通信情報保護學會誌
第1卷, 第2號, 1991. 8

금융전산망 안전대책에 관한 고찰

조이남* · 김형근*

1. 서 론

1972년 한국 외환은행의 보통예금 온라인 시스템 개발을 효시로 70년대 후반 시중은행을 중심으로한 금융기관들은 은행업무 전산화에 박차를 가해왔고 '84년 금융전산망 기본 추진방안이 확정됨에 따라 금융결제원을 센타로한 은행간 네트웍이 구축되어 '88. 7월 CD 업무를 기점으로 음성정보 시스템(ARS, Automatic Response Service) 및 타행환 서비스를 실시하게 되었다.

또한 최근 국제적인 전산화 경향에 맞춰 금융전산망에서도 PSTN(Public Swithed Telephone Network)을 통한 고객거래 내역에 대한 음성정보 서비스 뿐만 아니라 다량의 고객정보를 취급할 수 있는 팩시밀리 및 퍼스널컴퓨터 서비스도 조만간에 실시할 예정으로 금융전산망에서 취급되는 고객의 금융정보도 더욱더 다양, 확대될 것이다.

이에 따라 금융전산망의 안전에 관한 대책이 통신네트웍을 포함한 중계 센터와 각행 시스템의 하드웨어 및 소프트웨어에서 포괄적으로 검토되어져야 한다. 특히 고객 금융거래 내역의 누설이 법상에도 금지되고 있듯이 이를 위하여도 각종 보안대책이 마련되어져야 한다.

본고에서는 이러한 취지에서 금융전산망에 필요한 하드웨어, 소프트웨어적인 조치 및 통신설비상에 대한 문제와 시스템 보안문제를 검토하여 금융전산망 운영의 안정성 향상 방안에 대한 대책을 고찰하고자 한다.

2. 금융전산망의 일반적인 보안대책

2.1 컴퓨터 시스템의 사고 유형

컴퓨터를 이용한 범죄행위를 일정한 기준에 의하여 분류해 보려는 시도는 그 분류방법이 아직 확립되어 있지 않아 학자에 따라 그 유형을 다르게 하고 있다. 따라서 본고에서는 금융업무와 관련한 경험적 기준에 의하여 ① 컴퓨터 부정사용 및 조작, ② 컴퓨터 파괴, ③ 컴퓨터 스파이, ④ CD 범죄로 분류코자 한다.

① 컴퓨터 부정사용 및 조작

컴퓨터의 부정사용 및 조작은 컴퓨터의 유자격자 또는 무자격자가 본인의 부정한 목적을 위하여 컴퓨터를 사용하거나 컴퓨터의 처리결과 혹은 인쇄출력 등을 변경하여 자신의 재산적 이익을 얻기 위하여 자료처리 영역의 부분적인 변경을 수행하는 것이다.

* 정회원, 금융결제원

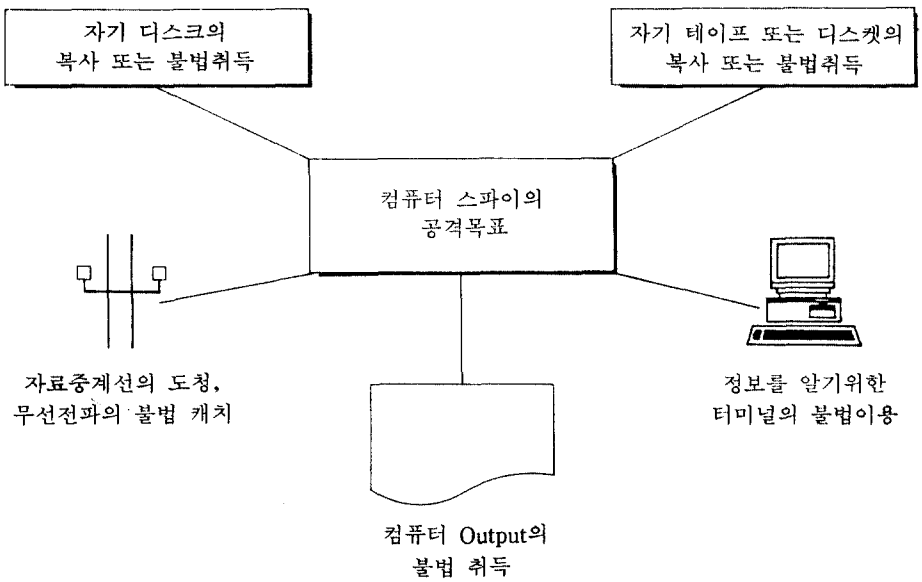


그림 1. 컴퓨터 스파이의 공격목표

1981년도 S 은행에서 발생한 은행지점 대리가 예금계좌 2개를 개설한 후 단말기로 각각 현금을 대체 입금한 사건이 있었는데 컴퓨터 부정 조작의 대표적인 예라 하겠다.

