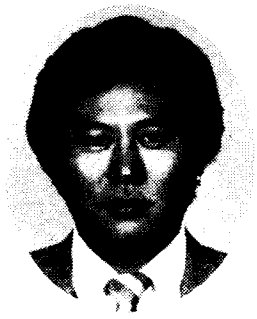
<技術解說>



컴퓨터 犯罪의 實態와 豫防對策

The State of Computer Crime and Counter-Measures

金 麗 腥*
Kim, Ryo Sung

1. 머리말

犯罪者에 대한 일반인의 認識은 대체로 다음과 같이 설명될 수 있을 것이다. 즉 범죄자는 성질이 포악(暴惡) 하거나 부정적이고, 인상이 험상궂고 우락부락하거나, 정상적인 양질의 사회적·가정적 교육을 충분히 받지 못했거나 따뜻한 가족적 유대관계가 결여된 가정환경하에서 성장했거나, 정당한 노력없이 도박등으로 일확천금을 꿈꾸는 사람들의 부류라고 생각하는 것이 일반적인 관념인 것이다.

그러나 컴퓨터犯罪者에 관한 한, 이제까지의 일반적인 범죄자와는 인상착의뿐만 아니라 교육수준이나 기술능력면에서 여러가지로 差異가 있다는 사실을 알 수 있다. 그들(컴퓨터犯罪者)은 대체적으로 젊고, 교양이 있으며, 기술면에서 有能하며, 매우 공격적인 사람들로 분류된다. 또 개인적으로는 한탕을 위해 지혜를 짜 내기도 하며, 도전적으로 일확천금을 얻으려고 기도하거나 또는 큰 조직의 앞잡이로서 협력하는 범죄자도 있다. 이들에게는 컴퓨터犯罪가 범죄라는 의식이 희박하며, 직무상 책임을 위배하는 背任의 경우와 도덕적 윤리성이 결여되어 있다는 점도 특기할만 하다.

이러한 관점에서 「컴퓨터犯罪란 무엇인가」를 생각해 보자.

컴퓨터범죄라 함은 「부정한 목적을 위해 외부의 인위적 힘에 의해서 컴퓨터가 직접적·간접적으로 혹은 즉시적·잠재적으로 얼마간의 형태로서 개재된 정상적 처리를 일탈한 社會惡 行爲」를 말한다. 이와 같이 정의를 내린다면 컴퓨터범죄의 범위는 일응 상당한 확대해석이 가능한 일면이 있지만 이는 주로 情報와 소프트웨어를 중심으로 하여 일어나고 있다.

그 대표적 유형으로서 프로그램의 조작, 데이터절취, 데이타파괴, 데이타조작, 소프트웨어의 부정사용, 통신망 부정접속, 입출력조작등을 例로 들 수 있는데 범죄자체가 교묘하고 지능적이며 또 증거를 잘 남기지 않는다는 점에서 범행사실의 발견과 추적이 어렵다는 속성을 가지고 있다. 또한 그 범죄가 경제사회 전반에 미치는 부정적 영향이 지대하며, 특히 데이타베이스에 관련된 범죄 및 事故는 정보화사회에 치명적인 혼란을 유발할 것으로 예견되고 있다.

따라서 本稿에서는 그간 발생하였던 컴퓨터범죄 事例를 살펴보고 범죄의 특징과 범죄행위를 분류하여 범죄자들이 어떤 방법으로 컴퓨터범죄를 일으켰는지 그 접근방법을 분석한 연후 그에 따른 각각의 예방대책을 고찰하여 봄으로써 다가오고 있는 情報化社會 구현에 一助가 되고자 한다.

2. 컴퓨터犯罪의 事例

우리나라에서 最初로 프로그램을 변경하여 일

* 情報處理技術士(電子計算組織應用), 韓國證券電算(株) 市場시스템部長

으킨 컴퓨터犯罪는 1973년 10월 반포 AID 차관 아파트의 입주자 추첨과정에서 발생되었다. 당시는 아파트 붐이 본격적으로 일기 前이었지만, 아파트는 신흥 경제계급의 富의 상징으로서 서울지역에 속속 들어서면서 인기를 끌기 시작한 때였다.

이 사건은 반포 AID 차관 아파트 입주 추첨의 전산처리 용역을 맡은 중앙전자계산소(GCC)의 프로그래머인 鄭某氏가 뇌물을 받고 특정 9세대분을 당첨시키도록 프로그램을 임의로 조작한 것이었다. 이와 같이 기존의 프로그램에 부정한 목적을 수행키 위해 새로운 프로그램을 끼워 넣는 방법을 컴퓨터범죄행위 중에서는 "트로이 목마(Trozan Horse)"라고 부른다.

이는 고대 그리스 시대의 아가멤논 장군이 트로이城을 공격할 때 木馬의 배속에 군사를 싣고 들여보내 트로이 城을 함락시켰다는데서 연유한 것으로서 부정한 목적의 프로그램이 마치 트로이 木馬속의 병정이 된 셈이다.

이 사건이 배치(Batch) 프로그램 변조작업에 의해 발생된 최초의 범죄인 반면, 온라인·시스템(On-line System)에서 일어난 최초의 범죄로서 서울 시내 某은행 전산부에서 1982년 4월에 발견된 프로그램을 이용한 온라인 횡령 사건을 들 수 있다. 이때의 횡령금액은 1천 3백여만원이었다. 이 처럼 온라인 시스템에서 일어나는 사건은 배치(Batch)처리 형태에서 발생하는 사건보다 범행규모나 방법이 더욱 대형화되고 高度化되고 있으며 향후 가정과 은행, 가정과 기업, 은행과 은행을 연결하는 전국적 규모의 통신 네트워크를 추진하고 있는 정보화사회의 관점에서 생각해 본다면 온라인 시스템에서의 컴퓨터 범죄는 자못 심각한 경제·사회적인 문제점이라고 생각할 수 있겠다.

