컴퓨터 犯罪의 現況과 對應 方案

金 世 憲
(科學技術院 敎授)

Ⅰ. 서 론

컴퓨터 기술이 눈부시게 발달하여 컴퓨터는 이제 일반회사, 관공서 및 공공기관에 널리 사용되고 있다. 이에 따라 업무가 더욱 신속, 정확히 처리되고 있다. 그러나 컴퓨터의 이러한 바람직한 기능 뒤에는 고의적인 범죄 행위에 의한 피해가 존재하고 있다.

최근 국내에서 확인된 컴퓨터 범죄만도 30여 건에 이르고 있다. 하지만 공신력 실추를 우려한 나머지 숨겨진 사건들, 또한 발각되지 않은 사건들을 포함하면 그 건수는 수백 건에 이를 것으로 추정된다.

모든 범죄는 항상 돈이 있는 곳에서 발생하듯, 컴퓨터 범죄 역시 예외는 아니다. 다만 이 경우는 현금뿐 아니라 가치가 있는 회사경영정보, 소프트웨어, 개인신상정보 등 모든 것이 대상이 되고 있다는 점에서 그 범위는 실로 엄청나다 하겠다.

이렇게 신종 범죄가 급증하는 이유는, 전에는 사무 처리가 주로 종이를 이용하여 이루어진 것과는 달리 현재는 컴퓨터의 보급으로 컴퓨터와 단말기를 통해 이루어지기 때문이다.

종이를 기록 매체로 쓴 경우 각 업무의 담당자가 취급하는 사무처리의 범위는 매우 한정되어 있다. 이에 따라 각 담당자가 부정행위를 행할 가능성도 그의 담당업무 범위에 한정되어 있다. 또 모든 기록은 옆사람이나 상급자가 쉽게 눈으로 보고 확인 할 수 있는 형태로 작성되고 보존되었기 때문에 기록 내용을 변조하거나 허위내용을 기재하는 행위는 다른 사람에 의해 발각될 가능성이 높다.

그러나 컴퓨터를 이용한 사무 처리가 보급됨에 따라 이러한 상황

이 변하기 시작하였다. 각종 업무의 자료가 중앙 컴퓨터에 집중되고 여기에 연결된 단말기로 업무를 처리하게 됨으로써 한 직원이 단말기를 통해 접근할 수 있는 자료의 범위는 자신의 담당 업무 범위를 벗어나 사무 전반으로 확대되는 것이다.

이에 따라 자신의 담당 업무를 벗어난 자료를 입수하고 이를 변조 또는 말소하고 원하는 데이타를 입력시키는 작업을 한 개의 단말기로 수행할 수 있게 된 것이다. 여기에다 기록들은 쉽게 눈으로 확인할 수 있는 형태가 아니고 꼭 기계를 통해야만 읽을 수 있게 되어 있기 때문에 옆 사람이나 상급자가 조작 사실을 우연히 발견해 낼 가능성이 줄어들었다.

컴퓨터 범죄에 대한 대책을 강구하기 위해 먼저 컴퓨터 범죄가 어떠한 유형으로 발생하는지 알아보도록 하자.

Ⅱ. 데이타 조작을 통한 금융범죄

단말기를 이용하여 데이타를 조작함으로써 현금을 횡령하는 금융범죄는 가장 빈발하는 컴퓨터 범죄이다. 최근 모 신문에 게재된 사례를 몇 가지 인용하면 다음과 같다.

"81년 9월, 모 은행 온라인 예금계산감사담당 대리는 예금계산 담당 여직원이 키를 맡기고 자리를 비운 사이 2개의 가명 예금 구좌를 개설, 각각 1억원씩 허위 입금한 후 다음날 영업 개시 전 다른 지점이 발행한 자기앞 수표를 대불한 것처럼 허위전표를 만들고 장부를 꾸며 대·차변을 조정한 후 이 은행 여러 지점에서 인출해 갔다."

"85년 5월, 서울 모 은행 전산담당 직원은 온라인 단말기를 조작, 자신의 명의로 된 예금계좌에 1억 4백만원을 허위 입금시킨 뒤 3회에 걸쳐 1천 9백만원을 인출했다. 며칠이 지나도 아무 이상이 없자 그는 쾌재를 부르며 부산까지 가 나머지 8천 5백만 원을 인출하려다 동료 행원에게 발각되 검거되었다."

