電子金融과 정보보호에 관한 연구

김 인 석

금융감독원 IT감독팀장

전자금융거래는 통장이나 카드를 사용하는 전통적 금융거래와 달리 비대면, 비서명의 특성이 있어 도용, 도청, 해킹, 피싱 등 고도의 새로운 유형의 범죄에 노출되어 있다. 금융회사들은 방화벽설치, 암호화, OTP사용 등 다양한 대책을 운영중에 있으나 금융회사만으로는 대응하는 데는 한계가 있으므로 이용자들의 적극적인 협조가 필요한 바, 무엇을, 어떻게, 왜 하여야 하는가를 제시함으로써 안전한 전자금융거래환경을 마련하고자 한다.

Ⅰ. 서 론

1. 연구목적 및 배경

어느 날 갑자기 은행에 맡겨 놓았던 예금이 쥐도 새도 모르게 없어 졌다면 당신은 어떻게 할 것인가? 또 자신의 주식이 자기도 모르게 팔려 나갔다면, 자신의 신용카드로 수백만원이 결제되었다면? 과연 이러한 일들이 일어날 수 있는가?

우리나라는 인터넷의 이용자 비율[1]이 세계에서 가장 높을 뿐 만 아니라 이를 이용한 전자금융거래[2] 또한 급속히 증가하고 있다.

증가하는 전자금융거래 만큼 위와 같은 일들이 발생하고 있으며, 앞으로도 지속적으로 발생할 것이다. 따라서 이러한 사고를 방지하기 위하여 금융기관들은 어떠한 대책을 준비해 놓고 있으

1) 통계청의 발표에 의하면 100명당 인터넷 이용 인구는 51.07명으로 세계에서 가장 높은 비율을 나타내고 있음

2) 전자금융거래법 제 2조 1항.
전자금융거래라 함은 금융기관 또는 전자금융업자가 전자적 장치를 통하여 금융상품 및 서비스를 제공(이하 "전자금융업무"라 한다)하고, 이용자가 금융기관 또는 전자금융업자의 종사자와 직접 대면하거나 의사소통을 하지 아니하고 자동화된 방식으로 이를 이용하는 거래를 말한다.

며, 정부나 감독기관은 법적 제도적 장치를 적절히 마련하고 있고, 나는 어떻게 해야 안전하게 예금, 주식, 카드를 보호하고, 안심하고 사용할 수 있는가, 그래도 사고를 당했을 경우 어떻게 해야 보상을 받을 수 있는 가를 아는 것이 필요하다.

본 자료는 현재 법이나 제도적으로 정하고 있는 전자금융거래에 대한 안전 대책과 안전한 이용방법을 제시함으로써 금융기관 종사자들은 안전한 전자금융서비스를 위한 대응책을 마련하고 이용자들은 안전한 전자금융거래 방법을 알게 됨으로써 사고를 방지하기 위해 작성하였다.

2. 연구방법

본 자료는 국내 모든 금융회사가 제공하고 있는 전자금융거래 관련 법규 즉, 전자거래법, 전자금융거래법, 전자서명법과 미국의 전자자금이체법, Regulation E(미국 전자자금이체감독규정), UNCITRAL 등과 금융감독원의 금융기관전자금융업무 감독규정, 국가정보원의 국가정보보호지침 등의 규정을 참고로 하였으며, 그 동안 발생된 사고사례도 이용하여 작성하였다.

그러나 지면의 한계로 인하여 세부적인 내용을 제시하지 못한 경우도 있으므로 이번 자료에 발표한 내용이 모든 것이라는 판단을 하지 말아야 할 것이다.

Ⅱ. 전자금융거래 유형 및 이용현황

1. 은행 전자금융거래

우리나라 은행들은 1970년대 후반 본지점간 온라인 업무를 시작한 이래 1980년대 중반에는 모든 은행들을 연결하여 다른 은행과도 실시간으로 거래가 가능한 금융공동망을 구축하였으며, 1990년대 들어 PC뱅킹(홈뱅킹, 펌뱅킹), 텔레뱅킹 등 대고객 온라인 업무를 시작하면서 전자금융거래라는 새로운 금융서비스를 출현하였으며, 이후 인터넷, 모바일의 등장에 따라 인터넷 뱅킹, 모바일 뱅킹 등 새로운 개념의 전자금융거래가 개발 제공되고 있다.

1) 인터넷 뱅킹

1990년 후반에 등장한 인터넷은 고속의 통신이 가능함에 따라 그 동안 속도가 느려 다양한 형태의 화면을 제공하거나 복잡한 금융거래를 제공할 수 없는 PC뱅킹의 문제를 해결하고 PC

가 있는 곳이면 시간과 장소에 구애됨이 없이 바로 은행에 접속할 수 있어 쉽고 간편하게 금융거래를 수행할 수 있을 뿐 만아니라 수수료가 저렴하여 이용자가 급속히 증가하는 등 새로운 금융거래 수단으로 자리를 잡아가고 있다.

인터넷 뱅킹은 1995년도부터 일부 은행에서 서비스를 시작하였으나, 1996년도에 통신망을 도청하여 획득한 고객정보를 이용하여 고객의 예금을 사취한 사고가 발생함에 따라 보안상 취약점으로 인하여 서비스를 중단하였다. 그 이후 1998년 11월 한국통신 자회사인 Banktown과 은행이 공동으로 개발한 인터넷 뱅킹시스템이 금융감독위원회의 보안성 심의를 통과한 이후 본격적인 서비스가 시작되어 그 역사는 그리 길지 않다고 볼 수 있다.

□ 서비스 업무 내용

인터넷 뱅킹은 자금이체, 대출, 잔액 및 거래내역 조회, 등으로 구분할 수 있다. 다만 신규 계좌개설, 사용자 등록, 신용정보 이용동의 등은 금융실명거래및비밀보장에관한법률[3]에서 요구하는 대면확인으로 인하여 제한되고 있다.

