Computer Security에 관한 小考

— 事故犯罪予防을 中心으로 —

(A Study on Computer Security and Controls)

李 鍾 哲*

序 言

우리나라는 1967年 처음으로 경제기획원이 IBM 1401-6型을 도입하여 人口調査 結果를 컴퓨터로 처리한 것을 基點[1]으로 그동안 매년 평균 35%내지 40%의 높은 증가율을 보여 1978年의 約 370臺(Mini, SBC포함)[2]에서 1980年 6月末 현재 컴퓨터설치대수는 475대에 이르고 있으며 端末機는 5,416대에 달하고 있는 것으로 나타났다. 한편 금액으로 본다면 1980年 6月까지 컴퓨터 導入을 위해 4,550萬 달러를 지급하였으며 賃借料는 8,200萬 달러를 지급했으며 5차 5개년 계획이 끝나는 1986년에는 6,320대의 컴퓨터가 도입되어 이용될 것으로 예상하고 있다.[3]

이는 우리나라의 산업구조와 경제성장의 실질을 잘 나타내고 있다. 전 세계적으로 보면 1977년말 현재 IDC조사에 의하면 범용컴퓨터의 총 設置臺數는 157,208臺로서 設置金額은 927億 2,300萬달러에 이르고 있다.[4]

이와같이 컴퓨터導入에 따른 투자의 巨大化와 그 效率化의 要請은 물론 對象範圍의 확대에 따른 컴퓨터 시스템은 급속하게 대규모화되고 복잡하게 되었으며 더우기 온라인 시스템, TSS의 도입, 데이터 베이스의 구축 등은 Hardware, Software의 진보와 더불어 많은 사람이 컴퓨터시스템에 개재되어 대량의 중요한 데이터를 취급하고 관리하게 되었다.[5]

이러한 업무의 實行과 더불어 컴퓨터의 에라(error)와 악용의 위험도 뒤따르게 되며 이제는 이러한 위험의 분석을 위하여 많은 노력을 기울이게 되었다. 다시 말해서 컴퓨터의 事故와 犯罪를 방지하고 시스템의 안전을 위한 문제점을 검토하지 않으면 안되게 되었다.

근래에 發生한 컴퓨터 事故를 보면 지난 2月에는 B會社給與担當職員이 이 會社의 給與計算用役을 받은 컴퓨터 센터의 職員과 함께 會社의 公金을 횡령한 事故를 비롯하여, 3月의 A銀行과 B銀行의 事故는 信用을 生命으로 하는 銀行의 公信力과 正確·迅速으로 存在意味를 誇示하는 電算處理에 대한 信賴를 크게 失墜시켰다.[6]

그런데 이번 事故를 계기로 컴퓨터의 利用形態를 본다면 前者는 컴퓨터센터에서의 Batch processing 과정에서 發生한 事故이며, 後者는 Online system 을 利用하였다는 점이다. 이러한 事故는 컴퓨터를 犯罪의 道具로서 이용한 것이라고 볼 수 있다. 그러나 컴퓨터 事故는 반드시 人間에 의해서 침해를 당하는 것은 아니다.

자연에 의한 침해도 생각할 수 있다. 지난 4月 15日 浦項 동쪽 해저에서 일어난 地震이 바로 그것이다. 만일 진원이 육지였더라면 상당한 피해를 입었을 것이며 컴퓨터라고 예외는 아니었을 것이다.

다음은 컴퓨터 自體의 故障으로 인한 業務의 중단으로 顧客에 불편과 피해를 주는 事故도 자주 發生하고 있다.[7]

이는 우리나라도 컴퓨터와 관련된 범죄와 事故가 싹트기 시작하는 징조라 볼 수 있는데 이는 기업의 업무처리나 관리를 점차 컴퓨터에 의존해 가고 있기 때문이다. 따라서 앞으로 발생할 수 있는 컴퓨터 범죄를 사전에 방지하고 컴퓨터 시스템을 안

* 明知實業專門大學 副教授

1) 科學技術處編, '77컴퓨터總覽, 1977, p. 3.
2) 日本情報處理開發協會編, 世界コンピュータ年鑑, 昭和55年, p. 277.
3) 每日經濟新聞, 1981年2月7日字 參照.
4) 日本情報處理開發協會編, 世界 コンピュータ年鑑, 昭和54年, p. 305.
5) 横山保·監譯, Security, 秀潤社, 1978, 譯者序文.
6) 東亞日報 1981年3月28日字, 朝鮮日報 1981年3月31日字 參照.
7) 朝鮮日報 1981年7月4日字 參照.

전하게 관리할 수 있는 방안으로 컴퓨터 시스템 周邊의 Security[8] 에 관한 必要性에 대해서 考察해 보고자 한다.

Ⅰ. 컴퓨터 이용에 따른 Risk

컴퓨터를 이용함으로써 발생가능성이 있는 Risk는 컴퓨터범죄, Error, 사고, Privacy 침해 등을 들 수 있으며 security 대책을 강구하는 경우에는 모든 것이 대상이 된다. 결국 이러한 제문제는 개별적으로 해결하기 이전에 컴퓨터 시스템의 開發段階, 運用段階를 통하여 종합적이고 유기적으로 해결해야 할 성격의 문제이다.

