정 보 보 호 학 회 지
제25권 제6호, 2015. 12

인터넷 뱅킹 서비스에서의 사고사례와 관련 법률 분류 및 분석

임 하 빈*, 육 형 준**, 이 경 률***, 임 강 빈****

요 약

인터넷 뱅킹 서비스 규모가 증가하면서 외부에서의 위협으로부터 안전성을 확보하기 위하여 보안기술을 도입하였다. 하지만, 악의적인 공격자에 의한 사고사례가 지속적으로 발생하고 있으며, 그 원인을 분석하기 위한 자료가 필요한 실정이다. 추가적으로 보안기술과 더불어 사고를 방지하기 위하여 국내/외에서 관련 법률을 제정하였으며, 이 또한 사고를 방지하기 위한 자료로 활용이 가능하다. 따라서 본 논문에서는 인터넷 뱅킹 서비스에서 발생하는 사고사례의 원인을 분석하기 위하여 현재까지 발생한 사고사례에 대한 조사 결과를 서술하며, 사고를 방지하기 위한 지표의 일환으로 국내/외에서 제정된 관련 법률에 대한 조사 결과를 서술한다.

Ⅰ. 서 론

인터넷 뱅킹 서비스의 규모가 급증하면서 온라인을 통한 재화와 용역의 교환이 국가경제의 큰 부분을 차지하고 있다. 이러한 경제성장의 기반을 마련하기 위하여 다양한 보안기술을 적용함으로써 안전성을 확보하였지만, 2005년 5월, 인터넷 뱅킹 서비스에서의 해킹사건이 최초로 발생하였다. 이 사건을 기점으로 유사한 해킹사건과 텔레뱅킹, 도청사건 등으로 인한 피해가 지속적으로 발행하여 (구)정보통신부에서는 금융감독위원회, 금융감독원, 산업자원부, (구)한국정보보호진흥원과 공동으로 “전자거래 안전성 강화 종합대책”을 발표하였지만, 사고사례가 지속적으로 증가하는 추세에 있다. 이러한 사고가 발생하는 원인은 보안기술이 적용되더라도 적용된 환경에서 발생하는 문제점이 대부분의 원인이다.

상기 안전성을 확보하기 위한 방법으로 보안기술 외에 법률을 제정하였다. 법률을 제정한 목적은 악의적인 행위를 규제하고 공격자로 하여금 의욕을 상실하게 만들거나 법적인 조치를 취하기 위함이다. 법률은 강제적인 성격을 지니고 있어 사고를 미연에 방지함으로써 안전성을 보장한다.

따라서 본 논문에서는 국내에서 발생한 인터넷 뱅킹 서비스에서의 사고사례를 금융기관 구간과 네트워크 구간, 사용자 구간으로 분류하여 조사한 결과를 서술하며, 인터넷 뱅킹 서비스와 관련된 국외와 국내 법률에 대하여 조사한 결과를 서술한다.

본 논문의 구성은 다음과 같다. 2장에서 사고사례를 분류하고 사고 현황에 대한 조사 결과를 서술하며, 3장에서 사고사례를 분석한다. 4장에서 국외와 국내에 제정된 인터넷 뱅킹 서비스와 관련된 법률을 서술하고 5장에서 결론을 도출한다.

Ⅱ. 사고사례 분류 및 현황

2.1. 사고사례 분류

인터넷 뱅킹 서비스 전 구간에 존재하는 보안위협과 이로 인한 본인확인수단에서의 보안위협이 존재함으로 인하여 악의적인 공격자에 의하여 본인확인수단 및 보안기술을 우회하여 무력화하거나 사용자의 부주의로 인

본 연구는 2015년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2015R1A6A3A01019717)
* 순천향대학교 정보보호학과 (habin103@sch.ac.kr)
** 순천향대학교 정보보호학과 (goodyug@sch.ac.kr)
*** 순천향대학교 보안안전융합기술사업화센터 (carpedm@sch.ac.kr)
**** 순천향대학교 정보보호학과 (yim@sch.ac.kr)

한 실제 사고사례가 발생하였으며, 본 절에서는 지금까지 발생하였던 인터넷 뱅킹 서비스에서의 사고사례를 [표 1]과 같이 금융기관 구간과 네트워크 구간, 사용자 구간으로 분류하여 조사한 결과를 서술하고자 한다.

〔표 1〕 인터넷 뱅킹 서비스에서의 사고사례 분류

구간	사고사례
금융기관 구간	· 금융기관에서의 사고사례 · 금융기관 내부자에 의한 사고사례 · 금융보조업자에 의한 사고사례 · 웹 취약점에 의한 사고사례 · 금융기관 프로세스에서의 사고사례 · DDoS 공격에 의한 사고사례 · 데이터 유출에 의한 사고사례
네트워크 구간	· 네트워크 도청에 의한 사고사례 · 네트워크 취약점에 의한 사고사례
사용자 구간	· 중간자 공격에 의한 사고사례 · 메모리 해킹에 의한 사고사례 · 원격제어에 의한 사고사례 · 악성 프로그램에 의한 사고사례 · 도청에 의한 사고사례 · 카드복제에 의한 사고사례 · 피싱에 의한 사고사례 · 파밍에 의한 사고사례 · 사기에 의한 사고사례

2.2. 사고현황

금융사고란 금융기관 소속 임직원이나 소속 임직원 이외의 자가 금융업무와 관련하여 스스로 또는 타인으로부터 권유, 청탁 등을 받아 위법이나 부당한 행위를 함으로써 당해 금융기관 또는 금융거래자에게 손실을 초래하거나 금융질서를 문란하게 하는 행위를 의미한다. 다만, 여신심사 소홀 등으로 인하여 취급여신이 부실화된 경우에는 이를 금융사고로 보지 아니한다. 금융사고는 금전사고와 금융질서문란행위로 구분된다. 금전사고는 횡·유용, 사기, 업무상 배임 및 도난·피탈 사고 등 금융회사 또는 금융거래자에게 금전적 손실을 초래하는 사고이며, 금융질서문란행위는 사금융알선, 금융실명법 위반, 금품수수 등 금전적 손실은 없으나 금융관계법을 위반하는 사고이다[1]. 2010년부터 2012년까지 국내에서 발생한 금융사고 현황은 [표 2]과 같다[2].

