情 報 保 護 學 會 誌
第18卷 第5號, 2008. 10

전자금융 침해사고 예방 및 대응 강화 방안

이 정 호*

요 약

편리한 금융거래 수단으로써 인터넷뱅킹을 포함한 전자금융 서비스가 생활화 되었으며 그 중요성 또한 갈수록 증가하고 있다. 이에 대한 부작용으로서 사용자의 실수나 금융기관, 쇼핑몰, 포털 등의 해킹을 통한 전자금융 접근매체의 유출, 비정상적인 지불결제나 인터넷뱅킹 이체 사고 등 침해사고 또한 함께 증가하고 있다.

금융권은 금융감독원을 중심으로 전자금융 종합보안 대책 수립(2005년) 및 전자금융거래법 시행(2007년) 등을 통해 고객 PC의 해킹방지를 위한 다양한 보안프로그램 제공 의무화, 보안등급에 따른 이체한도 차등화, 금융권 통합 OTP 인증체계 구축 등 전자금융 침해사고 예방을 위한 적극적인 노력을 기울여오고 있으나, 최근 들어 피싱/파밍 등 신종 사이버 사기 기법이나 해외의 전문 해커에 의해 개발된 고도의 지능화된 해킹툴이 사용되어 보안프로그램을 무력화시킨 후 고객정보를 유출해가거나 일반 포털사이트, 웹하드, 웹메일 등의 해킹을 통해 인터넷 사이트에 등록된 고객의 인터넷뱅킹 접근매체를 유출하여 인터넷뱅킹 침해 사고를 일으키는 등의 신종 침해사고를 완벽히 차단하지는 못하고 있어, 더욱 강력한 전자금융 침해사고 예방 통제 방안의 수립과 함께 침해사고 발생 시 원인 파악 및 범인 검거를 위한 역추적 시스템의 구축 등 기존 보안체계를 대폭 강화할 필요성이 발생하고 있다.

본 연구에서는 시중 은행의 인터넷뱅킹 침해사고 발생 현황 조사를 중심으로 최근 발생한 전자금융 침해사고의 추이 분석, 침해사고 주요 원인과 기존 대응 체계의 현황, 한계점 등을 파악하였다. 그리고 전자금융 침해사고의 효과적인 예방 및 대응 강화 방안으로서 사용자 관점에서 공인인증서를 중심으로 한 전자금융 접근매체의 관리 강화 방안을 제안하였으며, 전자금융 서비스를 제공하는 금융 기관 관점에서 효과적인 전자금융 거래 로깅 및 역추적 시스템의 구축 및 전체 금융기관과 감독기관 간의 유기적인 공조를 기반으로 한 침해사고 공동 대응체계의 구축 및 운영을 위한 시스템의 구성 방법, 운영 프로세스, 관련 법률의 검토 및 대응 방법 등을 제안하였다.

Ⅰ. 서 론

인터넷을 통한 주식 거래나 인터넷 쇼핑몰에서 전자지불 사용이 일반화되고 있다. 특히 은행권역의 경우, 최근 한국은행에서 발표한 통계자료에 따르면 전자금융 서비스를 통한 금융거래가 최초로 전체 거래량의 80%를 초과했으며, 새로 출범한 정부에서도 인터넷 전문은행을 적극적으로 추진하는 등 인터넷을 기반으로 한 금융거래가 생활화 되면서 전자금융 서비스 전반에서 정보보안의 중요성 또한 지속적으로 증가하고 있다.

1.1 전자금융의 생활화

2008년 4월 28일, 한국은행에서 발표한 '2008년 1/4분기 국내 인터넷뱅킹서비스 이용현황'에 따르면 2008년 3월말 현재 금융결제원의 인터넷뱅킹용 공인인증서 발급수는 1,207만개로 전년말 대비 4.8% 증가했으며, 19개 금융기관에 등록된 인터넷뱅킹 고객수는 중복을 포함하여 합산했을 때 4,694만명으로 전년말 대비 5.0% 증가하여 사상 처음으로 4,500만명을 초과했으며, 2002년말 1,771만명과 비교하면 약 5년 만에 265%의 폭발적인 증가세를 기록하였다

2008년 3월중 금융서비스의 전달채널별 업무처리비중(건수 기준)은 전체 입출금거래 기준으로 비대면거래 비중이 80.2%이며 그중 인터넷뱅킹이 24.4%를 차지했으며, 조회서비스의 경우 비대면 거래 비중이 80.5%이며, 그중 인터넷뱅킹이 56.8%로 가장 높은 비중을 나타내었다.

* 신한은행 IT기획부 (guardian@shinhan.com)

〔표 1〕 금융기관 인터넷뱅킹 등록 고객수

(단위 : 천명, 천개社, %)

	2006. 12월말	2007				2008. 3월말
		3월말	6월말	9월말	12월말	
개인	34,123 (3.9)	36,232 (6.2)	38,064 (5.1)	40,274 (5.8)	42,396 (5.3)	44,564 (5.1)
기업	1,789 (5.2)	1,878 (5.0)	2,047 (9.0)	2,171 (6.1)	2,302 (6.0)	2,378 (3.3)
합계	35,912 (4.0)	38,110 (6.1)	40,111 (5.3)	42,445 (5.8)	44,698 (5.3)	46,942 (5.0)

※ ( ) 내는 전분기말 대비 증감률

2008년 1/4분기의 전체 인터넷뱅킹 이용 건수 및 금액(일평균 기준)은 2,118만건, 22조 3,179억원으로 전분기 대비 각각 3.6% 및 3.8% 증가한 것으로 나타났으며, 그중 인터넷뱅킹 이체 건수는 3,102천건에 22조300억원으로 건당 평균 이체 금액은 약 71만원으로 분석되었다[8].

1.2 전자금융 거래에서 정보보안의 중요성

한국은행에서 발표한 공인인증서 발급 건수 자료에 의한 국내 인터넷뱅킹 가입자 수는 약 1,207만명으로 추정되며, 이는 통계청에서 발표한 2008년 3월 기준 국내 경제 활동 인구 2,411만명의 50%를 초과하는 수치로서 국민의 반 이상이 인터넷뱅킹을 직접 사용함을 의미하는 것이다.

〔표 2〕 2008년 3월중 금융서비스의 전달채널별 업무처리비중(건수 기준)

구 분	대면거래 (창구거래)	비 대 면 거 래				합 계
			CD/ ATM	텔레 뱅킹	인터넷 뱅킹	
입출금거래 건수 기준	19.8	80.2	44.3	11.5	24.4	100.0
조회 건수 기준	19.5	80.5	11.6	12.1	56.8	100.0

또한, 2008년 6월 금융위원회 공보자료의 "금융규제 개혁 기본방향 및 진입규제 개선방안"에 따르면 고객이 영업점에 찾아가지 않아도 인터넷으로 일반적인 은행업무를 처리할 수 있는 '인터넷 전문은행'[1] 의 적극적인 추진이 예정되어 있다. 인터넷 전문은행은 대부분의 거래를 인터넷뱅킹을 중심으로 한 전자금융 서비스를 통하여 제공하게 되며, 이는 기존 금융실명제법이나 전자금융감독규정에서 반드시 영업점에서 대면 확인을 통해 이루어지도록 하고 있는 최초 통장 개설, 인터넷뱅킹

〔표 3〕 인터넷뱅킹서비스 이용실적(일평균 기준)

(단위 : 천건, 십억원, %)

	2007								2008. 1/4분기중	
	1/4분기중		2/4분기중		3/4분기중		4/4분기중			
	건수	금액	건수	금액	건수	금액	건수	금액	건수	금액
조회 서비스	13,295 <83.8> (13.8)	-	14,194 <84.1> (6.8)	-	15,750 <85.2> (11.0)	-	17,469 <85.4> (10.9)	-	18,075 <85.3> (3.5)	-
자금 이체	2,564 <16.2> (11.8)	16,645.1 - (21.6)	2,681 <15.9> (4.6)	17,440.4 - (4.8)	2,736 <14.8> (2.1)	18,643.9 - (6.9)	2,977 <14.6> (8.8)	21,498.5 (15.3)	3,102 <14.7> (4.2)	22,300.6 (3.7)
대출 1) 신청	2.7 <0.0> (35.0)	14.0 - (10.2)	1.8 <0.0> (-33.3)	8.6 - (-38.6)	2.1 <0.0> (16.7)	19.3 - (124.4)	1.4 <0.0> (-33.3)	11.9 - (-38.3)	3.0 <0.0> (114.3)	17.3 - (45.4)
합계	15,862 <100.0> (13.5)	16,659.1 - (21.6)	16,877 <100.0> (6.4)	17,449.0 - (4.7)	18,488 <100.0> (9.5)	18,663.2 - (7.0)	20,447 <100.0> (10.6)	21,510.4 - (15.3)	21,180 <100.0> (3.6)	22,317.9 - (3.8)

1) 전자외상매출채권담보대출, 기업구매자금대출 제외
※ < > 내는 인터넷뱅킹서비스에서 차지하는 비중
( ) 내는 전분기대비 증감률

1) "인터넷 전문은행(Internet Primary Bank)"이란 소수의 영업점 또는 영업점 없이 은행업무의 대부분을 인터넷 및 CD, ATM 등의 전자매체를 통해 영위하는 은행을 지칭함.[2]

가입, 보안카드 또는 OTP(One Time Pad)의 발급 등 주요 거래의 업무 규정 중 상당 부분이 비대면 채널이나 기타 간접적인 대면 확인 방법을 통해 수행될 수 있는 새로운 전자적인 인증 방법의 제도화를 의미하는 것으로, OTP 및 보안토큰 의무화, 생체 인식과 같은 강력한 인증체계의 도입과 함께 전자금융거래법 및 관련 감독 규정 개정 등의 제도적인 개선이 수반될 것으로 예상된다.

인터넷뱅킹을 중심으로 HTS(Home Trading System), 온라인 지불결제 등 전자금융 사용자의 증가와 인터넷 전문은행과 같은 전자금융 서비스의 영역 확대 및 관련 제도 개선 등을 고려하면 이제 전자금융 서비스는 개별 금융회사의 서비스로만 볼 것이 아니라 국가 경제의 주요 인프라 차원에서 바라보아야 할 것이며, 안정적인 서비스 제공을 위한 정보보안 체계의 확립 또한 국가적인 차원에서 주도해야할 핵심 기반이라고 할 수 있다.

Ⅱ. 전자금융 침해사고 및 대응 현황

전자금융 서비스의 안전성 강화를 위하여, 금융권은 금융감독원을 중심으로 전자금융종합보안 대책 수립 및 전자금융거래법 시행 등을 통해 기술적, 제도적으로 다양한 보안 체계를 수립하는데 많은 노력을 기울여왔다. 하지만 고객의 실수를 유도한 고객 정보 유출이나 전문 해커에 의해 고객 PC나 인터넷 사이트에 저장된 고객 정보의 해킹을 통한 인터넷뱅킹 침해 사고 등 다양한 신종 해킹 기법을 통한 침해사고가 지속적으로 발생하고 있다.

2.1 인터넷뱅킹 침해사고 현황

2008년 7월, 일본 금융청이 발표한 은행관련 범죄건수와 피해 보상 현황에 따르면, 2007년 한 해 동안 발생한 인터넷뱅킹 사고는 231건으로 2006년도 대비 2배 이상 증가하였으며, 평균 피해액수는 82만엔이었다. 국내에서 전자금융 침해사고와 관련된 정확한 현황 파악이나 공식적인 통계 자료는 발표되지 않고 있으며, 금융기관 특성상 외부로 공개가 어려운 점 등으로 인해 전체 발생 건수와 피해금액은 파악하기 불가능하지만 침해 사고 증가율은 일본의 경우와 비슷할 것으로 추정된다.[10]

전자금융 침해사고의 대표적인 사례인 인터넷뱅킹 서비스를 통해 고객의 자금이 직접 유출된 사고 민원 유무 및 주요 원인에 대하여 시중 은행의 업무 담당자를 대상으로 설문 조사를 통해 현황을 파악한 결과는 다음과 같다.