② 컴퓨터 파괴

컴퓨터의 파괴는 컴퓨터 자체, 컴퓨터 프로그램, 컴퓨터 내부나 외부 기억장치에 기억되어 있는 자료를 객체로 하는 파괴 행위를 말한다. 만약 금융공동전산센터의 시스템이나 프로그램의 파괴 행위가 이루어진다면 이는 국민경제나 국가 경제의 막대한 손실을 초래할 것이다.

또한 통신 네트워을 통한 컴퓨터 프로그램 및 데이타를 파괴할 수 있는 핵커들의 침입이 날로 점증되는 시점에서 이에 대한 보안대책이 마련되어야 할 것이다. 이러한 사례에 대한 국내 자료는 입수하지 못했으나 미국에서 발생한 사건으로 뉴욕의 한 회사에 근무하는 프로그래머가 해고될 듯한 예감이 들자 자신의 프로그램을 변경하여 어떤 상황이 발생하면 컴퓨터 자료를 파괴하는 프로그램을 삽입하여 그가 해고된 후 데이타를 무조건 파괴시켰던 예가 있다.

③ 컴퓨터 스파이

컴퓨터 스파이란 컴퓨터 시스템 자료를 권한 없이 획득하거나 누설하여 타인에게 재산적 손해를 야기시키는 행위를 말하며 앞으로 금융전산망이 확대되어 더욱더 많은 고객정보를 처리 다루게 됨에 따라 고객 경쟁기업 등에 누출되어 불법적으로 활용될 가능성이 있기 때문에 이 부분에 대하여도 포괄적인 대책 수립이 필요하다. 이에 대한 유형이 그림 1에 나타나 있다.

1988년 모 회사에서 S/W 및 회로기판을 훔쳐내 경쟁회사에 판매한 사건이 발생한 사례가 있었다. 이들은 컴퓨터 프로그램 보호법 위반 및 절도혐의로 검찰에 의해 구속영장이 청구되었다.

④ CD 카드의 범죄

CD 범죄란 현금 자동지급기(CD기)를 중심으로 발생하는 범죄로 카드의 취득방법에 따라 우연히

습득하거나 절취한 경우 위·변조하여 사용한 경우가 있다.

사례로는 '89년 10월 춘천에서 CD기에서 우연히 습득한 CD용 카드로 여러 지점의 CD기에서 현금을 인출한 사건이 발생했다.

특히 CD 시스템은 1975년 외환은행에서 처음 도입하여 시설한 이래 거의 모든 기관에서 이를 설치하고 금융전산망 업무도 이 업무를 최초로 시행하여 '91년 현재 일 10만건 정도를 처리하고 있을 정도로 현금을 선호하는 우리나라 환경에서는 중요한 업무이다.

또한 일본에서 1971년부터 '83년까지 발생한 사고 중에 98.2%를 CD와 관련하여 발생했을 정도로 컴퓨터 범죄중에 가장 큰 비중을 차지한다. 따라서 이에 대한 보안대책을 철저히 수립하는 것이 필요하다.

2.2 금융전산망과 관련한 보안문제 유형

앞에서 언급한 컴퓨터 시스템 사고유형에 따라 현 금융전산망 시스템의 구성(그림 2)에 필요한 보안종류를 나열하면 다음과 같다.

① 창구 단말의 보안

창구단말의 보안은 은행지점에 설치된 단말을 이용하여 고객 금융정보의 부정취득, 또는 부정계좌에 대한 입금 및 오조작에 대한 입금, 무자격자의 무단점유 등 창구단말에서 발생할 수 있는 사고에 대한 보안이다. 창구 직원의 고의적인 행동에 의하여 이러한 유형의 사고는 쉽게 이루어질 수 있고, 은행의 공신력에 영향을 미쳐 이를 철저히 예방할 수 있는 보안대책이 수립되어야 한다.

② CD상의 부정 사용

CD상의 범죄는 CD의 보급 확대가 증가함에 따라 범죄 발생 가능성도 그만큼 많아지며, 특히 옥외 CD가 설치되어 이에 대한 보안의 문제도 중요하게 취급되어야 할 것이다. CD기 상에서 사고 카드의 회수방법, 인출금액 제한, 비밀번호 검증 횟수 등의 문제뿐만 아니라 CD의 암호화 등을 추진하여 위, 변조 등에 대비하여야 한다.