사고현황을 살펴보면, 사고건수와 금액의 변동이 심하지만 2010년의 경우 다른 연도에 비하여 월등히 높은 것을 확인할 수 있다. 이는 4,132억원 허위지급보증서

〔표 2〕 권역별, 유형별 금융사고 현황(건, 억원)

구분		2010		2011		2012	
		건수	금액	건수	금액	건수	금액
은행	횡령 유용	43	676	50	173	47	154
	배임	5	5,1	7	217	1	54
	사기	7	53	11	131	8	74
	도난 피탈	3	1	6	13	3	1
	계	58	5,8	74	534	59	283
중소 서민	횡령 유용	47	93	30	45	54	184
	배임	7	476	8	305	14	88
	사기	15	66	11	250	5	32
	도난 피탈	1	-	-	-	2	0
	계	70	635	49	600	75	304
금융 투자	횡령 유용	12	264	9	34	11	56
	배임	2	6	1	1	2	8
	사기	3	118	2	36	1	60
	도난 피탈	-	-	-	-	-	-
	계	17	387	12	71	14	124
보험	횡령 유용	41	25	39	18	30	28
	배임	1	2	1	3	-	-
	사기	4	2	4	14	6	8
	도난 피탈	-	-	-	-	-	-
	계	46	29	44	35	36	36
합계	횡령 유용	143	1,0	128	270	142	422
	배임	15	5,6	17	525	17	150
	사기	26	239	28	431	20	174
	도난 피탈	4	1	6	13	5	1
	계	191	6,9	179	1,2	184	747

발급사고로 인하여 사고금액이 증가하였기 때문이며, 다양한 보안기술과 법률에도 불구하고 끊임없이 발생하는 것을 확인할 수 있다. 더욱이 인터넷 뱅킹 서비스에서의 사고는 사용자와 금융기관 모두 입증하기 어려운 문제일 뿐만 아니라 사고를 인지하기도 어렵기 때문에 통계를 내기에는 한계가 있어 실제로는 더욱 많은 사고가 발생하였을 것으로 사료된다. 인터넷 뱅킹 서비스에서 발생하는 사고의 특징은 공격 기법이 지능화되고, 사용자 구간과 네트워크 구간, 금융기관 구간 모두에서 발

생하며, 접속 및 로그인, 거래정보 입력 및 전송, 거래승인과 같은 서비스와 관련된 모든 단계에서 발생한다. 그 중 특히, 상대적으로 취약한 사용자의 전자적 장치인 PC를 집중적으로 공격하고, 이러한 사고가 전 세계적으로 흔히 발생할 뿐만 아니라 국제적으로 조직화되어 국가 간 수사협조와 법률적으로 공조하는 측면에서는 한계점을 가진다[3].

Ⅲ. 사고사례 분석

인터넷 뱅킹 서비스에서의 사고사례는 다양한 구간과 공격기술에 의하여 발생하였으며, 이와 같은 사고사례는 금융기관 구간과 네트워크 구간, 사용자 구간으로 분류된다.

3.1. 금융기관 구간에서의 사고사례

금융기관 구간에서의 사고사례는 금융기관에서의 사고사례, 금융기관 내부자에 의한 사고사례, 금융보조업자에 의한 사고사례, 웹 취약점에 의한 사고사례, 금융기관 프로세스에서의 사고사례, DDoS 공격에 의한 사고사례, 데이터 유출에 의한 사고사례로 분류된다.

금융기관에서의 사고사례로, 2004년, 컴퓨터 동아리 활동을 하는 대학생 김 씨에 의하여 인터넷 뱅킹 서비스에서 인증서를 이용하지 않고도 타인계좌의 잔액 및 입/출금 내역의 조회가 가능한 사고가 발생하였다. 이 사고는 해당 은행이 시스템 변경작업 중 암호화 과정을 제외함으로써 발생한 문제였다[3]. 또한, 다른 사례로 악의적인 목적으로 국내의 두 은행에 해킹을 시도하였지만 실패하여 제2금융권에 다시 시도하여 내부 전산망의 루트 권한을 획득한 후, 금융기관 내부에 저장된 고객정보를 암호화하였다. 금융기관에서는 공격자에 의하여 암호화된 고객정보를 열람할 수 없게 되었고, 이들은 복호화하는 대가로 거액을 요구하는 사고가 발생하였다[3]. 그리고 일본의 스미토모 은행의 컴퓨터 시스템을 해킹하여 전 세계의 은행계좌로 이체를 시도하다 영국과 이스라엘 경찰에 적발된 사례도 있다[3]. 2011년 4월에는 영업점에서 해킹으로 인한 서비스의 장애가 발생한 사례도 있다[4].

금융기관 내부자에 의한 사고사례로, 2002년, 인터넷 뱅킹 솔루션 개발업체 직원이 고객정보를 탈취하여 탈취한 고객의 은행계좌에서 고액을 인출한 사례가 있으며[3], 2011년에는 구찌 미국지사의 전직 직원이 가짜 VPN 계정을 생성하여 원격접속으로 데이터를 삭제한 사고가 발생하였으며, 이 사건으로 약 20만 달러의 피해가 발생하였다[5].