- 설문 기간 : 2008.7.1 ~ 2008.8.6
- 설문 대상 : 시중 15개 은행 정보보안 담당자
- 설문 방법 : e-mail을 통한 설문조사 및 전화 인터뷰

인터넷뱅킹 서비스의 이체 사고 관련 설문 조사 결과, 응답 대상 15개 은행 중 10개 은행에서 고객이 인가하지 않은 자금 이체가 발생하여 전체의 약 67% 에 해

〔표 4〕 인터넷뱅킹서비스 이체 사고 관련 설문 결과

설문 사항	응답 결과	비고
1. 전자금융종합보안대책이 발표된 2005년 9월부터 2008년 7월까지, 인터넷뱅킹을 통해서 고객 계좌에서 타인에게 금전이 이체되어 고객 민원이 직접 접수되거나 감독기관 또는 수사기관으로부터 수사 협조 요청이 발생한 사례가 있습니까? (O, X 답변)	있음(10) 없음(5)	수도권 시중은행 (7/8), 지방 및 특수 은행(3/7)
2. 1번 질문에서 O 로 답변한 경우, 고객의 공인인증서, 비밀번호 등 인터넷뱅킹 접근매체가 유출된 주요 원인은 무엇입니까? (해당 항목 복수 기재) 1) 고객 PC에 설치된 악성 프로그램(키로거)에 의한 유출 2) 고객 PC에 비밀번호를 텍스트 파일로 저장해서 사용 중 악성 프로그램에 의해 공인인증서와 함께 유출 3) 인터넷 피싱, 파밍 등에 의해 고객 정보와 함께 유출 4) 고객이 인터넷 웹메일, P2P, 웹하드 등에 공인인증서, 비밀번호 파일 등을 보관하여 사용 중 인터넷 사이트의 해킹을 통한 유출 5) 고객이 지인이나 대부업체 등에 제공한 후 유출이나 비인가 사용 6) 고객 가족에 의한 사용 7) 지갑, 신분증 등의 일시 또는 영구 분실에 의한 유출 8) 은행 서버의 해킹이나 내부 직원에 의한 고객 정보 유출 9) 고객 실수로 추정되나 원인 불명확 10) 기타 ( )	1)번 1개사 2)번 2개사 3)번 1개사 4)번 1개사 5)번 4개사 6)번 2개사 9)번 4개사 10)번 2개사	10)번 기타 답변은 시스템 오류 1건, 전자화폐 관련 침해사고의 중간 경로로 악용 1건

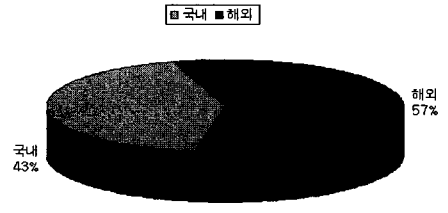
당하는 은행에서 관련 민원이나 사고 접수 등이 있었던 것으로 파악되었다. 특히 수도권 시중 은행의 경우 응답 대상 8개 은행 중 7곳에서 민원 접수가 한 건 이상 접수되어 대부분의 주요 은행에서 고객이 인가하지 않은 자금 이체 사고가 발생했던 것으로 파악되었다.

인터넷뱅킹 이체 사고와 관련된 주요 발생 원인은 고객 실수로 추정되나 원인이 불명확한 경우와 고객이 지인이나 대부업체 같은 곳에 인터넷뱅킹 접근 매체를 제공하여 공유하던 중 이체 사고가 발생한 경우가 각각 4개 은행에서 1건 이상 발생한 사례가 있어 가장 많았으며, 고객이 집이나 사무실의 PC에 비밀번호를 텍스트 파일로 저장해서 사용 중 악성 프로그램에 의해 공인인증서와 함께 유출된 경우와 고객 가족에 의한 비인가 사용이 발생한 경우가 각각 2개 은행에서 발생 사례가 있었으며, 그 외 고객 PC에 설치된 악성 프로그램(키로거)에 의한 비밀번호 유출, 인터넷 피싱, 파밍 등에 의해 고객 정보와 함께 유출, 고객이 인터넷 웹메일, P2P, 웹하드 등에 공인인증서, 비밀번호 파일 등을 보관하여 사용 중 인터넷 사이트의 해킹을 통한 유출 등이 각각 1개 은행에서 발생한 사례가 있었다.

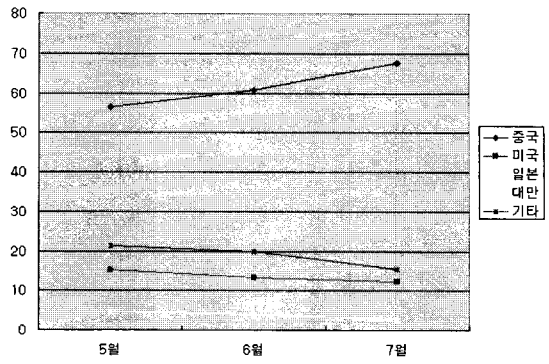
2.2 해외로부터의 인터넷 침해 시도 증가

국내 전자금융 침해사고의 공격자에 대한 통계자료는 공식적으로 집계된 사례가 없으나, 시중 은행권의 인터넷뱅킹 침해사고와 관련되어 사례 분석 결과 가장 최근에 발생한 3건의 이체 사고가 모두 중국으로부터 접속하여 발생하였으며, 업무 담당자 인터뷰 결과에서도 그동안 발생한 이체 사고는 대부분 중국으로부터의 접속을 통해 발생한 것으로 조사되었다.

한국정보보호진흥원(KISA)의 KrCERT에서 발간하는 2008년 7월 해킹 바이러스 통계 및 분석 월보에서도 KISC[2] 허니넷에 유입된 해외로부터의 침해 시도가 전



〔그림 1〕 KISC 허니넷 유해 트래픽의 IP소재지별 분류
(2008.5월~7월, 3개월 평균)



〔그림 2〕 KISC 허니넷 유해 트래픽의 IP소재지별 분류
(2008.5월~7월, 3개월 평균)

체 침해시도의 50%를 초과하였으며, 특히 중국으로부터의 침해 시도가 전체 해외로부터의 접속 시도의 60%를 초과하는 등 매월 증가 추세에 있었다.

2.3 전자금융 침해사고의 추이 및 특징

최근 실제 금전 이체 사고가 발생한 전자금융 침해사고의 추이 및 주요 특징은 주로 중국의 전문 해커에 의해 피싱/파밍 등을 통한 사용자의 실수 유발 또는 부주의를 악용하거나, 인터넷 메일, 웹하드 등 자료실을 해킹하여 고객이 저장해둔 인터넷뱅킹 접근매체[3] 를 가로챈 후 수사 기관의 역추적을 차단하기 위해 해외에서 인터넷뱅킹을 통하여 국내 미리 개설해둔 대포 통장으로 이체하는 인터넷뱅킹을 통한 고객 계좌의 자금 이체 방식의 침해사고가 증가하는 것으로 분석되었다.

국내 인터넷뱅킹 서비스는 2000년도부터 본격화되기 시작하였다. 인터넷뱅킹에 대한 직접적인 해킹은 2005

2) KISC은 한국정보보호진흥원(KISA)에서 운영하는 인터넷침해사고 대응센터를 의미함.

3) 본 논문에서 "접근매체"의 의미는 다음의 전자금융 거래법 제2조(정의)의 제10항을 따름.

10. "접근매체"라 함은 전자금융거래에 있어서 거래지시를 하거나 이용자 및 거래내용의 진실성과 정확성을 확보하기 위하여 사용되는 다음 각 목의 어느 하나에 해당하는 수단 또는 정보를 말한다.
가. 전자식 카드 및 이에 준하는 전자적 정보
나. 「전자서명법」 제2조제4호의 전자서명생성정보 및 같은 조제7호의 인증서
다. 금융기관 또는 전자금융업자에 등록된 이용자번호
라. 이용자의 생체정보
마. 가목 또는 나목의 수단이나 정보를 사용하는데 필요한 비밀번호

년 5월, 19세 입시 준비생에 의해 최초 발생하였다. 당시 범인은 포털 게시판을 통해 "NetDevil" 이라는 원격접속 및 키로깅[4]이 가능한 악성 프로그램을 유포한 후 고객이 인터넷뱅킹을 사용할 때 키로깅을 통해 회원 ID 및 비밀번호, 계좌번호/비밀번호, 보안카드 비밀번호, 공인인증서 비밀번호 등 모든 인터넷뱅킹 접근 매체를 유출하여 공인인증서를 재발급 받은 후 타인명의 계좌로 5,000만원을 인출하였다.[1,3,6]

2005년 9월, 금융권은 이러한 침해사고를 차단하기 위해 전자금융종합보안 대책을 수립하였다. 그러나, 2006년경부터 고객이 지인이나 대부업체 등에 인터넷뱅킹용 접근매체를 제공한 것이 악용되어 이체사고가 발생하거나, 인터넷뱅킹용 비밀번호와 보안카드를 스캔한 이미지 파일을 보안이 허술한 가정 내 PC나 웹하드, 웹메일 등 인터넷 사이트에 저장하는 점 등을 노린 중국의 전문 해커에 의해 고객의 인터넷뱅킹 접근 매체 정보가 모두 유출된 후 수사 기관의 역추적을 피하기 위해 해외에서 인터넷뱅킹을 통해 국내에 사전 공모된 대포 통장으로 고객의 자금을 불법 이체하는 등의 수법을 사용하는 해외의 전문 해커에 의한 침해사고가 증가하기 시작하였다.

2.4 전자금융 보안대책의 개선 필요 사항

2005년 9월, 금융감독원은 금융권역별 주요 보안담당자와의 공동 T/F를 통해 "전자금융 종합보안대책"을 수립하여 고객 PC의 해킹방지를 위한 보안프로그램 설치 의무화, 보안카드 비밀번호 분할 사용 및 관리 강화, 보안등급에 따른 이체한도 차등화, 통합 OTP 인증 체계 운영, 정보보안 전담인력 확충 등 보안 대책을 수립하였으며, 2007년 1월 전자금융거래법 시행을 통해 전자금융 전반에 대한 보안 체계를 대폭 강화하였다. 그러나 사용자의 부주의나 실수에서 비롯한 전자금융침해사고에 대해서는 완벽히 차단하지 못하고 있으며, 침해사고 발생 후 금융권이나 감독기관에서 사고 경위 파악 및 수사기관에서 범인 추적에 어려움을 겪는 등 일부 개선 필요 사항이 나타나고 있다.