③ 무자격자의 단말 Access

사용자의 적절한 Access 통제를 하지 않으면 다량의 고객정보에 대한 누출과 소프트웨어의 불법적 Copy 등을 당할 가능성이 높아진다. 따라서 이에 대한 식별방법과 데이타 Access 접근의 제한 및 패스워드의 관리체제가 체계적으로 이루워져야 한다.

④ 통신회선상의 보안

통신회선상에서 누화, 도청 등에 의하여 고객정보전문의 누출 또는 변경 등이 가능하다.

특히 금융전산망의 전문등은 표준화되어 제 3 자가 이에 대한 정보를 쉽게 판독할 수 있다. 따라서 암호화 기법의 도입 등 필요한 조치를 취하여 누화, 도청, 전문의 변경 등에 대비하여야 한다.

또한 통신회선상의 신뢰성을 유지하기 위하여 중앙집중식의 네트웍 관리체제가 필요하다.

⑤ 시스템의 보안

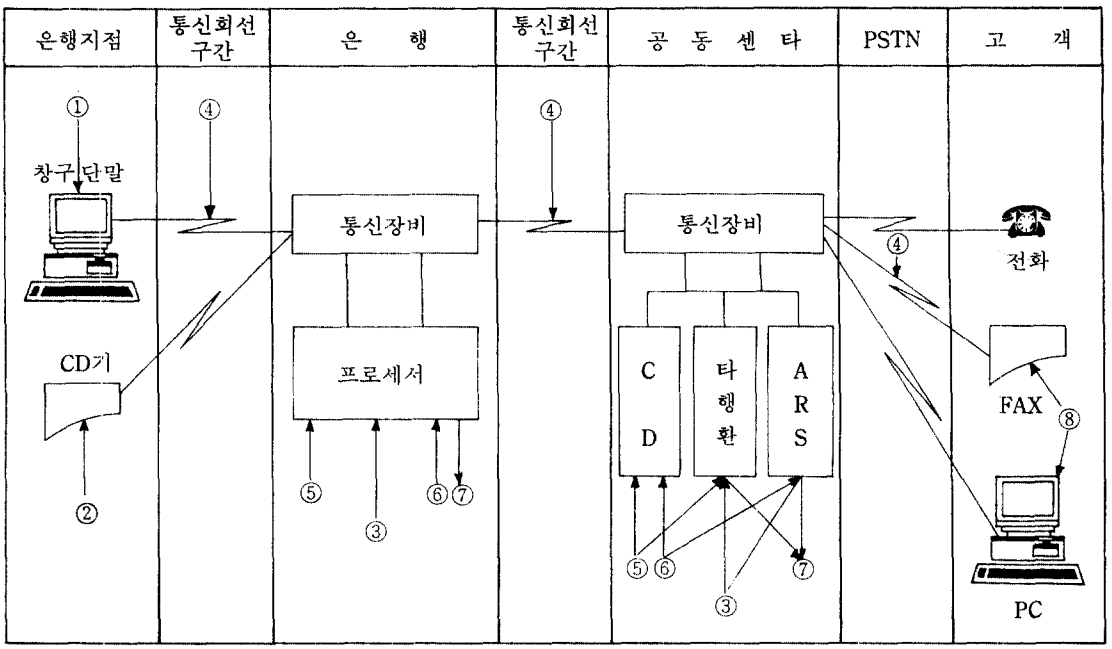
제 3 자에 의한 시스템의 파괴나 자연재해와 화재 등으로 인한 시스템의 파괴는 크나큰 재산적 손실을 가져온다. 이를 위한 입지선정, 공조설비, 전원장치 등의 설계 및 시스템의 출입자 감시 등에 대한 포괄적인 대책이 필요하다. 또한 시스템 장애시 시스템 운영이 가능하도록 무정지(Fault Tolerant) 시스템의 채택이 바람직하다.

⑥ 소프트웨어의 보안

소프트웨어는 그 종류별로 운영체제 및 데이타 관리 소프트웨어, 각종 UTILITY 응용프로그램과 패케이지, 업무용 프로그램으로 분류할 수 있다. 이에 대한 불법적인 Access, 핵커 등의 침입 등은 자칫 시스템의 안정성에 크나큰 영향을 미칠수 있다. 따라서 이들에 대한 Back-up 체제, 등록관리 체제, Access 금지 등에 대한 대책 마련이 필요하다.