1. 컴퓨터 犯罪

컴퓨터 범죄가 최초로 발생한 것은 1950年代 말이다. 그 후 60年代가 되면서 특히 미국에 있어서 여러가지 種類의 컴퓨터 범죄가 발생하여 사회문제화로 되기 시작하였다. 1970年代에 들어와서는 發生件數가 급격히 증가함과 동시에 미국 이외의 나라에서도 각종의 컴퓨터 범죄가 발생하게 되었다.

그리하여 70年代 후반에 이르러 컴퓨터 이용의 Demerit 의 대책으로서 privacy 保護法의 立法化가 진전되면서 다음으로서의 문제는 컴퓨터 범죄의 방지책 이라고 말하게 되었다. 이에 대해서 구체적으로는 security 면에서의 방지책과 더불어 컴퓨터 犯罪防止法이라는 관점에서 연구가 진행되게 되었다. 즉 80년대는 컴퓨터 범죄에의 대처가 정보화사회의 큰 과제로 되고 있다.[9]

컴퓨터 범죄를 大別해 보면 하나의 이득을 목적으로 하는 범죄를 비롯하여 기타는 Damage 를 주는 것을 목적으로 하는 범죄라고 할 수 있다. 前者에는 정보나 컴퓨터 관련 資産의 절취, 金錢의 절취, 사기, 횡령, Machine time 의 절취 등을 생각할 수 있으며, 後者의 경우는 피해를 줄 목적으로 컴퓨터 센터나 File 등에 대한 爆破, 기타의 파괴행위 등이다. 한편 Jhon M. Carroll 은 이를 크게 3단계로 나누어 ① 직접적인 컴퓨터실의 습격 또는 폭파, ② 外部로부터의 침입에 의한 入力資料 또는 EDP 資産에의 피해, ③ 요원들에 의한 태만이나 과괴 등으로 분류하고 있다.[10]

컴퓨터 범죄의 연구에는 세계적인 권위자인 SRI International 의 Donn B. Parker 의 조사에 의하면 記錄된 컴퓨터 범죄는 현재 세계적으로는 表 1에서 보는 바와 같이 약 700건에 달하고 있지만 이것은 빙산일각에 지나지 않는다고 지적하고 있다.[11]

表 1. 世界 컴퓨터犯罪 (1979年 1月 現在)

國名	件數
美國	472
스웨덴	35
英國	23
西獨	21
이태리	19
프랑스	9
노르웨이	7
캐나다	5
호주	4
덴마크	4
日本	3
南아프리카	3
韓國	3
홀랜드	2
필리핀	2
벨기	1
유고슬라비아	1
멕시코	1
뉴질랜드	1
기타	17
合計	633

(SRI International 調査)

이를 다시 연도별 形別로 나눈 컴퓨터 범죄를 보면 다음 네가지 형으로 분류하고 있다(表 2 參照).

① 破壞行爲
② 情報 혹은 재산의 절취
③ 金錢上의 사기, 횡령
④ 未承認된 컴퓨터사용, 서비스賣却

表2 에서 컴퓨터 犯罪를 연도별로 본다면 60년도까지는 겨우 57건에 불과한 것이 70년대에 들어와서 급증하고 있다. 70년부터 78년까지의 9년간에서, 1년간 發生件數가 60年代 10년간의 발생건수를 上廻하는 해가 7년이나 되는 것이 주목된다. 다시 말해서 컴퓨터범죄는 60년대에는 특수하고 드물게 볼 수 있는 범죄였으나 70년대가 되면서 서서히 일상다반처럼 되고 말았다.

8) Security 를 論하는 경우 여러 가지 觀點이 있다. 예를들면 Physical Security 나 Data Security 등은 그 代表的인 分野라 말할 수 있다. 여기에서는 넓은 의미의 Computer System 周邊의 Security 란 情報處理資料(사람, 機械, data, 기타 諸設備)를 自然現狀 및 人爲的인 社會惡行爲로부터 安全하게 保護하는 것이라고 定義해 두고자 한다.

9) 日本情報處理開發協會編, 世界コンピュータ年鑑, コンピュータ・エージ社, 昭和 55年, p. 151.

10) Jhon M. Carroll, Computer Security, Security World Publishing Co, Inc, 1977. p. 67.

11) Donn B. Parker, コンピュータ犯罪とその防止策, コンピュトピア, コンピュータ・エージ社 Feb. 1980, p. 58.

表2. 年別 形別 컴퓨터犯罪

年度	破壞行爲	情報 혹은 財産의 窃取	金錢上의 詐欺·橫領	未承認使用 써비스의 賣却	合計
1958			1		1
1962	2				2
1963	1				1
1964	1	2	3		6
1965		1	4	3	8
1966	1		1		2
1967	2			2	4
1968	2	3	6	2	13
1969	4	8	4	4	20
1970	8	6	13	11	38
1971	7	20	24	8	59
1972	17	18	19	18	72
1973	10	25	30	11	76
1974	7	19	35	13	74
1975	5	21	46	9	81
1976	5	18	30	4	57
1977	13	15	44	13	85
1978	9	8	12	2	31
合計	94	164	272	100	630