〔그림 1〕 인터넷 뱅킹 서비스 내용

3) 법 제3조(금융실명거래) 금융기관은 거래자의 실지명의에 의하여 금융거래를 하여야 한다.

□ 이용현황

2006. 1/4분기 기준 인터넷뱅킹 서비스를 제공하고 있는 은행은 17개 국내은행과 홍콩상하이 은행 및 우체국 등이 있으며, 고객수는 약 2,700백만명에 이르고 있으며, 인터넷뱅킹을 통한 자금이체 이용건수는 264백만건이며, 자금이체금액은 1,475조원으로 나타났다.[4)]

2) 텔레뱅킹

인터넷 뱅킹의 발달로 인하여 많은 거래가 인터넷 뱅킹으로 전환되었음에도 전통적인 전화를 이용한 텔레뱅킹은 여전히 많은 이용도를 보이고 있다. 이러한 텔레뱅킹은 모든 은행에서 서비스를 제공하고 있으며, 다양한 서비스 보다는 자금이체와 잔액 조회용으로 고객들의 사랑을 받고 있다.

□ 이용현황

2006. 1/4분기 기준 텔레뱅킹 고객수는 약 2,800백만명에 이르고 있으며, 자금이체 이용건수는 162백만건에 금액은 161조원으로 나타났다.[4)]

3) 모바일 뱅킹

무선전화의 발달은 통신과 금융의 융합이라는 새로운 형태의 전자금융거래를 출현시켰는바, 모바일 뱅킹이 바로 그것이다. 모바일 뱅킹은 IC Chip에 계좌번호를 저장하고, 인터넷 뱅킹과 같은 화면을 제공하므로써 기존 텔레뱅킹의 문제인 계좌번호, 주민번호 등 많은 입력을 제거하고, 인터넷 뱅킹에서 제공하는 서비스를 제공하며, 통신내용을 암호화하여 편리성과 안전성을 향상시킨 새로운 개념의 텔레뱅킹이라고 할 수 있다. 이러한 모바일 뱅킹은 2003. 9월 국민은행의 Bank-on을 시작으로 모든 은행들이 서비스를 제공 중에 있다.

□ 이용현황

2006. 1/4분기 기준 모바일 뱅킹 고객수는 약 2백만명으로 급속히 증가하고 있으며, 자금이체 이용건수는 9백만건에 금액은 6천억원으로 나타났다.[4)]

4) 기타 전자금융거래

최근에는 양방향 TV의 개발에 따라 IPTV를 이용한 TV뱅킹이 개발되어 서비스를 제공하고

4) 2006. 1/4분기 전자금융이용 현황(우체국 제외). 2006. 6월 금융감독원 발표

있으나 일반화는 되지 않고 있다. PC뱅킹은 일부 사용자가 있으나 보안상의 문제로 인하여 은행들이 서비스를 점차 중단해가고 있다.

또한 기업이나 개인들의 자금을 원활히 관리해주기 위해 거래은행에서 제공하는 자금관리시스템에 모든 거래 금융회사의 계좌를 등록하면 한 번에 잔액을 조회해주는 자산관리시스템(CMS: Cash Management Service)이 많이 이용되고 있다.

2. 증권사 전자금융거래

온라인트레이딩의 범위는 PC통신, Internet, Mobile, ARS, Web TV 등 다양한 채널을 포함하는 트레이딩시스템과 뉴스, 시황, 기술적 분석, 재무분석 중심의 투자정보시스템으로 분류되어 오다가 현재의 증권사 온라인트레이딩시스템은 투자정보 서비스와 온라인트레이딩이 통합된 환경을 제공하고 있다.

온라인트레이딩 방식을 대표하는 것에 HTS와 WTS가 있다. WTS(Web-based Trading System)은 Web Browser 기반의 매매 시스템이고, HTS는 전용프로그램 기반의 매매시스템을 말한다. 이런 전용 프로그램을 HTS라고 하는 이유는 기존의 PC통신 시절의 명칭을 그대로 사용하기 때문이며 별도의 프로그램을 다운받아서 사용하므로 Emulator 프로그램이라고도 부르기도 한다.

1) 서비스 업무내용

온라인 증권시스템에서 제공하고 있는 업무는 기본적으로 주식, 선물, 옵션, 채권 등 국내 증권시장을 망라하고 있으며, 개별 시장의 조회, 주문, 계좌관리, 매매동향, 금융지표, 챠트분석, 자동매매 등이 제공되고 있다.

〔그림 2〕 온라인증권서비스 내용

2) 이용현황

온라인 증권거래 현황을 살펴보면 2006년 1/4분기중 36개 증권사의 온라인증권거래대금(수탁거래 기준)은 1,532조원으로, 전체 증권거래금액의 약 65.1%를 차지하고 있다.

〈표 1〉 온라인증권거래대금현황 2006년 1/4분기, 금융감독원

(단위: 10억, %)

구 분	'05. 4/4분기(A)		'06. 1/4분기(B)		증 감(B-A)		
	거래대금	비중	거래대금	비중	거래대금	증감률	비중
주 식	519,758	24.4 (39.0)	520,137	22.1 (33.9)	379	0.1	△2.3 (△5.1)
선 물	781,441	36.7 (58.7)	978,223	41.6 (63.8)	196,782	25.2	4.9 (5.1)
옵 션	29,992	1.4 (2.3)	33,620	1.4 (2.3)	3,628	12.1	- (-)
기 타	76	0.0 (0.0)	138	0.0 (0.0)	62	81.6	- (-)
온라인 거래대금	1,331,267	62.5 (100.0)	1,532,118	65.1 (100.0)	200,851	15.1	2.6 (-)
전체거래대금	2,131,790		2,351,059		219,269	10.3	-

3. 사이버 보험

사이버 보험은 업무의 특성상 인터넷 뱅킹이나 온라인 증권거래 업무에 비하여 시작도 늦고 대상 업무도 제한적이기 때문에 크게 활성화가 되지는 못하였다. 그러나 인터넷을 이용한 전자금융업무에 대한 효과가 크게 부각되면서 보험 분야에도 개발이 급속히 증가하고 있다. 특히 자동차 보험에 대한 할인 등의 특정 분야에 대한 서비스로 인하여 그 증가 속도는 급속하게 빨라지고 있는 것이 특징이다.