⑦ 정보누설

자기테이프 및 디스크, 인쇄 출력물 등에 의한 정보의 누설은 다량의 정보가 불법적으로 이용될 수 있기 때문에 이들에 대한 보관장소 및 기록방법, 폐기방법, Access 금지 등 대책이 마련되어야 한다.



① 창구단말의 보안
② CD의 부정 사용
③ 무자격자의 단말 Access
④ 통신회선상의 보안
⑤ 시스템의 보안
⑥ 소프트웨어의 보안
⑦ 정보 누설
⑧ 고객단말의 부정 이용

그림 2. 금융전산망의 보안 유형

현재 금융전산망에서는 사고시 거래내역을 확인하기 위한 방법으로 거래기록 자료를 일정 기간 보관하고 있으며, 이에 대한 보관방법은 비밀번호를 생략하여 누출시의 사고에 대비하고 있다.

⑧ 고객 단말의 부정 이용

이는 ARS(Automatic Response Service)에서 센타와 고객 사이에 직접 연결되어 있는 단말을 무자격자가 부정 Access하여 정보를 취득하는 경우로 이에 대비하기 위하여 고객 패스워드 입력 및 비밀번호 점검 등 필요한 조치를 수행할 예정이나, 부정 취득한 고객 암호등을 사용하는 경우는 이에 대비할 적절한 조치가 불가능한 실정이므로 고객 스스로가 철저한 관리를 수행하여야 한다.

2.3 시스템상의 보완 대책

자연적, 인위적 피해로부터 정보자원을 보호하며, 주요 정보자원에 대한 실체적 접근 통제와 지속적 접근 감시에 의한 안정성 평가, 정보시스템 작동의 지속성을 유지하여야 한다.

이를 위하여는 정보처리센터의 위치 및 구조, 접근통제(Access Control), 자연 재해방지를 위하여 필요한 조치(표 1 참조)를 하여야 하며, 신뢰성 향상을 위하여 분산 처리시스템을 이용한 지역별 백업 체제 및 무정지 시스템의 구축과 중요한 화일의 이중 보안 등의 조치가 필요하다.

또한 운영조작시의 신뢰성도 중요한 요소이므로 시스템 운용시의 신뢰성을 향상시키기 위하여 오퍼레이션의 단순화 및 자동화, 타당성 검토기능이 충실히 지켜져야 한다.

표 1. 시스템 보안에 필요한 주요 점검사항

점검대상	점 검 사 항
설치장소	- 홍수, 악천후, 지진, 전기장등 - 통신설비 이용성 - 건물에 대한 보안(범죄 우발지역, 외부와의 차단) - 긴급시 경보체제 - 교통환경 - 화 재
접근통제 (Access Control	- 부정출입 및 정보자원의 이동 통제 - 안전구역의 설정 - 운영중 출입 통제 - 방문객 통제 - 추가 안전통제(CCTV 등)
내부설계	- 전력 콘트롤 - 습도 콘트롤 - 냉·난방 콘트롤 - 먼지 콘트롤 - 화재 콘트롤 - 비상시의 조치
기 타	- 자료매체의 보관 - 주요 S/W 및 Document 보호 - 안전대책에 대한 정기 점검 - 안전교육 - 지원시설의 보호(전원, 통신선로, 공조설비 등) - 자기장으로부터의 보호(자기장으로부터 건물 외벽이 50m이상 분리) - 정전기 피해 방지 - 보험(장비, S/W, DATA등)

2.4 네트웍상의 보안대책

네트웍상의 주요한 보안 유형은 통신회선의 신뢰성 유지와 전송데이타의 보안유지이다.

통신회선의 신뢰성 유지를 위한 조치로는 적정 전송회선의 선택, 표준의 통신장비(Modem, Multiplexer)의 사용, 전송 오류에 대한 검출과 정정 절차 등 종합적인 회선관리 등이 필요하다.

현재 금융전산망에서는 사용 통신회선의 신뢰성을 유지하기 위하여 중계센터에 회선관리 시스템(Network Management System)과 Intelligent Modem을 사용하고 있으며, 전송 에러의 검출 및 정정을 위하여 CCITT X.25 Protocol을 채택하고 있다.

금융전산망에서 통신상의 신뢰도의 향상 및 오류점검을 위하여 설치된 회선 관리시스템은 표 2와 같은 기능을 수행하여 장애 발생시 복구를 위한 신속한 조치를 취하고 있다.

회선상의 전송 DATA의 보안을 위하여는 암호화 기법을 우선 들 수 있다.

암호화 기법은 암호화에 필요한 시간과 비용에 따라 분류될 수 있으며, 기술적인 유형으로는 전치 암호화(Transposition Ciphers), 대치 암호화(Substitution Ciphers)와 Product Cipher가 있다.

