제 점

○ 카드 정보 유출 위험

- 일부 카드사에서는 전자상거래 결제시 카드사 제공 결제 시스템을 미적용하여 카드 결제 정보 유출 위험

- 카드사 제공 결제시스템에 키보드 해킹방지 프로그램을 미 적용하여 키보드 해킹에 의한 전자 결제시스템 비밀번호 유출로 인한 부정사용 위험

- 안심클릭의 경우 쇼핑몰에서 카드번호를 입력하도록 설계되어 해킹에 의한 카드번호 유출 위험

□ 대 책

o 전자상거래시 카드사 제공 결제시스템 사용범위 확대 [의무, 2006. 12월]

- 모든 전자상거래에서 카드사 제공 결제시스템을 사용토록 의무화 하고 대학 원서비 납부, 항공권 구입 등 소액, 입금자가 명확한 거래에 대해서만 카드정보 입력에 의한 결제 방식을 허용하여 안전한 전자금융거래 환경 구축

o 카드사 제공 결제시스템(ISP, 안심클릭)에 키보드 해킹방지 프로그램 적용 의무화[의무, 2005. 12월]

- 카드사 제공 결제시스템에 키보드 해킹방지 프로그램을 적용하여 결제시스템 비밀번호 유출로 인한 부정사용 방지

o 안심클릭 입력 프로세스 변경[의무, 2006. 6월]

- 안심클릭은 카드번호 입력화면을 카드사제공 결제시스템에서 입력토록 설계를 변경하여 카드번호 유출 위험 제거

o 쇼핑몰 등에서 카드번호, 계좌번호 등을 입력하는 경우 키보드 해킹방지 프로그램 설치(산자부에 요청)

Ⅶ. IT보안관리 부문

1. 정보보호 인력

□ 현 황

o 개 요

- 전자금융업무와 관련한 금융회사 정보보호 관련 인력 비율 및 경력 현황 분석

o 인력현황(전업계 6개 카드사)

① 정보보호인력 비율 및 인력수

(단위 : %)

(전체인력대비) IT 인력 비율	(IT인력 대비) 정보보호인력비율	비 고
14.5	2.7	전체인력 대비 정보보호 인력은 0.3%임

(단위 : 명)

정보보호인력	카드회사 수	비 고
7명 초과	1	IT 보안업무 담당인력 기준
7명 이하	1	
5명 이하	2	
3명 이하	2	

② 정보보호인력 정규직 및 비정규직 비율

(단위 : 명)

정 규 직	계 약 직	기 타 (상주용역 등)
61.4	11.0	27.6

③ 정보보호인력 경력별 비율

(단위 : %)

경력 구분	인력 비율	비 고
1년 이내	16.5	IT 보안업무 경력
3년 이내	14.7	
5년 이내	58.8	
5년 이상	9.9	

□ 문 제 점

ㅇ 정보보호업무 수행을 위한 관리 및 통제인력 부족

- IT정보기술의 발전과 더불어 다양한 매체를 통한 비대면 온라인 전자금융거래가 급속히 확산되고 있음

- 또한, 해킹/컴퓨터바이러스의 지속적 증가와 신종 전자금융거래 위협요소의 출현(피싱, 피망 등)으로 상시감시체계의 강화가 필요함에도 이를 수용할 인력채용에는 소홀

□ 대 책

ㅇ 전자금융거래 보안업무 수행을 위한 정보보호 인력 적정수준 유지[권고]

- 금융회사 정보보보호전담인력의 적정한 규모는 업무 수행환경(조직체계, 전문인력, 통합관리, 외부 전문 컨설턴트 활용 등)에 따라 상이하므로 각 사가 자율적으로 운영

- 보안점검, 정보보호체계 강화 등 적절한 보안관리 및 통제활동 수행뿐만 아니라, 비상사태, 전자적 침해 사고 발생시 즉각적인 대응이 가능하도록 적정한 정보보호 인력 유지

ㅇ 정보보호업무 수행 직원은 책임있는 정규직원 채용[권고]

- 중·장기 보안 계획, 보호대책 수립, 문서자료 관리, 보안사고 대응, 서버/네트워크 보안, 보안정책 수립, 보안솔루션 도입 등 정보보호의 기획 및 운영업무는 대부분 전문적이고 책임이 따르는 업무로

- 해외 선진금융기관에서도 정보보호업무의 중요성을 고려하여 정보보호 전담인력은 대부분 정규직원을 선호·채용하고 있으므로 전문적 지식·경험을 가진 정규직원 비율을 높이도록 권고