금융보조업자에 의한 사고사례로, 2008년, 외부업체에 의하여 운영되는 홈페이지를 제공하는 일부 상호저축은행이 외국 공격자의 경유지로 악용된 사례가 있으며[3], 2010년에는 프랜차이즈 음식점의 POS(Point Of Sale) 시스템을 해킹하여 카드결제와 판매내역과 같은 고객정보가 유출되어 해외에서 부정으로 사용된 사례가 있다[6].

웹 취약점에 의한 사고사례로, 2007년, 카드고객 20여명이 타인에 의하여 5천만원 정도가 결제된 사례가 있었다. 이 사례는 결제대행 서비스업체의 하위 가맹점 사이트가 해킹되어 발생하였으며, 20만원 미만의 거래에서는 공인인증서와 CVC(Card Verification Code)가 필요하지 않으며, 카드번호와 아이디, 비밀번호, 그리고 개인정보 6가지 중 임의의 질문에 올바른 답을 입력할 경우에는 결제가 가능하여 발생한 사례이다[7]. 2009년과 2011년에는 캐피탈 및 증권, 신용정보 회사의 홈페이지를 해킹하여 고객정보가 유출된 사례가 있다[4].

금융기관 프로세스에서의 사고사례로, 2006년, 신용카드번호를 악용한 사례가 발생하였다. 공격자는 검색엔진을 활용하는 사이트를 통하여 특정한 사이트에 가입된 사용자의 아이디와 비밀번호를 수집한 후, 수집한 인증정보로 쇼핑몰과 같은 사이트에 무작위로 방문하여 정상적으로 접속이 가능한 사이트를 선별하고, 접속된 사이트에 남겨진 사용자의 신용카드 결제내역을 토대로 신용카드번호를 조합하고 비밀번호를 탈취하여 악의적으로 활용한 사례로, 신고된 53명의 신용정보 55건을 도용하였다[8].

DDoS 공격에 의한 사고사례로, 2003년, SQL-overflow 웜에 의하여 전자금융 서비스가 중단된 사고가 발생하였고[9], 2008년에는 증권사에서 인터넷 서비스 장애가 발생하였으며[10], 2009년에는 한국과 미국의 주요 정부기관과 포털 사이트, 은행 사이트의 인터넷 뱅킹 서비스가 일시적으로 중단된 사고인 7.7 DDoS 공격이 발생하였다. 이 공격은 총 2차에 걸쳐 시도되었으며, 7개 은행의 인터넷 뱅킹 서비스가 일부 중단되거나 지연되었지만 금전적인 문제는 발생하지 않았다[3, 4,

10]. 그리고 2011년에는 한 증권회사에서 3시간 정도 접속이 지연되는 사례가 있었으며[4], 2013년에는 업데이트 서버 취약점으로 인하여 금융회사 내부에 악성코드가 유포되면서 서버의 데이터를 삭제하는 3.20 전산망 마비사태가 발생하였다. 이 사고로 일부 금융사 및 언론사를 비롯하여 금융회사의 업무용 컴퓨터 총 3만 2,000대 정도가 마비되어 인터넷 뱅킹 및 영업점의 창구업무 등이 2시간 정도 지연되었다[6, 11].

데이터 유출에 의한 사고사례로, 2008년 옥션해킹으로 11만명의 거래정보가 유출되었고, 선불 전자지급수단 발행과 관리업무를 수집하는 금융업자의 시스템에 침입하여 약 1,000만명의 개인정보와 100만명의 계좌번호를 포함하는 금융정보가 탈취되었으며, 하나로텔레콤과 상호저축은행, 다음의 한메일 사용자 55만명, 국민연금, 건강보험공단, 연예인 개인정보, LG데이콤의 인터넷 전화 가입자, NHN의 신규 이메일 서비스를 테스트하기 위하여 모집된 사용자 약 2만 6,000명, GS 칼텍스의 사용자 개인정보가 유출되었다. 2009년에는 평가원 수능자료와 같은 중요자료가 유출되었고, 100여개의 사이트가 해킹되어 탈취된 개인정보가 도용되었다. 2010년에는 신용카드 대리점에서 결제정보가 유출되었고, 유명백화점 인터넷 회원 고객정보 유출, 미국 뱅크오브아메리카의 전직 개발자에 의한 기밀파일 유출, 주요 포털사이트의 개인정보가 유출되었다. 2011년에는 ATM 운송과 폐기를 담당하는 업체에서 ATM 내의 하드디스크를 분리하여 소각하지 않아 약 2,000만건의 금융정보가 유출되었고, 중국 해커에 의하여 국내 100여개 업체의 개인정보가 유출되었으며, 네이트와 싸이월드의 개인정보 유출, 곰TV, 엔트랙, 한국앱손, 행정안전부와 관련된 사이트, 수시모집 응시자 개인정보와 합격정보가 유출되었다. 게다가 카드사 직원이 개인정보를 매매한 사례와 대리운전업체의 고객정보, 경찰이 개인정보를 조회하여 판매한 사례가 있었다. 2012년에는 골프장과 EBS, 새누리 당원, 4.11 총선 유권자, KT의 사용자 개인정보가 유출되었고, 인터넷 쇼핑몰 운영자가 1,175만건의 개인정보를 유출하였으며, SKT와 KT 협력업체 직원이 별도의 프로그램을 개발하여 개인정보를 유출한 사례가 있다[5, 18, 19].

3.2. 네트워크 구간에서의 사고사례

네트워크 구간에서의 사고사례는 네트워크 도청에 의한 사고사례, 네트워크 취약점에 의한 사고사례로 분류된다.

네트워크 도청에 의한 사고사례로, 2008년, 공격자가 차량을 은행 건물 앞에 주차한 후, 은행에 설치된 무선 공유기의 패킷을 감청하여 접속하는 관리자의 아이디와 비밀번호를 탈취한 후, 이를 이용하여 은행 내부의 네트워크에 접속하여 고객의 정보를 빼내고 자금을 이체하려고 시도한 사례가 있다[18].