① 전치 암호화(Transposition Ciphers)

위치교환법이라고도 하며 문자열내의 데이타의 자리바꿈을 기본으로 한다.

예) 전 문 : PEACE IS OUR OBJECTIVE
암호문 : EPCA ESIO RUO JBCEITEV

이 방법에는 통계적 방법 등에 의하여 쉽게 해독될 수 있기 때문에 중요 데이타 보호에는 이용되지 않는다.

② 대치 암호화(Substitution Ciphers)

특정한 문자열을 암호 Key로 하여 평문을 암호화하여 이를 규칙에 따라 전문을 대치하는 방식이다. 이 방법도 철자의 빈도 분포에 의한 통계적 해독이 가능한 단점이 있으므로 한 문자가 아닌 문자 블럭단위로 암호화 하여 해독을 어렵게 한 것도 있다.

예)

평 문 철 자 : ABCDEFGHIJKLMNOPQRSTUVWXYZ
암호문 철자 : UNCOPYRIGHTABLEDFJKMQSVWXZ
암호 KEY
전 문 : PEACE IS OUR OBJECTIVE
암 호 문 : DPUCP GK EQJ ENHPCMGSI

③ Product Cipher

표 2. 공동망 NMS의 주요 점검사항

점 검 사 항	설 명
Receive Level	수신 레벨을 체크한다(12−25db 양호).
Signal to Noise Rate	Analog Signal과 Noise의 비율을 체크(15−35db 양호)
Error Probability	30−70을 양호로 함
Phase Jitter	연속적인 위상변화 체크(15db 이상이면 불량)
Gain Hit	수신되는 Level에 Hit 현상이 일어나는 경우(15db 이상이면 불량)
Impulse Hit	순간적으로 일어나는 높은 진폭잡음 체크(25db이면 불량)
Drop out	신호의 진폭이 순간적으로 떨어지는 현상(5db 이상이면 불량)
Frequence Offset	신호의 주파수 편이현상 체크(±5db내의 상태유지)
Retain	회선상태가 좋지 않아 모뎀간 통신이 자주 두절될때 상태 체크
Harmonic Distortion	신호의 감소가 진폭에 따라 변화상태가 심하면 analog를 digital로 복조하는데 미치는 영향(25db 이하여야 한다)

전치 암호화와 대치 암호화를 조합하여 암호화하는 방식으로 강력한 암호능력을 갖고 있어 오늘날 가장 널리 이용되는 방식이다. 이는 세계 제2차 대전을 기점으로 등장하게 되었으며, 현재 여러가지 암호화 제품이 나와 있다. 특히 Shannon에 의해 발표된 암호화 기법은 현대 암호화 이론에 크게 기여하였다. 표 3은 1949년 Shannon에 의해 발표된 암호화 시스템의 5가지 구비요건이다.

표 3. 암호화 시스템의 5가지 구비요건

구비요건	설 명
해독성	암호 해독자가 해독하기 어려워야 한다.
작은 Key	암호키가 쉽게 변경될 수 있도록 Key size는 작아야 한다.
단순성	복잡한 암호화 시스템은 비용을 초래한다.
오류의 독립성	한 전문의 오류가 이어지는 전문에 영향을 미치지 않아야 한다.
전문 Size의 확 장	통계적인 방법에 의해 해독이 불가능하도록 Message상의 잡음등을 삽입할 수 있도록 하여야 한다.

2.5 소프트웨어의 보안대책

소프트웨어의 종류는 메이커 제공용 소프트웨어와 사용자가 만든 소프트웨어로 분류할 수 있다.

메이커가 제공하는 소프트웨어로는 운영체제(O/S), 데이터 관리 소프트웨어, 유틸리티, 프로그램 진단용 소프트웨어, 응용프로그램 및 패케이지가 있다. 이들이 어떠한 오류를 갖고 있다면 자칫 시스템에 커다란 영향을 줄 수 있기 때문에 시스템 도입시 이들에 대한 철저한 검증을 가져야 할 것이다. 특히 시스템 Access의 점검, 데이타 및 소프트웨어의 보호기능 등을 기본적으로 갖춰야 할 것이다.

사용자가 만드는 소프트웨어는 주로 업무처리에 쓰이는 프로그램으로 직접적으로 업무에 관계하기 때문에 이들에 대한 보안대책은 다음과 같이 마련되어야 한다.

① 개발시의 보안대책

업무시스템 개발시에는 먼저 시스템 업무분석 단계에서의 보안대책 수립이 필요하다. 특히 자료입력시 무자격자 체크방법, DB의 Access 제한등 업무의 신뢰성을 유지하기 위한 시스템 구축이 필요하다.