최초의 온라인 횡령사건의 요지는 다음과 같다. 범인은 '81년말 저축예금 이자횡령의 방법으로 3회에 걸쳐 1백 2십만원과 콘솔(console) 조작에 의한 잔액 증액방식으로 1천 1백 5십만원을 늘리는 등 4~5개월 동안에 1천 3백여만원을 불법적으로 횡령하였다.

사고를 낸 이 行員은 고등학교를 졸업한후 2년 1개월간을 전산실에서 근무하였는데 혼자서 가족의 생계를 책임지고 야간대학을 다녀, 모범행원으로서 인정받고 있었다.

범행은 '81년 3/4분기 저축예금 이자결산업무를 야간에 혼자 작업하면서 자신의 저축예금 계좌의 이자계산용 적수를 늘리면서부터 시작되었다. 저축예금의 한도는 1천만원으로 당시의 이자율 14.4%로 계산하면 1천만원의 분기별 이자가 3십 4만 9천원이 되었다. 자신의 計座에 이자를 가산한 후 원장내용이 통장에 기록되는 것을 막기위해 트레일러(trailer)를 콘솔로 삭제하였다. 이렇게 야간 근무시간에 저축예금이자 횡령을 완벽하게 성공하자 이듬해인 '82년 초에도 동일한 방법으로 이자를 불법 취득했다.

원금의 積數를 이용해 이자만을 지속적으로 늘려 나갔다면 이 범행은 장기간에 걸쳐 노출되지 않고 계속되었을 것이라는 專門家의 지적이 있었는데 결국 이 범인은 "네트워크 거래"를 이용해 자신의 계좌에 입금한 것이 換의 不一致로 발각되어 범행의 전모가 밝혀지게 되었다.

컴퓨터를 이용한 범죄행위는 점차 고도로 知能化되기 시작하였다.

前記의 범죄사례이외에도

○某방적회사의 給與부정 사건

○某은행 대리의 가짜 計座개설 및 허위 入力 사건

○某은행 대리의 허위 傳票작성 입력사건

○某보험회사 入金額 造作사건

○某증권회사 지점장의 ID카드 不正사용

○某은행 전산실 직원의 현금카드 偽造사건등 10여건이 발생했으나 국내에는 아직 컴퓨터범죄에 관한 관계법률 이 없으며 判例도 충분치않기 때문에 상기의 각종 컴퓨터犯罪에 대해서는 특정범죄 가중처벌죄, 횡령죄 등의 유사한 법을 적용하는 편법을 써왔다.

한편 우리나라보다 컴퓨터의 導入이 앞선 歐美諸國과 日本에서는 우리의 경우보다 범죄규모가 더 크고, 그형태도 다양한 것으로 나타났다.

<외국의 犯罪事例>

○1971년 美國 뉴욕 센트럴 철도창에서 200대 이상의 貨車가 증발 ; 컴퓨터와 연관된 조직적인 범죄로서 1천 2백만불의 규모였다.

○ 1972년 美國 캘리포니아대학 L.A 공대생 제리·슈나이더가 전화와 컴퓨터코드(Secret Entry Code)를 사용하여 100만불을 훔친 사례가 있다. 공모자인 그 회사 종업원의 배반으로 발각되어 60일간의 징역과 3년의 보호관찰 판결을 받았다.

○ 1971년 2월 日本의 日經맥그로힐社의 磁氣화일(file)이 누군가에 의해서 복사되어 同業者인 日本리더스 다이제스트社에 매각된 범죄사건

○ 1974년 8월 日本의 유명한 俳優의 유아를 유괴하고서 몸값을 받는데 은행 온라인예금을 이용하려 했던 "眞由子事件".

○ 英國의 유럽지사에 마그네틱 테이프(Magnetic Tape) 500개를 절취하여 資料를 파괴하겠다고 협박한 事件.

〈별표 1〉 犯罪事例分類

手段	發生頻度(%) 日本	發生頻度(%) 歐美	備考(事例)
○不正데이타 入力	65(26件)	20(4件)	架空口座入金等
○카드의 不正入手使用	10(4)	—	現金카드窃取後現金引出等
○컴퓨터의 不正使用	7.5(3)	—	二重帳簿를 作成하여 詐欺등
○컴퓨터 便益의 惡用	5(2)	5(1)	幼兒人質後架空口座入金要求등
○데이타의 不正入手	7.5(3)	—	File復寫後賣却등
○Hardware 破壞	5(2)	10(2)	電算室破壞등
○프로그램 窃盜	—	15(3)	프로그래머가 自己會社의 프로그램을 賣渡
○암호不正入手	—	15(3)	컴퓨터 顧問이 暗號不正入手後送金등
○情報破壞	—	15(3)	資料管理職員이 磁氣테이프의 記憶消去 또는 다른 라벨附着등
○情報의 窃盜	—	10(2)	前오퍼레이터가 磁氣테이프를 窃取後金錢要求등
○프로그램 僞造	—	5(1)	利子計算의 端數를 特定口座에 入金되도록 프로그램化등
○데이타 變更	—	5(1)	職員이 詐欺團의 앞잡이가 되어 記錄變更등
合計	100% (40件)	100% (20件)	

○ 美國의 信用정보회사에서 고객과 공모하여 信用記錄을 조작하였던 犯罪.

○ 西獨의 한 保險會社 여직원이 마그네틱 테이프(M/T) 기록을 삭제하고 라벨(Label)을 엉터리로 붙여서 혼란에 빠트린 事件등등 여러가지 컴퓨터犯罪들이 발생하고 있다.