1) 서비스 업무내용

주로 보험 상품안내를 중심으로 수행되던 업무 형태에서 보험사에서 취급하는 전체의 업무로 서비스 내용이 확대되고 있으며, 조회서비스, 입・출금서비스, 증명서 발급, 자동이체 등의 업무가 제공되고 있다.

2) 이용현황

2006. 1/4분기 중 인터넷 보험계약실적은 3.2만건(68억원)으로 전체 보험계약에서 인터넷 보험계약이 차지하는 비중은 건수기준 0.2%, 금액기준 0.0%로 미미하다. 이러한 인터넷 보험도 대부분 자동차보험을 중심으로 이루어지고 있는바, 이는 보험상품이 다양하고 조건도 까다로워 온라인에 의한 가입을 회피하는 보험계약 특성이 반영된 것이 아닌가 생각한다.

4. 온라인 신용카드

신용카드는 가맹점의 단말기를 이용하거나 은행의 현금출납기를 이용하는 등 Off-line 거래가 일반적이었다. 그러나 인터넷의 출현에 따른 인터넷 쇼핑몰이 발달하면서 온라인 결제가 증가하게 되어 온라인 신용카드의 대부분을 차지하고 있다.

1) 서비스 업무내용

온라인 신용카드는 인터넷 쇼핑몰과 같은 전자상거래에서 발생하는 구매 대금을 신용카드를 이용하여 결제하거나, 카드론, 현금서비스, 거래내역조회 등을 인터넷으로 제공하는 것을 말한다. 신용카드의 발급은 본인확인 문제로 인하여 은행계좌 개설과 마찬가지로 온라인으로 발급되지 않는다.

2) 이용현황

2006. 1/4분기 중 온라인 신용카드 거래건수는 49.3백만건으로 전체 신용카드 거래건수 733백만건의 6.8%를 차지하였으며, 온라인 신용카드 거래건수 중 신용판매가 차지하는 비중은 78.5%이며 현금서비스(18.5%), 카드론(3.0%) 순이었다.

3) 온라인 결제 방법

과거에는 온라인상의 신용카드 결제시에는 신용카드번호, 유효기간, 비밀번호(2자리), 주민번호를 입력하였으나, 해킹 또는 결제과정에서의 정보 유출로 인한 사고위험이 높아 온라인 결제 전용 ID인 안심결제와 안전지불이 사용되고 있다.

○ 안전지불(ISP: Internet Secure Payment): 국민, BC, 우리카드 등이 사용

○ 안전결제: VISA 계열 카드사(ISP 이외의 카드사 전체)가 사용

※ 전자화폐

전자화폐는 고객의 예금을 전자적인 방법으로 IC칩이 내장된 카드(IC카드형)나 인터넷 등 공중통신망과 연결된 PC 등의 매체(네트워크형)에 이전·저장하고 이를 물품 및 서비스 구매 등에 사용할 수 있는 지급결제수단이다.

- 전자상거래 대금지급에 적합한 형태의 전자화폐로 디지캐쉬사의 eCash, 사이버캐쉬사의 CyberCoin 등이 있음

Ⅲ. 전자금융 ISSUE

전자금융거래는 거래의 편리성, 신속성, 낮은 수수료 등의 장점이 있는 반면에 정보유출, 불법거래, 위·변조 등에 의한 사고가 발생될 수 있는 등 다음과 같은 문제점을 가지고 있어 이에 대한 대응책이 요구된다.

□ 고객정보 및 금융거래정보 유출

○ 고객 정보가 유출될 경우 해당 고객의 재산적 피해는 물론 금융회사도 치명적인 신용리스크, 평판리스크, 영업리스크 등의 피해를 입게 된다.

□ 서비스 마비

○ 서비스 마비는 거래 지연, 미처리 등으로 인하여 정보 유출과 같은 리스크 이외에 피해보상에 대한 법률적인 리스크(Legal Risk)가 추가로 발생되게 된다.

□ 거래 과정 장애 또는 결과 오류 등으로 인한 법적 문제

○ 전자금융거래는 온라인상의 비대면 거래로 인하여 거래 성립시점, 거래 내용의 변경 여부, 결과의 전달, 접속수단의 정당성 등 다양한 법률적인 문제가 발생될 수 있다.