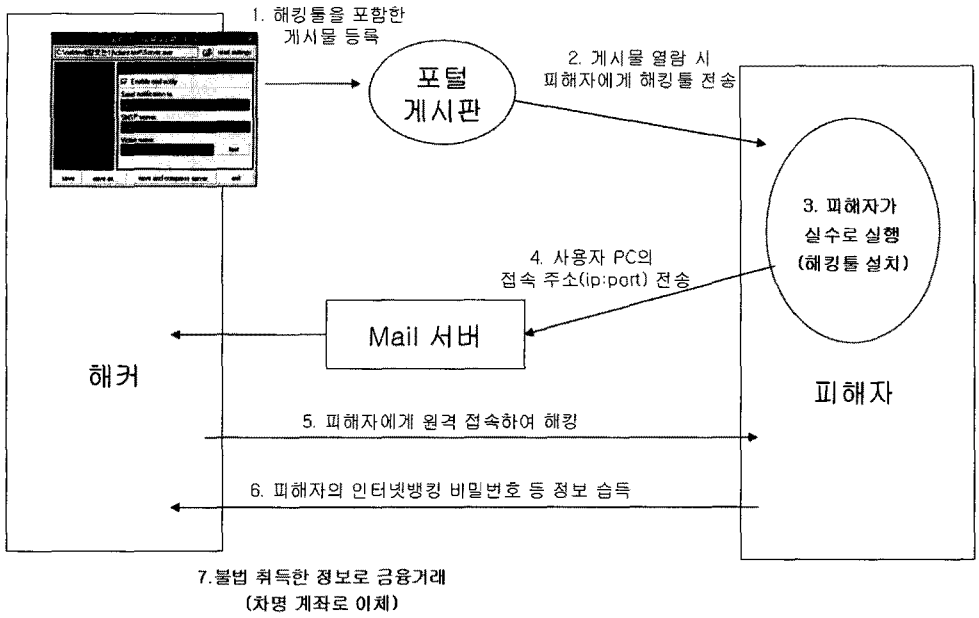
Ⅲ. 전자금융 침해사고 예방 강화 방안

인터넷뱅킹서비스 이체 사고 관련 설문 결과, 현재까지 은행권의 서버가 직접 해킹되어 일반 고객의 금전적인 손실이 발생한 사례는 전혀 없으며, 최근 발생한 고

〔표 5〕 연도별 전자금융 주요 침해 사고

연도	주요 내용
2002년	현금/신용카드 위조·복제를 통한 현금인출 사고 증가
2003년	1.25 대란(SQL-Overflow 웜에 의한 인터넷 마비로 모든 전자금융 서비스 중단 사고 발생)
2004년	텔레뱅킹 감청에 의한 비밀번호 유출 및 이체 사고 5건 발생
2005년	- 인터넷뱅킹에 대한 직접적인 해킹 최초 발생(악성프로그램을 이용하여 인터넷뱅킹 접근 매체 유출 및 5,000만원 인출)
2006년	- 안심클릭, 안전결제 비밀번호 해킹(인터넷 포탈, 쇼핑몰 등의 해킹으로 50여개의 신용카드 번호와 인터넷 결제용 비밀번호를 유출한 후 1억 8천만원 인출)
2007년	- 포털 사이트 메일함의 공인인증서 유출 후 사이버머니 구입, 계좌이체 PG 등을 이용한 환전 등으로 120여건, 3,000여만의 피해 발생 - 파밍 사이트를 통한 수백여건의 공인인증서 및 인터넷뱅킹 접근 매체 유출 사고 발생 - 악성 프로그램을 이용한 인터넷뱅킹 사용자 정보 및 접근매체 유출, 이를 이용한 인터넷뱅킹 이체 사고 발생으로 6,000여만원의 피해 발생
2008년	- 고객이 대부업자에게 인터넷뱅킹 접근 매체 정보 제공 후 예금 이체 피해 발생 - DDoS 공격을 통한 증권사 인터넷 서비스 장애 발생 - 상호저축은행의 서버 해킹을 통한 대량의 고객정보 유출사고 발생 - 개인PC해킹, 전자메일 보관함, 웹하드 등의 해킹을 통한 공인인증서를 포함한 인터넷뱅킹 접근매체 유출 및 이체 사고로 수천만원의 피해 발생

4) 키로깅은 고객 PC에서 고객이 키보드를 통해 입력하는 정보를 로깅하는 기능으로 고객이 입력하는 비밀번호를 가로채기 위해 악성프로그램에서 흔히 사용하는 기능임.



〔그림 3〕 악성 프로그램을 이용한 인터넷뱅킹 해킹 흐름도

객의 금전이 타인에게 이체되어 손실이 발생한 침해사고는 모두 고객의 직간접적인 실수 또는 부주의에 의해 전자금융 접근매체가 외부로 유출된 후 발생하였다. 그러므로 이러한 침해사고를 예방하기 위해서는 고객의 아이디/패스워드와 공인인증서, 보안카드 등의 전자금융 접근매체의 관리 강화를 통한 외부 유출 방지가 가장 중요하며, 금융권에서도 이를 위해 대고객에 대한 주의 홍보 강화와 함께 전자금융 접근 매체의 안전한 사용을 위한 능동적인 방안 제시 등 더욱 적극적인 대고객 정보보안 강화 활동이 추진되어야 한다.

3.1 전자금융 접근 매체의 구성

전자금융 거래를 위한 접근 매체, 즉 사용자와 거래에 대한 인증 요소는 기본적으로 사용자가 사전에 상대 금융기관에 설정한 비밀번호 즉, "what you know" 요소를 근간으로 하고 있으며, 보안 강화를 위해 "what you have" 요소로서 공인인증서와 보안카드 또는 OTP 사용을 주요 거래에 대해 의무화하고 있다.

3.2 고객의 비밀번호 관리 강화

전자금융에 사용되는 각종 비밀번호는 보안상 가장 중요한 요소로서 사용자가 최초 설정 시 복잡도 증가, 외부 유출 방지를 위한 노력이 필수적이며, 금융기관에서도 인증 정보 DB의 암호화 강화 등을 통해 내부 직원이나 외부 해킹에 의한 침해 사고 발생 시에도 절대 유출되지 않도록 보안을 강화하여야 한다.

3.2.1 비밀번호 안전성 검증 결과

금융기관의 사용자 인증 DB에서 관리하는 사용자 비밀번호나 사용자가 직접 관리하는 공인인증서의 비밀번호는 각각 전자금융감독규정[5]이나 [PKCS #5, Password-Based Encryption] 의 표준에 의해 역함수가 없는 MD5, SHA1 등의 Hash 함수를 근간으로 암호화 후 저장하므로 인증 DB 정보나 공인인증서 파일이 유출되더라도 안전한 것으로 판단하기 쉽다.

특히, 사용자의 공인인증서는 외부로 유출되더라도 접근 암호를 모르면 사용이 불가능 하므로 일반 고객의 경우 공인인증서 파일이 외부에 유출되더라도 보안 문제가 전혀 없는 것으로 판단하고 사후 관리에 소홀하기

5) 전자금융감독규정 세칙 제 28조(이용자 비밀번호 관리) 1항 해설서
원장비밀번호, 현금카드 비밀번호 등과 같은 중요 이용자 비밀번호의 암호화 방법은 해쉬 함수를 이용하고, 정보처리시스템에 저장하여 금융회사 업무담당자도 조회가 불가능하도록 운영.

〔표 6〕 전자금융 사용자 및 거래 인증 요소 분류

분류	인증요소
what you know	홈페이지 로그온 비밀번호, 계좌 비밀번호, 이체 비밀번호 및 공인인증서의 접근 암호
what you have	공인인증서 파일, 보안카드 또는 OTP

※ 일부 금융기관에서만 제공하는 SMS(Short Message Service), 생체인증, ACS(Auto Calling System) 등의 부가적인 인증수단은 생략함

〔표 7〕 전자금융 종합보안대책 주요 내용과 개선 필요 사항

분류	주요 내용	개선 필요 사항
영업점 창구 직원의 고객 인증 강화	행정안전부가 정부기관에 제공하는 사진 또는 지문에 의한 위조 확인서비스를 금융회사에서도 이용할 수 있도록 제공	정부 부처 간 협조 미흡 및 정책, 기술적인 문제로 추진되지 못하고 있으며, 이로 인해 위변조한 신분증을 사용한 대포통장 개설 등 금융사기 예방 어려움
공인인증서 보관방법 및 재발급 체계 개선	공인인증서를 HSM[6] 에 저장하여 사용 권장 및 공인인증서 재발급 시 보안카드 S/N 중 3자리 인증 추가	HSM에 대한 고객 인식 저하와 금융권간 호환성 불가로 사용률이 낮으며, 고객의 인터넷뱅킹 접근 매체와 보안카드가 함께 유출될 경우 공인인증서 재발급이 가능함
일회용 비밀번호 보안 강화	보안카드 비밀번호 분할 사용으로 유효 번호 확대	장기적인 키로깅을 통한 보안카드 비밀번호 수집 또는 고객의 관리 소홀로 인한 보안카드 전체 유출 시 대응 불가
인터넷뱅킹 고객 PC용 보안 프로그램 설치 강화	백신 프로그램 제공 의무화	알려지지 않은 신종 또는 변종 악성 프로그램 대응 불가
키보드 보안프로그램 기능 개선	키보드 포트 폴링, 메모리 해킹 등 신종 해킹 기법 차단 어려움	
PC 방화벽 제공 의무화	해킹툴에 의한 보안 프로그램 강제 종료 대응 어려움 및 인터넷뱅킹 종료 후 고객 정보 유출 차단 불가	
휴대폰 SMS 통지 강화	이체 거래, 공인인증서 발급, 중요 개인정보 변경 시 고객의 휴대폰으로 SMS 통지 강화	고객의 휴대폰 번호가 변경되어 금융회사 원장에 등록된 번호와 맞지 않거나, 해커에 의해 수신 번호가 착신 전환 된 경우 실제 고객이 SMS 수신 불가함
기타	-	인터넷을 통한 전자금융 침해사고 발생 시 역추적을 위한 금융기관 간 공동 대응 체계 없음

쉽다. 그러나 모든 비밀번호는 복잡도가 낮은 경우 전수대입기법[Brute force attack]에 의해 유출될 가능성이 아주 높다.

예를 들어, 공인인증서의 암호는 숫자와 특수문자, 대소문자를 구분하는 영문을 포함하여 8자리 이상을 사용할 수 있으나, 보통 사용자의 경우 숫자와 소문자로 조합된 8자리만을 사용한다. 이때 공인인증서의 비밀번호를 역으로 풀어내기 위해서는 가장 간단한 방법으로서 전체 모든 경우의 수를 대입해보면 되므로, 36개 문자의 8승인 2,821,109,907,456 번의 반복 대입이 필요하다. 이는 일반인의 경우 상상하기도 힘든 큰 수이므로 그 해독이 불가능하다고 생각될 수 있다.

그러나, 최근 출시되는 보급형 데스크탑 PC(Intel 2.66 Ghz Duo CPU 탑재)에서 검증 결과, 비밀번호 보안에 사용되는 대표적인 함수인 MD5 Hash 연산[7] 수행 시 1천만번의 반복 연산에 약 2.8초 밖에 소요되지 않아 초당 3,571,428.6 번의 연산이 가능했으며, 이는 모든 경우의 수를 단순 반복 대입 연산으로 수행 시 전체 789,911 초, 즉 약 219 시간 밖에 소요되지 않는 것을 의미한다.

그러므로 전문적인 해커에 의해 좀 더 고사양의 PC를 사용하거나, 여러 대의 PC 또는 다수의 고사양 CPU가 내장된 서버나 암호화 가속기 등의 전용 장비를 사용하는 경우 일반적인 공인인증서 파일은 유출 시 비밀번호 해독 및 악용이 대부분 가능할 것으로 판단할 수 있다.

6) HSM(Hardware Security Module) 은 고객용 공인인증서를 안전하게 저장하기 위한 IC칩 기반의 스마트카드나 USB 등의 휴대용 저장장치를 의미함.

7) 본 검증에서는 128 Bit MD5 DIGEST 연산을 암호화 성능 검증의 기준으로 하였음.

```
#define LOOP_COUNT 10000000 // 반복 횟수(1천만번)

void HashPerformanceTest(void)
{
   unsigned char plain[BUF_SIZE]= "0123456789abcde"; /* 15 Bytes 평문값 */
   unsigned char hashed[MD5_DIGEST_LENGTH+1];
   unsigned char hashencoded[BUF_SIZE];
   unsigned long i, st, et;

   st=IS_GetMilliTick(); // 현재 시각 정보를 구하는 함수 호출
   for ( i=1; i<=LOOP_COUNT; i++ )
   {
            // MD5 연산을 수행하는 Hash 함수 호출
            IS_MD5((unsigned char*)plain, strlen(plain), hashed );
   }
   et=IS_GetMilliTick(); // 현재 시각 정보를 구하는 함수 호출

   printf( "HASH Performance Test Results, Elapsed Time : %u ms \n", et-st );
   IS_Hex_Encode(hashencoded, hashed, MD5_DIGEST_LENGTH); // 16진수 변환
   printf("HASH Value of [%s] is [%s] \n", plain, hashencoded );
}

void main(void)
{
   int i;
   for(i=0; i<5; i++) // 5회 반복
            HashPerformanceTest();
```

3.2.2 비밀번호 설정 시 안전성 강화 방안

사용자가 설정하는 비밀번호는 모두 Hash나 대칭키 방식의 암호화를 수행하여 관리하더라도 비밀번호에 사용되는 문자가 단순하거나 자릿수가 짧은 경우, 암호화 로직과 암호화된 정보가 함께 노출되면 암호화키 값이 유출되지 않더라도 무차별 전수 대입 공격(Brute force attack)에 취약하게 된다.