〈별표 1〉은 歐美諸國 및 日本의 은행, 보험회사, 기타업무에서 발생하였던 범죄手段, 發生頻度, 事例分類 등을 나타내고 있다. (첨부한 별표 1 犯罪事例分類는 '83년 2월 21일 발간한 日本通產省의 컴퓨터 관련통계와 主要犯罪事例를 參照하였음).

3. 犯罪의 特徵

컴퓨터는 현대문명의 총아로서 우리의 일상생활에서 점하고 있는 그 존재의 중요성이 날로 더해 가고 있는 반면에, 세계적으로 컴퓨터犯罪가 확산되고 있는 만큼 우리가 언제 어디서 컴퓨터범죄의 피해당사자가 될 것인지는 어느 누구도 예견할 수 없는 것이다. 따라서 컴퓨터범죄의 특성을 미리 알아 두는 것이 유용할 것이다. 지금까지 발생되었던 컴퓨터범죄에서 드러난 特徵을 살펴 보도록 한다.

첫째, 單獨犯行이 비교적 쉽고 간단하다.

범행이 노출되지 않기를 바라는 犯人에게 있어서 保安維持에 관한한 단독범행보다 더 좋은 방법은 없을 것이다. 이 점에서 컴퓨터는 아주 매력적이다. 미국의 事例를 보더라도 컴퓨터事故의 62%가 단독범행에 의한 것이었다.

둘째, 일시에 巨額의 橫領이 가능하다.

즉, 資料(Data)나 소프트웨어를 조작하는 경우 물리적인 제한이 없기 때문에 원하는 만큼, 橫領이 얼마든지 가능한 것이다.

세째, 범행이 現場에서 他人에게 노출되지 않는다.

직원들이 업무를 함께 전산처리할 때 정상적인 업무처리인지 아니면 범행을 저지르고 있는지 쉽게 識別되지 않을 뿐만 아니라 전산처리는 타인이 알 수 없는 것이 일반적이다.

네째, 범행사실이 쉽게 發見되지 않는다.

전산처리를 시행한 결과는 보통 사람의 肉眼

으로 識別할 수 없는 磁性媒體(magnetic tape, disk, drum, diskette 등)에 記錄되기 때문에 이것이 변조되었는지 확인하기 위하여서는 또 다시 별도의 전산처리를 실행하여야 확인할 수 있다는 단점이 있다.

다섯째, 證據湮滅이 가능하다.

歐美나 日本에서 컴퓨터범죄가 發覺되어 범인이 잡힌다고 할지라도 누가 犯行을 저질렀는지에 대한 분명한 指紋이나 筆跡등 직접적 證據가 없고 다만 상황에 미루어 본 심증만이 있으므로 범행을 否認할 경우 無罪 내지는 가벼운 刑을 받게 되어 사회적으로 큰 문제가 되고 있다.

여섯째, 범행후 逃走할 수 있는 시간이 充分히 있다.

범행 현장에서는 他人이 알지 못하므로 현장에서 발각되지 않는 한 범행이후에 綻露난다 할지라도 범인이 이를 먼저 알 수 있으므로 도주할 시간은 충분한 것이다.

컴퓨터犯罪는 상기한 바와 같이 범인들이 원하는 모든 條件을 다 갖춘 매력적인 것이다. 단지 이를 위해서는 컴퓨터에 대한 상당한 知識이 필요할 뿐이다. 그러므로 선진국에서 컴퓨터범죄는 知識人 그룹인 화이트 컬러(White Color) 그룹의 범죄의 대종을 이루고 있으며 長期化, 知能化, 巨額化되고 있는 것이 현재의 추세이다.

더구나 다가오고 있는 情報化社會는 컴퓨터와 通信이 주축을 이루는 사회인데 이에 대한 逆作用 내지는 不信을 초래한다는 것이 컴퓨터犯罪가 지니는 나쁜 屬性인 것이다.

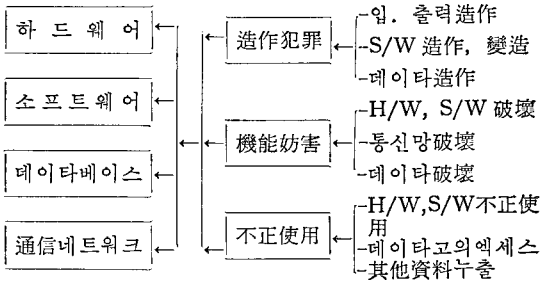
4. 犯罪行爲의 分類

컴퓨터犯罪者가 범죄를 일으키는 내용을 對象(object) 별로 구분해 보면 다음과 같다.

① 하드웨어(hardware) ; 機器 및 設備
② 소프트웨어(software) ; 프로그램, 文書(document) 및 資料(Data)
③ 데이타베이스(data base) ; 磁化된 情報
④ 通信네트워크(network) : 通信途中의 情報

상기한 범죄 대상에 접근해서 入·出力을 造作하거나 소프트웨어나 데이타를 造作·變造하는 ① 造作犯罪를 일으키기도 하고, ② 機能을

〈별표 2〉



〈별표 3〉 컴퓨터犯罪行爲分類

大分類	中分類	小 分 類
犯 罪	破 壞	破壞行爲
	절 취	Data Base, Program, Output,
	사 취	Data 等의 절취, 사취, 횡령
	횡 령	
		Machine Time 도용, Data Base, Program, 자기기록 등의 Copy
	기밀누설	Data Base 누설
		Output·Data의 전송에 따른 누설
		기타
	Privacy 침 해	명예훼손
		인권침해

妨害할 목적으로 하드웨어, 소프트웨어, 통신망 또는 데이타를 破壞하기도 하며, 하드웨어나 소프트웨어를 不正使用하거나 故意的으로 허가되지 않은 데이타를 접속(access) 하거나 기타資料를 漏出시키는 ③ 不正使用으로 犯罪를 일으키거나 不當利得을 취하기도 한다.