설계단계에서는 프로세스의 Module화를 추진하여 한 Module의 오류시에도 전체 시스템에 영향을 미치지 않도록 설계가 이루워져야 할 것이다. 또한

프로그램 Coding이 완료된 후에도 검토회(Walk Through) 등을 거쳐 프로그램 오류 및 프로그래머에 의한 사고에 대비하여야 한다.

② Test시의 보안대책

Test 단계에서는 개발 프로그램의 안정성을 확인하기 위하여 필요한 절차를 취하여야 하는데, 이때는 먼저 각각의 Module별로 Module의 Test를 수행한 후 단위 프로그램별로 Test를 실시한다. 단위 프로그램 Test가 이루워진 후 종합 Test를 실시한다.

이 때 Test 방법으로는 미리 만들어진 Test Data에 의한 Test 실시가 바람직하며, Test Data는 정상 및 오류 데이타 등을 준비하여 정상, 비정상 처리에 대한 안전성 등을 체크한다. 이의 처리가 이루워진 후 병행 Test를 실시하여 이상이 없으면 실시에 들어가는데 이 때에는 개발팀 뿐만 아니라 실 운영팀과 단말 조작자도 포함시켜 문제점에 대한 의견을 수렴한다.

③ 운영시의 보안대책

운영시에는 특히 준비된 운영지침서 등에 의하여 업무시스템의 가동이 될 수 있도록 하여야 하며, 장애처리 등에도 운영자가 능숙하게 조치할 수 있도록 하여야 한다.

또한 만약의 경우에 대비하기 위하여는 소프트웨어의 Back-up 절차를 마련하여 핵커의 침입이나 내재적인 재해 또는 시스템 장애 등에 대비하여야 한다. 자기테이프와 디스크 등의 내용은 안전한 장소와 내화금고 등 보관장소도 이원화하여 백업화일을 보관하여야 하며, 주기적인 Back-up 절차와 백업시간 등의 관리도 함께 수행되어야 한다.

④ 프로그램 변경관리

프로그램이 완성되어 업무처리를 실시하고 있는 경우에는 아무리 작은 보수사항이 발생할 경우라도 적당한 프로그램 변경절차에 따라야 한다. 이러한 절차를 위하여 조직내에는 프로그램 변경 및 시스템 변경을 통제할 내부감사제를 도입하는 것이 바람직하다.

변경 통제담당은 시스템 관리담당 밑에 두며, 변경 통제위원은 이용부서의 책임자, 전산실 운영관리 책임자, 감사실 책임자, 시스템 프로그래머 등으로 구성한다.

일반적인 변경절차는 변경할 필요가 있는 Module 등을 조사하고, 변경 프로그램, 테스트 데이타와 출력자료 등을 변경 통제위원에 제출하여 사용 여부에 대한 승인을 받은후 프로그램 등록을 한다. 이 방법은 긴급을 요하는 변경사항에는 장애가 될 수 있지만 시스템 안전을 위하여는 좋은 방법이라 할 수 있다.

3. 현 금융전산망 시스템의 보안체제 및 안정성 향상 방안

3.1 CD 업무

'88년 7월 실시한 CD(Cash Dispenser) 공동이용 시스템은 한 은행에서 발행한 CD용 카드를 타은행의 CD기에서도 이용이 가능한 시스템으로 예금잔액 조회 및 현금인출이 가능하며, 일 10만건의 처리가 이루어지고 있다.

이 시스템은 현금카드의 사용을 전제로 하기 때문에 현금카드의 분실, 위조, 변조가 이루어지면 부정사용이 가능하다. 따라서 은행별로 현금카드의 마그네틱 스트라이프에 수록되어 있는 데이타에 대한 고객 비밀번호 등이 암호화 되어 있어 1차적인 보안장치가 되어 있지만, CD기가 설치된 취급은행 및 중계센터, 고객 거래은행(개설은행)이 연결되어 있는 시스템이므로 현금카드 발급, 취급은행, 개설은행과 센터간의 전송구간 및 은행 시스템과 센터 시스템의 보안유지가 필요하다.

① 현금카드의 보안방법

현금카드의 발급과정에서 고객의 신원확보 절차가 수반되어야 하며, 현재 마그네틱 스트라이프에 수록되어 있는 데이타도 타인에 의하여 위·변조 및 판독이 불가능하도록 암호화 할 필요성이 있으며, 또한 현금카드 사용 여부를 원장화일에 등록하고 현금카드를 제작하며, 고객에게 직접 카드를 교부할 때까지 원장화일에 미교부 표시를 하여 카드의 교부전 부정 사용에 대한 보안대책을 강구하여야 한다.