2. 정보보호 전담조직

□ 현 황

○ 개 요

- 전자금융업무를 위한 IT보안 전담조직과 보안통제 형태 파악

○ IT 보안전담조직 현황(전업계 6개 카드사)

(단위 : 조직수)

전담조직 보유	전담조직 미보유	비 고
4	2	

□ 문 제 점

○ 정보보호전담조직의 총괄적 통제력 부족

- 비대면 전자금융거래의 급격한 확산으로 IT투자확대, IT의존도 증가에 따른 리스크관리가 중요함에도

- 전자금융거래의 안전성, 신뢰성 등 IT보안관리 업무를 수행하는 정보보호 전담조직이 IT부서 및 일반 업무부서에 소속되어 정보보호에 대한 총괄적 통제력이 취약

□ 대 책

○ 정보보호 전담조직을 CIO직속의 독립된 별도조직으로 개편하고, 총괄적 통제체제 구축[권고]

- 전자금융거래의 안정성 및 신뢰성 증대와 강화를 위해서는 실질적 정보보호 활동을 보장하고 정보보호전담조직의 인원확충을 통해 CIO직속의 별도로 독립된 조직으로 조직체계를 개편하여 총괄적 통제체제를 강화하고 책임을 부여

3. 정보보호 예산

□ 현 황

○ 개 요

- IT예산 대비 정보보호예산 현황 조사

○ 정보보호예산 비율(전업계 6개 카드사)

(단위 : %)

구 분	(IT예산 대비) 정보보호예산 비율	비 고
2004년	1.2	
2005년	2.6	

□ 문 제 점

○ 정보보호에 대한 투자 미흡

- 해외 금융기관의 정보보호 예산에 대한 투자(IT예산대비 약 5~10%)에 비하여 상대적으로 정보보호에 대한 투자가 미흡(해외 금융기관 정보는 은행부문 붙임8 참조)

□ 대 책

○ **정보보호 예산은 IT 예산 대비 적정한 수준 유지[권고]**

- 적정한 정보보호예산은 각 금융회사의 업무계획에 따라 자율적으로 결정될 사항이나, 정보보호 예산은 IT예산(신규 시스템, 차세대시스템 구축 등)과 밀접한 관계를 가짐

- 해외 선진금융기관이 IT예산대비 약 5%이상의 정보보호 예산을 배정하고 있음을 감안하여 IT예산대비 적정수준 이상을 배정하도록 권고

Ⅷ. 기 타

1. 매출전표 인자 정보 제한

□ 현황 및 문제점

○ 일부 카드 가맹점(주요소, 음식점 등)의 경우 카드 매출 전표에 카드번호 및 유효기간이 인자되고 있음

○ 동 정보만을 이용하여 결제가 가능한 가맹점(수기특약* 가맹점)이 있어 제3자에 의한 불법 매출 발생 가능

* 수기특약 : 거래의 진위성 및 부정사용 여부에 대한 책임은 가맹점의 책임으로 하는 계약

□ 대 책

○ **향후 모든 카드 매출 전표에 유효기간 인자를 금지토록 변경[의무, 2005. 12월]**

2. VAN사 정보보호 체계 강화

□ 현 황

○ 개 요

- 고객이 신용카드 결제시 카드 결제정보가 VAN사를 통하여 카드사에 전달되고 있으며 거래 로그를 위한 일부 정보는 VAN사에 저장

- 우리원에서 VAN사도 카드사에 준하는 고객 정보 보안 및 해킹 방지, 주요 데이터에 대한 보호의 필요성을 인식하여 카드사를 통하여 VAN사의 고객정보보호 강화를 지도*

  * 'VAN사업자와의 업무위탁 계약에 따른 유의사항 통보', (검업지6770-00030, 2004.7.5)

- 카드사와 VAN사는 동 지도내용과 관련하여 'VAN사와 카드사간 카드정보 보호 및 보안체계 강화를 위한 업무 협약서'를 체결하고 세부적인 추진 방안에 대하여 협의 중

□ 문 제 점

○ 결제 정보 유출 위험

- 카드 결제정보를 중계하고 거래 내역 증명을 위하여 카드정보를 저장하고 있어 해킹*이나 직원(내부 및 용역 직원)에 의하여 카드 결제 정보 유출 위험