이것을 도표로 표시한 것이 별표 2의 분류표이다.

상기한 바와 같이 ① 造作犯罪, ② 機能妨害, ③ 不正使用 등에 의해 발생되는 범죄행위를 刑法上 用語로 분류해 보면 ① 破壞, ② 竊取, ③ 詐取, ④ 橫領, ⑤ 機密漏泄, ⑥ privacy 侵害 등으로 구분할 수 있으며 그것을 다시 小分類한 行爲는 별표 3 컴퓨터犯罪行爲分類에 圖示한 바와 같다.

5. 犯罪時 接近方法

그렇다면 범죄자들은 컴퓨터시스템에 언제, 어떤 方法으로 접근하여 犯罪를 일으키는 것일까?

컴퓨터의 施設이나 設備面에 관해서는 별도로 고찰하겠지만 전산처리(data processing) 過程을 따라가며 犯人이 접근하는 方法을 살펴보면 다음과 같이 다섯가지 경우를 나누어 볼 수 있겠다.

첫째, 入力時

○架空計座를 설정하여 놓고 다른計座의 資料를 移轉시켜 竊取한다.

○入力時 誤謬(error)를 發生시켜서 錯誤金額을 절취한다.

○制限된 接近(access)을 무시하고 마구자비로 接近(access) 한다.

둘째, 프로그래밍時

○特定한 코드(code)를 check하여 不當한 處理(processing)를 하도록 고친다.

○특정한 命令語를 수행시킨다.

○특정한 條件(condition)을 변경시켜서 프로그램이 不正한 처리가 되도록 한다.

○특정한 資料(data)가 隱匿되도록 프로그래밍(programming) 한다.

세째, 處理過程(operating)에서

○시스템을 破壞하여 不正한 犯罪를 은폐한다

○시스템 運用(operating) 중 重大한 缺陷을 故意로 유발시켜서 不正을 자행한다.

네째, 出力 및 資料(data)를 保管할 때

○情報를 流出시켜 損害를 준다.

○出力된 정보를 配布하거나 保管할때 고의로 부적격한 者에게 보여주거나 넘겨 준다.

○競爭회사의 情報를 빼내어서 不當利得을 취한다.

다섯째, 通信線이나 通信裝備와 연관시켜서

○傳送도중에 盜聽한다.

○傳送中에 있는 데이타를 變質시킨다.

○暗號 解讀방법을 이용하여 정보를 절취한다

○非認可者가 故意로 통신시설에 接近(access)하여 정보를 파괴하거나 變質시킨다.

6. 犯罪豫防對策

컴퓨터시스템이 점차적으로 大規模化해 가고 通信네트워크(Network) 등이 사회적으로 확대되어 감에 따라 각종 端末機로 부터 컴퓨터시스템에의 接續이 가능해 짐으로써 不正한 接近(access), 데이타나 프로그램의 變更 또는 不正使用으로 因하여 컴퓨터犯罪가 발생하거나 개인의 Privacy가 侵害 또는 노출당하는 중대한 사회적문제가 야기될 소지가 다분하다.

이러한 不正行爲를 방지하기 위해서는 다음과 같은 일련의 方法을 동원하여 컴퓨터犯罪를 막고자 노력하고 있다.

<例>

○Password나 ID카드를 許可된 者에게만 배부하여 컴퓨터가 설치된 場所를 出入할때 出入管理를 철저히 한다.

○端末機, 利用者(end user) 및 利用하려는 화일(file) 등에 접근하는 正當性을 제어하는 acess control方法을 사용한다.

○暗號化를 실시해서 자료(data)의 不正使用을 방지한다.

○監視(CCTV 등)나 記錄을 철저히 관리하여 不正을 早期에 發見토록 한다.

○要員管理(또는 人事管理)를 철저히 시행하여 부정발생의 가능성을 사전에 제거 또는 방지한다. 등등

여러가지 方法의 例를 들어 보았는데 컴퓨터犯罪에 對한 豫防對策을 크게 大別하여 보면 技術的 측면과 運用管理 측면으로 나눌 수 있겠다 그리고 기본적으로는 이 技術과 運用管理를 잘 조화시켜서 범죄 의도를 가지고 있는 者에게 약점이 노출되지 않도록 관리하는 것이 중요하다고 할 수 있겠다.

가. 技術的 對策

過去에 발생하였던 컴퓨터犯罪中에서 代表的인 5가지 유형의 犯罪와 그에 대한 對策은 다음과 같다.

1) 破壞 및 data 媒體竊取 대책

주로 컴퓨터室이나 빌딩등의 運用管理에 문제가 있었다. 그러나 最近에는 出入管理시스템, TV Monitor, 遠隔制御, 컴퓨터에 의한 綜合빌딩管理시스템 등이 開發되어 運用管理를 技術的 側面에서 지원할 수 있도록 보완되어가고 있다.

○入退室管理機能

—本人確認用 出入카드 發給

—出入門의 開閉장치(card-key, pass word)
—映像에 의한 監視記錄 및 원격제어장치 설치.

2) 컴퓨터의 不正使用 대책

컴퓨터에 직접 접근(access) 하거나, 通信回線을 통하여 컴퓨터를 不正하게 使用하는 犯罪를 防止하여야 할 必要가 있다. 이것에 대해서는 access control이 重要한 機能을 수행한다. 現在는 pass word 등에 의한 本人確認, user-profile에 의한 資源(resource) 접근 許容과 operating system에 의한 管理, access monitoring이나 console log에 의한 Access 履歷의 記錄 등으로 不正使用을 밝혀낼 수 있겠다.