네트워크 취약점에 의한 사고사례로, 2004년, VAN사와 PG사와 같은 신용카드 정보를 처리하는 업체의 전산망을 공격하여 카드정보가 유출되면서 10억 이상의 피해가 발생한 사례가 있으며, 2004년과 2005년, 미국에서 카드정보를 처리하는 회사의 전산망을 공격하여 각각 8백만건과 4천만건의 카드정보가 유출되었으며, 2003년부터 2006년까지 대형 유통 업체의 전산망을 공격하여 카드거래정보가 유출된 사례가 있다[10]. 그리고 2008년, 공격자가 추적의 가능성을 낮추기 위하여 공공장소에서 인증을 요구하지 않는 무선 공유기에 접속하여 금융기관의 네트워크와 서버의 취약점을 수집한 후, 데이터베이스와 웹하드 계정을 탈취하고 이를 활용하여 7개 상호저축은행과 여타 기관 고객의 금융정보 970만건 정도를 유출시킨 사례가 있다[18].

3.3. 사용자 구간에서의 사고사례

사용자 구간에 의한 사고사례는 중간자 공격에 의한 사고사례, 메모리 해킹에 의한 사고사례, 원격제어에 의한 사고사례, 악성 프로그램에 의한 사고사례, 도청에 의한 사고사례, 카드복제에 의한 사고사례, 피싱에 의한 사고사례, 파밍에 의한 사고사례, 사기에 의한 사고사례로 분류된다.

중간자 공격에 의한 사고사례로, 2006년, 미국 시티은행의 citibusiness 서비스 사용자를 대상으로 중간자 공격을 시도하여 OTP 생성기를 무력화시킨 사례가 있다[3].

메모리 해킹에 의한 사고사례로, 2007년, 사용자가 입력한 거래정보를 전송하기 전에 메모리에 저장되는 취약점을 이용하여 거래정보를 변조한 사례가 있고[7,

10], 2009년에는 독일의 한 은행에서 사용자 PC에 저장된 거래정보를 메모리 해킹으로 변조하여 약 4억원을 이체한 사건이 있으며[16, 17], 2010년에는 증권사의 홈 트레이딩 시스템(HTS, Home Trading System)이 메모리 해킹에 의하여 다른 계좌로 이체가 가능한 위협에 대하여 보도되었다[10]. 2013년에는 공인인증서를 이동식 디스크에 저장하고 보안 프로그램으로 PC의 보안을 강화하였음에도 불구하고 메모리 해킹에 의하여 300만원이 인출된 사건이 발생하였다[11].

원격제어에 의한 사고사례로, 윈도우즈 운영체제에는 원격제어 기능이 있어, 2007년과 2008년, 공격자가 원격제어로 사용자 PC에서 6,200만원을 인출한 사례가 있다. 이 사고는 포털 사이트의 카페에 바이러스를 업로드한 뒤, 해당 바이러스가 설치된 사용자 PC에서 보안카드정보와 같은 거래정보가 탈취되어 발생한 사고이다[3].

악성 프로그램에 의한 사고사례로, 2004년, 미국의 뱅크오브아메리카에서 악성코드로 인하여 9만 348달러가 이체되었고[3], 2005년에는 국내에 처음으로 인터넷 뱅킹 서비스에서 19세 입시 준비생에 의하여 사고가 발생하였다. 이 사고는 다음 포털 사이트의 짠돌이라는 재테크 카페에 악성 프로그램인 넷데블(Net devil)이 자동으로 설치되는 글을 게시하였고, 사용자가 글을 열람하면 사용자의 PC에 악성 프로그램이 설치되며, 사용자가 인터넷 뱅킹 서비스를 이용하면 설치된 악성 프로그램은 키보드 보안 프로그램과 개인침입차단시스템과 같은 보안 프로그램을 무력화하고 거래정보와 공인인증서 비밀번호, 계좌비밀번호, 보안카드번호와 같은 거래와 관련된 비밀정보를 실시간으로 탈취하여 공격자에게 전달하였다. 이 후 공격자가 탈취한 비밀정보를 이용하여 공범명의 5개 계좌로 5,000만원을 이체한 사례이다[3, 9, 12, 13, 14]. 일본의 인터넷은행과 미즈호은행에서 악성 프로그램을 이용하여 인터넷 결제용 아이디와 비밀번호를 탈취하고 10개의 타인 계좌에서 1,140만엔을 이체한 사고가 발생하였다[3]. 2006년, 중국의 북경과 남경, 항주, 합비 등 약 10개 도시의 70여명의 사용자들이 30만 위엔에 해당하는 피해를 당하였고 호남성 경찰이 체포한 인터넷 은행전문 강도 집단은 1,000개가 넘는 계좌번호를 관리하였으며, 이들에 의하여 40만위엔 이상의 피해가 발생하였다[7]. 2007년에는 중국 해커로 추정되는 집단들이 특정 웹 사이트에 악성 프로그램이 설치되도록 한 후, hosts 파일의 내용을 수정하여 공격자가 만든 가짜의 은행 사이트에 접속하도록 유도하여, 접속하는 사용자의 공인인증서 4,000여개를 복제하고 공인인증서 비밀번호, 계좌비밀번호와 같은 비밀정보를 탈취한 사례가 발생하였다[14, 15]. 2008년 3월부터 2009년 6월까지 중국의 공격자에 의하여 사용자 PC에 악성 프로그램이 설치되어 인터넷 뱅킹 서비스의 아이디와 비밀번호를 탈취하고, 이메일과 PC에 저장된 보안카드를 이용하여 32개의 금융기관에서 4억 4,000만원을 이체한 사례가 있다[16, 17]. 2009년, 웹 보안 업체인 Finjan사가 공개한 문서에 따르면 웹 브라우저의 취약점을 이용하여 약 6,400개의 사용자 PC에 악성 프로그램을 설치하고 그 중 수백 대의 PC에서 22일 동안 30만 유로에 해당하는 금액이 이체된 사례가 있으며, 설치된 악성 프로그램에서 지속적으로 보안카드번호를 감시한 후 공인인증서를 다시 발급받아 불법으로 이체한 사례가 있다[11, 18, 20]. 2011년에는 농협 협력업체 직원의 노트북에 설치된 악성 프로그램에 의하여 수개월 동안 정보를 수집한 후, 농협 내부에 접속하는 방법을 습득하여 30분 만에 내부 서버 절반을 파괴함으로써 전산망이 마비되어 금융업무가 지연되는 사례가 있고[6, 11], 2013년에는 악성 프로그램에 의하여 공인인증서 700여개가 탈취된 사례가 있다[6]. 게다가 상기와 같은 PC뿐만 아니라 모바일에서도 악성 프로그램이 설치되어 발생한 사고도 존재하며, 2009년에는 Droid09라는 아이디를 사용하는 앱 개발자가 합법적인 모바일 뱅킹 앱으로 가장한 로그 피싱 앱을 안드로이드에 등록하였는데, 이 앱은 실제로 모바일 뱅킹의 인증정보를 불법으로 탈취하는 것이 그 목적이었으며[21], 2010년에는 Zeus Trojan이라 불리는 개인인증정보를 유출하는 모바일 악성 프로그램으로 인하여 유럽 12개 은행에서 모바일 뱅킹 사고가 발생하였다[22].