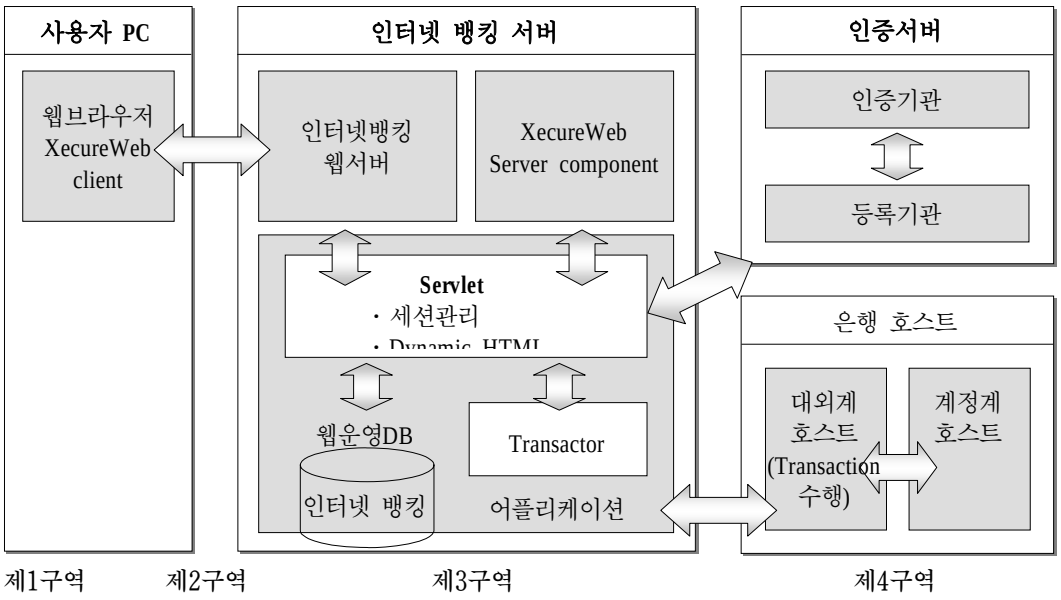
□ 본인 확인 미비로 인한 분쟁 발생

○ 전자금융거래는 사용자-ID, 비밀번호 또는 카드번호, 유효기간 등을 통하여 본인을 확인하고 있고, 거래 내용도 여러 단계를 거치므로 데이터의 위·변조 여부가 매우 큰 문제이다. 이는 사고 발생시 책임 범위에 큰 영향을 줄 수 있어 매우 중요하다.

1. 고객정보 및 금융거래 정보 유출

전자금융업무의 처리 절차는 유형별로 차이가 있고 종류도 다양하여 전체에 대하여는 설명할 수 없으나, 가장 일반적으로 사용되고 있는 인터넷 뱅킹을 예를 들어 각각의 노드에서 어떠한 방법으로 정보가 유출될 수 있으며, 이에 대한 대책은 무엇인가를 설명하고자 한다.

우선 인터넷 뱅킹 구성도를 4개의 단위로 구분하여 개인 PC를 제 1구역, 통신망을 제2구역, Web 서버, 뱅킹서버 등이 위치한 DMZ 구간을 제3구역, 고객정보가 수록된 HOST 부문을 제4구역으로 구분하였다.



〔그림 3〕 인터넷뱅킹 시스템 구성도

1) 사용자 PC 구역(제1구역)

사용자 PC에는 Backdoor 프로그램[5]과 Key Stroke 프로그램 등의 해킹에 의하여 고객이 직접 입력하는 계좌번호, 계좌비밀번호, 인증서 비밀번호, 보안카드비밀번호 등의 정보가 유출될 수 있으며, 공인인증서가 복제될 수 있다.

대책으로는 PC용 방화벽을 설치하고, Key Stroke 해킹방지프로그램을 설치하도록 하고 있다. 특히 이용자들은 금융회사가 설치한 보안프로그램의 작동을 임의로 중단할 경우 사고 발생 시 피해보상을 받을 수 없으므로 각별히 주의하여야 한다.

아울러 최근에는 은행 홈페이지와 동일한 모방사이트를 제작하여 이용자들로 하여금 금융거래 정보를 입력토록 유도하여 입력한 정보를 가지고 범죄에 사용하는 수법, 일명 "피싱(Pshing)"이라는 새로운 형태의 해킹 수법이 등장하여 많이 사용되고 있어 주의가 요구된다. 이러한 피싱은 그 방법과 대응방법이 다양함에 따라 별도로 설명하고자 한다.

5) 백도어 프로그램(trojan horse)은 개인 PC에 설치되어 입력하는 내용을 훔치거나 컴퓨터에 저장된 자료를 복사하는 해킹프로그램으로 패스워드크래킹, Rhost++ 백도어, Checksum과 Timestamp 백도어, Login 백도어, Telnetd 백도어 등이 있다. 자료소스 hcjung@{certcc,kisa}.or.kr

2) 인터넷 통신망 구역(제2구역)

인터넷 통신방법은 모든 사람이 쉽게 내용을 볼 수 있는 개방형 통신방식을 사용하고 있어 도청, 중계기관, 업무담당자 등에 의하여 송·수신되는 정보가 노출될 수 있다.

대책으로는 모든 금융거래정보는 암호화 통신을 기본으로 하고 있으며, 통신사, 중계기관 등의 중간 노드에서의 정보 유출을 방지하기 위하여 고객 PC에서 암호화하여 은행에서 복호화하는 End to End 암호화를 원칙으로 하고 있다.

3) 인터넷 뱅킹시스템 구간(제3구역)

은행에 설치된 시스템으로 해킹이나 내부 직원에 의하여 정보가 유출될 수 있다.

4) 은행호스트 구간(제4구역)

고객원장, 거래기록, 개인정보 등의 중요정보가 집중되어 있고, 프로그램의 개발 등의 사유로 다수의 내부 직원의 접근이 필요함에 따라 이들에 의한 정보 유출 문제가 가장 심각한 부문임

인터넷 뱅킹시스템 구간(제3구역)과 은행호스트 구간(제4구역) 대책은 다음과 같다.

(1) 해킹으로부터의 보호

해킹 공격을 방어하기 위해서는 해킹 공격을 차단하는 침입차단시스템(방화벽)과 침입된 경우 이를 탐지하여 대응하는 침입탐지시스템(최근에는 차단과 탐지가 함께 수행되는 IPS가 개발되어 있음)을 설치하여야 하며, 컴퓨터 바이러스 백신도 최신의 Version을 유지하여 예방과 치료를 병행하여야 한다. 방화벽과 탐지시스템은 그 성능을 보장하기 위해 국가기관에서 평가·인증을 받았거나 국제공통평가인증기준(CC: Common Criteria)을 통과한 제품을 사용하여야 한다.