이 변하기 시작하였다. 각종 업무의 자료가 중앙 컴퓨터에 집중되고 여기에 연결된 단말기로 업무를 처리하게 됨으로써 한 직원이 단말기를 통해 접근할 수 있는 자료의 범위는 자신의 담당 업무 범위를 벗어나 사무 전반으로 확대되는 것이다.

이에 따라 자신의 담당 업무를 벗어난 자료를 입수하고 이를 변조 또는 말소하고 원하는 데이타를 입력시키는 작업을 한 개의 단말기로 수행할 수 있게 된 것이다. 여기에다 기록들은 쉽게 눈으로 확인할 수 있는 형태가 아니고 꼭 기계를 통해야만 읽을 수 있게 되어 있기 때문에 옆 사람이나 상급자가 조작 사실을 우연히 발견해 낼 가능성이 줄어들었다.

컴퓨터 범죄에 대한 대책을 강구하기 위해 먼저 컴퓨터 범죄가 어떠한 유형으로 발생하는지 알아보도록 하자.

Ⅱ. 데이타 조작을 통한 금융범죄

단말기를 이용하여 데이타를 조작함으로써 현금을 횡령하는 금융범죄는 가장 빈발하는 컴퓨터 범죄이다. 최근 모 신문에 게재된 사례를 몇 가지 인용하면 다음과 같다.

"81년 9월, 모 은행 온라인 예금계산감사담당 대리는 예금계산 담당 여직원이 키를 맡기고 자리를 비운 사이 2개의 가명 예금 구좌를 개설, 각각 1억원씩 허위 입금한 후 다음날 영업 개시 전 다른 지점이 발행한 자기앞 수표를 대불한 것처럼 허위전표를 만들고 장부를 꾸며 대·차변을 조정한 후 이 은행 여러 지점에서 인출해 갔다."

"85년 5월, 서울 모 은행 전산담당 직원은 온라인 단말기를 조작, 자신의 명의로 된 예금계좌에 1억 4백만원을 허위 입금시킨 뒤 3회에 걸쳐 1천 9백만원을 인출했다. 며칠이 지나도 아무 이상이 없자 그는 쾌재를 부르며 부산까지 가 나머지 8천 5백만 원을 인출하려다 동료 행원에게 발각되 검거되었다."

"88년 10월, 신한은행 서소문지점의 한 직원은 창구 직원이 점심 식사를 하러간 사이에 자신이 갖고 있던 7개 통장에 5억 5천 8백만원이 입금된 것처럼 컴퓨터를 조작한 후 바로 다른 지점에서 전액을 빼내 달아났다."

"89년 8월, 조흥은행 서울 충무로 지점에 근무하던 K씨는 이날 오전 창구가 혼잡한 틈을 이용해 컴퓨터 단말기를 조작, 자신의 명의로 갖고 있던 2개의 보통예금 통장에 모두 3억 5천만원이 입금된 것처럼 입력시켰다. K씨는 하루 뒤 이 은행의 다른 지점을 찾아가 이들 2개의 통장에서 2억 4천만원을 빼내 달아났다. 은행에서는 K씨가 며칠간 무단 결근하자 수상하게 생각, 점검에 나서 뒤늦게 이같은 사실을 알아냈다."

Ⅲ. 그외의 컴퓨터 범죄

앞에서 언급한 유형 이외에도 다양한 형태의 컴퓨터 범죄가 국내외에서 발생하고 있다. 단말기 대신 프로그램을 직접 사용하거나 일부 변조하여 현금이나 물품을 빼돌리는 사건은 매우 빈발하는 사건이다.

'73년에 발생한 AID아파트 추첨 조작 사건에서는 전산 요원이 프로그램을 조작하여 9명을 부정 당첨시켰다. 또 '81년 9월에는 모 은행 전산 프로그래머가 예금 이자 결산 때 자신의 저축 예금 이자 계산서 프로그램을 조작, 7백 23만원을 부정 인출했다. 또 '71년 대구 미군 기지에서는 여기서 일하던 한국인들이 5년간 1억 달러에 해당하는 물품을 횡령하였다. 이들은 컴퓨터를 통해 물품을 적당하게 빼돌리기 좋은 장소에 옮기도록 지시해 놓고 물품을 빼돌린 후 그 기록을 지워 버리는 수법을 썼다.