예를 들어, 보급형 PC에서 비밀번호 검증에 소요되는 시간을 기준으로 한 반복 테스트 결과, 숫자와 소문자(또는 대문자)만을 사용할 경우 전체 비밀번호로 사용 가능한 문자수는 36자리이며, 이를 조합하여 8자리의 비밀번호를 생성할 시 2,821,109,907,456 개의 전체 경우의 수가 발생할 수 있으며, 그 해독에는 약 9일 밖에 소요되지 않는다. (Case1)

그러나, 비밀번호 생성 시 대소문자와 일반 키보드에서 입력 가능한 33개의 특수문자를 함께 조합하여 사용하는 경우(Case4) 동일한 8자리 비밀번호를 생성하더라도 전체 경우의 수는 6,634,204,312,890,620 개가 가능하며, 전체 해독에는 약 21,500 일이 소요되므로 Case1 대비 보안 강도는 2,351.63% 증가하게 되며, 단순히 숫자와 소문자만을 사용하더라도 비밀번호를 10

```
선택 "C:₩_SHField₩_SHFieldSecTest₩BASIC 함수 테스트₩Release₩stdtest.exe"
HASH Performance Test Results, Elapsed Time : 2781 ms
HASH Value of [0123456789abcde] is [32A120CC6C02E2BE926B4C785C440CD8]
HASH Performance Test Results, Elapsed Time : 2813 ms
HASH Value of [0123456789abcde] is [32A120CC6C02E2BE926B4C785C440CD8]
HASH Performance Test Results, Elapsed Time : 2797 ms
HASH Value of [0123456789abcde] is [32A120CC6C02E2BE926B4C785C440CD8]
HASH Performance Test Results, Elapsed Time : 2797 ms
HASH Value of [0123456789abcde] is [32A120CC6C02E2BE926B4C785C440CD8]
Press any key to continue
```

[그림 4] Hash 함수 연산 성능 검증 결과

〔표 8〕 비밀번호 문자 조합에 따른 암호화 비도 증감율

분류	숫자	소문자	대문자	특수 문자	전체 문자수	전체 경우의 수 (8자리 기준)	소요시간 (초)	소요시간 (일)
Case1	10	26			36	2,821,109,907,456	789,911	9
Case2	10	26	26		62	218,340,105,584,896	61,135,230	708
증감율					172%	7740%	7740%	
Case3	10	26		33	69	513,798,374,428,641	143,863,545	1,665
증감율					192%	18213%	18213%	
Case4	10	26	26	33	95	6,634,204,312,890,620	1,857,577,208	21,500
증감율					264%	235163%	235163%	

- 증감율은 각각 Case1 을 기준으로 함
- 비밀번호 자릿수는 모두 8자리를 기준으로 함

〔표 9〕 숫자와 소문자로 10자리의 비밀번호를 사용할 경우 암호화 비도

분류	숫자	소문자	문자수 합계	10자리 경우의 수	전체 소요시간(초)	전체소요시간(일)
Case5	10	26	36	3,656,158,440,062,980	1,023,724,363	11,849

자리의 문자로 사용할 경우(Case 5) 전체 해독에 약 11,849일이 소요되므로 일반적인 전자금융거래용 비밀번호 설정 시에는 실용적으로 적절한 안전성을 가지는 것으로 분석되어 사용자에게 적극 권고될 수 있다.

3.2.3 금융기관 인증 DB의 보안 강화

인터넷 홈페이지 로그온 비밀번호나 계좌비밀번호, 이체 비밀번호, 무매체 거래 전용 비밀번호 등 다양한 사용자 인증용 비밀번호는 전자금융감독규정에 따라 금융기관의 인증 DB에서 직접 Hash를 기반으로 한 암호화를 수행하여 복호화가 불가능하도록 변환 후 저장 관리하여야 한다. 그리고 일반계좌의 비밀번호나 폰뱅킹, 모바일뱅킹 등에서 사용되는 이체 비밀번호, CD/ATM (자동화기기)에서 사용되는 무매체 거래 전용 비밀번호 등은 사용할 수 있는 전자금융 접근 채널의 특성에 의해 숫자만 사용 가능 하거나 자릿수가 4~8자리 이내로 제한되며, 다양한 문자 조합을 통한 복잡한 비밀번호 설정이 가능한 인터넷 홈페이지의 사용자 로그온 비밀번호 또한 일반 사용자가 모두 보안 강도가 높은 비밀번호를 사용한다고 보장할 수 없다.

그러므로 금융기관의 사용자 인증 DB는 단순히 각각의 비밀번호를 암호화하여 저장하는 것만으로는 외부 유출 시 충분히 안전하다고 평가할 수 없기 때문에, 금융기관에서는 사용자가 비밀번호 최초 설정 또는 변경 시 가능한 복잡도가 높은 비밀번호의 사용을 권고 또는 강제화를 하여야 하며, 이와 함께 내부적으로도 사용자 인증 DBMS에 대하여 추가적인 서버, DB보안 체계와 감사 체계의 구축을 의무화하여 강력한 접근제어 정책과 주기적인 감사 활동을 수행하여 대량의 고객 인증 정보 유출에 의한 대형 금융사고의 발생을 사전에 예방하여야 한다.

3.3 사용자 공인 인증서의 보안 강화

공인인증서는 전자서명법에 의해 전자금융거래에서 사용자와 서버의 인증 수단 제공 및 전자서명을 통한 부인방지 기능을 제공하는 대표적인 전자금융 접근매체이다. 그러나 최근 발생한 전자금융 침해사고에서 사용된 공인인증서는 대부분 사용자의 직/간접적인 관리 소홀로 인해 다음의 3가지 방법에 의해 유출되거나 재발급 되어 악용이 가능한 것으로 조사되었다.

1. 사용자 PC가 악성프로그램에 감염되어 PC에 저장된 공인인증서 파일과 비밀번호 유출
2. 사용자가 웹메일, 웹하드 등에 저장한 공인인증서 파일이 웹사이트 해킹에 의해 유출
3. 사용자의 인터넷뱅킹 비밀번호, 보안카드 등이 모두 유출된 후 해커에 의해 재발급

그러므로, 전자금융 침해사고를 예방하기 위해서는

〔표 10〕 금융기관 홈페이지 로그인 방식 현황표

홈페이지 로그인 방식	금융 기관	계
공인인증서	은행[14], 중앙회[3], 증권[2], 보험[2], 상호저축은행[18], 기타[2]	41
ID+PWD+공인인증서	증권[24], 중개[2], 선물[5], 기타[1]	32
주민등록번호+공인인증서	보험[23], 카드[5]	28
ID+공인인증서	증권[2], 선물[1]	3
주민등록번호+성명+공인인증서	보험[1]	1
합 계		105

공인인증서를 포함한 전자금융 접근매체 전체에 대한 사용자의 보안 의식 제고가 가장 중요하며, 금융기관 또한 전자금융 접근매체의 더욱 안전한 관리 방법 제공 등 대고객 정보보안 강화 활동을 강화하여야 한다.

3.3.1 공인인증서의 사용 현황과 중요성

2007년 4월 금융보안연구원의 금융 정보보호 기술세미나 발표 자료에 따르면, 국내 금융기관에서 인터넷 홈페이지 로그인 방식으로 공인인증서만을 사용하는 곳이 41개 기관으로 가장 많으며, 그 다음으로 접속 ID 및 패스워드와 함께 공인인증서를 사용하는 곳이 32개 기관, 주민등록번호와 공인인증서를 함께 사용하는 곳이 28개 기관 등의 순으로 나타났다.[4]

공인인증서는 전자서명법에 의해 발급, 갱신, 폐기 등의 운용 과정이 아주 엄격히 관리되고 있으며, 전자금융거래법에 의해 인터넷뱅킹 뿐만 아니라 온라인 주식거래, 쇼핑몰을 통한 지불결제 등 모든 전자금융거래에 사용이 의무화되어 있으므로 활용 범위의 확대와 함께 보안상의 중요도도 더욱 증가하고 있다.[8)]

3.3.2 공인인증서 비밀번호 설정 안전성 강화 방안

일반 사용자의 경우 공인인증서의 비밀번호를 홈페이지 로그온 비밀번호나 계좌비밀번호, 전화번호 등 개인정보를 적절히 조합하여 사용하는 경우가 많으므로 공인인증서 파일이 유출되어 인증서 비밀번호가 해독된 경우 사용자의 다른 비밀번호까지 유출될 확률이 그만큼 높아지게 된다.

또한 일반적인 사용자의 경우 영어나 한글사전에 있는 단어를 조합하여 암호를 만드는 경향이 있으므로 Dictionary Attack 등 좀 더 효율적인 암호 해독 방법을 적용할 경우 더욱 효과적으로 공인인증서 비밀번호를 알아낼 수 있을 것으로 추정할 수 있다.

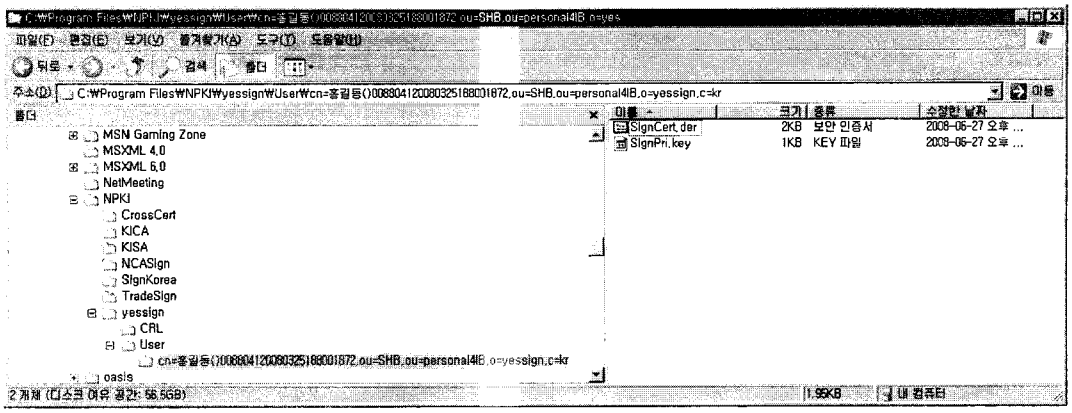
그러므로 공인인증서의 비밀번호는 사용자의 개인정보나 전자금융거래용 비밀번호와는 무관한 값을 반드시 사용하여야 하며, 일반 사전에는 없는 단어를 조합하는 것이 좋으며, 특히 단순 반복 연산에 의한 유출을 방지하기 위해서는 특수문자 및 대소문자를 함께 혼용하고 비밀번호의 자릿수도 8자리 이상, 최대한 늘릴 것을 사용자에게 권장하여야 한다.

예를 들어 일반 키보드의 경우, 숫자 10개와 33개의 특수문자, 대소문자 52개 사용 시 전체 95개의 문자가 사용 가능하므로 비밀번호가 8자리일 경우, 95개의 8승인 6,634,204,312,890,620 개의 조합이 가능하다. 이는 동일한 8자리 비밀번호를 사용함에도 불구하고, 숫자 및 소문자(또는 대문자)만으로 구성될 때와 비교했을 때 전체 경우의 수인 2,821,109,907,456 보다 보안강도가 약 2,352배 강력해져, 일반 PC에서 MD5 Hash 기반 전수 반복 대입으로 해독 시도 시 약 21,500일이 소요된다. 그러므로 개인 사용자의 공인인증서 유효기간이 1년으로 제한되는 점을 고려하면 이는 적정한 수준의 안전성을 확보하는 것으로 판단할 수 있다.