③ CD기에서의 보안유지

비밀번호에 대한 암호화 방식이 전체 은행에 통일되어 있지 않아 CD에서 입력한 비밀번호를 CD기 자체에서 검증이 불가능하므로 이에 대한 규격화와 계좌번호에 대한 암호화 채택이 바람직하다.

④ 통신회선상의 보안대책

CD 공동이용 시스템은 CD기에서 취급은행 시스템으로, 취급은행에서 중계시스템, 중계시스템에서 개설은행 시스템 그리고 이의 역방향으로 전문이 여러 단계를 거치면서 전송되기 때문에 그만큼 정보가 노출되어 있다. 따라서 전문의 노출 및 도청 등을 방지하기 위한 방안의 수립이 중요하다.

현재 Data의 고유번호 등에 의한 부분적인 Data의 검증을 수행하나 이에 대한 보안대책이 미흡한 형편으로 보안의 향상대책으로 고객정보에 대한 암호화 기법 등이 필요하다.

④ 각행 시스템과 중계센터 시스템상에서의 보안유지

각행 시스템 및 중계센터 시스템에서는 현금을 이동시키는 업무의 특성에 맞춰 관련 S/W의 무단 복사 및 변경 등을 대비할 수 있도록 프로그램 등록관리 및 보관에 철저한 보안대책을 마련하여야 한다.

현재 거래내용의 검증을 위하여 거래 Journal File을 일정기간 보관관리 하고 있으며, 비밀번호의 누출을 방지하기 위하여 비밀번호는 여기서 생략한다. 그러나 고객 비밀유지의 차원에서도 이 Journal File의 보관관리가 철저하게 이루워져야 한다.

개설은행 센터에서는 고객 비밀번호, 오류입력의 한도 횟수, 사용한도 금액에 대한 검증을 수행하고 있으며, 이에 대한 S/W의 신뢰성을 확보해야 할 것이다. 또한 운영자에도 보안교육을 실시하여 운영상의 오류가 발생하지 않도록 해야 하며, 주기적인 보안감사가 필요하다.

3.2 ARS(Automatic Response Service) 업무

자동응답서비스 시스템은 전화기를 이용한 예금잔액, 무통장 거래내역 등에 대한 고객의 금융정보를 제공해 주는것 뿐만 아니라 '91년 6월부터는 팩시밀리를 통한 서비스도 실시할 예정이다. 따라서 고객의 프라이버시와 비밀을 보장하기 위하여 여러가지 보안대책이 필요하다.

특히, 자동응답서비스 시스템은 고객과 센터 사이의 사용회선은 PSTN망으로 되어 있어 음성서비스나 팩시밀리가 아닌 PC 서비스의 경우는 고객 Password 관리 및 암호화 기법의 제공이 필요하다.

향후 은행간 송금이나 계좌이체가 가능하게 될 경우 전화회선의 무단 접속을 통하여 타인의 거액자금을 특정 계좌로 이체시킬 수 있는 가능성이 있다. 이러한 금융사고의 발생 가능성은 전화기가 데이타 통신용이 아니라 음성통신을 위한 것이므로 거래 데이타의 전부 또는 일부를 암호화 시킬 수 없고, 이용회선이 널리 보급되어 있는 공중전화 회선이므로 모든 사람에게 음성정보 서비스 시스템을 이용하는 금융 거래과정이 노출될 수 있기 때문이다.

따라서, 조회 서비스만 할 경우에는 비밀번호 사용 이외의 다른 보안대책이 마련되어 있지 않더라도 큰 사고나 문제가 발생되지 않지만 은행간의 계좌이체를 실시할 경우에는 이용 가능 매체의 제한 및 거래 데이타의 암호화 방법을 마련하여 별도의 안전대책을 강구하여야 한다. 그러나, 거래자 계좌에서 자신의 다른 계좌로 이체하거나 공공요금 납부와 같은 대량 수납이체에 국한하여 전화기를 이용한 계좌이체 서비스를 실시하는 것은 가능하다.

3.3 타행환 업무

타행환 시스템은 은행의 영업점에 설치된 온라인 단말기를 이용하여 타행으로 현금을 송금하는 일과 타행 발행 자기앞수표 조회를 온라인으로 할 수 있는 시스템으로 '89년 10월에 실시되었다.