  * 최근 비자, 마스터카드 등 미국 카드회사의 고객 정보 처리를 담당하는 카드시스템스 솔루션스사가 해커 공격에 의해 4,000만명 이상의 고객 정보를 도난(연합뉴스, 2005.06.19 (일))

○ VAN사와 카드사간 체결한 보안 협약서 실천 추진 방안에 대한 이견

- VAN사와 카드사간 체결한 'VAN사와 카드사간 카드정보 보호 및 보안체계 강화를 위한 업무 협약서'의 구체적인 추진 방안 및 일정에 대하여 이견이 있어 합의안 도출에 어려움 발생

□ 대 책

○ VAN사업자와 카드사간 협의 내용을 지속적으로 모니터링하여 우리원 지도사항의 이행 여부 점검 및 필요시 이견 사항에 대하여 중재

  * <참고> 정보보호를 위한 기술부문 협의 내용(진행중)

  - 단기 : VAN사에서 카드 유효기간 저장 금지

  - 중기 : VAN사 저장 정보중 거래일로 부터 3개월이 경과된 자료는 카드번호 일부(9 ~ 12번째 자리) 삭제

  - 장기 : VAN사 저장 정보중 거래일로 부터 3개월이 경과되지 않은 정보는 카드번호를 암호화 하여 저장

(붙임1)

PC용 보안프로그램 개선방안

<현재 문제점>	
공통부문	ㅇ 비은행권의 보안 솔루션 적용 부족 ㅇ 보안 솔루션간의 보호 영역이 중첩되지 않아 취약점 발생 **예) 키보드 보안 솔루션과 응용 프로그램 보안(PKI)** ㅇ 보안 솔루션 업체간 특허 공유 체계 미비로 보안 기능상의 제한과 법적분쟁 발생 가능성 ㅇ 일부 보안 솔루션의 품질 문제로 전자 금융 거래의 편리성 저하 **예) PC 자원의 과다사용, 보안 프로그램간 상호충돌 등**
키보드 보안제품	ㅇ Port, Interrupt Service Routine(ISR) 수준의 보안 위협 ㅇ 키보드 입력 값의 암호화에 대한 해독 가능성 ㅇ 응용 프로그램, 웹 브라우저 환경에서의 입력 값 보호를 위한 PKI 프로그램과의 연동 부족
백 신	ㅇ 대고객용 악성프로그램 제거 솔루션에서 **상용 키로거**, 원격 제어 프로그램 등 해킹에 악용될 수 있는 프로그램의 차단 시 법적분쟁 발생 ㅇ 인터넷을 통한 악성 프로그램의 전파 차단을 위한 기반 인프라 부족
PC 용 방 화 벽	ㅇ 기능상 어려움으로 일반 사용자의 활용성 저하

가. 대 책

□ 현행 키보드 해킹방지 프로그램 기능 강화

- ㅇ Port, Interrupt Service Routine(ISR)을 이용한 공격에 대응할 수 있도록 기능 제고
- ㅇ PC관리를 위해 제공되는 상용 키로거, 원격제어 툴을 통한 정보유출 방어기능 추가
- ㅇ 키보드 해킹방지 프로그램과 PKI 응용 프로그램간 연계를 통하여 공인인증서 비밀번호 유출 방지

□ PC수준별 장애, 성능저하, 타 기능과의 충돌 해소

나 . 요 조치사항

<종합대책 T/F>

□ 키보드보안 프로그램의 취약점 보완조치(~8월말)

- ㅇ 각 보안업체에 Port, ISR 등에 대한 보안조치 요구
- ㅇ 키보드보안 프로그램과 PKI 응용 프로그램 간 연동강화 요구

※ 붙임3 "해킹툴을 통한 키보드보안 프로그램 점검결과" 참조

< 카 드 사 >

□ 전자금융거래시 PC용 보안프로그램(키보드보안프로그램, PC용 방화벽) 제공**[의무, 2005. 12말]**

□ 금융회사에서 사용되는 키보드보안제품 및 PC용 보안프로그램의 기능 및 취약점 점검(상시)

□ 취약점에 대한 보완조치 또는 불가시 제품교체(상시)

< 정 부 >

□ 전자금융 거래시 백신프로그램에서 해킹에 악용될 수 있는 상용키로거 프로그램 등에 대한 강제적 차단토록 조치

□ 네트워크 백본을 관할하는 통신사업자의 악성프로그램 차단 프로그램 운영 의무화 요청

□ 게시판, 자료실 등을 운영하는 포탈사이트에 대하여 악성프로그램 차단 프로그램 설치 의무화

※ 상기사항은 정통부에 요청

< 공 통 사 항 >

□ 키보드해킹방지 보안프로그램 품질인증제도 도입

○ 전자금융거래시 제공되는 PC용 보안프로그램 중 키보드 해킹 방지프로그램은 가장 중요한 기능 및 역할을 하게 되므로 이에 대한 품질보장이 우선 되어야 함