3.3.3 공인인증서 저장 매체 보안 강화

일반 사용자 PC의 하드디스크에 저장되는 사용자용 공인인증서 파일은 NPKI(National Public Key Infrasucture, 국가 공개키 기반구조) 표준 규격에 의해 저장되는 위치가 고정되어 있으므로, 사용자 PC가 악성 프

8) 전자금융 감독규정 제3장 전자금융거래의 안전성 확보 및 이용자 보호
제7조(공인인증서 사용기준) 모든 전자금융거래에 있어 「전자서명법」에 의한 공인인증서를 사용하여야 한다. 다만 기술적·제도적으로 공인인증서 적용이 곤란한 전자금융거래로 감독원장이 정하는 경우에는 그러하지 아니하다.



〔그림 5〕 사용자 PC에 저장된 공인인증서

로그램에 감염될 경우 쉽게 외부로 유출이 가능하므로, 보안 강화를 위해 USB 메모리를 비롯한 이동형 저장장치의 사용이 일반적으로 권장된다.

그러나, 일반적인 휴대용 USB 저장장치는 하드웨어적인 암호화 장치나 접근 통제 기능이 없으므로, USB 저장장치를 PC에 연결하고 있는 순간에는 일반 하드디스크에 공인인증서를 저장한 것과 동일한 취약점이 발생하므로 악성프로그램에 의해 공인인증서의 유출이 가능하다. 그러므로, 하드웨어적인 암호화 장치(HSM)가 내장된 USB 방식의 보안토큰이나 IC칩 기반의 스마트카드를 사용하여 공인인증서를 저장하는 것이 일반 사용자 입장에서 현실적으로 사용 가능한 가장 안전한 공인인증서 저장 방법으로 권장 되어야 한다.

3.3.4 공인인증서 사용 시 주의 및 인증서 관리 프로그램 개선 방안

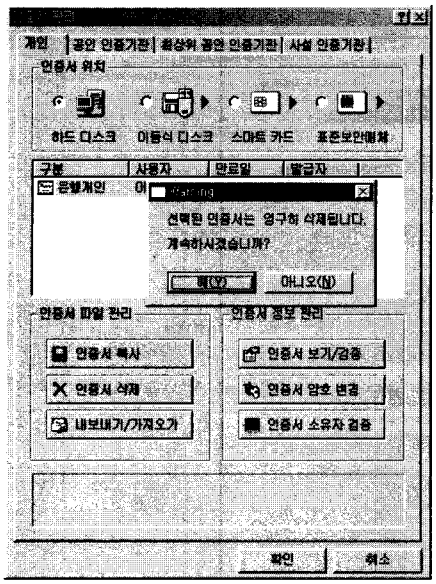
최근 발생한 전자금융 침해사고의 원인 분석 결과, 다수의 사용자가 공인인증서와 비밀번호를 가족과 함께 사용하거나 이동 중에도 사용하기 위하여 자신의 메일함이나 웹상의 개인 자료실 등 인터넷 사이트에 보관하면서 필요할 때마다 PC로 다운로드 받아 사용하고 있었다.

사용자가 인터넷상에 보관 중이던 공인인증서와 비밀번호 저장 파일 등이 웹사이트 해킹에 의해 유출되어 전자금융 침해사고가 발생한 경우는 인터넷뱅킹 이체사고가 발생하여 고객이 금전적 손실을 입더라도 전자금융거래법에서 사용자가 보호받지 못하는 중과실의 사유[9]에 해당될 수 있으므로 고객이 입은 손실을 금융기관으로부터 보장 받기가 어려워진다.

또한, 고객이 이동 중 임시로 사용한 PC에는 사용자가 저장한 공인인증서 파일이 그대로 남아 있게 되며, 사용자가 인증서 관리 프로그램을 통해 삭제하여도 인터넷상에서 일반적으로 구할 수 있는 파일 복구 유틸리티로 재생되어 제 3자에게 유출될 수 있다.

그러므로 사용자는 자신의 공인인증서 파일과 비밀번호를 절대 외부 인터넷사이트에 저장해서는 안 되며, 공인인증서를 집과 회사, 또는 가족 간 함께 사용하는 경우 등 사용하는 장소가 일정하지 않거나 다수가 함께 불가피하게 사용하여야 하는 경우에는 휴대용 HSM 기반의 저장매체 사용 등 더욱 인증서 보안 관리에 주의하여야 한다. 또한 금융기관에서도 이러한 보안 방법에 대한 대고객 홍보와 함께 공인인증서 관리 프로그램의 개선을 통해 한번 삭제된 공인인증서 파일은 절대 다시 복구될 수 없도록 하여야 하며, 영업점 내 일반 고객에게 제공하는 네비게이터용 PC는 주기적으로 공인인증서 저장 및 복구 가능 여부 등을 점검하여 고객의 공인

9) 전자금융 거래법
제9조(금융기관 또는 전자금융업자의 책임) ①금융기관 또는 전자금융업자는 접근매체의 위조나 변조로 발생한 사고, 계약체결 또는 거래지시의 전자적 전송이나 처리과정에서 발생한 사고로 인하여 이용자에게 손해가 발생한 경우에는 그 손해를 배상할 책임을 진다.
②제1항의 규정에 불구하고 금융기관 또는 전자금융업자는 다음 각 호의 어느 하나에 해당하는 경우에는 그 책임의 전부 또는 일부를 이용자가 부담하게 할 수 있다.
1. 사고 발생에 있어서 이용자의 고의나 중대한 과실이 있는 경우로서 그 책임의 전부 또는 일부를 이용자의 부담으로 할 수 있다는 취지의 약정을 미리 이용자와 체결한 경우 (이하 생략)



〈그림 6〉 인증서 관리 프로그램에서 사용자 PC에 저장된 인증서 삭제 화면

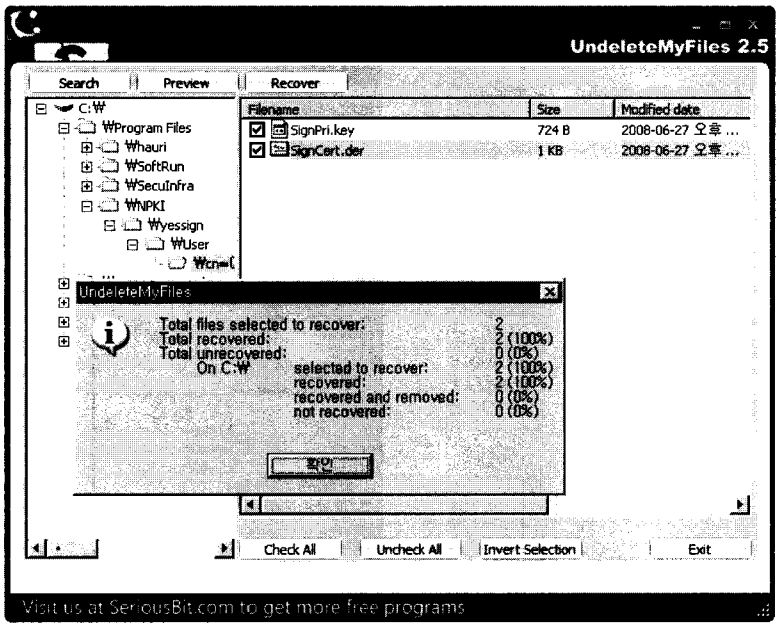
인증서 파일이 외부로 유출되지 않도록 하여야 한다.

그러므로 사용자는 자신의 공인증서 파일과 비밀번호를 절대 외부 인터넷사이트에 저장해서는 안 되며, 공인인증서를 집과 회사, 또는 가족 간 함께 사용하는 경우 등 사용하는 장소가 일정하지 않거나 다수가 함께 불가피하게 사용하여야 하는 경우에는 휴대용 HSM 기반의 저장매체 사용 등 더욱 인증서 보안 관리에 주의하여야 한다. 또한 금융기관에서도 이러한 보안 방법에 대한 대고객 홍보와 함께 공인인증서 관리 프로그램의 개선을 통해 한번 삭제된 공인인증서 파일은 절대 다시 복구될 수 없도록 하여야 하며, 영업점 내 일반 고객에게 제공하는 네비게이터용 PC는 주기적으로 공인인증서 저장 및 복구 가능 여부 등을 점검하여 고객의 공인인증서 파일이 외부로 유출되지 않도록 하여야 한다.

3.4 전자금융 접근 매체의 관리 강화와 OTP 사용 권장

공인인증서를 HSM 기기에 보관하여 사용하는 경우 인터넷뱅킹 거래 시 보안 1등급으로 분류되어 이체 금액 한도 확대 등의 혜택을 부여하고 있다. 하지만 사용자의 인터넷뱅킹 비밀번호, 보안카드 등이 모두 유출될 경우 공인인증서를 신규로 재발급 받아 악용하는 편법이 가능하므로 반드시 추가적인 보안 대책이 필요하다.

인터넷뱅킹에서 사용되는 계좌비밀번호나 이체비밀번호는 사용자의 휴대폰 번호나 주소 등의 개인정보나, 휴대폰 비밀번호 및 일반 인터넷 포털, 메일 시스템 등에 접속할 때 사용하는 비밀번호와 다르게 설정하여야 사용자의 개인정보가 일부 노출되더라도 안전성을 보장



〔그림 7〕 파일 복구 유틸리티를 통한 공인 인증서 파일 복구 화면

받을 수 있다.

또한, 보안카드의 일련번호와 시리얼번호는 계좌 이체 및 보안카드 재발급 시에 사용되는 가장 중요한 값임에도 불구하고, 사용자가 사용상의 편의나 가족 간 공유 등을 위해 스캔 파일 또는 타이핑을 쳐서 텍스트 파일로 만들어 PC나 웹 메일, 웹하드 등에 저장하여 사용 중 웹사이트 해킹에 의해 모두 유출되어 공인인증서 재발급을 통한 이체사고가 발생한 사례가 있었다.

그러므로, 금융권에서는 인터넷뱅킹 거래 시 보안 1등급으로 인정받을 수 있는 전용 OTP(One Time Pad)의 사용을 안전한 전자금융 거래 인증 방법으로 적극 권장하여야 하며, 아주 부득이하게 보안카드를 공유하여 사용하여야 하는 경우에도 일반 복사기를 통한 종이로의 복사를 사용하도록 주의 깊게 안내하고 반드시 보안카드의 재발급 및 이체 거래 시 사용자의 휴대폰 문자메시지(SMS)로 통보 받을 수 있게 유효한 휴대폰 번호를 등록하도록 함께 권고하여야 한다.

Ⅳ. 전자금융 침해사고 대응 강화 방안

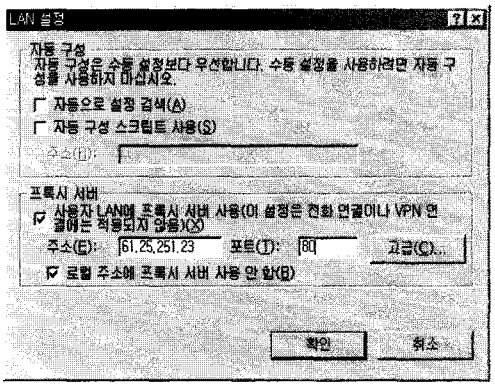
사용자가 전자금융 접근 매체를 안전하게 관리하여 유출을 차단하고, 금융기관의 서버가 해킹당하지만 않는다면 전자금융 침해사고는 발생하지 않을 것이다. 하지만 전자금융의 보편화에 따라 모든 고객이 안전하게 전자금융 접근 매체를 관리한다고 보장할 수 없다.

본 장에서는 금융기관 관점에서 유출된 고객 정보를 악용한 해커의 전자금융 접속, 이체 사고 차단 및 신속한 범인 검거 등을 위한 전자금융 침해사고 대응 방안으로서 가장 효과적인 전자금융 거래 로깅 및 역추적 시스템의 구축 및 금융기관 간 침해사고 정보 공유를 통한 공동 대응 체계의 구축 및 운영 방안을 제안한다.