世界 コンピューター 年監 1980年度別 p. 153

다음은 컴퓨터범죄를 發生分野別(表3參照)로 본다면 금융기관이 가장 많은 120건, 다음으로 정부의 103건, 교육의 64건의 순으로 되어있다. 그리하여 이 3者가 컴퓨터범죄 발생건수 중에서 전체의 10% 이상을 점하고 있는 多發分野가 되었다. 이 결과는 表2에서 金錢上의 사기, 횡령이 630건중 272건으로 이는 직접적인 금전을 목적으로 저지른 범죄로서 전체의 43.1%를 점하고 있다는 것은 흥미있는 사실이다. 또한 앞으로는 Mini-computer 나 Office computer 등 휴대용이 보급되면 될수록 컴퓨터관련 資産의 절취가 증가할것이라고 생각된다. 表4와 같이 日本은 1974년 이후 금융기관의 온라인 시스템을 둘러싼 소위 CD(Cash dispenser : 自動現金支給機) 범죄의 증가가 뚜렷해지고 있다. 즉 CD범죄는 1974년에 겨우 3건에 불과한 것이 1979년에는 141건으로 격증하고 있다. 어쨌든 우리나라도 세계 컴퓨터범죄 633건 가운데 3건을 記錄하고 있다는 점과 은행의 온라인화와 더불어 CD의 설치에는 상당한 주의를 기울여야 할 것이다. (表4참조)

表3. 発生分野別 컴퓨터犯罪件数

發生分野	件數	%
銀行	120	19.2
政府	103	16.5
教育	64	10.2
製造	62	9.9
個人	43	6.9
컴퓨터써비스	32	5.1
小賣	28	4.5
保險	19	3.0
크레디트리포팅	14	2.2
運輸	13	2.1
Security	10	1.6
個人써비스	8	1.3
Communication	7	1.1
石油	6	1.0
職業學校	4	0.6
公益事業	3	0.5
特定不可能	89	14.2
合計	625	100

世界コンピューター 年鑑, 1980年度版 p. 153

表4. 日本의 CD犯罪

年度	件數
1974	3
1975	8
1976	23
1977	64
1978	131
1979	141
合計	370

世界 コンピューター 年監 1980年度版 p. 155

2. 컴퓨터犯罪의 犯人

Stanford 연구소의 자료에 의하면 컴퓨터범죄

293건에 대해서 여기에 관련된 總 482명의 직업을 조사해본 결과는 表5와 같다.[12]

表5에 의하면 범죄자의 반이상은 전산업무의 당사자들임을 알 수 있으며, 1971년 미국재무성이 발표한 금융기관에서의 컴퓨터범죄 39건에 대한 조사에서는 관련자중 전산요원이 31명 (70.5%), 전산요원이외는 13명 (29.5%)으로 전산요원이 70%를 점하고 있다. 따라서 컴퓨터범죄는 대부분의 경우 전산요원에 의해서, 혹은 전산요원이 가담하여 범행을 한다는 것이다. 이것은 컴퓨터 범죄의 실행에는 전문기술이 필요함을 의미하는 것이나, 역으로 전문기술이 있기 때문에 범죄가 유발된다고 볼 수 있다. 결국 전산요원의 범죄에 대한 의식이 문제가 되는 것이다.

表5. 컴퓨터 犯罪者의 職業

구 분		人員數	%
電算要員	管 理 者	6	1.3
	프 로 그 래 머	32	6.6
	오 퍼 레 이 터	24	5.0
	키 펀 처	17	3.5
	保 守 要 員	99	20.5
	기 타	91	18.9
	小 計	269	55.8
電算要員 以外의 企業人	經營者·管理者	26	5.4
	一 般 從 業 員	30	6.2
	小 計	56	11.6
	一 般 人	91	18.9
	學 生	49	10.2
	기 타	17	3.5
	小 計	157	32.6
合 計		482	100.0

(SRI 資料)

3. Error

컴퓨터의 목적은 한마디로 데이터를 투입시켜 이것을 미리 정해둔 명령에 따라 처리하여 그 결과를 나오게 하여 이용하는데 있다. 이때 데이터의 투입을 Input, 처리한 결과가 인간이 볼 수 있도록 나오는 것을 Output 라고 하며, Input를 지시한대로 처리하여 그 결과의 Output 을 이용하는 것이 컴퓨터를 사용하는 목적이라고 할 수 있다.

따라서 컴퓨터 에라는 Input 에 관계없이 어떤 이유에 의하여 지시한대로 Output 가 되지 않는 상태를 말한다.[13]

이와같은 에라는 인간이 범하는 과실이라고 볼 수 있으며, 따라서 의도적인 것이 아니며 악의가 개재되어 있지 않다.

단지 중요한 것은 컴퓨터 이용에 따른 위험성이 실제로 표면화 되는 경우, 發生件數나 손해액은 대부분이 에라에 의한 것이라는 점이다.

表6. ERROR発生의 要約表 (單位 : %)

發 生 源	發 生 原 因							
	System의 欠陷	Data 作成 入力의 失手	Operation失手	program Error	機械故障	施設등의 支 障	業務節次등의失手	計
傳 票 作 成	*	72.5						72.5
端末裝置의 OPERATION	*	2.8			*			2.8
入力DATA의 送受	*	0.1			*			0.1
入力媒體作成		18.4			*			18.4
OPERATION	*		4.9	0.5	0.8	*		6.2
電算業務上의 事務過程							*	
出力情報의 送受	*							
計	*	93.8	4.9	0.5	0.8	*	*	100.0

鵜澤昌和著, コンピューター犯罪とエラー p. 131

表中의 *표는 信賴할 수 있는 data 가 없는 것을 뜻한다.