이들의 機能을 충분히 活用하면 컴퓨터 犯罪에 대하여 상당히 유용하게 作用할 것으로 생각된다. 그러나 한편으로는 password를 도둑맞으면 처리할 方法이 없다든가 온라인시스템의 通信回線을 둘러싼 盜聽防止, 不正接續 등 硏究 보완할 문제는 많다.

○ 利用者確認기능
—端末확인 ; 種別, 識別 code, password 등에 의한 資格확인
—本人확인 ; password, ID card, IC card, PIN-PAD, 인감, 指紋. 聲紋, 筆跡, 網膜, 手形 등에 의해 자격확인.

○ 相對方確認기능
—call back 方式
—digital 署名

○ 利用者의 file access 確認기능
—資源(resource) access 管理 program
—record 單位·data 項目 單位의 機密保護 기능

3) 情報竊取, 情報破壞 대책

情報를 copy하거나 通信回線을 통해서 프로그램과 情報를 도난당하기도 하고, 情報와 프로그램이 破壞당하는 것을 防止하지 않으면 안된다. 이것에 對해서는 access control, data 保護기능, 暗號化 등이 유효한 방법이라 할 수 있다 그러나 暗號化에 대해서는 解讀 key의 管理를 둘러 싼 문제 등이 아직도 과제로 남아 있다.

○ 暗號化의 方法
—慣用暗號方式 ; DES(data encryption standard) 方式 등
—公開 key 暗號方式 ; RSA(Rivest Shamir Adleman) 方式 등
—file 暗號化기능
—回線暗號化기능
—映像·音聲의 scramble 化(秘話機 등)

4) 不正入力 대책

僞造 전표등에 기초를 두는 不正入力에 대해서는 컴퓨터시스템內에서 正確한 것인가 不正確한 것인가를 판별하기는 상당히 어렵다. 다만 어느 程度까지는 技術的 대책으로 가능하겠지만 根本的으로는 管理面에 包含된 綜合的인 대책이 要望되고 있다.

○ 監視·記錄 및 監査
—cross check
—內部 견제기능
—監査기능 活用
—console log 및 data 入力 log 再確認

5) 프로그램 僞造 대책

프로그램을 不正으로 위조하는 犯罪는 많다고 생각되지는 않지만, 가령 그러한 위조가 發生한다면 그것을 發見하기 까지는 상당한 期間이 걸리고 發見이 용이 하지도 않지만 여기서 파급될 그 피해의 파장 또한 대단히 커질 可能性이 많다. 게다가 現 段階에서는 全面的으로 運用管理 側面에서의 대책을 강구하여야만 하는 문제가 있다.

○ 要員管理

컴퓨터시스템을 가장 잘 理解하고 있는 사람은 開發 담당자나 현재의 運用을 담당하고 있는 電算要員이라 하겠다.

따라서

① 시스템개발시 複數의 사람에 의해 시스템을 테스트한다든가, 중요 file에의 接近을 제한하고, 內部牽制·內部統制上 充分한 check 監視기능을 두어서 정기적으로 監視기능을 수행하도록 한다(註 ; 現實的으로 매우 어려운 일임을 附記해 둔다.)

② 컴퓨터시스템 관계자의 就業管理, 健康管理, 精神衛生管理, 相談 등의 관리적 배려를 충분히 시행하여 不正行爲가 발생되지 않는 환경을 조성하도록 유도한다.

③ 機密保護·機密 file 취급, 職務權限등 社內管理規程을 명확하게 정해서 周知시키고 교육을 철저히시킨다.

나. 運用管理的 對策

컴퓨터시스템 安全對策基準을 適用하고 시스템監査制度의 도입이 필요하다.

컴퓨터시스템의 效率的인 運用管理를 위해 會社內에 安全對策委員會나 安全管理室을 설치하고 安全對策 敎本(manual)을 작성한다. 그 敎本을 전 部署에 배포시켜서 敎育訓練과 監督을 위한 guide line으로 使用하게 한다.

그리고 安全對策의 주요한 사항은 機密保持, 文書(document) 管理, Building 出入관리, 기계실(computer 및 설비실) 관리, 컴퓨터 運用과 障害對策, 入出力資料取扱, magnetic file 管理 컴퓨터 關聯설비의 運用, 巡回監視, 災害對策, 委託業務관리등에서 각각 어떻게 처리를 하는 것이 좋은지 具體的으로 規定하게 한다.

다. 컴퓨터犯罪 防止技術 方向

컴퓨터犯罪를 防止하기 위한 技術은 여러가지가 있다. 이것들 중에는 컴퓨터의 安全對策으로 적극적으로 도입·보급해야 할 技術이 많다.

그러나 다른 한편으로는 확대·高度化하여 가는 컴퓨터시스템에 대하여 또 한층 높이 要求되는 技術들이 많다. 그것은 ① access control 技術, ② data 保護技術, ③ 暗號化技術 등이다.

(1) access Control

access control은 使用者가 컴퓨터시스템에 access하는 時點에 그 使用者가 정당한 access 권한이 있는지 여부를 검증해 주는 技術이다.

○本人確認技術

ID number와 password 外에 다음과 같은 새로운 本人確認技術의 硏究가 진행되어지고 있다.

① 指紋照會技術, ② 聲紋判定技術, ③ sign 判定技術, ④ 手形(손의 면적, 크기, 손가락 길이등) 照會技術, ⑤ 網膜

○通信回線에 誤接續防止技術

전용회선에 관해서는 接續하는 단말기를 고정시키기 때문에 回線에 誤接續은 상당히 어렵다. 공중회선(전화회선)의 경우에는 電話番號만 알면 누구라도 자유롭게 接續하기 때문에 誤接續이 쉽게 가능하다. 日本의 DDX(Digital Data Exchange)에서는 接續하려고 하는 상대방의 address를 미리 通知하는 機能과 단말기 address를 DDX의 電子交換器에 미리 登錄하는 閉域接續에 의해 誤接續 등을 피하고 있다.