4.1 검토 배경

2007년 1월 전자금융거래법이 시행됨에 따라 모든 전자금융 사고에 대해 고객의 민원이나 수사기관의 요청 시 금융기관은 신속하게 접속 내역 조회, 고객의 중과실 여부 확인 및 입증 등의 책임이 대폭 강화되었다.[10]

그러므로 금융기관은 고객의 인터넷뱅킹 접속매체 정보 유출에 따른 인터넷뱅킹을 통한 자금이체, PG사를 통한 지불결제 등 인터넷을 통한 모든 전자금융 침해사고와 관련하여 고객 민원이나 감독기관, 수사기관



〔그림 8〕 웹브라우저에서 Proxy 서버 설정 화면

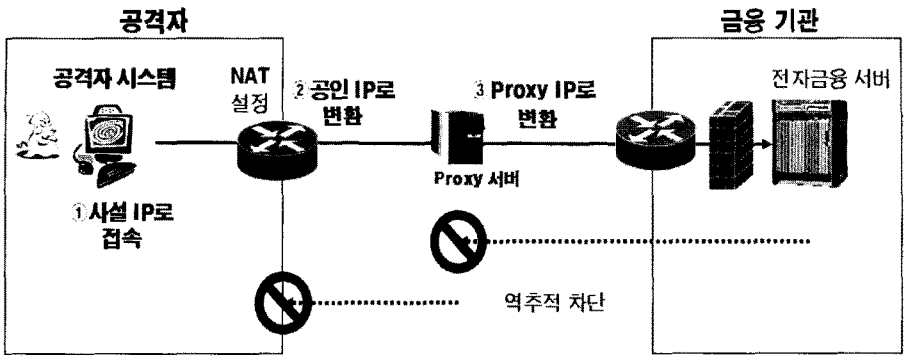
등의 사고 조사 요청 시 사고와 관련된 모든 접속 내역을 역추적하여 사고 원인 파악 및 범인 검거에 협조, 추가적인 피해 방지를 위한 대응 방안 수립 등의 침해사고 대응 활동을 수행하여야 한다.

4.2. 전자금융 침해사고의 대응 현황 및 문제점

전자금융 거래 로깅 및 접속경로 역추적 시스템을 구축하여 운영중인 A은행에서, 민원이 접수된 전자금융 침해사고의 접속 경로를 분석한 결과, 대부분 중국 IP 대역에서 자체 사설 IP를 사용하며 IP공유기나 라우터 등의 통신 장비에서 공인 IP로 NAT(Network Address Translation)에 의해 변형되거나, 해외 사용자에게도 국내 접속 IP 대역을 제공하는 VPN 기반 Proxy 서버를 경유하여 인터넷뱅킹 서버에 접속하고 있었다.

그러므로 [그림 9]과 같이 일반적인 금융기관의 웹서버에서 로깅하는 사용자의 공인 IP로는 Proxy 서버나 NAT 장비를 경유한 경우 실제 접속자의 공인 IP, 사설 IP 및 시스템 정보를 직접 확인할 수 없으므로, 접속자

10) 전자금융거래법 관련 주요내용을 요약하면 다음과 같다.
접근매체 위변조, 해킹 등 사고시 배상 책임, 무과실 입증책임 (9조)
- 계약체결 또는 거래지시의 전자적 전송이나 처리과정에 발생한 사고
- 해킹, 피싱(파밍), 전산 장애 등의 배상 책임 강화
→ 이용자의 고의, 중과실을 입증하지 못하는 경우 금융기관의 손해배상 책임 부담 강화
접근매체 분실, 도난으로 인한 사고 시 배상 강화 (10조)
고객의 손해배상 등 분쟁 시 15일 이내 조사, 처리결과 통보 의무화 (14조)



〔그림 9〕 일반적인 사용자 공인 IP 정보를 통한 역추적 체계

의 신원 확인을 위한 접속 경로의 신속한 역추적이 어려울 뿐만 아니라, 공격자가 접속하는 공인 IP를 매번 변경할 경우 유사 사고를 막기 위한 접속 경로 차단 방안 수립 등 효과적인 침해사고 대응이 불가능한 문제점이 발생한다.

4.3 전자금융 거래 로깅 확대 시스템 구축 현황 및 한계점

인터넷을 통한 전자금융 침해사고 발생 시 일반적인 인터넷 접속 로그에 기록된 공인 IP 만으로는 역추적에 근본적인 한계가 있으므로, 금융감독원의 권고안[11]에 따라 주요 금융기관에서는 자체적으로 전자금융 접속자의 식별 정보 로깅 범위를 확대하고 있다.

인터넷뱅킹 접속자에 대한 식별 정보 로깅 강화와 관련하여 각 은행의 관련 업무 담당자를 대상으로 설문조사를 통한 현황 파악 결과는 다음과 같다.

- 설문 기간 : 2008.7.15 ~ 2008.8.6
- 설문 대상 : 시중 15개 은행 정보보안 담당자
- 설문 방법 : email을 통한 설문조사 및 전화 인터뷰

인터넷뱅킹 서비스 이체 사고 관련 설문 조사 결과, 응답 대상 15개 은행 중 7개 은행에서 인터넷뱅킹 접속에 대한 접속자 식별 강화를 위한 확대 로깅 체계가 이미 구축되어 운영 중이었다. 그러나 활용된 사례에 대한 조사 결과, 실제 인터넷뱅킹을 통한 불법 자금이체 등의 침해사고가 발생한 경우에도 단순히 접속한 사용자의 IP, MAC(랜카드주소) 정보 확인 수단으로만 참조되어 접속 국가의 식별과 정상 접속과 비인가 접속을 구분하는 등의 제한적인 용도로만 활용되었다.

또한, 금융기관 간 침해사고 공동 대응을 위한 사고정보 공유 체계는 아직 구축되어 있지 않아 기구축된

〔표 11〕 인터넷 뱅킹 접속자 식별 및 역추적체계 관련 설문 결과

설문 사항	응답 결과	비고
1. 인터넷뱅킹 접속을 통한 계좌 정보 조회, 금전 이체 등의 침해사고 발생 시 접속자 식별을 위한 사설, 공인 IP, MAC 등의 로깅 강화 체계가 구축되어 있습니까? (O, X 답변 및 기타 의견)	구축되어 있음(7)	년내 구축 예정(5)
2. 1번 질문의 답변이 O 라면, 이체 사고와 관련된 고객의 민원이나 수사에 도움이 된 사례가 있습니까? (O, X 답변)	있음(2)	
3. 2번 질문에 대한 관련 사례나 의견을 기술해주시기 바랍니다.	- 사고 관련 접속에 대하여 정상 거래 시와 동일한 PC 사용 여부 식별이 가능하므로 정상 접속과 비인가 접속의 구분 용이했음 - 실제 접속자의 국내 또는 해외 거주 등의 국가 정보를 파악할 수 있었음	

11) 총복IT-00081, 전자금융거래 기록 추가에 대한 검토 결과 송부(2008.2.5)

확대 로깅 시스템의 활용 범위는 해당 은행 내부로 제한되는 한계가 있는 것으로 조사되었다.

4.4 효과적인 전자금융 거래 로깅 및 역추적 시스템의 구축 방안

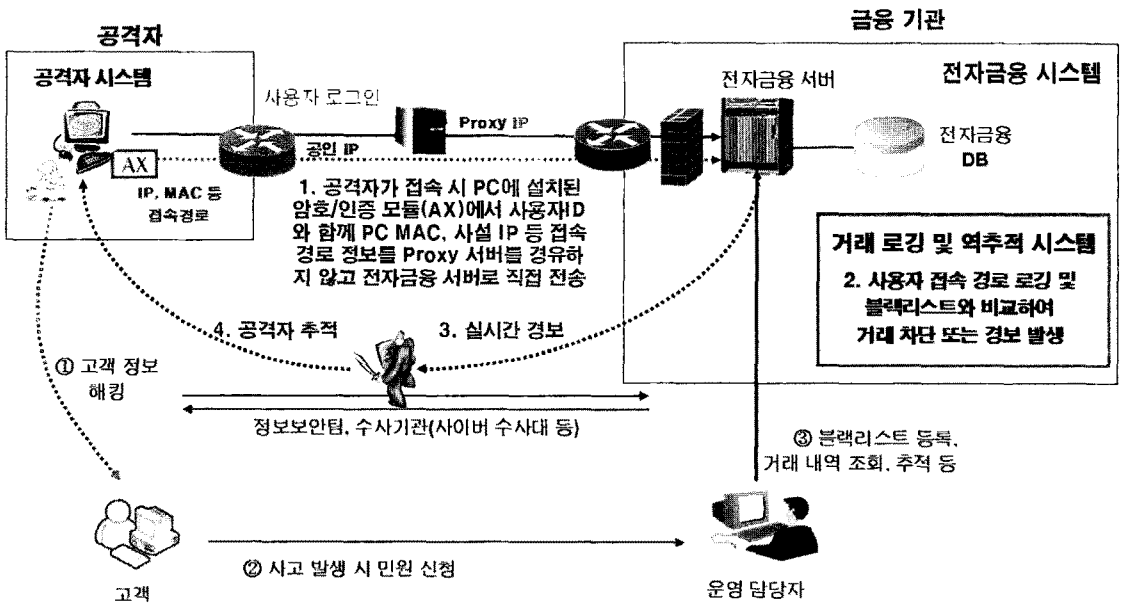
본 논문에서는 기존 전자금융 접속자 정보 확대 로깅 체계의 한계점을 해결하기 위하여 다음과 같이 전자금융 거래 로깅 및 역추적 시스템의 구축 방안과 이를 기반으로 한 금융기관 간 침해사고 공동 대응 체계를 제안한다.

전자금융 거래 로깅 및 역추적 시스템은 인터넷뱅킹, HTS(Home Trading System), 인터넷 지불결제 등 전자금융 거래 시 사용자 PC에 필수적으로 설치되는 기존 ActiveX 기반의 암호화 보안프로그램이나 사용자용 실행 프로그램을 일부 개선하여 사용자 시스템의 식별정보와 사용자 시스템의 운영체제 또는 웹브라우저에 설정된 Proxy 설정 정보를 함께 수집하여 전자금융 거래를 위해 접속하는 금융기관의 서버로 내부적으로 전송하는 기능을 추가하여 이를 금융기관의 전자금융 서버에서 기존 사용자 접속 정보와 함께 로깅한 후 침해사고 발생 시 역추적에 활용하는 체계이다.

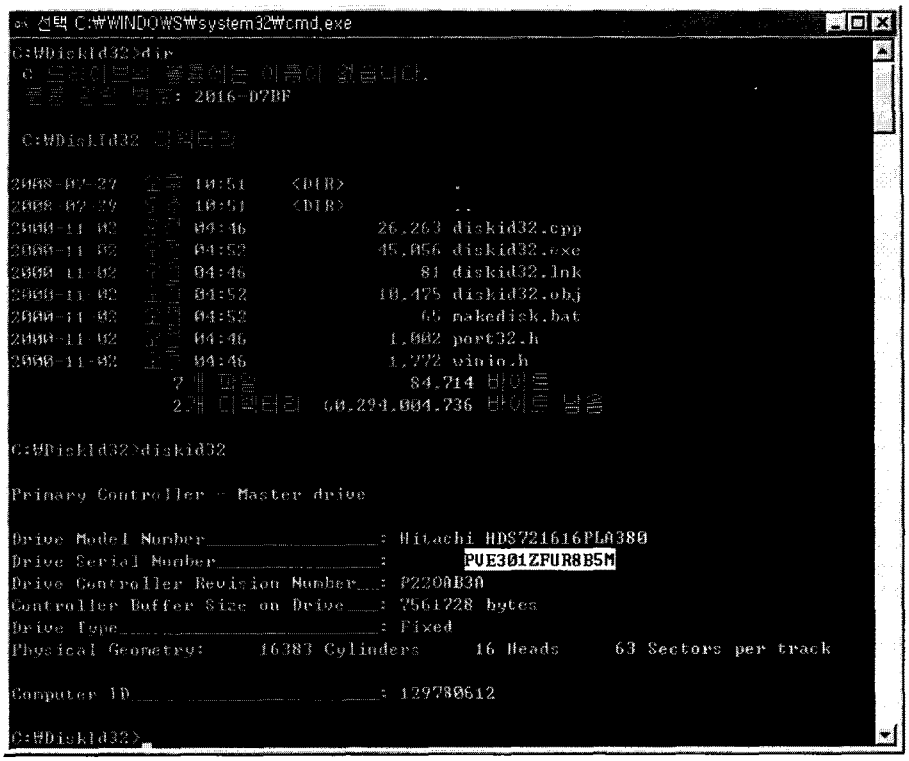
전자금융 거래 로깅 및 역추적 시스템 구축을 위한 주요 기술 요소는 다음과 같다.