Error 는 Programming, Input, Operation과정에서 發生할 가능성이 높다. 그 중에서도 특히 Input 시에 있어서 Error 가 압도적으로 많다는 것은 表6과 表7에서도 알 수가 있다.

表7. 컴퓨터 시스템의 脆弱性

rank	脆弱性의 領域	%
1	施設에의 物理的인 access	25
2	Input data 의 取扱	23
3	資産에의 論理的인 access	15
4	Business 倫理	8
5	Output data 의 取扱	8
6	Application program에의 access	7
7	Machine readable data의 取扱	7
8	System program 에의 access	3
9	Back up / Recovery	2
10	Data 通信	1

(SRI International)

12) 鵜澤昌和著, コンピュータ犯罪とエラ, 日本經濟新聞社, 昭和53年, p. 83.

13) 岩尾達男著, コンピュータ, エラー創元社, 昭和49年, p. 3.

Error의 내용은 Input data의 變換時에 있어서 키펀처의 잘못을 비롯하여, 자리수, 란상이 등에 의한 것이 상당히 많다. 즉 어느 경우든 원인은 "무관심"에 , 일어난 결과는 단지 웃음으로 끝낼정도에서 금전에 관계되어 Trouble로 발전하는 사건등 그 영향은 여러 가지인 것이다.

생각해보면 인간은 데이터처리의 정상적인 흐름만을 주로 자동화하여 왔으며 에라의 訂正回復手段등의 自動化에는 태만하였던 것이다. 그 때문에 컴퓨터 에라의 피해는 처리의 自動化의 확대에 따라 加速度的으로 증대하여 個人이나 기업은 말할 것도 없이 公共組織이나 일반사회에 이르기까지 피해를 입으며 이러한 피해의 내용도 금전, 物的資産, 인권, 정신, 육체적인 면 등 상당히 광범하다. 이러한 피해의 종류를 피해자와 그 패턴에 따라서 분류해보면 表8과 같다.[14]

더욱 앞으로 컴퓨터 중심의 정보화가 발전하면할수록 피해의 범위는 커질 것이며 이에 따른 컴퓨터 에라의 방지책과 被害求濟策의 確立이 필요하다.

4. 事 故

컴퓨터사고의 경우는 여러 가지가 있으나 日本情報開發協會와 日本情報센터協會에서 整理한 「情報處理서비스업에 있어서의 事故對策」중에서 컴퓨터 관련사고의 원인을 보면 내부적인 요인과 외부적인 요인으로 구별하고 있다.[15]

내부적인 요인으로서는

① 시스템적인 결함
② 방법, 절차, 기술적인 잘못에 의한 것.
③ 업무의 지시, 진행관리의 잘못에 의한 것.
④ EDP관련 資材, 資源의 管理不備에 의한 것.
⑤ operator의 잘못에 의한 것.

表 8. 컴퓨터에라의 被害者와 被害의 対応

被害者	被害			
	金錢 (設備를 包含)	사 람 (組織·社會)	情 報	기 타
個 人	• 個人의 金錢, 財産이 입는 損害	• 個人의 名譽, 信用등의 훼손 • 個人의 社會的地位의 실각 • 기타 個人이 입는 精神的, 肉體的被害	• 個人情報의 誤認, 個人의 誤情報에 의한 個人活動 혹은 他人에 대한 判斷, 處遇取扱上의 損失	• 個人이 입는 기타의 被害
企 業	• 企業의 資金, 資産이 입는 損害	• 企業의 名譽, 信用등의 훼손, 失墜	• 情報의 誤認에 의한 企業活動上의 損失	• 企業이 입는 기타의 被害
公共 및 一般	• 公共的事業, 公共組織이 입는 金錢的, 物的損害 • 社會一般이 입는 金錢的, 物的損害	• 公共的事業, 公共組織의 權威性, 信用의 失墜 • 一般社會에 미치는 精神的 損害	• 情報의 誤認에 의한 公共的事業活動上의 損失 • 報情의 誤認으로 一般社會에서 일어나는 誤解, 混亂	• 公共的事業, 公共組織, 一般社會에 미치는 기타의 被害

⑥ 機械障害에 의한 것.
⑦ Software의 장해에 의한 것.
⑧ 시설의 管理不備에 의한 것.
⑨ 인간의 악의, 부정에 의한 것.
⑩ 기 타

외부적인 요인으로서는

① 入力데이터의 不備
② 화재, 풍수해, 지진 등의 災害에 의한 것.
③ 파격파 등에 의한 파괴폭력행위
④ Data, Program 類의 도난이나 관련기업으로부터 파생해 온 사고
⑤ 外注處의 사고
⑥ 기 타

이와같은 사고원인을 주요사고종류와 관련시켜 보면 그림 1과 같다.[16]

以上은 主로 Hardware的인 事故이나 앞으로는 Software的인 사고도 상당히 발생될 것이 예상되며 다음과 같은 Pattern으로도 분류할 수 있다.[17]

① 컴퓨터의 物理的被壞.
② Program이나 Data類의 物理的被壞.
③ 컴퓨터화된 經務處理시스템의 悪用.
④ 특수한 勤務形態의 이용.
⑤ 컴퓨터時間의 盜用.
⑥ 프로그램이나 데이터 등의 情報의 轉賣.