○使用者 profile 管理技術

이것은 使用者마다 시스템을 使用하는 권한 또는 資源(Resource)의 범위를 管理하는 技術이다. 이미 商品化 되어 있으며 使用者管理機能(使用者 姓名과 屬性 및 File 管理)과 資源管理機能(使用者 등의 利用可能한 File 管理)이 包含된다.

○access monitoring

使用者의 컴퓨터 Access 記錄을 잡는 技術로서 不正 access monitoring, system monitoring(정확한 access monitoring), console log 등 3個의 機能으로 나뉜다.

(2) data 保護技術

今後, 開發을 必要로 하는 data 保護技術로서는 다음과 같은 것이 있다.

○data base의 領域制限

使用者 DB에 access하는 경우 통상은 檢索言語를 使用하는 일이 많다. 그러나 使用者의 검색문이 나타나는 data base 領域은 그 使用者가 access하는 일이 許容되어 있는 領域과 꼭같이 일치하지는 않는다. 保安上 허용되어 있는 領域만을 검색시키는 control이 요망된다.

○flow 制御

秘密等級이 높은 data의 경우 부당하게 外部로 流出되어서는 곤란하다. 일반적으로 비밀등급이 낮은 data의 경우 外部로 流出되기가 쉽다. 이 때문에 컴퓨터시스템 內에서 data가 흐를 때 data가 비밀등급이 낮은 방향으로 흐르는 것을 막고 control할 必要가 있다.

○推論의 制御

예를 들면 data base를 TSS(time sharing system)로 利用하려고 하는 경우 정당한 檢索의 質問을 짜 맞추는 것에 의해서 本來 秘密로 되어 있어야 할 data가 질문자의 手中으로 넘어가는 可能性이 있다. 이것은 質問에 의해 얻어진 回答에서 完全히 관련이 없는 data가 推論되는

경우에 일어난다. 이러한 推論이 곤란하게 되도록 質問方法에 規制를 두도록 하는 등의 必要가 있다.

(3) 暗號化 技術

暗號는 주로 軍과 外交方面에서만 使用되어 왔지만 오늘날은 컴퓨터시스템에서 重要하게 대두되고 있다. 요사이는 情報를 盜聽하는 것이 쉬워졌으며 事業上의 많은 業務(電話, 電子郵便, 전자송금등)가 통신매체를 통해 處理되고 있으며 컴퓨터네트워크의 利用이 급격히 增加되고 있는 실정이다. 그러나 大部分이 本格的으로 暗號技術을 採擇하고 있지 않는 理由는 아직도 解決되지 않은 많은 問題點들이 존재하고 있기 때문이다.

주요한 問題點으로는 다음과 같은 것들을 들 수가 있겠다.

- 暗號方式導入의 必要性이나 效果가 보다 明確해지지 않으면 안된다.
- 너무 高價이다.
- 暗號를 푸는 key의 傳達·管理가 번잡하다
- 暗號方式은 컴퓨터시스템 處理能力을 저하시킨다.

이러한 問題點들이 해결된다면 暗號方式은 유효한 手段이 될 것으로 예상된다.

앞으로 더욱 많은 硏究가 進行되어 效果的인 暗號方式이 開發되는 것이 要望된다. 그때 POINT가 되는 것은 다음의 條件들이 必要하다.

- 暗號의 强度를 보다 높이고 解讀이 不可能하게 할 것.
- 經濟的으는 使用者가 導入할 수 있는 cost가 될 것.
- 暗號化와 그 解讀法에 있어서 컴퓨터시스템에 부하를 적게 줄 것.
- 解讀 key의 管理가 容易할 것.
- 誤謬의 影響度가 적을 것.
- 현행 system에서 무리없이 導入할 수 있을 것.

暗號方式의 基本은 換字, 轉置, 또는 雙方의 組合을 짜 맞춘 것이며 그 種類는 다음과 같다.

- 換字方式

문자를 特別히 다른 문자로 바꾸어 놓은 方法으로 다음과 같은 種類가 있다.

(a) CODE BOOK 方式
(b) CISA 方式
(c) BIJINERU 方式
(d) PANAM

- 轉置方式

문자의 위치를 바꾸는 方法이다. 發生頻度가 높은 문자는 바꾸어 놓더라도 그대로 發生頻度가 높지만 暗號强度는 CODE BOOK 方式보다 높다고 전해진다.

- 混合方式

換字方式·轉置方式을 混合한 方式이다. 이 方式의 대표적인 例는 DES(data encryption standard) 方式이다. DES는 美國商務省 標準局이 1973年에 暗號規格을 公募한 때에 採擇된 것으로서 IBM이 提案한 方式이다.

DES는 平文을 64bit 單位의 block으로 나누어서 이것을 64bit(8bit는 parity bit)의 key를 이용해서 換字·轉字를 16回 반복하는 方法이다.

- 公開 key 方式

DES 方式에 있어서 key管理의 번잡함을 해소하기 위해서 고안된 方法이다.

이것은 어느 Group의 加入者에 對한 暗號 key는 電話番號簿 같은 것으로 登錄·公開해 놓고 解讀時에는 각기의 key를 秘密로 놓는 方式이다.

(a) RSA(Rivest, Shamir, Adleman)
(b) MH 法(Merkle, Hellman)
(c) R 法(Rabin)

- mix 法

美國의 郵政省이 1982年 6月에 發表한 方法으로서 DATA 暗號 key를 公開 key 方式으로서 暗號化하여 配送한 다음 DATA의 暗號化는 DES 方式으로서 行하여 진다.