(2) 내부 직원으로부터의 보호

정보유출사고는 내부 직원들에 의한 경우가 가장 많이 발생하고 있다. 내부직원은 전산업무를 개발하는 전산부서 직원과 이를 이용하는 현업부서 직원으로 구분된다.

전산부서 직원들에 대하여는 담당직무를 상호 견제가 가능토록 분리하여 획득한 정보를 이용하여 사고를 발생시키지 못하도록 하여야 한다. 예를 들어 프로그램 개발과 운영을 분리하고, 개발자는 고객 정보가 수록된 시스템에는 접근을 못하도록 하여 개발 과정에서 고객 정보를 알았다 하여도 사용할 수 없도록 하여야 한다. 아울러 고객원장이나 프로그램 변경에 대한 통제를

철저히 하고 있다.

현업부서 직원들에 대하여는 일일감사를 철저히 하고 주요 거래에 대하여는 책임자 승인거래를 사용토록 하여야 한다, 아울러 업무와 관련 없는 고객정보의 접근을 엄격히 금지하여야 한다.

2. 서비스 마비

금융회사들은 서비스 마비를 방지하기 위해 컴퓨터는 물론 전력, 통신망 등 주요 기기들을 이중으로 구성하고 있다. 아울러 전산센터 마비를 방지하기 위해 재해복구센터를 구축하여 전산센터 마비시 3시간 이내에 정상적인 서비스를 재개할 수 있도록 준비하고 있다.

정부와 금융감독당국에서도 금융전산분야를 자연재해, 인적재해(테러, 파업), 전자적침해(해킹, 컴퓨터 바이러스), 기술적 재해(기기, 프로그램오류)의 4가지 유형의 재해로 분류하고 위기수준에 따라 관심, 주의, 경계, 심각의 4단계로 구분하여 위기관리를 하고 있다.

3. 거래 과정 장애 또는 결과 오류 등으로 인한 법적 문제

현재 전자금융거래의 사고에 대한 피해보상은 은행들이 공동으로 제정한 전자금융거래기본약관에 의하여 피해보상을 해 주고 있다. 개인이 고의 또는 과실이 아닌 것으로 확인 되면 금융회사들은 피해보상을 해주고 있다. 그러나 고의나 과실이 아니라는 것에 대한 입증을 개인이 하도록 되어 있어 피해보상을 받기까지는 매우 복잡한 과정을 거쳐야 한다.

2007. 1. 1부터 발효되는 전자금융거래법[6]에서는 사고 발생시 개인에 대하여는 고의・과실이 아닌 경우 금융회사가 피해보상을 해주고, 고의 과실에 대하여도 금융회사가 입증하도록 책임을 부과하고 있다.

4. 본인 확인 미비로 인한 분쟁

전자금융거래가 갖는 비대면 거래로 인하여 거래에 필요한 접근 매체의 발급은 매우 중요하

6) 전자금융거래법
전자금융거래의 법률관계를 명확히 하여 전자금융거래의 안전성과 신뢰성을 확보하고, 전자금융업의 건전한 발전을 위한 기반조성을 함으로써 국민의 금융편의를 꾀하며, 국민경제의 발전에 이바지함을 목적으로 2006. 4월 제정

다. 현재 전자금융거래시 필요한 접근 매체는 OTP(보안카드 포함), 공인인증서 등이 있으며, 이들을 발급받기 위해서는 금융회사 영업점을 방문하여 본인을 확인하여야 한다. 이때 위조된 신분증을 이용하여 접근매체를 발급받아 범행에 사용하였다면 발생된 피해에 대하여는 신원확인을 소홀히 한 해당금융회사가 책임을 지도록 하고 있다.

Ⅳ. 전자금융거래 보호 장치 및 이용방법

1. 전자금융거래 보호 장치

1) OTP(One Time Password)

계좌비밀번호는 거래시마다 변경이 불가능하다. 고정되어 있어 해킹에 의하여 쉽게 유출될 수 있다. 따라서 계좌비밀번호만으로는 사고를 방지 할 수가 없어 계좌비밀번호이외에 거래시 다른 비밀번호를 사용하여 사고를 방지하기 위해 도입된 것이 OTP다. 이러한 OTP는 비밀번호 발생기와 보안카드 형식이 있다. 현재 일반화되어 있는 보안카드는 비밀번호의 개수가 35개로 한정되어 있어 해킹이 쉽게 되어 기업고객과 1억원 이상 이체할 경우에는 수천 개의 비밀번호를 발생시키는 OTP 발생기를 사용토록 하고 있다. OTP는 가격이 비싸고, 소지가 불편하여 한개의 OTP로 모든 금융회사를 공통적으로 사용할 수 있도록 하기 위해 OTP통합인증센터를 구축중에 있으며, 2007년 초에 업무가 시작될 것이다.

2) 공인인증서

OTP는 비밀번호를 이용하여 거래의 안전성을 확보하고 있다. 그러나 누군가가 거래한 사실에 대하여 부인 할 경우 금융회사는 본인이 거래했다는 사실을 입증하여야하는데 본인이 부인할 경우 입증이 쉽지 않다. 이러한 문제점을 방지하기 위해 전자서명을 사용하고 있으며, 사용된 전자서명이 법[7]에 의하여 설립된 공인인증기관[8] 발급하였다는 것을 입증하기 위해서 공인인증서를 발급하고 있다.

---

7) 전자서명법: 전자문서의 안전성과 신뢰성을 확보하고 그 이용을 활성화하기 위하여 전자서명에 관한 기본적인 사항을 정함으로써 국가사회의 정보화를 촉진하고 국민생활의 편익을 증진함을 목적으로 2001. 12월 제정.