14) 渡辺和英, コンピュータ犯罪とエラー, p. 99.

15) 池田泰則外, コンピュータ事故, 安全對策そして情報化保險, コンピュータ・エージ社, Nov. 1975, pp. 10 ~ 11.

16) 岡本行二著, 機密保護と安全管理, オーム社, 昭和49年, p. 111.

17) 石崎純夫著, 未來の銀行, 金融財政社, 昭和54年 p. 345

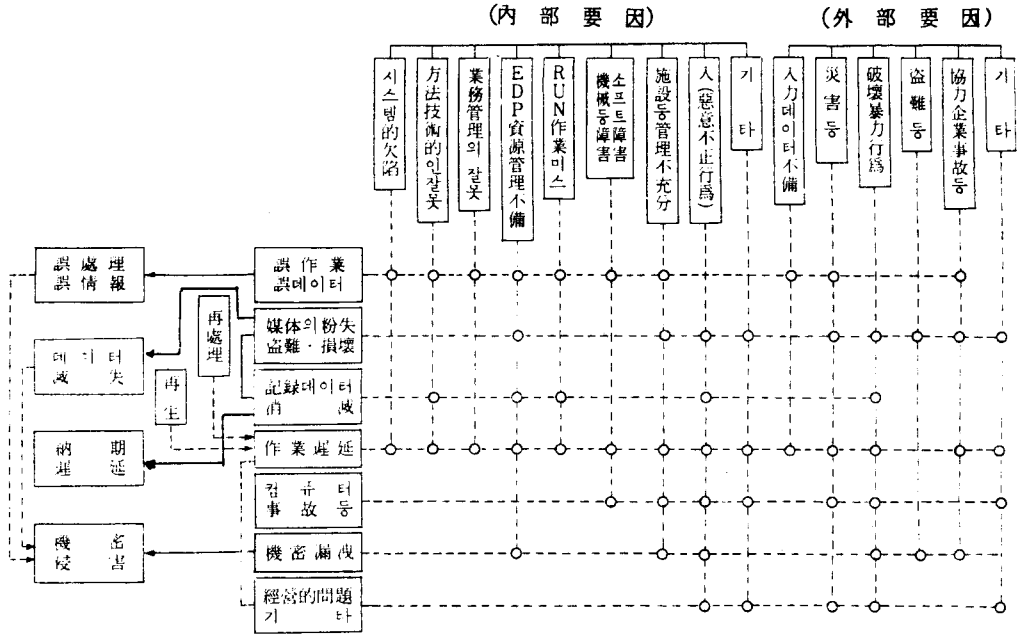

그림 1. 主要事故種類와 原因과의 關聯

⑦ 通信回線의 盜用·
⑧ 시스템 에라의 逆用·
⑨ 프로그램의 수정·
⑩ 磁氣Card의 悪用·

5. Privacy 侵割

Privacy 침해는 公共的 시스템의 電算化에서 현재 가장 문제로 되어 있는 部門이다. 이것은 企業側에서 본다면 기업기밀의 침해가 되는 것이나, 특히 문제시되는 것은 防衛力이 약한 개인의 Privacy의 침해이다. 예를 들면 電算시스템으로 File化 되어있는 住民記錄이나 의료기관에 File化 되어 있는 病歷데이터, 개인별 신용데이터, 범죄데이터 등이 부적격한 내부자나 외부자에 의해서 檢索되거나 부적절하게 이용될 위험성이 있는 것이다. 이러한 프라이버시 문제는 기본적 인격에 관계되므로 개인데이터 처리상의 문제가 되며 각 조직체는 Security상의 Safeguard, Input data 및 Output data의 관리 등 프라이버시를 보호하는 조치를 강구할 필요가 있다.[18]

II. Risk 대책의 방법

이상으로 기술한 컴퓨터이용에 따른 Risk에는 컴퓨터 시스템의 개발단계 및 운영단계를 통해서 대처하지 않으면 안된다.[19] 더우기 개개의 Risk마다 대책을 세우기 보다는 정보처리를 통해서의 기능면, 관리면의 쌍방으로 부터 종합적인 대책이 필요한 것이다.

정보처리의 환경을 간단하게 생각해 볼 경우 먼저 컴퓨터 시스템을 비롯하여, 다음으로 컴퓨터의 요원과 User가 있으며 컴퓨터로부터 가장 멀리 떨어져 있는 일반시민이 있다(그림 2).

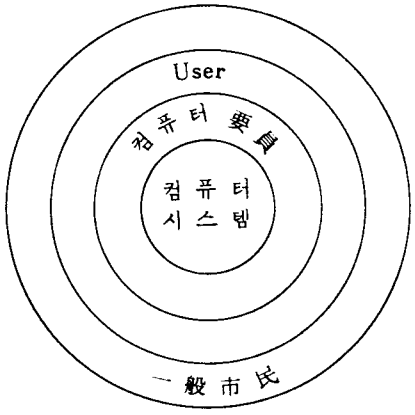

그림 2. 컴퓨터 環境

1. 컴퓨터 시스템

컴퓨터 시스템에 대해서는 컴퓨터실을 생각해보는 것이 좋을 것이다. 여기에는 Hardware, Software 및 關聯諸設備가 있다. 이러한 것은 정보처리의 중

18) 日本情報處理開發協會編, システム監査體制確立への道, コンピュータ・エージ社, 昭和52年, pp. 14～15.