도청에 의한 사고사례로, 1995년, 전화기지국에서의 도청에 의한 정보유출로 인하여 1996년에 인터넷 뱅킹 서비스가 일시적으로 중단되었다가 1998년에 다시 서비스된 사례가 있고[3], 2004년에는 텔레뱅킹 감청에 의하여 비밀번호가 유출되어 이체사고가 5건 발생하였다[9]. 카드복제에 의한 사고사례로, 2002년, 현금 및 신용카드를 위조하거나 복제하여 현금을 인출하는 사고가 증가하였다[9].

피싱에 의한 사고사례로, 2003년, 호주의 웨스트팩은

행을 대상으로 전 세계에서 최초로 피싱 공격이 발생하였고, 2005년에는 국내의 은행을 대상으로 피싱 사이트가 최초로 발견되었으며[3, 6], 2006년에는 산업은행의 영문 이니셜인 kdb와 영국을 의미하는 uk를 혼합하여 산업은행의 런던지점을 사칭하는 kdbuk.com, kd-buk.com, kd-b.com, k-d-b.com, kdbuk.net, kd-buk.net과 같은 피싱 사이트가 발견되었다. 2007년에는 악성 프로그램을 설치하는 피싱 사이트를 만들어 hosts 파일을 변경하여 고객 30명의 계좌번호와 비밀번호, 보안카드번호와 같은 비밀정보가 탈취된 사례가 있고[3, 23], 2009년에는 미국의 코메리카은행을 대상으로 피싱 메일을 악용하여 55만달러가 무단으로 인출된 사례가 있으며[3], 2010년에는 “당신의 비자카드 결제가 거부되었습니다.”라는 제목으로 비자카드를 사칭하는 피싱 메일이 발송되어 신용카드번호와 계좌번호, 비밀번호와 같은 비밀정보를 탈취하기 위한 시도와 카드사의 이용대금 명세서를 보기 위한 링크를 포함한 피싱 메일이 발송되어 링크를 클릭하면 금융회사의 보안 프로그램으로 위장한 악성 프로그램이 설치되도록 유도한 사례가 있다[15]. 2011년 말부터 국민은행과 농협의 웹 사이트를 위장한 피싱 사이트가 등장하기 시작하면서 우리은행과 신한은행 등 다른 금융기관의 피싱 사이트가 등장하였고, 이후 2012년, 우리은행은 13건의 피싱 사이트를 신고하였다[21].

파밍에 의한 사고사례로, 2007년, 스웨덴 노르데아은행의 주소를 속이는 파밍으로 인하여 250명 계좌의 800만크로나가 부정적으로 이체된 사례가 있고[3], hosts 파일을 변조하여 특정 은행의 웹 사이트에 접속할 때 대만에 위치한 서버의 피싱 사이트로 접속하도록 악성 프로그램을 배포하여 5,000여명의 공인인증서와 계좌비밀번호, 보안카드번호가 유출된 사례가 있으며[10], 세계 65개 이상의 금융회사와 전자상거래 업체 고객의 인터넷 뱅킹 서비스 아이디와 비밀번호를 탈취하는 파밍 공격이 미국의 보안업체인 웹센스에 의하여 밝혀졌으며, 영국의 바클레이스은행과 스코틀랜드은행, 미국의 아메리카익스프레스카드, 디스커버카드, 인터넷 경매업체인 이베이, 국제 송금 사이트인 페이팔 등의 업체에서 하루 평균 1,000명 이상의 피해자가 발생하였다[7].