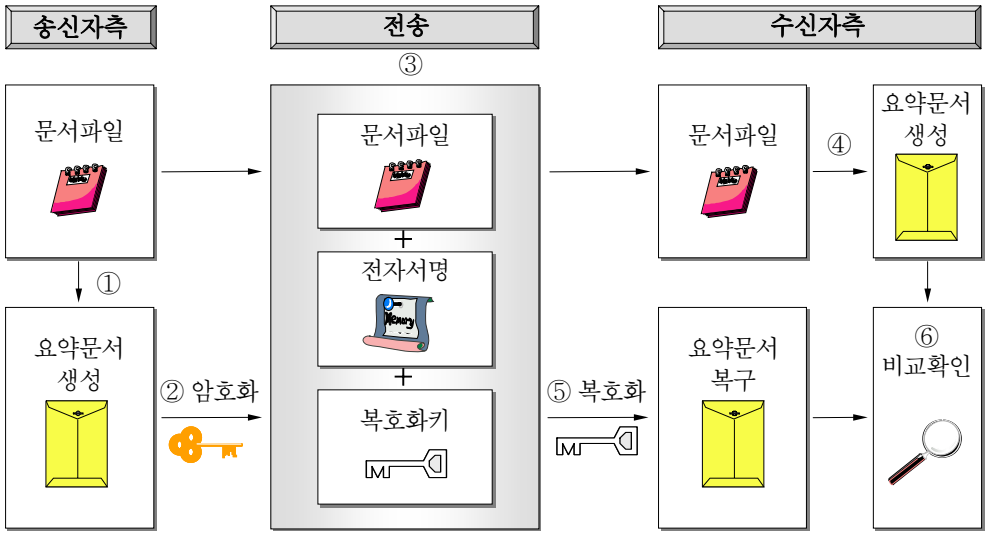
8) 한국전산원, 금융결제원, (주)KOSCOM, (주)한국정보인증, (주)한국전자인증, (주)한국무역정보통신

이러한 공인인증서는 거래사실에 대한 부인을 방지하는 부인방지 기능과 제출한 거래내역이 변경되지 않았음을 보증하는 무결성 보증 등의 기능을 갖고 있다.

공인인증서는 인터넷 뱅킹, 사이버증권거래, 사이버보험, 전자상거래 등에서만 사용이 가능하며, 텔레뱅킹은 공인인증서 저장이 불가능하여 사용을 하지 않고 있다.

○ 송신자가 개인의 전자서명 생성키를 이용해 암호화한 전자문서와 동 문서파일의 요약메세지에 의한 전자서명을 전송하고, 수신자는 전자서명 검증키를 이용해 전자문서와 요약메시지를 읽고, 수신 받은 요약 메시지와 원본에 의해 생성된 요약 메시지를 상호 비교하여 문서의 변조여부를 확인

〈전자서명의 검증절차〉



(송신자측)
① 송신하고자 하는 파일을 이용하여 고유한 요약메시지를 생성
② 동 요약메시지와 전자서명 생성키를 이용하여 전자서명을 생성
③ 원본 파일과 전자서명, 공인인증서(복호화키 포함)를 수신자에게 전송

(수신자측)
④ 수신된 원본파일을 이용하여 고유한 요약메세지를 다시 생성
⑤ 전송받은 전자서명 검증키를 이용하여 전자서명으로부터 압축메시지를 복구
⑥ ④, ⑤에서 생성된 압축메시지를 비교하여 서명자 신원 및 문서 위변조 여부확인

〔그림 4〕 전자서명 공개키기반구조(public key infrastructure) 인증시스템 처리절차

2. 안전한 전자금융 이용방법

1) 금융회사에서 제공하는 보안프로그램을 반드시 설치하기

전자금융거래를 위해 금융회사의 홈페이지에 접속하면 해당 금융회사에서 제공하는 보안프로그램이 자동적으로 설치됩니다. 이 때, 임의로 설치를 중단하거나 설치된 보안프로그램의 실행을 중지시키지 않아야 합니다. 또한 자동적으로 설치가 되지 않을 경우에는 설치 안내에 따라 수동으로 보안프로그램을 꼭 설치한 후에 전자금융거래를 해야 합니다. 이는 금융거래 내용을 타인에게 노출되지 않도록 하기 위함입니다.

2) 전자금융에 필요한 정보는 수첩, 지갑 등 타인에게 쉽게 노출될 수 있는 매체에 기록하지 않고 타인에게(금융회사 직원을 포함) 알려 주지 않기

전자금융 거래에 필요한 정보가 타인에게 알려지는 일이 없도록 분실가능성이 있는 수첩, 지갑 등에는 관련 정보를 기록하지 말아야 합니다. 또한, 타인에게 절대 전자금융거래 관련 정보를 알려주지 말며, 특히 은행 직원을 사칭하여 정보를 취득하는 경우가 있으므로, 은행창구가 아닌 곳에서는 은행직원이라고 말 하더라도 금융정보를 알려주지 말아야 합니다. 금융기관에서는 전화나 메일 상으로 개인의 금융정보를 요구하지 않습니다.

3) 금융 계좌, 공인인증서 등의 각종 비밀번호는 서로 다르게 설정하고 주기적으로 변경하기

비밀번호는 본인확인을 위한 수단이므로 생일, 전화번호 등과 같이 타인이 알기 쉬운 번호를 사용해서는 안 됩니다. 또한, 가능한 범위에서 비밀번호 자릿수를 최대한 늘리고, 영문자도 혼합·사용하며, 각각 다른 번호를 사용하고, 주기적으로 변경하여 타인이 비밀번호를 예상하지 못하도록 해야 합니다.