19) 日本情報處理開發協會編, システム監査實施への道標, コンピュータ・エージ社, 昭和55年 參照.

축을 이루고 있으므로 당연히 안전성이 높게 유지되도록 요구되고 있다.

따라서 컴퓨터 시스템을 각종의 위험으로부터 보호하기 위하여 security대책이 검토되지 않으면 안된다. 구체적으로는 物理的, 管理的인 면에서 safe-guard를 실시할 필요가 있다.

2. 컴퓨터 要員

Error나 범죄를 범하는 것은 역시 인간인 것이다. Donn B. Parker는 電算要員의 범죄에 점하는 비중이 크므로 採用時의 충분한 신원조사를 강조하고 있지만 사실 별로 효과를 거두지 못하고 있다는 것이다. 무엇보다 문제는 요원의 도덕성에 있는 것이다.

J. Martin은 전산요원의 도덕성이 저조하면 에라나 범죄를 일으키기 쉽다고 지적하고 있다. 그러나 도덕성 앙양은 단지 어떤 캠페인 만으로는 실현되기 어려움으로 직장의 인간관계, 작업의 적절한 할당, 적성이나 능력의 파악, 장래의 전망, 특히 급여수준 등을 충분히 고려하지 않으면 안된다.

최근 전산시스템의 보급 및 발달에 따른 전산기술자, 전산요원의 우위성이 점차 저하되고 있다. 이는 과거의 키펀처만 되어도 일종의 高技能職으로 생각하였으며, 프로그래머는 엘리트적인 존재로 여겼지만 오늘날에는 키펀처는 물론 프로그래머에 대해서도 특별한 직종이라고 누구도 생각하지 않고 있다. 말하자면 전산부문은 고도한 직장이 아닌 다만 일종의 專門職 부문에 지나지 않는 것으로 보고 있다. 따라서 이와같은 환경에서 더우기 요원의 도덕성을 앙양시키려면 관리에 충분한 배려와 責任과 권한에 따른 組織上의 분리도 바람직하다.

예를들면

① Operator는 專任으로 할 것.
② 조작은 항시 복수의 operator로 할 것.
③ 정기적인 근무교체를 할 것.
④ Operator의 근무일지를 검사할 것.
⑤ Scheduling 담당자와 operator 와의 겸임을 피할 것.
⑥ 작업분담을 명확히 할 것.[20]

등으로 컴퓨터실의 안전대책으로는 요원관리가 무엇보다 중요한 과제임을 알 수 있다.

3. USER

User에 대해서는 컴퓨터 이용에 관한 규정이 명확해야 한다. 물론 user에도 여러 가지의 경우가 있다. 예를 들면 처리가 끝난 output를 수령하는 경우만 있는가 하면 user가 직접 컴퓨터를 조작하여 업무처리에 임하는 경우도 있다.

On-line Realtime System의 경우에는 User부문에서 端末機를 소유하여 직접 조작하고 있다. 특히 은행의 On-line system에서는 고객에게 CD카드를 발행하여 Cash dispenser로부터 직접 조작되고 있다.

User는 어떠한 방식을 취할 것인가는 별도로 하고 컴퓨터에 access할 수 있는 입장에 놓여 있다. 따라서 Access control (접근 및 조작의 제어)이 중요한 의미를 갖게 되며, 이는 컴퓨터 시스템 및 關聯設備, 시설 등에 대한 접근과 더불어 조작을 control 하지 않으면 안된다는 것은 user에 한해서만 필요한 것은 아니며 컴퓨터요원에 대해서도 기타 제3자에 대해서도 마찬가지이다.

4. 一般市民

이것은 당연히 제3자로서의 개인으로 컴퓨터와는 직접적으로 관련을 가지고 있지는 않다.

그러나 이러한 개인에 관한 data가 컴퓨터로 처리되고 있는 경우에는 privacy보호문제가 나오게 된다.

가령 自己의 data가 컴퓨터로 처리되고 있는 경우에 그 data의 내용에 부적합한 점이 있으면 자기의 data를 자신이 살펴, 만일 잘못되었으면 수정할 수 있는 권리의 부여 등이 필요해 진다.

이상과 같이 위험대책으로서 컴퓨터 시스템, 컴퓨터 요원, user, 일반 시민을 대상으로 할 경우 이를 간단히 종합해 보면 表9와 같으며 대책 후의 情報處理環境은 그림3과 같이 생각할 수 있다.

Ⅲ. 시스템 監査의 役割

컴퓨터 이용에 관련되는 Security를 논하는 경우에 중요한 것은 어떠한 risk가 가능성으로 존재하는가를 명확히 할 것과 이에 대한 Security 대책을 세워 이후 계속하여 Security감사를 실시하도록 하는 것이다.