○ 현재 도출된 문제점은 단기간에 해결이 불가능하며, 지속적인 보안 관리와 급속히 발전하는 IT·금융환경의 다양한 보안이슈에 신속하고 유기적인 대응을 위한 전담조직 필요

⇒ 붙임2 "전자금융보안전담기구 설립 검토"와 연계하여 검토

□ 전자금융거래 이용자에게도 책임·의무를 부과 추진

○ 금융회사에서 보안프로그램을 적극적으로 제공하여도 고객이 활용하지 않을 경우 실제적 대응이 불가능하므로 금융회사에서 제공하는 보안프로그램 등을 고의 또는 자의로 실행하지 않는 경우 책임·의무를 부과토록 법적제도 장치 마련 추진

※ 과거 사고분석결과 공모·허위·고의 등 은행의 책임의무 약점을 이용한 사례가 많음

□ PC용 보안프로그램으로 해킹에 대한 근본적 대응에는 한계가 있으므로 전자금융거래 본인인증강화, 공인인증서 관리체계 개선방안 등과 연계하여 추진

(붙임2)

전자금융 보안전담기구 설립 검토

<현재 문제점>

○ 금융권의 전자금융부문 보안사항에 대한 상호연동 및 호환성 부족 등으로 인하여, 지속적으로 발생되는 보안이슈사항에 대한 대처 미비 및 지연, 중복투자 등 문제점 대두

1. 필 요 성

□ 신규 보안 취약점, 위협에 대한 분석 및 대응

□ 전자금융 보안 솔루션의 품질 검증(인증) 및 지속적인 품질 관리

□ 보안 솔루션 간 특허 분쟁 조정, 상호 연동 표준 지원 및 호환성 검증

□ 상용 프로그램을 사용한 해킹사고 공동 대응

□ 신규 위협 요소, 보안패치 등 다양한 보안 이슈에 대한 사용자 홍보 강화, 보안 의식 제고

2. 보안전담기구설립 방안

□ 금융정보보호협의회 부속 조직 추가

○ 현재 기 운영중인 금융정보보호협의회(사무국 : 금융감독원)에 부속되는 전자금융 보안사항에 대한 실질적인 운영 및 대응 조직 설립

□ 운영기관별 역할 및 전담조직 인력구성(기본 案)

기 관 구 분		역 할
금융감독원		○ 협의회 및 전담조직 운영에 관련된 업무 총괄조정
금 정 협		○ 금융부문에서 필요한 정보보호 기준, 표준화, 통합 등 정책에 대한 검토, 개발 등 협의 및 결정
전 담 조 직	역할	○ KISA, 국가사이버안전센터 등으로부터 제공받은 해킹프로그램 테스트 및 대응 ○ 정보보호제품 평가, 검토 및 인증 ○ 정보보호 및 금융IT에 대한 정책 연구 및 개발
	인력 구성	○ 관리자 : 전문계약직 채용(상근) ○ 운영인력 : 보안전문업체 경쟁입찰 등을 거쳐 아웃소싱으로 운영(계약기간을 두어 재계약 또는 신규 경쟁입찰 실시) ※상세인력소요, 예산 및 조직체계는 별도 T/F에서 재검토

□ 비용 분담 : 참여 기관 분배

□ 조치필요사항

○ 전담기구설립 금융권 협의

○ 전담기구설립 추진 T/F 구성

○ 금정협 시행세칙 등 관련 근거 변경 및 마련

□ 초기 조직설립절차마련을 위한 소규모 T/F 구성하여 다음사항을 검토(2005. 12말)

○ 효율적 조직운영을 위한 구성형태 및 관리체계

○ 초기 설립을 위한 예산, 인력 등 소요내역

○ 감독기관, 금융기관, 보안업체간의 협의체 운영방안

○ 관련 근거규정 변경 및 마련

○ 수행업무범위 및 조직체계

○ 보안관련업체 및 아웃소싱인력의 적극적 활용 체계

○ 초기 분담금 내역 및 체계 마련

○ 조직설립절차(案)에 대한 금융권 의견수렴 및 세부 추진일정 수립

(붙임3)