CD 공동이용 시스템은 고객이 CD를 직접 조작하지만 타행환 시스템은 고객이 송금이나 수표조회 의뢰에 의하여 창구직원이 온라인 단말기를 조작하여 처리하므로 취급은행 영업점에서의 업무처리 정확성과 신뢰성이 요구된다.

영업점의 오퍼레이터가 입력한 금액에 대하여 금액 검증부호 성격의 복기부호를 책임자가 입력하고, 취급은행 센터에서는 복기부호에 해당하는 금액과 오퍼레이터가 입력한 금액이 일치되어야만 정당한 거래로 처리하며, 일정금액 이상(일반적으로 1백만원 이상)의 경우에는 책임자 카드키를 사용하여 단말기를 조작할 때만 거래를 발생시킬 수 있다.

4. 결 론

앞으로는 고객이 은행을 직접 찾지 않고도 금융거래가 개인용 컴퓨터, 단말기, 전화기 등을 통하여 가정이나 사무실에서 거래가 이루워져 금융기관은 현재 보다 다양한 고객 금융정보를 보유하게 될 것이다.

따라서, 공동망센타를 중심으로한 전체 금융기관은 고객 금융정보의 기밀유지와 안전유지를 위하여 통신망을 포함한 컴퓨터 시스템의 안전유지에 만전을 기하여야 할 것이다.

특히 통신시스템의 발달로 개인용 컴퓨터 등에서도 쉽게 통신망 등의 이용이 가능해지므로 데이타의 도청 등 불법행위에 쉽게 노출될 가능성이 점증될 것이다. 따라서 통신회선을 이용한 모든 금융거래는 DES와 같은 표준 암호화 방법 제정 및 적용이 필수적이다. 이 암호화 방법은 CD 단말기나, 고객의 개인용 컴퓨터, 은행센타 등에 적용되어야 하므로 과도한 비용이 수반되는 시스템은 바람직하지 못하며, 따라서 한글 환경하에 적용될 수 있도록 국내 실정에 맞게 제정되어야 할 것이다. 또한 인위적인 사고를 방지하기 위하여 시스템 분석, 설계, 프로그램 개발, 전산실 운영, 은행단말 조작자 등에 대한 체계적인 보안대책과 통제방법 등이 수립되어야 하며, 보안교육 등의 실시도 제도화 해야 할 것이다.

마지막으로 자연재해, 테러 등 불가항력적인 사고에 대비하기 위하여 앞으로 중계시스템에 대한 분산처리 시스템 및 Network 구축에 대한 검토도 신중히 고려해야 할 것이다.

참 고 문 헌

1. 금융결제원 : 금융기관 컴퓨터 시스템의 안전대책 기준 해설서(조사연구 제4호), 1988. 9.

2. 금융결제원 CD 공동이용 시스템 기본 설계서, 1988. 8.

3. 금융결제원 : 타행환 기본 설계서, 1988.

4. 정재현 : 온라인 실무와 범죄, 협동연구원, 1988. 7.

5. 안용근, 조이남 : EDP 시스템 감사, 정익사, 1980. 9.

6. 한국금융연수원 : EDPS 감사 및 전산 안전관리 세미나, 1988.

7. 김세헌 : 컴퓨터 범죄와 프라이버시 침해, 회성출판사, 1989.

8. 上園忠弘 : ユンピユータセキユリテイ, 近代科學社, 1981.

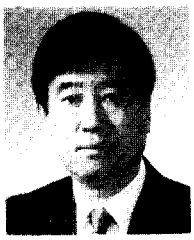
9. Charles, P. Pfleeger : Security in Computing, Prentinxe-Hall International Inc., 1989.

10. William, F. Brown. Pbd. : AMR's Guide Computer and Software Security, AMR International Inc., 1971.

11. IB., the Considerations of Data Security in a Computer Environment. G520-2160-01970

12. Ron, Weber : University of Queensland Australia, EDP Auditing Conceptual Foundations and Practice Second Edition, 1988.

□ 著者紹介



조 이 남(正會員)

1965年 서울大學校 師範大 數學科 卒
1970年 成均館大學校 經營大學院 電子資料處理學科卒(經濟學 碩士)
1987年 建國大學校 産業大學院 電算學科卒(工學碩士)
1991年 弘益大學校 大學院 電算學科 博士過程 修了
1970年~現在 金融決濟院 金融電算推進部長
1991年 韓國情報科學會 監査
1986年~現在 韓國情報處理 專門家協會 理事

김 형 근(正會員)

1984年 高麗大學校 工科大學 産業工學科 卒業
1984年 金融決濟院 入社
1991年 金融決濟院 金融電算推進部 調査課
研究分野 소프트웨어 엔지니어링, 컴퓨터 네트워크