사기에 의한 사고사례로, 2006년, 국세청을 사칭하여 세금환급을 빌미로 800만원을 송금한 사례가 있고, 2009년에는 대학등록금 640만원을 사기당하여 투신자살한 사례가 있으며, 친구에게 공인인증서가 저장된 USB와 계좌번호, 계좌비밀번호, 보안카드번호가 적힌 쪽지를 건네어 대포통장으로 5천만원을 이체시킨 후, 자신의 계좌에서 불법으로 이체되었다고 신고하여 보상금을 지급받은 자작극에 의한 사례가 있다. 2010년에는 불법으로 이체된 경우에 보상금이 지급된다는 이유로 친구의 공인인증서와 보안카드를 훔친 후, 3회에 걸쳐 불법으로 1,900만원을 이체하여 서울지방경찰청 사이버범죄수사대에 붙잡힌 사례가 있다. 2011년에는 “피해자의 금융정보를 알고 돈을 인출하는 것 같으니 검찰에 신고하라.”는 전화를 받은 피해자는 곧 “검찰인데 은행에서 전화를 받았느냐, 금융감독원에 넘겨 수사를 하려고 하니 계좌번호와 비밀번호, 텔레뱅킹번호를 알려 달라.”고 하여 비밀정보를 탈취한 후, 총 9회에 걸쳐 3,472만원이 불법으로 이체된 사례가 있다. 2012년에는 중국에 출장 중인 친구로부터 비자금이 들켰다는 카카오톡 메시지를 받은 피해자가 600만원을 이체하였고, 이체가 된 후 메시지를 보낸 사람이 다른 사람으로 변경된 것을 확인하여 신고하였지만 이미 인출되어 피해가 발생한 사례가 있다[3, 21].

Ⅳ. 관련 법률 분석

상기와 같이 인터넷 뱅킹 서비스에서의 사고사례가 발생함에 따라 악의적인 행위를 규제하여 공격자로 하여금 의욕을 상실하게 만들거나 법적인 조치를 취하기 위한 강제적인 성격을 지닌 법률을 제정함으로써 안전성을 보장한다. 따라서 본 절에서는 인터넷 뱅킹 서비스와 관련된 국외와 국내 법률에 대하여 조사한 결과를 서술하며, 이를 [표 3]에 나타내었다.

〔표 3〕 인터넷 뱅킹 서비스와 관련된 법률

국가	관련 법률
미국	전자자금이체에 관한 전국위원회의 전자자금이체법을 구체화하고 보완하여 Regulation E 제정
유럽연합	지급결제서비스지침 제정
영국	금융서비스시장법의 하위규범으로 지급결제서비스규정 제정

독일	민법에 자금이체에 관한 조항 삽입	
호주	전자자금이체규약 제정, 이를 수정 및 보완하여 전자지급결제규약 제정	
국내 법률	전자금융거래법	전자정부법
	전자서명법	정보통신기반보호법
	전자거래기본법	주식회사의 외부감사에 관한 법률
	자본시장과 금융투자업에 관한 법률	공공기관의 개인정보보호에 관한 법률
	국가정보화기본법	장애인차별금지 및 권리구제 등에 관한 법률
	신용정보의 이용 및 보호에 관한 법률	금융실명제 및 비밀보장에 관한 법률
	정보통신망 이용촉진 및 정보보호에 관한 법률	정보시스템의 효율적인 도입 및 운영 등에 관한 법률
	특정 금융거래 정보의 보고 및 이용 등에 관한 법률	전자상거래 등에서의 소비자보호에 관한 법률

4.1. 국외 법률

4.1.1. 미국

전자자금이체에 관한 전국위원회(NCEFT, National Commission on Electronic Fund Transfer)는 1977년 10월에 기존의 금융에 관한 법률이 전자자금이체에 대하여 고려하지 않았음을 밝히며, 1978년 11월 10일에 전자자금이체법(EFTA, Electronic Funds Transfer Act)을 구체화하고 보완하여 1979년 6월 6일에 Regulation E를 제정하였다[24]. 전자자금이체법은 이체나 송금 등에 대하여 이해당사자 간의 권리와 채무 등을 규율하는 것을 목적으로 하며(15 U.S.C. 1693(b)) 적용대상을 전자기기, 전화기, 자기테이프 등으로 규정하였다. 특히, 권한이 없는 거래로 인하여 발생하는 사고에 대한 책임을 규정하는데, 원칙적으로는 금융회사가 입증책임을 부담하며(15 U.S.C. 1693g(b)), 사용자가 60일 이내에 피해사실을 알렸다면 책임이 없지만, 60일 이후에 통지하였을 경우에는 피해금액 전부에 대한 책임이 있다. 그리고 접근매체를 분실하거나 도난당한 경우, 2일 이내에 통지하였다면 피해액의 최대 50달러까지만 책임이 있으며, 2일부터 60일 이내에 통지한 경우에는 최대 500달러, 60일 이후에 통지한 경우에는 피해금액 전부에 대한 책임이 있다(15 U.S.C. 1693g(a))[25].

4.1.2. 유럽연합

유럽연합의 지급결제서비스지침(PSD, Payment Services Directive)은 2007년 11월에 제정되었으며 유럽경제지역(EEA, European Economic Area)에서 시행되는 이체와 송금 등의 모든 지급결제서비스의 규제와 감독 등을 규율한다. 미국에서와 같이 사용자가 접근매체를 분실하거나 도난당한 경우, 13개월 내에 통지하여야 하며(article 56(1)b), 통지하지 않았을 경우에는 최대 150유로의 책임을 부담한다(article 61). 하지만 사용자의 고의가 입증된 경우, 서비스제공자는 책임을 면하며, 사용자에게 통지할 수 있는 수단을 제공하고 통지사실을 18개월 간 확인시켜 줄 수 있어야 한다(article 57(1b))[25].

4.1.3. 영국

영국은 유럽연합이 제정한 지급결제서비스지침을 자국법에 반영할 의무가 있으며, 금융서비스시장법(FSMA, Financial Services and Markets Act)의 하위규범으로 지급결제서비스규정을 제정하였다. 영국의 경우에는 유럽연합의 지침을 반영하였기 때문에 거의 비슷하지만 접근매체의 도난이나 분실 등의 경우, 최대 50파운드의 책임만 부담한다[25].