현금 카드를 절취하거나 습득하여 그 비밀 번호를 적당한 방법으로 알아내어 현금을 인출하는 사례는 일본에서 특히 다량 발생하고 있고 우리나라에서도 많이 발생하고 있다. 일본에서는 은행직원이 비밀 번호를 알아내기도 했고, 현금 카드를 절취한 범인이 카드 직원을 찾아가 은행 직원임을 사칭하여 알아내기도 했으며, 아버지

"88년 10월, 신한은행 서소문지점의 한 직원은 창구 직원이 점심 식사를 하러간 사이에 자신이 갖고 있던 7개 통장에 5억 5천 8백만원이 입금된 것처럼 컴퓨터를 조작한 후 바로 다른 지점에서 전액을 빼내 달아났다."

"89년 8월, 조흥은행 서울 충무로 지점에 근무하던 K씨는 이날 오전 창구가 혼잡한 틈을 이용해 컴퓨터 단말기를 조작, 자신의 명의로 갖고 있던 2개의 보통예금 통장에 모두 3억 5천만원이 입금된 것처럼 입력시켰다. K씨는 하루 뒤 이 은행의 다른 지점을 찾아가 이들 2개의 통장에서 2억 4천만원을 빼내 달아났다. 은행에서는 K씨가 며칠간 무단 결근하자 수상하게 생각, 점검에 나서 뒤늦게 이같은 사실을 알아냈다."

Ⅲ. 그외의 컴퓨터 범죄

앞에서 언급한 유형 이외에도 다양한 형태의 컴퓨터 범죄가 국내외에서 발생하고 있다. 단말기 대신 프로그램을 직접 사용하거나 일부 변조하여 현금이나 물품을 빼돌리는 사건은 매우 빈발하는 사건이다.

'73년에 발생한 AID아파트 추첨 조작 사건에서는 전산 요원이 프로그램을 조작하여 9명을 부정 당첨시켰다. 또 '81년 9월에는 모 은행 전산 프로그래머가 예금 이자 결산 때 자신의 저축 예금 이자 계산서 프로그램을 조작, 7백 23만원을 부정 인출했다. 또 '71년 대구 미군 기지에서는 여기서 일하던 한국인들이 5년간 1억 달러에 해당하는 물품을 횡령하였다. 이들은 컴퓨터를 통해 물품을 적당하게 빼돌리기 좋은 장소에 옮기도록 지시해 놓고 물품을 빼돌린 후 그 기록을 지워 버리는 수법을 썼다.

현금 카드를 절취하거나 습득하여 그 비밀 번호를 적당한 방법으로 알아내어 현금을 인출하는 사례는 일본에서 특히 다량 발생하고 있고 우리나라에서도 많이 발생하고 있다. 일본에서는 은행직원이 비밀 번호를 알아내기도 했고, 현금 카드를 절취한 범인이 카드 직원을 찾아가 은행 직원임을 사칭하여 알아내기도 했으며, 아버지

의 카드를 절취한 여고생이 은행에 찾아가 비밀 번호를 잊어버렸다고 주장해 알아내기도 하였다.

단말기를 통해 데이타를 조작하여 각종 면허증을 허위 발급한 사례와 가짜 기차 승차권을 대량 발매한 사건도 일본에서 발생했다.

데이타의 부정유출도 빈발하고 있는 컴퓨터 범죄중의 하나이다. 이것은 경쟁 회사의 경영에 관한 정보를 탐지하기 위한 경우, 경쟁 회사의 고객 리스트를 빼내가서 자기 회사 광고 목적으로 사용하기 위한 경우, 현금 횡령을 하기 전에 목표가 된 금융기관의 현금 입출 상황을 알아 보기 위한 예비적 목적으로 수행하는 경우가 있다. 또한 공공기관이나 금융기관이 갖고 있는 개인 신상에 관한 자료가 다른 기관에 유출되어 개인에 대한 불필요한 감시, 통제, 수색 등의 목적으로 오용되는 사례도 크게 우려할 필요가 있다.

프로그램의 부정 유출은 전문 지식을 갖춘 내부 담당자가 경쟁적 이득을 얻기 위해, 또는 다른 회사로 스카웃되기 위한 조건 등으로 발생하고 있다.