4) 금융거래 사이트는 주소창에서 직접 입력하거나 즐겨찾기로 사용하기

스팸메일 본문이나 게시판, 대출사이트 등에 링크되어 있는 URL을 그대로 클릭할 경우 개인정보나 금융정보를 빼내 가려는 해당 기관의 사칭사이트로 연결될 수 있기 때문에 금융거래 사이트는 주소창에 올바른 주소를 직접 입력하거나 즐겨찾기에 추가하여 사용해야 합니다.

5) 전자금융거래 이용내역을 본인에게 즉시 알려주는 휴대폰 서비스 등을 적극 이용하기

금융회사에서는 신용카드 사용내역, 계좌 이체내역 등 전자금융거래 이용내역을 실시간으로

휴대폰 SMS나 메일을 통해 알려주는 서비스를 제공하고 있으니, 이를 적극적으로 활용하시어 타인이 무단으로 전자금융거래를 이용하였을 경우 곧바로 이를 신고하여 피해를 예방할 수 있도록 해야 합니다.

6) 공인인증서는 USB, 스마트카드 등 이동식 저장장치에 보관하기

공인인증서는 신원확인 및 거래사실 증명 등을 위해 사용되는 중요한 거래 수단이므로, 해킹 위험을 예방하고 공인인증서를 보다 안전하게 이용하시기 위해서는 하드디스크에 저장하여 사용하는 것보다는 이동식 저장장치를 활용하시는 것이 좋습니다. 또한, 이동식 저장매체를 이용하면 어느 PC에서든 공인인증서를 편리하게 이용하실 수 있습니다. 단, 이동식 저장장치를 분실하지 않도록 유의해야 합니다.

7) PC방 등 공용 장소에서는 인터넷 금융거래를 자제하기

여러 사람이 사용하는 공용 PC는 바이러스나 트로이목마 등 악성코드가 설치되기 쉬어 해킹 당하기 쉽습니다. 또한 공용 PC에서 공인인증서를 다운받아 전자거래를 이용할 경우 개인정보나 비밀번호 등 금융거래 정보의 노출 위험이 있습니다. 따라서, 공용장소에서는 가급적 전자금융 거래 이용을 하지 않는 것이 좋습니다.

8) 바이러스백신, 스파이웨어 제거프로그램을 이용하고 최신 윈도우보안패치를 적용하기

백신프로그램과 스파이웨어 제거프로그램은 pc의 보안을 위해 꼭 설치하며, 컴퓨터가 시작되면 자동 실행 및 자동 업데이트 되도록 설정합니다. 또한 윈도우즈 취약점을 이용한 해킹이나 웜바이러스를 막기 위해 윈도우 보안패치를 설치하고, 최신 업데이트를 유지하기 위해 자동 업데이트 기능을 이용하도록 합니다.

9) 의심되는 이메일이나 게시판의 글은 열어보지 말고, 첨부파일은 열람 또는 저장하기 전에 백신으로 검사하기

출처가 불분명하고 본문 내용이 본인과 직접적인 관련이 없는 경우 메일이나 게시물은 삭제하거나 무시하고, 꼭 필요한 경우에는 실행하거나 저장하기 전에 반드시 백신으로 점검하여 바이러스나 악성코드에 감염되지 않았는지 여부를 확인하여야 합니다.

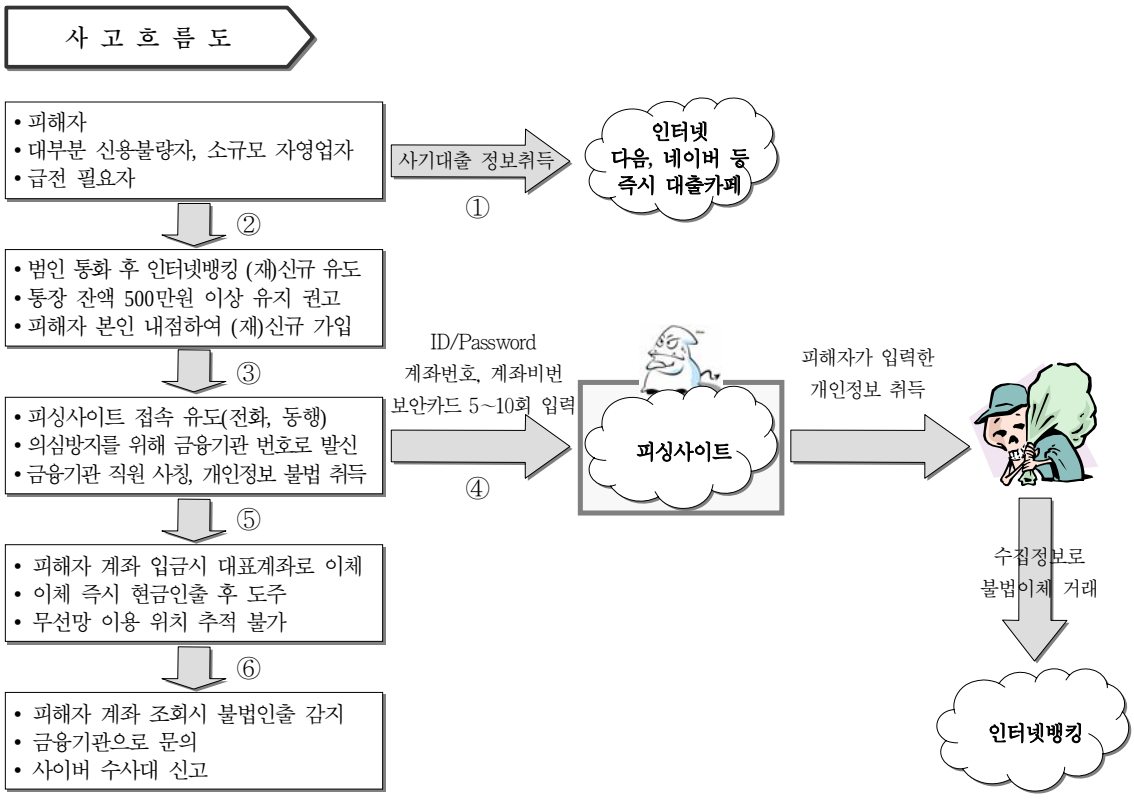
10) 선수금 입금 요구, 상식수준 이상의 대출 조건을 제시하는 경우 해당 금융회사에 동 대출 취급여부를 직접 확인하기

최근 인터넷 포털 사이트 등에 신용에 관계없이 즉시대출을 해준다는 등 상식수준 이상의 대출 조건을 제시하는 광고를 게재한 후 이를 통해 급전이 필요한 사람에게 접근하여 은행직원을 사칭, 거래실적이 필요하다면서 돈을 입금토록 하는 등 선수금 입금을 요구하는 사기 금융사고가 발생하고 있으므로 이에 유의해야 합니다.