4.1.4. 독일

독일은 민법을 개정하여 자금이체에 관한 조항(§675c와 §676c)을 삽입하여 자금이체 파트를 1999년 7월에 제정하였다. 독일 역시 영국과 마찬가지로 유럽연합의 지침을 대부분 반영하였지만, 접근매체의 도난이나 분실 등의 경우, 최대 150유로의 책임만 부담하며, 13개월 이내에 이를 통지할 의무가 있다[25].

4.1.5. 호주

호주는 1986년에 전자자금이체규약(EFT Code, Electronic Funds Transfer Code of conduct)을 제정하였고 2010년 12월에 이를 수정하고 보완하여 현재의

〔표 4〕 국내 금융 IT 관련 법률 현황

구분	법률 현황	설명
금융기관 IT 관련 국내 법률	1. 전자금융거래법 (전자금융감독규정)	금융기관 IT 시스템 요구사항을 전반적으로 규정
	2. 전자서명법	공인인증서 이용부문
	3. 전자거래기본법	전자거래 문서 이용부문
	4. 자본시장과 금융투자업에 관한 법률	증권사의 지급결제 참가, 정보의 차단
	5. 주식회사의 외부감사에 관한 법률	금융기관 내부통제에 대한 외부감사
	6. 정보통신망 이용촉진 및 정보보호에 관한 법률	침해사고 대응, 안전진단 및 ISMS, 주민번호 대체수단, 금융정보암호화, 통신과금업자의 규제기관 변경
	7. 신용정보의 이용 및 보호에 관한 법률	신용정보 전산시스템의 기술적, 물리적 보안대책
	8. 금융실명제 및 비밀보장에 관한 법률	실지명의에 의한 금융거래
	9. 특정 금융거래 정보의 보고 및 이용 등에 관한 법률	자금세탁방지를 위한 금융거래 모니터링
	10. 정보통신기반보호법	주요정보통신기반시설의 지정, 금융 ISAC의 운영
	11. 공공기관의 개인정보보호에 관한 법률	개인정보의 수집, 처리 및 보호에 관한 사항
	12. 전자상거래 등에서의 소비자보호에 관한 법률	전자거래 시 소비자의 의사표시 확인
	13. 장애인차별금지 및 권리구제 등에 관한 법률	인터넷 뱅킹, CD/ATM 등 금융서비스의 장애인 접근성 강화
	14. 전자정부법	공공기관 등의 보안대책은 국가정보원장이 확인
	15. 정보시스템의 효율적인 도입 및 운영 등에 관한 법률	정보기술 구성에 대한 사항을 행정안전부장관에게 제출
	16. 국가정보화기본법 (정보화촉진기본법)	정보보호 제품의 평가 및 인증(CC 등)에 대한 사항

전자지급결제규약(e-Code, ePayments Code)을 제정하였으며, 2011년 9월부터 과도기를 거친 후 2013년 3월 20일부터 시행하였다. 호주는 다른 주요국이 구속력을 가진 법령으로 규율하는 것과는 다르게 자율규약으로써 구속력에 한계가 있지만 실효성을 갖추고 있다. 다른 주요국과 같이 접근매체의 도난이나 분실 등의 경우, 통지하지 않으면 피해금액 전부를 부담하여야 하고(clause 11.2), 통지한 경우에는 최대 150호주달러의 책임이 있으며(clause 11.7), 금융회사의 거래승인절차의 안전성 등과 같은 적법한 조치여부를 고려하여 책임을 경감할 수도 있다(clause 11.9)[25].

4.2. 국내 법률

국내의 경우, 금융기관 등과 직접적으로 관련이 있는 IT(Information Technology) 관련 법률은 총 16종으로 파악되며, 이를 [표 4]에 나타내었다[26].

Ⅴ. 결 론

본 논문에서는 인터넷 뱅킹 서비스에서 발생한 사고사례를 금융기관 구간과 네트워크 구간, 사용자 구간으로 분류하여 조사한 결과를 서술하였다. 조사한 사고사례는 인터넷 뱅킹 서비스에서 발생하는 위협의 원인을 분석하기 위한 자료로 활용이 가능할 것으로 사료된다. 또한 사고를 방지하기 위하여 국내/외에서 제정한 법률에 대한 조사 결과를 서술하였으며, 이 역시 사고를 방지하기 위한 자료로 활용이 가능할 것으로 판단된다.

향후 연구로는 사고사례에 해당하는 위협을 방지하기 위하여 현재 제정된 법률에서 필요한 요소를 정의하는 연구와 조사한 사고사례를 정밀하게 분류하여 인터넷 뱅킹 서비스에서 발생하는 보안위협에 대한 정의, 그리고 그 결과를 기반으로 안전성을 확보하기 위한 보안 요구사항에 대한 정의를 도출하는 연구가 필요할 것으로 사료된다.

참 고 문 헌

[1] 금융감독원, “금융사고의 정의”, http://www.fss.or.kr/fss/kr/bbs/view.jsp?url=/fss/kr/1207386918383&idx=50000001201&bbsid=1207386918383, 2014년 10월 14일 열람.

[2] 금융감독원, “2012년 금융사고 현황 및 감독 대응방안”, 보도자료, 2013년 3월 11일.

[3] 김시홍, “인터넷뱅킹 해킹사고와 손해배상책임: 전자금융거래법 제9조의 해킹사고 요건과 면책사유를 중심으로”, 고려대학교 법무대학원, 석사학위논문, 2010년 7월.

[4] 금융보안연구원, “2011년 주요 금융보안 이슈 및 2012년 전망”, 이슈리포트, 2012(1), 2012년 1월.

[5] 금융보안연구원, “금융IT 내부통제 강화전략: 내부자 위협 중심으로”, 2011(8), 2011년 6월.

[6] 조강유, 민상식, 성재모, “전자금융 보안위협 관련 대응기술 연구 추진 방안”, 한국정보보호학회 학회지, 23(6), pp.49-53, 2013년 12월.