일본의 경우를 보면 1974년 日本 情報開發協會가 시스템 감사를 제창하였으며 이 중에서 시스템 감사의 한 측면으로서 Security감사의 위치를 다지게 되었다.[21]

결국 Security감사란 안전성의 관점에서 컴퓨터 시스템을 과실, 사고, 부정 등으로부터 보호하기 위한 감사라고 할 수 있다. 바꾸어 말하면 Security의 상태를 감사하는 것이다. 이하 Security감사를 포함하는 시스템 감사에 대해서 간략하게 기술해 보

20) 日本情報センタ協會編,電子計算機システム安全對策 基準解說書, 昭和52年, p. 259.

21) 日本情報處理開發協會編, わが國におけるシステム監査のあり方, 昭和51年, p. 2.

表 9. 컴퓨터環境에의 対策

對 象	對 策	具 體 例
컴퓨터 시스템	物理的安全對策	Selfguard
컴퓨터 要員	責任·權限의 明確化	內部牽制
User	利用面의 규정화	Access Control
一般市民	Privacy 의 保護	監査의 權利

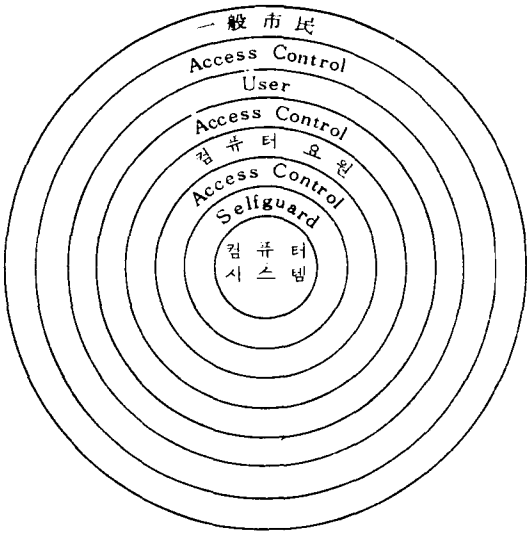

그림 3. 對策이 강구된 컴퓨터環境

고자 한다.

1. 시스템 監査란

시스템 감사란 감사대상으로부터 독립한 객관적인 입장에서 컴퓨터를 중심으로 하는 정보처리 시스템을 종합적으로 점검·평가하여 관계자에게 조언·권고하는 것을 말하며, 이의 有效利用의 촉진과 弊害의 제거를 동시에 추구하여 시스템의 건전화를 도모하는 것이다.[22]

즉, 시스템 감사란 다음과 같이 요약할 수 있다.

① 컴퓨터의 有效利用을 도모하며
② 컴퓨터 이용에 따르는 error·사고·범죄 Privacy의 침해 등의 弊害를 제거하며
③ 시스템 품질을 유지하며
④ 위의 제사항에 의해서 시스템의 건전화를 도모하는 것을 목적으로 하는 감사활동이다.

이것은 컴퓨터를 이용하고 있는 조직체 자신에 있어서 필요한 것이며, 따라서 시스템 감사는 第1義的으로는 조직체의 내부적 요청에 기인한 것이라고 말할 수 있다. 민간기업에 한정하여 말한다면 당연히 경영자가 스스로 기업경영을 위하여 솔선하여 시도해야 할 부문이다.

2. 시스템 監査人의 役割

시스템 감사가 무엇인가를 理解한다면 시스템監査人의 역할도 자연히 명백해질 수 있다. 즉, 시스템監査人이란 컴퓨터와 監査의 쌍방에 대해서 능력을 지닌 內部監査人으로 그 역할을 살펴보면,

① 경영에 도움을 주기 위하여
② 컴퓨터 부문에서 독립한 객관적인 입장에서
③ 효율의 추구, 弊害의 제거, 품질의 보증 등의 관점에서 컴퓨터 시스템을 감사하며
④ 그 결과에 대해서 조언, 권고 등을 내포한 report를 관계자에게 제출한다.

좀더 구체적으로 말하면 시스템 감사인의 임무는 다음과 같이 정의할 수 있다.[23]

시스템 監査人은 시스템監査를 통해서 다음의 각 항의 실현에 공헌할 수 있도록 노력하지 않으면 안 된다.

① 시스템의 유효이용을 促進하고 처리의 정확성을 확보하는 일.
② Error의 발생을 방지하는 일.
③ 地震등의 自然災害對策을 충분히 습득하여 사고의 발생을 방지하는 일.
④ Privacy 침해를 방지하는 일.
⑤ 컴퓨터 범죄를 방지하는 일.
⑥ 기타 종합적인 시스템의 건전화를 도모하는 일 등이다.

3. 컴퓨터 犯罪와 시스템監査

최근 컴퓨터 범죄가 증가경향에 있다는 것은 이미 기술한 바 있다. 여기에서 「컴퓨터 범죄란 컴퓨터가 직접적으로 혹은 간접적으로 어떤 형태로 개재된 사회악 행위이다」[22]라고 정의해 본다면 컴퓨터 범죄를 연구하는 입장으로서는 첫째로 컴퓨터 범죄의 사례 등을 분석, 연구하여 컴퓨터 시스템 guard를 위한 방법론을 생각해 내는 것을 目的으로 하는 연구이며 이것은 범죄방지라는 견지에서의 연구이며, Security 에의 접근방법이다.