마지막으로, 정보화 사회가 진전됨에 따라 앞으로 가장 큰 문제점으로 간주되는 것이 자신의 단말기를 남의 컴퓨터에 불법으로 연결하여 사용하는 행위이다. 이것은 전화를 이용하여 원거리에 있는 컴퓨터에 연결시킬 수 있는 시스템이 잘 발달되어 있는 미국이나 유럽에서 널리 발생하고 있다. 앞으로 한국에서도 공공 정보 통신망이 발생하고 컴퓨터가 국제 통신망에 연결됨에 따라 이러한 해악 행위를 하는 외국의 도용자들에 의해 국내 컴퓨터들이 피해를 당할 가능성이 매우 높다. 최근 컴퓨터 소프트웨어에 침투해 프로그램을 파괴하고 다른 프로그램도 감염시킨다고 하여 국내에 큰 충격을 주었던 (C) 브레인이라는 컴퓨터 바이러스는 파키스탄에 사는 10대 소년에 의해 제조되어 세계에 번진 것으로 밝혀졌다.

Ⅳ. 컴퓨터 범죄의 대응 방안

컴퓨터 범죄에 대한 대책은 그 성격상 광범위한 시각에서 보아야 한다. 컴퓨터나 단말기가 있는 건물의 출입통제, 단말기에 대한 직원의 접근통제, 담당 직원이 쉽게 범죄를 저지를 수 있는 환경의

의 카드를 절취한 여고생이 은행에 찾아가 비밀 번호를 잊어버렸다고 주장해 알아내기도 하였다.

단말기를 통해 데이타를 조작하여 각종 면허증을 허위 발급한 사례와 가짜 기차 승차권을 대량 발매한 사건도 일본에서 발생했다.

데이타의 부정유출도 빈발하고 있는 컴퓨터 범죄중의 하나이다. 이것은 경쟁 회사의 경영에 관한 정보를 탐지하기 위한 경우, 경쟁 회사의 고객 리스트를 빼내가서 자기 회사 광고 목적으로 사용하기 위한 경우, 현금 횡령을 하기 전에 목표가 된 금융기관의 현금 입출 상황을 알아 보기 위한 예비적 목적으로 수행하는 경우가 있다. 또한 공공기관이나 금융기관이 갖고 있는 개인 신상에 관한 자료가 다른 기관에 유출되어 개인에 대한 불필요한 감시, 통제, 수색 등의 목적으로 오용되는 사례도 크게 우려할 필요가 있다.

프로그램의 부정 유출은 전문 지식을 갖춘 내부 담당자가 경쟁적 이득을 얻기 위해, 또는 다른 회사로 스카웃되기 위한 조건 등으로 발생하고 있다.

마지막으로, 정보화 사회가 진전됨에 따라 앞으로 가장 큰 문제점으로 간주되는 것이 자신의 단말기를 남의 컴퓨터에 불법으로 연결하여 사용하는 행위이다. 이것은 전화를 이용하여 원거리에 있는 컴퓨터에 연결시킬 수 있는 시스템이 잘 발달되어 있는 미국이나 유럽에서 널리 발생하고 있다. 앞으로 한국에서도 공공 정보 통신망이 발생하고 컴퓨터가 국제 통신망에 연결됨에 따라 이러한 해악 행위를 하는 외국의 도용자들에 의해 국내 컴퓨터들이 피해를 당할 가능성이 매우 높다. 최근 컴퓨터 소프트웨어에 침투해 프로그램을 파괴하고 다른 프로그램도 감염시킨다고 하여 국내에 큰 충격을 주었던 (C) 브레인이라는 컴퓨터 바이러스는 파키스탄에 사는 10대 소년에 의해 제조되어 세계에 번진 것으로 밝혀졌다.

Ⅳ. 컴퓨터 범죄의 대응 방안

컴퓨터 범죄에 대한 대책은 그 성격상 광범위한 시각에서 보아야 한다. 컴퓨터나 단말기가 있는 건물의 출입통제, 단말기에 대한 직원의 접근통제, 담당 직원이 쉽게 범죄를 저지를 수 있는 환경의

배제, 사용이 허락되지 않은 직원의 컴퓨터 사용을 막을 수 있는 기술적 조치, 정보 통신망 도청방지 등의 대책이 적절하게 관점에서 각각 종합적으로 강구되어야 한다.

일반적으로 사람들은 세 가지 이유로 범죄 행위를 자제하고 있다. 첫째로는 도덕적 양심때문이며, 둘째로는 범죄를 일으킬 기회가 사실상 없기 때문이며, 셋째는 범죄 수행후 발각되어 처벌 받을 것이 두렵기 때문이다. 이에 따라 컴퓨터 범죄를 막기 위해서는 다음과 같은 점을 고려해야 한다.