[7] 이상진, 황소연, 김경곤, 여성구, “인터넷 뱅킹 서비스 취약점 분석 및 보안대책”, 정보·보안논문지, 7(2), pp.119-128, 2007년 6월.

[8] 이창조, “인터넷 게임과 뱅킹 인증을 위한 개선된 보안 알고리즘의 설계 및 구현”, 한국컴퓨터게임학회 논문지, 14, pp.159-166, 2008년 9월.

[9] 이정호, “전자금융 침해사고 예방 및 대응 강화 방안”, 한국정보보호학회 학회지, 18(5), pp.1-20, 2008년 10월.

[10] 성재모, “국내외 전자금융 보안정책 분석을 통한 효과적인 전자금융 보안 대응체계”, 전남대학교 대학원, 박사학위논문, 2011년 2월.

[11] 손보형, “전자금융거래 침해사고에 대한 포렌식 조사 적용방안 연구: 인터넷 뱅킹 사고를 중심으로”, 동국대학교 국제정보대학원, 석사학위논문, 2014년 2월.

[12] 이원철, 이석래, 이재일, 김인석, “전자금융거래시스템 취약점 분석 및 안전성 강화방안 연구”, 한국정보보호학회 학회지, 15(4), pp.43-48, 2005년 8월.

[13] 이재익, “전자금융거래 보안강화를 위한 종단간 암호화와 고려사항”, 성균관대학교 정보통신대학원, 석사학위논문, 2008년 4월.

[14] 서호진, “모바일 디바이스에서의 사용자 입력패턴 분석기반 생체인증 방법: 전자금융사고 예방대책을 중심으로”, 고려대학교 정보보호대학원, 석사학위논문, 2012년 2월.

[15] 금융보안연구원, “피싱·파밍 사고 대응 절차서”, 2010년 12월.

[16] 유한나, “금융거래 시스템에서 모바일 인증서를 이용한 Two Channel 인증방식”, 숭실대학교 대학원, 석사학위논문, 2010년 6월.

[17] 박운암, “강화된 RSA 암호키와 프로세스 감시, 차단 Agent를 통한 안전한 금융서버 인증 프로토콜 설계”, 숭실대학교 정보과학대학원, 석사학위논문, 2012년 6월.

[18] 정상각, “전자금융거래에서의 QR CODE 기반 투-채널 인증기법의 제안”, 고려대학교 정보경영공학전문대학원, 석사학위논문, 2010년 12월.

[19] 금융보안연구원, “DB 암호화 최신동향 및 보안기술 분석 보고서”, 2012(3), 2012년 9월.

[20] 이상호, 김성호, 강전일, 변제성, 양대헌, 이경희, “콘텐츠 기반 캡차를 이용한 인터넷 뱅킹 서비스의 보안성 향상 기법”, 한국정보보호학회 논문지, 23(4), pp.571-583, 2013년 8월.

[21] 정순채, “전자금융사기 등 정보통신망 이용 금융사기 대응방안 고찰”, 경희대학교 국제법무대학원, 석사학위논문, 2012년 8월.

[22] RSA, “RSA 2011 cybercrime trends report: the current state of cyber crime and what to expect in 2011”, 2011.

[23] 금융보안연구원, “전자금융 이용자 보안가이드”, 2007년 10월.

[24] 손남숙, “전자금융거래에 관한 연구 - 전자자금이체를 중심으로”, 고려대학교 법무대학원, 석사학위논문 2005년 8월.

[25] 금융보안연구원, “주요국 전자금융사고 책임소재 관련 법규 분석 및 시사점”, 금융보안리포트, 2013(1), 2013년 6월.

[26] 금융보안연구원, “금융부문의 IT 컴플라이언스 분석 결과 보고서”, 2009년 11월.

〈저 자 소 개〉

임 하 빈 (Habin Yim)
학생회원

2012년 3월~2014년 2월 : 동신대학교 정보보안학과 학사과정
2014년 3월~현재 : 순천향대학교 정보보호학과 학사과정
관심분야 : 인터넷 뱅킹, 시스템 보안, 하드웨어 보안, 취약점 분석

육 형 준 (Hyeungjun Yeuk)
학생회원

2010년 2월 : 동양대학교 전자유도기술학과(공학사)
2012년 8월 : 순천향대학교 정보보호학과(공학석사)
2013년 3월 ~ 현재 : 순천향대학교 정보보호학과 박사과정
관심분야 : 취약점 분석, 시스템 보안, 내부자 공격, 하드웨어 보안

이 경 률 (Kyungroul Lee)
정회원

2008년 8월 : 순천향대학교 정보보호학과(공학사)
2010년 8월 : 순천향대학교 정보보호학과(공학석사)
2015년 2월 : 순천향대학교 정보보호학과(공학박사)
2011년 5월~2011년 12월 : (미)퍼듀대학교 방문연구원
2015년 6월~현재 : 순천향대학교 박사후연구원
관심분야 : 취약점 분석, 시스템 보안, 하드웨어 보안, 인터넷 뱅킹, 사용자 인증, 디바이스 인증

임 강 빈 (Kangbin Yim)
종신회원

1992년 2월 : 아주대학교 전자공학과(공학사)
1994년 2월 : 아주대학교 전자공학과(공학석사)
2001년 2월 : 아주대학교 전자공학과(공학박사)
1999년 3월 ~ 2000년 2월 : (미)아리조나주립대학교 연구원
2003년 3월~현재 : 순천향대학교 정보보호학과 교수
2005년 3월~현재 : 한국정보보호학회 이사
2009년 3월~현재 : 한국인터넷정보학회 이사
2010년 12월~2012년 2월 : (미)퍼듀대학교 객원교수
관심분야 : 취약점 분석, 내부자 공격, 보안 하드웨어 구조, 인증 프로토콜, 홈랜드 시큐리티