(4) 其他 技術

컴퓨터犯罪 防止技術에서 以上으로 서술한 것 以外에도 다음과 같은 分野의 各種 技術들이 있다.

- 接近의 防止 : 赤外線 感知器, 超音波 探知器, monitor TV camera, 磁氣探知, building 綜合管理시스템 등
- 隔離 : 通信回線의 埋設, 耐火金庫, 컴퓨터

COMPUTER 犯罪 防止技術 일람표

防止對策 \ 防止技術		HARD-WARE	O. S	APPLICATION	其 他 技 術
HARDWARE	CPU	KEY, HARDW-ARE TRACE	PSW, ICP, UP, AM	PSW	PP
	주 변 단 말	ID CARD, KEY	PSW, ICP, UP, AM	PSW	PP
	DISK 단 말	ID CARD, KEY	PSW, ICP, UP, AM	PSW	
	통 신 기 기		PSW, ICP, UP, AM	PSW	매설(맨홀뚜껑검착) PP
	매 체				COMPUTE BACK-UP CENTER 내화실, 금고전자차폐, PP
SOFTWARE	O.S	MEMORY 保護	PSW, HARDWA-RE ICP, UP, AM	PSW	
	APPLICATION	MEMORY 保護	PSW, ICP, UP, AM	PSW	
DATA	FILE	暗 號	PSW, DB保護, ICP Vol Ser NO. UP 暗號, AM, RAC	PSW, 暗號, DB 保護, HARDWARE KEY	
	MEMORY	記憶保護 STORA-GE(主記憶 KEY)	PSW, SOFTWARE KEY, ICP 暗號, UP, AM		
	通 信 回 線	暗 號		PSW, 暗號	
	出 力 情 報			USER 情報의 기호화	PP
對 替 設 備					빌딩統合管理 SYS-TEM ID, 이중화, 예비기, PP

(주) PSW: Password
ICP: 부정접속방지
UP: User Profile管理
AM: Access Monitoring
RAC: Resource Access Control
PP: 물리적보호(방화, 방수, 방염, 침입방지)
Vol Ser No: 매체통번

專用建物 등

- Key : Operator Key, Auditor Key
- data의 無效化 : 磁氣소거등

이것들 중에서도 특히 秘密의 强度가 높은 情報에 대해서는 특별 Label을 붙여놓고 이 자기테이프가 도난에 의해 몰래 반출되는 경우 出口를 통과하는 순간 出口에 설치된 感知器에 의해 감지되어 强力한 힘으로 磁力을 發生시켜 情報의 流出을 피하게 하는 方法이다.

라. 컴퓨터犯罪 防止를 위한 運用管理의 方向

컴퓨터犯罪를 防止하기 위해서는 신기술의 開發도 重要하지만 어디까지나 컴퓨터시스템의 運用管理體制를 충실히 하는 것이 基本이다. 특히 중시해야 할 것은 組織·人事·教育 등의 社內管理體制의 충실과 시스템監査의 도입이 정말로 重要한 對策이다. 따라서 이런 管理體制와 시스템監査를 충실히 추진하기 위해서는 制度面에서 行政的 뒷받침이 强力히 要求되고 있다.

(1) 運用管理面에서의 對應

- 組織體制

컴퓨터犯罪 防止의 관점에서는 특히 職務權限의 分割로써 適正化를 도모하는 것이 要望된다. 合理化를 도모하고 컴퓨터處理의 自動化도 進行하며 그 處理能力이 擴大되고 있는 것에도 불구하고 컴퓨터要員의 增加는 그 處理速度를 못 따라가고 있으며 아직도 手作業에 의해서 開發과 運用이 이루어지고 있는 實情이다. 따라서 繼續

사람의 努力에 의해서 이루어지고 있는 電算運用은 종래사람들끼리 內部的으로 견제해가며 실행하던 過去手作業에 비해 통제가 불능한 部分이 增加되고 있는 것이 電算要員 管理의 問題點이다. 따라서 이렇게 잃어져 가고 있는 內部統制機能을 되돌아 보고 그 機能을 무엇인가의 形態로 남기도록 再檢討할 必要가 增大되고 있다. 效率化를 도모하는 것은 당연한 일이지만 잃어서는 안되는 體制까지 소멸시키고 있는 경우에는 강한 警告를 바로 하여야 한다.

○ 人事管理

컴퓨터犯罪防止의 관점에서는 人事管理의 適正化도 重要한 要素가 된다. 예를 들면 하나의 position에 同一人物이 장기간 머무르는 것에 의해 폐해가 나온다고 하면 거기에는 rotation이 有效한 方法이 되겠다. 그러나 rotation은 專門化 指向과는 상반하는 一面을 갖기 때문에 企業의 특성, 方針이 고려되어 運用되어야 하는 것이 당연하다.

다른 관점에서 보면 컴퓨터犯罪 防止對策으로서는 不平·不滿分子를 생기지 않도록 하는 것, 特定部門에 있어서 절대권자를 만들지 않는 것 등을 人事管理面에서 해 가는 일이 重要하다고 하겠다.

○ 教育 訓練

犯罪를 범하는 것은 어디까지나 사람이다. 그것은 倫理觀이 결여되어 있다는 것이 바로 問題다. 특히 컴퓨터와 關聯해서는 비교적 새로운 業務이므로 職業倫理가 確立되어 있지 않다고 지적하는 경향도 있다. 또 한편에서는 業務의 重要度에 비하여 業務가 기계화되어 標準化되는 것에 의해 단순화하고 그 unbalance가 눈에 띄는 業務도 볼 수가 있다. 결국 重要한 業務를 대하는 態度가 安易하게 되어 버리는 경향이 있다고 생각된다.