3. 주요 사고사례

1) 2005. 9월에 국내 모 은행에서 발생한 피싱을 이용한 예금인출사고

(1) 사고개요



〔그림 5〕 주요 사고흐름도

피해자 A는 평소 금전적인 어려움을 갖고 잊던 차에 인터넷 사이트에서 좋은 조건에 대출을 해준다는 광고를 보고 해당 사이트에 접속을 하여 범인들과 접촉을 시작하였고 이후 범인들의 요구대로 보증금을 입금하고 보안카드 비밀번호, 공인인증서 비밀번호를 알려준 결과 입금된 보증금을 사취 당하였다.

(2) 피해보상

동 사고는 피해자 본인이 인터넷 뱅킹 거래에 필요한 보안카드, 공인인증서 의 비밀번호를 알려준 사고로 고객의 과실에 해당되어 피해보상을 받기가 어려웠다.

(3) 시사점

범인들은 피해자를 안심시키기 위해 은행의 인터넷 뱅킹과 동일한 모양의 사이트를 만들었고 은행의 전화번호로 발신자 번호를 남기는 등 일반인이 의심할 수 없을 정도로 교묘하게 위장하였다. 그러나 비밀번호를 전화로 알려달라는 것과 대출 보증금을 미리 입금시켜 달라고 하는 것 등은 정상적인 금융기관에서는 발생하지 않는 것으로 피해자가 조금만 주의를 기울였으면 방지할 수 있는 경우로 판단된다.

2) 2005. 5월에 국내 모 은행 인터넷 뱅킹 해킹사고

(1) 사고개요

2005. 5. 10 ○○은행 고객 B모씨(42, 여)는 본인의 통장에서 5,000만원이 인출된 사실을 확인하고 해당은행 및 경찰청에 신고하였다.

(2) 범행수법

범인은 피해자는 유명웹사이트의 게시물에 해킹프로그램을 첨부하는 방법으로 B씨의 컴퓨터에 입력내용을 절취할 수 있는 해킹프로그램을 설치하여 획득한 정보를 이용, 고객의 계좌에서 5,000만원을 인출하였다.

(3) 문제점

인터넷 뱅킹은 입력정보의 유출을 방지하는 프로그램을 작동하도록 되어 있으나 해당 은행은 사고 발생시 방지프로그램이 작동되지 않았다.

(4) 피해보상

해킹방지프로그램이 고객의 중단 조치가 없었음에도 작동되지 않는 것은 은행의 책임사항으로 피해금액 전액을 은행에서 보상하였다. 만약 고객이 방지프로그램의 작동을 인위적으로 중단

시켰다면 고객의 과실로 인정되어 피해보상을 받기가 어려웠을 것으로 판단된다.

Ⅴ. 결 론

전자금융거래는 서비스가 다양해지고, 새로운 이용 수단들이 등장함에 따라 이용자들이 지속적으로 증가하고 있으나, 정보유출, 범죄노출위험이 증가하고 있으며, 해킹, 피싱 등의 새로운 범죄 수법도 나타나고 있어 이용자들을 더욱 불안하게 하고 있다.

다행히 전자금융거래법이 2007. 1. 1부터 발효되어 각종 안전대책이 마련될 것이며, 사고 발생 시 개인 이용자들의 입증책임이 없어지고, 피해보상이 용이하게 되었지만, 본인의 실수나 과실에 대하여는 피해보상이 되지 않는다는 점을 명시하여야 할 것이다.

정보보호 강화는 이용의 편리성을 저해하고 비용투자를 요구하는 것으로 이용상 다소 불편한 점이 있다하여도 이용자들의 이해가 필요하다고 생각한다.

정부나 금융회사에서는 최상의 안전대책을 강구하여 고객들이 안심하고 전자금융거래를 이용할 수 있도록 노력을 다해야 할 것이다.

참 고 문 헌

전자거래법. 사법연수원, 2002.
전자거래기본법 및 시행령. 2002. p.50
전자서명법 및 시행령. 2002. p.50
김영진, 최형광 공저, IT 재해복구 전략과 구현, 전자신문사. 2002. 3.
전자금융거래 기본약관. 2002. p.50
금융기관 전자금융업무감독규정 및 시행세칙. 금융감독원. 2001. 4
금융기관 IT부문 비상대응방안. 금융감독원. 2001. 10
계좌통합서비스 도입에 감독대응방안. 금융감독원. 2001. 6
IT 및 전자금융업무 안전성 제고 대책 방안. 금융감독원. 2003. 4
IT 검사업무편람. 금융감독원. 2000. 12

김진환. 약관의 계약편입과 전자약관. 2001. 6

전자서명과 전자인증제도에 관한 법률적 연구. 김호영. 2001. 2.

UNCITRAL모델법. UN 국제상거래법위원회

Donald L. Pipkin, Information Security Protecting the Global Enterprise. www.hp.com

Information Systems Examination Handbook. FFIEC. 1996.

Risk Management Principles for Electronic Banking. BIS. 2001. 5