1. 사용자 시스템의 정보 수집
   사용자 시스템의 식별 정보로는 사설 IP, MAC 주소(LAN 카드 고유번호) 값 외 추가로 내부 라우터 주소(Default Gateway IP Address), 하드디스크 시리얼번호, MAC 주소(LAN 카드 고유번호), 메인보드 고유번호 및 운영체제(OS)의 국가정보, 버전정보, 라이선스 번호 등이 있으며, 이러한 정보는 Microsoft에서 제공하는 MSDN(Microsoft Developer Network) 자료나 인터넷상에 공개된 소스코드 등을 응용하여 구현이 가능하다.

2. 사용자 시스템의 수집 정보 전송 및 접속 경로 로깅
   전자금융 거래 시 사용자 PC에 설치되는 SSL 암호화 및 공인인증서를 통한 인증 기능을 제공하는 ActiveX 방식의 전용 보안프로그램은 TCP 443 등의 전용 포트를 사용하며, C/S 방식의 경우 사용자용(Client) 실행 프로그램은 금융기관의 서버와 직접 소켓 통신이 가능하므로, 이를 이용하여 전자금융 거래를 위해 로그인하는 사용자의 아이디(ID)와 사용자 시스템의 식별정보 및 운영체제나 웹브라우저 상의 Proxy 설정 정보를 함께 수집한 후 사용자에 의해 설정된 Proxy 서버를 거치지 않은 채 인터넷을 통하여 직접 금융기관의 전자금융 로깅 시스템으로 식별정보를 전문 형식으로 전



〔그림 10〕 전자금융 거래 로깅 및 역추적 시스템의 기본 운영 프로세스



※ 실행 예제는 웹사이트(http : //www.codeguru.com) 에서 제공하는 공개 자료를 사용하였음

〔그림 11〕 전자금융 거래 로깅 및 역추적 시스템의 기본 운영 프로세스

송할 수 있다. 이를 통하여 금융기관의 전자금융 로깅시스템에서는 사용자의 로그인 정보와 실제 공인 IP를 포함한 접속 경로 정보 및 사용자의 시스템 정보까지 모두 로깅할 수 있다.

3. 침해정보 공유 DB(블랙리스트) 및 실시간 경보 체계 구축

전자금융 침해사고가 접수된 경우 관련된 접속 경로를 역추적하여 해당 시스템의 식별정보를 침해정보 공유 DB에 등록한 후 동일한 사용자 시스템이나 접속 경로에서 재접속 시도가 있을 때 거래를 차단하여 추가적인 피해 발생을 예방하거나, 금융기관 내 보안관제실 담당자나, 정보보안담당자 또는 외부 수사기관에 실시간 경보나 휴대폰 문자메시지(SMS) 등으로 자동통보 되도록 연동하여 범인 추적에 활용할 수 있다.

4.5. 시스템 식별정보 수집의 한계점 검토

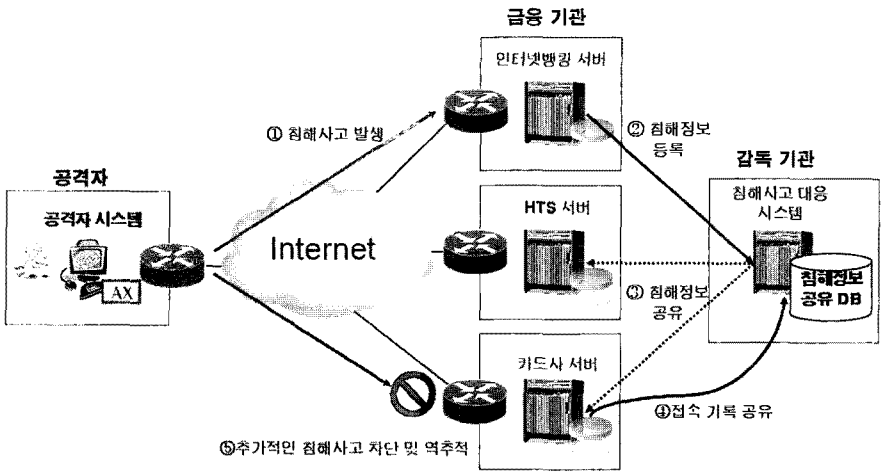
전자금융 거래 로깅 및 역추적 시스템 구축을 위한 주요 기술 요소 중 하나인 사용자 시스템의 식별정보 수집은 모두 사용자 시스템 내에서 실행되는 것이므로, 사용자가 시스템의 운영체제 정보와 전자금융 거래에 사용된 PC(하드웨어)까지 매번 변경할 경우 역추적을 할 수 없는 문제점이 있으며 이는 기술적으로 해결이 불가능한 한계점으로 판단된다.

그외 일반적인 운영체제의 설정정보나 레지스터리(Registry) 정보는 사용자가 단순한 시스템 유틸리티나 직접 조작을 통해 일부 조작이 가능[12]하므로 사용자 시스템의 식별 정보를 수집할 경우에는 사용자 시스템의 BIOS 정보나 커널 수준에서 고유정보 값을 직접 수집하여야 한다.

4.6 전자금융 거래 로깅 및 역추적 시스템의 효과와 한계

전자금융 로깅 및 역추적 시스템은 개별 금융 기관

12) 예를 들어 인터넷상에 공개된 macshift.exe 같은 유틸리티 사용 시 운영체제 메모리 상의 MAC 주소 정보나 네트워크 패킷상의 출발지 MAC 주소의 변경이 가능하다.



〔그림 12〕 침해사고 정보 공유 및 공동 대응 프로세스

내부적으로만 운영할 경우 활용 범위가 제한되므로 다음과 같은 한계점이 발생한다.

1. 타 금융기관에서 발생한 침해사고의 접속자 정보를 활용하여 자사에서 유사 사고가 발생하는 것을 사전 예방할 수 없다.
2. 자사에서 침해사고 발생 시 타 금융기관에서 보유한 동일한 사용자 시스템에서의 접속 기록을 조회하여 역추적에 활용할 수 없다.

4.7 침해사고 정보 공유 및 공동 대응 체계 구축 방안

본 논문에서는 전자금융 로깅 및 역추적 시스템을 효과적으로 활용하기 위한 방안으로, 개별 금융기관에서 관리하는 관련 로그 및 침해사고 정보를 공유할 수 있도록 침해사고 정보 공유 및 공동 대응 시스템을 감독기관 또는 감독기관이 신뢰도를 보장하는 기존 OTP 통합 인증센터와 같이 각 금융기관과 이미 전용선으로 연결된 인프라를 갖춘 곳에 신규 구축하여 금융기관 간 침해사고 정보 공유 및 공동 대응 체계를 운영하는 방안을 제안한다.

침해사고 정보 공유 및 공동 대응 체계의 구성도 및 이를 활용한 침해사고 공동 대응 프로세스의 예는 다음과 같다.

1. 공격자가 고객 PC 해킹 등을 통해 알아낸 고객정보로, 예를 들어 인터넷 뱅킹 시스템에 접속하여 불법 자금 이체 등 침해사고를 발생시킨다.
2. 금융기관은 고객 민원이나 수사기관의 신고 등을 통해 침해사고가 접수되는 경우 내부의 전자금융 로깅 및 역추적시스템에 기록된 공격자 시스템 정보와 접속 경로 등 침해 정보를 감독기관의 침해사고 대응 시스템에 즉시 전달하여 침해정보 공유 DB에 등록되도록 한다.
3. 감독 기관의 침해사고 대응 시스템은 개별 금융기관에서 접수되는 침해 사고 정보를 전체 금융기관에 신속히 통보하여 공유한다.
4. 개별 금융기관은 감독기관의 침해사고 대응 시스템으로부터 전달 받은 타사의 침해사고 정보를 자사의 침해 정보DB(블랙리스트)에 등록하고, 자사의 접속 로그 정보를 조회하여 관련 정보가 있을 경우 감독 기관에 통보하는 등 역추적에 협조한다.
5. 개별 금융기관은 동일한 공격자가 접속할 경우 자사의 침해정보 DB에 등록된 정보를 활용하여 추가적인 침해사고 예방 및 감독기관에 즉시 통보하여 범인 검거에 협조한다.

V. 침해사고 공동 대응 체계의 법률적 검토 및 대응 방안

전자금융 로깅 및 역추적 시스템과 이를 기반으로 한 침해사고 공동 대응체계는 전자금융 사용자의 시스템 정보 수집과 침해사고 발생 시 공격자 시스템의 접속정

〔표 12〕 개인정보 수집과 관련된 정보통신망 이용 촉진 및 정보보호 등에 관한 법률

조항	주요 사항	원문 내용
22조	이용자의 개인정보 수집 시 동의를 얻어야 함	① 정보통신서비스제공자는 이용자의 개인정보를 이용하려고 수집하는 때에는 다음 각 호의 모든 사항에 대하여 이용자에게 알리고 동의를 얻어야 한다. 다음 각 호의 어느 하나의 사항을 변경하려는 때에도 또한 같다. 1. 개인정보의 수집·이용 목적 2. 수집하는 개인정보의 항목 3. 개인정보의 보유 및 이용 기간 (이하 생략)
24조의 2	수집된 개인정보의 제3자 제공 시 동의를 얻어야 함	① 정보통신서비스제공자는 이용자의 개인정보를 제3자에게 제공하려는 경우 제22조제2항제2호 및 제3호의 규정에 해당하는 경우를 제외하고는 다음 각 호의 모든 사항에 대하여 이용자에게 알리고 동의를 얻어야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다. 1. 개인정보를 제공받는 자 2. 개인정보를 제공받는 자의 개인정보 이용 목적 3. 제공하는 개인정보의 항목 4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간 ② 제1항의 규정에 따라 정보통신서비스제공자로부터 이용자의 개인정보를 제공받은 자는 그 이용자의 동의가 있거나 다른 법률에 특별한 규정이 있는 경우를 제외하고는 개인정보를 제3자에게 제공하거나 제공받은 목적 외의 용도로 이용하여서는 아니 된다.

보 공유를 핵심으로 하므로 이와 관련된 정보통신망 이용 촉진 및 정보보호 등에 관한 법률, 금융실명거래 및 비밀보장에 관한 법률 등을 위반하지 않도록 구축 및 운영에 대한 사전 법적 검토가 수반되어야 한다.

5.1 정보통신망 이용 촉진 및 정보보호 등에 관한 법률 대응

사용자 시스템의 식별정보와 접속 경로의 취득을 위해서는 정보통신망 이용 촉진 및 정보보호 등에 관한 법률 제22조 및 제24조의 2에 따라 사용자의 동의를 얻어야 한다.

〔표 13〕 전자금융 거래법 제21조 및 제22조

제21조(안전성의 확보의무) ①금융기관·전자금융업자 및 전자금융보조업자(이하 "금융기관등"이라 한다)는 전자금융거래가 안전하게 처리될 수 있도록 선량한 관리자로서의 주의를 다하여야 한다.
②금융기관등은 전자금융거래의 안전성과 신뢰성을 확보할 수 있도록 전자금융거래의 종류별로 전자적 전송이나 처리를 위한 인력, 시설, 전자적 장치 등의 정보기술부문 및 전자금융업무에 관하여 금융감독위원회가 정하는 기준을 준수하여야 한다.
③금융감독위원회는 전자금융거래의 안전성과 신뢰성을 확보하기 위하여 「전자서명법」 제2조제8호의 공인인증서의 사용 등 인증방법에 대하여 필요한 기준을 정할 수 있다.

제22조(전자금융거래기록의 생성 및 보존) ①금융기관등은 전자금융거래의 내용을 추적·검색하거나 그 내용에 오류가 발생할 경우에 이를 확인하거나 정정할 수 있는 기록을 생성하여 5년의 범위 안에서 대통령령이 정하는 기간동안 보존하여야 한다.
②제1항의 규정에 따라 금융기관등이 보존하여야 하는 기록의 종류 및 보존방법은 대통령령으로 정한다.