컴퓨터業務 종사자의 教育訓練은 컴퓨터에 관한 技術的인 專門教育을 實施하는 것은 당연한 일이며 각각의 業務마다 그 重要性을 가르치는 일과 職業倫理에 관한 教育을 實施할 必要가 있는 것이다.

더우기 今後 學校에 있어서는 컴퓨터가 교과목으로 채택되어 질 것이므로 學校教育에서는 倫理教育을 包含한 컴퓨터教育을 實施하여야 할 것으로 생각하고 있다.

(2) system 監査에 對應

○ system 監査의 導入

요즘 System 監査의 必要性을 강조하고 있지만 실제에 있어서는 大企業을 中心으로 導入되고 있는 것에 불과하다. 시스템監査는 모든 使用者가 導入하여 實施하는 것이 必要하다. 이렇게 하기 위해서는 top manager가 시스템監査의 重要性을 인식하지 않으면 안된다.

○ System 監査人의 養成

시스템監査를 實施하기 위해서는 시스템監査人을 둘 必要가 있다. 시스템監査人을 養成하기 위해서는 監査人에게 컴퓨터教育을 實施하는 方法과 컴퓨터專門家에게 監査教育을 實施하는 方法이 있다. 시스템監査人을 養成하는데 긴시간이 걸리지 않기 위해서는 컴퓨터專門家에게 監査教育을 實施하는 것이 시스템監査人 養成에 있어서 훨씬 빠른 方法이다.

內部 監査部門이 設置되어 있지 않은 企業에 대해서는 project team을 編成하여 시스템監査를 實施하도록 공부를 시키는 것이 필요하다.

○ 行政의 對應

컴퓨터犯罪 防止를 위한 運用管理에 대해서는 行政的支援이 절대적으로 必要하다. 이러한 必要性을 인식시키는 일에 대해서는 모두가 경주해야 할 것이다.

○ 컴퓨터시스템 安全對策基準의 檢討

컴퓨터시스템 安全對策 基準은 Guide line으로서 책정될 뿐만 아니라 앞으로는 좀더 檢討, 추가, 修正하여 일반이 쉽게 活用할 수 있도록 보급시키는 일이 된다.

○ system 監査의 guide line의 책정, 教育 및 技術開發의 촉진

모든 컴퓨터 使用者에게 시스템監査를 實施하도록 政府가 시스템監査의 Guide line을 책정하는 일이 요구된다. 내용적으로는 使用者가 어떻게 對應하는 것이 좋은가 그 근거가 되는 基準을 나타내야 한다.

다음에 시스템監査를 正確히 이해시키고 넓게 보급·정착시키기 위해서는 時間은 걸릴지 모르지만 情報處理技術士 專門分野中 시스템監査分

野를 신설하는 것도 하나의 方法이다.

또 컴퓨터 메이커는 컴퓨터 판매시 各種의 시스템監査 tool을 提供하는 것도 바람직한 일이다. 따라서 政府는 컴퓨터 메이커에 대해서 시스템監査 tool을 開發하도록 지도하고 그 必要性이 認定된다면 적극적으로 권장해 나가야 한다.

ㅇ컴퓨터犯罪情報 center 設置

컴퓨터犯罪에 관한 情報를 수집 分析하고 그 防止에 도움이 되기 위해서 컴퓨터犯罪情報 center를 設置하여 本格的으로 硏究를 進行·指導하는 것이 必要하다고 생각된다.

마. 컴퓨터犯罪防止를 위한 法制的 檢討

情報化의 진전에 의해 컴퓨터가 産業·社會, 生活의 모든 경우에 넓고 깊게 活用되고 있다. 따라서 國民生活 全般에 많은 영향을 미치게 되는 컴퓨터犯罪는 그 輕重에 따라 法制的 檢討가 이루어져야 하여 그 犯罪의 性質과 類型을 分類, 刑量을 결정하여 이로부터 피해를 입을 선량한 國民을 保護하여야 할 것으로 사료된다.

參 考 文 獻

金麗暻, 「컴퓨터의 脈」(주) 민컴 1986.11.

Donn B. Parker, Fighting Computer Crime, Charles Scribner's Son's,: New York, 1983.

鳥居壯行, 「컴퓨터犯罪」 日本國 Computer Edge社 昭和 57.5

李鍾植, 金正成, 柳興洙, 金麗暻, 證券電算化에 따른 日本國 證券業務事故實態 및 豫防對策에 關한 調査報告書 1983.10.

李鍾植, 金榮均, 鄭泰哲, 金麗暻, 日本의 證券檢査制度와 電算業務 檢査實態 調査報告書 1986.5.

安勇根, 趙利男, 「EDP시스템 監査」 正益社 1981.1.

日本情報處理開發協會, 「시스템 監査基準 解說書」 1985.8.

金融情報시스템센터, 「金融機關 컴퓨터시스템의 安全對策基準 解說書」 1986.3.

科學技術處, 「컴퓨터 安全對策에 관한 硏究」 1981.9.

韓國情報産業協會, 第4回 「컴퓨터 시스템 利用實態調査」 1987.2.

韓國情報産業協會, 「情報産業 87.2」 1987.3.

日本情報處理開發協會, 「健全한 情報化社會의 構築을 향해서」 昭和 57.10.

한국정보시스템 감사인 협회(EDP. AA Seoul Chapter) 「컴퓨터 범죄와 예방대책」 1987.5.

金吉助, 채문규, 김궁헌, 김러성, 노연후 경영과 컴퓨터' 87.9月 10月號 민컴

유우일, 최학준, 이상률, 심우언 「미국, 영국 증권업계의 전산사고 실태 및 대책」 1983.10.