해킹툴을 통한 키보드보안 프로그램 점검결과

1. 개 요

□ 은행을 제외한 대부분의 증권, 보험, 카드사는 전자금융거래 사용자에게 보안프로그램 제공이 미진하며, 보안프로그램은 4개 보안업체에서 모든 금융권에 제공하고 있음

* 증권: 42개사중 6개사(14%), 보험 : 40개사중 8개사(20%), 카드 : 6개사중 3개사(50%)만이 보안프로그램 제공

□ 금융권에 보안프로그램을 제공하는 4개사의 제품을 해킹 툴을 통해 점검 실시

2. 점 검 방 법

□ 점 검 툴 : 한국정보보호진흥원(KISA)에서 제공하는 30개 해킹 및 상업용 프로그램으로 입력정보에 대한 해킹가능 여부

□ 점검대상 : 인터넷뱅킹 중심의 전자금융서비스 보안프로그램

□ 점검기간

○ 보안업체(4개사) 자체점검 : 7.8~7.13, 8.22~8.25(9일)

○ 종합대책 T/F점검 : 7.18~7.22, 8.22~8.26(10일)

※ 점검툴 : 키로그(20종), 원격제어(1종), 트로이목마(9종)

종 류	프로그램 명
Keylogger	Personal-Inspector, **Elite Keylogger**, **Activity Keylogger** Ghost Keylogger(3.40), Perfect Keylogger lite(1.62) Perfect Keylogger(1.47), SC-keylog pro 3.1 PAQ keylogger, abc keylogger v1.1 SpyPatrol Invisible KeyLogerv(1.3) SC-keylogger(2.8), PAL KeyLog Pro(3.2) Keyclient, KISA 작성 키로거, BHO 방식 키로거(Stealth Web Page Recoder), IK, DarkOmem, SKinNT, DeskTop Detective, KeyLogger Pro
원격제어툴	SMP 원격제어 툴
트로이목마	Net-Devil 1.5, Nishica1.1, Wredzioch, Beast 2.07 C.I.A Cruel Intentionz 1.3, Optix Pro 1.33, Y3k Rat 2k5 RC 1.0, ProRat 1.9, KaoticRAT.1.0

3. 점검결과

□ 모든 보안프로그램에서 일부 취약점이 발견

프로그램 명		보안프로그램 제공업체			
		A사	B사	C사	D사
KISA 작성 키로거	포트 레벨 키로깅	X	O	X	O
	서브클래싱 키로깅	O	X	O	X
BHO 방식 키로거 (Stealth Web Page Recoder)		X	X	X	X
Elite Keylogger		X	O	O	O
Activity Keylogger		O	O	O	X
기타 키로거 프로그램 등(26개)		O	O	O	O

○ KISA 1차 제공 해킹프로그램(9개)
- 테스트 결과 1개 보안프로그램에서 정보누출 확인(조치완료)

○ KISA 2차 제공 해킹프로그램(18개)
- 테스트 결과 1개 보안프로그램에서 정보누출 확인(조치완료)

○ KISA 3차 제공 해킹프로그램(3개)
- 테스트 결과 모든 보안프로그램(4개)에서 정보누출 확인(조치중)

※ 취약점에 대하여 2005년 11말까지 조치 완료키로 하였음

4. 조치사항 및 향후대책

□ 조치사항

○ 발견된 취약점에 대한 보안프로그램 제공업체에 즉시 보완토록 조치요구

⇒ 대부분 취약점에 대하여 보완조치 하였으나, 일부사항(서브클래싱 및 BHO)에 대해서는 프로그램 개발 등 단기간에 적용이 불가능

※ 서브클래싱 및 BHO 취약점에 대한 사항은 A사 : '05. 9말, B사 : '05. 11말, C사 : '05. 11말, D사 : '05. 9말까지 조치 완료키로 하였음

○ 키보드 해킹방지 프로그램과 PKI 응용 프로그램간 연계 강화를 통해 입력정보 노출방지 요구

○ 향후, 발견될 수 있는 새로운 취약점 또는 새로운 해킹프로그램에 대한 대책 요구

□ 향후대책

⇒ 붙임1 "PC용 보안프로그램 개선방안" 참조

※ 키보드 해킹방지 프로그램은 고객의 금융거래정보를 보호하는 기능을 하는 기본이 되는 보안프로그램으로 보안기능 및 신규 취약점에 대한 지속적인 점검 및 확인이 필요