〔표 14〕 개인정보취급 방침에 개인정보 수집 항목 명시 예시 [9,12]

개인정보의 수집 · 이용목적, 수집하는 개인정보의 항목

xxxx은 고객에게 적합한 금융서비스를 제공하기 위하여 전자금융거래법 제21조(안전성의 확보의무) 및 동법 제22조(전자금융거래기록의 생성 및 보존)에 의거하여 인터넷뱅킹 거래 이용시 필요 정보를 수집 할 수 있습니다.
수집하는 정보의 항목과 이용 목적은 다음과 같습니다.
- 전자금융거래의 내용 추적 및 검색 : 고객 아이디, 접속일시, IP Address, HDD Serial, MAC Address 등
- 보안정책 수립용 통계 자료 : 개인 방화벽 설정, 운영체제 종류, 운영체제 주요 보안패치 여부, 방화벽 설정, 원격접속 설정, 브라우저 버전, 키보드 타입 등

이를 위해 금융기관은 전자금융 서비스 이용 약관이나 홈페이지의 "개인정보취급방침"에 관련 사항 명시 등 고객의 동의를 얻는 절차를 수행하여야 하며, 고객의 시스템 정보와 접속 경로 등의 수집을 위해 고객에게 제시할 법률적인 근거로는 전자금융거래법 제21조(안전성의 확보의무) 및 동법 제22조(전자금융거래기록의 생성 및 보존) 등이 적절한 것으로 판단된다.

5.2 금융실명거래 및 비밀보장에 관한 법률 대응

전자금융 침해사고가 발생하더라도 고객의 금융거래 관련 정보를 임의로 공유하여서는 안 되며, 반드시 금융실명거래 및 비밀보장에 관한 법률, 전자금융거래법 등의 관련 규정을 준수하여야 한다.

〔표 15〕 금융 거래 정보 공유와 관련된 금융 실명거래 및 비밀보장에 관한 법률

조항	주요 사항	원문 내용
4조	금융거래 내용의 타인 제공에 대한 제한	①금융기관에 종사하는 자는 명의인(신탁의 경우에는 위탁자 또는 수익자를 말한다)의 서면상의 요구나 동의를 받지 아니하고는 그 금융거래의 내용에 대한 정보 또는 자료(이하 "거래정보등"이라 한다)를 타인에게 제공하거나 누설하여서는 아니되며, 누구든지 금융기관에 종사하는 자에게 거래정보등의 제공을 요구하여서는 아니된다. 다만, 다음 각호의 1에 해당하는 경우로서 그 사용목적에 필요한 최소한의 범위 안에서 거래정보등을 제공하거나 그 제공을 요구하는 경우에는 그러하지 아니하다. 1. 법원의 제출명령 또는 법관이 발부한 영장에 의한 거래정보등의 제공 2. 조세에 관한 법률에 의하여 제출의무가 있는 과세자료등의 제공과 소관관서의 장이 상속·증여 재산의 확인, 조세탈루의 혐의를 인정할 만한 명백한 자료의 확인, 체납자의 재산조회, 국세징수법 제14조제1항 각호의 1에 해당하는 사유로 조세에 관한 법률에 의한 질문·조사를 위하여 필요로 하는 거래정보등의 제공 3. 국정감사및조사에 관한법률에 의한 국정조사에 필요한 자료로서 해당 조사위원회의 의결에 의한 금융감독원장 및 예금보험공사사장의 거래정보등의 제공 4. 재정경제부장관, 금융감독위원회(증권·선물시장의 불공정거래조사의 경우에는 증권선물위원회를 말한다. 이하 이 조에서 같다), 금융감독원장 및 예금보험공사사장이 금융기관에 대한 감독·검사를 위하여 필요로 하는 거래정보등의 제공으로서 다음 각목의 1에 해당하는 경우와 제3호의 규정에 의하여 해당 조사위원회에 제공하기 위한 경우 가. 내부자거래 및 불공정거래행위등의 조사에 필요한 경우 나. 고객예금횡령·무자원입금기표후 현금인출등 금융사고의 적출에 필요한 경우 다. 구속성예금 수입·자기앞수표선발행등 불건전금융거래행위의 조사에 필요한 경우 라. 금융실명거래 위반과 부외거래·출자자대출·동일인 한도 초과등 법령 위반행위의 조사에 필요한 경우 마. 예금자보호법에 의한 예금보험업무 및 업의구조개선에관한법률에 의해 예금보험 공사 사장이 예금자표의 작성업무를 수행하기 위하여 필요한 경우 (이하 생략)
시행령 제6조	거래정보등의 범위	법 제4조제1항 및 이 영 제5조에서"금융거래의 내용에 대한 정보 또는 자료"라 함은 특정인의 금융거래사실과 금융기관이 보유하고 있는 금융 거래에 관한 기록의 원본· 사본 및 그 기록으로부터 알게 된 것(이하"거래정보등"이라 한다)을 말한다. 다만, 금융거래사실을 포함한 금융거래의 내용이 누구의 것인지를 알 수 없는 것(당해 거래정보등만으로 그 거래자를 알 수 없더라도 다른 거래정보등과 용이하게 결합하여 그 거래자를 알 수 있는 것을 제외한다)을 제외한다.

〔표 16〕 전자금융거래법

제26조	전자금융 거래정보의 제공 등	전자금융거래와 관련한 업무를 수행함에 있어서 다음 각 호의 어느 하나에 해당하는 사항을 알게 된 자는 이용자의 동의를 얻지 아니하고 이를 타인에게 제공·누설하거나 업무상 목적 외에 사용하여서는 아니된다. 다만, 「금융실명거래 및 비밀보장에 관한 법률」 제4조제1항 단서의 규정에 따른 경우 그 밖에 다른 법률에서 정하는 바에 따른 경우에는 그러하지 아니하다. 1. 이용자의 인적 사항 2. 이용자의 계좌, 접근매체 및 전자금융거래의 내용과 실적에 관한 정보 또는 자료

〔표 17〕 비밀보장의 대상에서 제외되는 예
(금융실명거래 업무해설 기준, 전국은행 연합회, 2006.7)[5]

특정명의인의 금융거래 사실 또는 금융거래에 대한 정보를 알 수 없는 것은 비밀 보장의 대상에서 제외
① 금융거래에 관한 단순통계자료 ② 성명, 주민등록번호, 계좌번호, 증서번호 등이 삭제된 다수 거래자의 금융거래 자료로서 특정인에 대한 금융거래정보를 식별할 수 없는 자료 (이하 생략)

개별 금융기관에서 침해사고 정보 공유 및 공동 대응 시스템으로 제공하는 정보에는 특정인을 식별할 수 있는 정보를 제외한 침해사고의 역추적을 위한 시스템 식별 정보와 접속 주소 등의 기술적인 정보만이 포함되어야 하며, 추가적인 정보 공유가 필요한 경우에는 반드시 감독기관으로부터 정보제공 동의서 접수 등의 관련 규정을 따라야 한다.

Ⅵ. 결 론

본 논문에서는 은행권의 인터넷뱅킹 침해사고를 중심으로 전자금융 침해사고 현황 및 주요 원인, 기존 대응 체계의 문제점 파악 등을 통해 사용자 관점과 금융기관 관점에서 각각 전자금융 침해사고의 예방 및 대응 강화 방안을 제안하였다.

전자금융 서비스는 은행, 카드, 증권 등 대부분의 금융권역에서 이미 기존의 대면 거래보다 높은 비중을 차

지하고 있으며, 거래 금액 또한 지속적으로 증가하고 있다. 하지만 국내외의 전문 해커에 의한 신종 침해사고 또한 함께 증가하고 있으므로, 금융기관은 대고객 신뢰도 향상과 전자금융거래법 시행에 따른 금융기관의 책임 증가 등에 따라 기존 대응체계의 개선이 필수적이다.

안정적인 전자금융 서비스를 위해서는 사용자 스스로 공인인증서와 비밀번호 관리를 철저히 하는 것이 가장 중요하므로 금융기관에서도 자체 고객과의 접촉 채널 및 언론 기관을 통하여 대고객의 정보보안에 대한 인식 제고 활동을 더욱 강화하여야 할 것으로 판단되나, 본 논문에서는 사용자에게 필요한 공인인증서와 비밀번호 보안 강화를 위한 기술적인 개선점만을 분석하였으며, 고객의 정보보안에 대한 인식 제고를 위한 구체적인 방안은 제시하지 못하였으므로 이를 위한 추가적인 연구가 필요할 것으로 생각된다.

금융기관 관점에서 전자금융 침해사고의 효과적인 대응을 위해 제안한 접속 경로 로깅 및 역추적체계는 유사 체계의 구축 사례에 대한 활용 효과를 분석한 결과, 침해사고와 관련된 민원 접수 시 사고 원인 파악과 범인 검거를 위한 접속 경로 역추적에 활용되어 실용성이 일부 입증되었으나, 구축 효과를 극대화하기 위해서는 금융기간과 감독기관 간의 유기적인 공조체계를 기반으로 하는 침해사고 정보 공유 및 공동 대응 체계을 수립하여야 하며, 이를 통해 금융권 전반에 대한 고객의 신뢰도 향상과 장기적으로는 전자금융 서비스의 운영리스크 최소화 및 개별 금융기관의 신BIS 비율 제고를 통한 경제적 이익까지 거둘 수 있을 것으로 기대된다.

참고문헌

[1] 국가사이버안전센터, "사이버 침해사고 사례분석", 2008. 4.

[2] 금융위원회 금융정책국 금융정책과, "금융규제개혁 기본방향 및 진입규제 개선방안", 2008. 6.

[3] 김인석, "전자금융 사고사례와 대응현황", NETSEC-KR 2008 발표 자료, 2008. 4.

[4] 머니투데이, 인터넷뱅킹 "공인인증서만 믿으면 낭패" 기사, 2007. 4. 5.

[5] 전국 은행 연합회, 금융실명거래 업무해설, 2006. 7.

[6] 정석화, "최근 전자금융 사고 사례" 금융정보보호 컨퍼런스 발표자료, 2007. 10.

[7] 통계청 홈페이지(http://www.nso.go.kr), 국내 경제활동 인구 통계 자료, 2008. 3.

[8] 한국은행 공보자료, 2008년 1/4분기 국내 인터넷뱅킹서비스 이용현황, 2008. 4. 28.

[9] 한국정보보호진흥원, 공인인증서 가입자 소프트웨어에서의 전자서명생성키 관리 가이드라인(안), 2007. 11.

[10] www.asahi.com/digital/kagi/TKY200807290164.html, 일본 금융청 인터넷뱅킹 사고 현황 발표, 2008. 7.

[11] www.codeguru.com, "Reading Hard Drive Manufacturing Information", 2000. 11.

[12] www.ietf.org/rfc/rfc2898.txt, Public-Key Cryptography Standards (PKCS) #5, Password-Based Cryptography Specification Version 2.0

[13] www.ietf.org/rfc/rfc5208.txt ,Public-Key Cryptography Standards (PKCS) #8, Private-Key Information Syntax Specification Version 1.2

[14] www.kbstar.com, "개인정보취급방침".

[15] www.krcert.or.kr, 인터넷침해사고대응센터 통계자료.

[16] www.shinhan.com, ""개인정보취급방침".

참고규정

[1] 전자금융거래법

[2] 전자금융 감독규정

[3] 전자금융감독규정 해설서

[4] 정보통신망 이용 촉진 및 정보보호 등에 관한 법률

[5] 금융실명거래 및 비밀보장에 관한 법률

〈著者紹介〉

이 정 호 (Jung-Ho Lee)

1994년 : 경북대학교 전자공학과 학사

1994년~2003년 8월 : 정보시스템 개발 및 컨설팅, 보안시스템 연구개발 등

2003년 8월~현재 : 신한은행 IT기획부 과장

<관심분야> IT보안(전자금융 보안, 내부정보 유출 방지 등)