첫째, 내부직원 또는 사회인의 도덕성을 높여야한다. 현재의 사회는 전반적으로 배금주의가 팽배해 가고 있으며, 이에 따라 도덕관념이 크게 떨어져 있는 상태에서 급속히 고도 정보화사회로 이행하여 가고 있다. 이러한 상황을 방치하게 될 때 머지않아 많은 모순이 노출되고 사회 각 부문에서 혼란이 발생할 것으로 예상되므로 국민 전체의 도덕성을 확보하기 위한 기본적인 조치가 강구될 필요가 있다. 이를 위해서는 행정당국의 구체적인 대책이 필요하고 기업에서는 직원들간의 융화를 도모하기 위한 노력이 이루어져야 할 것이다.

둘째, 범죄를 일으킬 수 있는 기회를 가능한한 줄임으로써 범죄의 충동을 줄여야 한다. 앞에서 약술한 대로 종이를 통한 사무에서 컴퓨터를 이용한 사무로 이행됨에 따라 과거에는 접근 할 수 없었던 많은 자료들이 혼자서 접근할 수 있게 되었으므로 범죄 수행의 기회가 크게 증대 하였다. 또한 단말기 조작만으로 쉽게 범죄를 저지를 수 있게 되었으며 같은 범죄를 반복적으로 계속하는 것이 더 용이 하여졌고, 한번의 범죄로 얻을 수 있는 금액의 크기도 대형화 되었다.

이러한 상황의 변화에 대처하기 위해서는 한 직원이 접근할 수 있는 자료의 범위를 제한하여야 한다. 또한 그 직원이 수행할 수 있는 작업의 범위도 제한하여야 한다. 예를 들어 A화일은 볼 수 없다든다, B화일은 볼 수 있으나 그 내용을 고칠 수 없다든가, 또는 C화일은 내용 수정은 가능하나 작업처리는 할 수 없다든가 등의 제한이다. 이러한 제한을 정하는 데에는 그 직원이 담당 업무를 수행하는 데 필요한 내용 및 작업으로만 한정 한다는 것이 원칙이

다.

이렇게 되면 단독 범행은 불가능하고 몇명의 공동 범행으로 가능하게 되는데 이 경우에는 범죄 수행이 더욱 어려워지고 또 범행 후에도 이 사실이 노출될 가능성이 높아지게 된다.

셋째, 범죄 수행후 발각될 가능성을 높이고 그것이 발각되는 경우 적절한 처벌을 함으로써 범죄에 대한 두려움을 높여야 한다. 범죄의 발각 가능성을 높이기위해서는 앞에서도 말한 바와 같이 한 업무를 직원들 간에 적당히 분리하여 옆 사람이나 상사가 그 직원이 하는 일에 연관이 되게 함으로써 직원들간의 견제 효과를 도입하면 범죄의 발각 가능성을 높일 수 있다.

또한 정보 시스템내에 있는 데이타나 프로그램들을 주기적으로 적절히 감사하여 부정을 발견하려는 노력이 이루어져야 하고 범죄 발견시 이를 입증할 수 있는 증거 자료의 확보가 중요하다. 이를 위해서는 컴퓨터 시스템내의 모든 작업에 대한 일지(로그)를 자동적으로 작성하는 로그 화일을 만들어 보관할 필요가 있다.

컴퓨터 범죄의 경우 실제로 범죄를 적발한 경우에도 증빙 자료의 확보가 어렵거나 또한 현행 법규상으로 범죄로 인정하기 힘든 이유로 말미암아 무죄 또는 가벼운 처벌만으로 끝나는 경우가 매우 많다. 이는 발각 때의 두려움을 경감시켜서 컴퓨터 범죄를 더욱 조장하는 결과가 되고 있다. 따라서 저지른 범죄에 합당한 적절한 처벌을 가할 수 있는 컴퓨터 범죄 관련 형법의 제정이 시급하다.

컴퓨터 보안 문제의 중심은 결국 사람이다. 살인을 한 것은 총이 아니라 사람이듯이 컴퓨터 범죄를 일으키는 것은 컴퓨터가 아니라 사람이다. 따라서 컴퓨터 범죄에 대한 대응 방안은 무엇보다도 인적 요소를 중요시하여 장기적인 안목에서 구체적으로 수립되어야 할 것이다.