둘째는 오늘날 정보화 사회에서의 違約된 법률을 어떻게 정비해 갈 것인가의 관점에서의 연구이다. 이것은 법률면에서의 접근방법이다.

그리하여 전자에 대해서는 시스템 監査가 아주 유효한 수단이 되며, 시스템 監査를 실시하므로써 그 컴퓨터 시스템의 脆弱性이 발견되면 사전에 대책을

22) 日本情報處理開發協會編, システム監査體制確立への道, 昭和52年, p. 12.

23) 日本情報處理開發協會編, システム監査實施への道標, p. 233 및 システム監査基準(試案) 參照.

24) 鳥居壯行, コンピュータ犯罪研究, 警察論集, 昭和54年, p. 79.

강구할 수가 있도록 하는 것이다.

단지, 현 단계에 있어서의 시스템 감사를 실시한 結果 컴퓨터 범죄가 발견되었다는 예는 없었다. 이것은 테크닉 기타 시스템 監査의 연구가 좀더 강력히 진행되지 않으면 안된다는 것이다. 무언가 이상한 징조가 보이는 경우에는 시스템 監査가 강력한 힘을 발휘할 수 있어야 하며 그 절차는 다음과 같다.

① 不規則性의 발견
② 시스템 監査의 실시
③ 不正 誤謬의 발견

그러나 이와같은 경우의 不規則性의 발견이라는 것은 말하자면 우연한 발견에 지나지 않는다. 컴퓨터 범죄는 범죄자와의 지혜를 견주어 보는 것 같은 요소가 많으므로 그 기미가 외부로 나타나게 된다는 것은 상당히 어려운 것이다. 그러므로 시스템 監査로 불규칙성을 발견한다거나 혹은 직접적으로 부정이나 오류를 발견할 수 있도록 하지 않으면 안된다.

4. 犯罪減少에 期待할 수 있는 要素

컴퓨터 범죄의 감소에 기대할 수 있는 요소가 없는 것은 결코 아니다. 우선 컴퓨터 시스템의 대규모화나 자동화를 들 수 있다. 대규모의 Program 개발에는 많은 Programmer가 분담하고 있다. 이것은 한 사람이 Programming 하는 경우에 비교해서 開發段階에서의 범죄의 가능성은 낮다고 말할 수 있다. 한편 자동화로 사람의 개입이 감소하면 할수록 범죄의 기회는 줄어들 것이라고 볼 수 있다.

다음은 안전대책의 강화를 들 수 있다. 이것은 物理的인 면이나 management면을 포함하여 최근에는 컴퓨터 센터에의 접근이나 情報保管場所의 접근이 아주 어렵게 되고 있다.

그러나 무엇보다 중요한 것은 사람의 문제이다. 기업과 종업원의 결속과 신뢰관계가 우선 내부로 부터의 범죄를 막는데 도움이 될 것이다.

結 言

이상과 같이 다양화된 정보를 신속히 처리하기 위하여 컴퓨터화가 되면 될수록 컴퓨터 시스템에 의한 사고의 영향범위가 확대될 것이 예상되며 따라서 컴퓨터 시스템의 脆弱性을 徹底히 保完하면서 시스템 監査體制를 확립하고 안전대책의 기준을 설정하는 등 컴퓨터를 중심으로 하는 정보처리 시스템의 신뢰성을 향상시킬 수 있도록 노력해야 할 것이다.

參 考 文 獻

1) James Martin, Security, Accuracy and Privacy in Computer Systems, Prentice-Hall, Inc. 1973.
2) L. J. Hoffman, Modern Methods for Computer Security and Privacy, Prentice-Hall Inc. 1977.
3) J. G. Burch. Jr., and J. L. Sardinas, Jr, Computer Control and Audit, John Willy & Sons, 1978.
4) Peter Hamilton, Computer Security, Auerbach Pub. Inc. 1973.
5) John M. Carroll, Confidential Information Sources : Public & Private, Security World Publishing Co., Inc, 1975.
6) S. H. Lavington (ed.), Information Processing '80 North-Holland Publishing Co. 1980. pp. 845～849.
7) 日本經營協會編, システムの運用と管理, 昭和52年.
8) 石崎純夫編, 實例コンピュータ・バキング, 近代セールス社, 昭和54年.
9) 伏見章編著, EDP監査の實際, 中央經濟社, 昭和47年
10) 大矢知浩司著, EDP會計監査, 白桃書房, 昭和51年.
11) 谷村外志男著, コンピュータの運用管理, 日刊工業新聞社, 昭和 51年.
12) 菅野文友著, ヒューマンエラのメカニズム, 日科技連出版社, 1980.
13) 掘內慕一著, コンピュータ犯罪－情報とプライバシー, 日本工業新聞社, 昭和49年.
14) Donn B. Parker, 羽田三郎譯, コンピュータ犯罪, 秀潤社, 昭和1979.
15) AFIPS, 横山保, 萬代三郎監譯, セキュリティ, 秀潤社, 1978.
16) CICA, 平野皓正, 高梨智弘譯, コンピュータコントロールの手引き, 日刊工業新聞社, 昭和54年.

Abstract

Recently there has been a marked increase in concern for security in computerized operations. The purposes of computer security controls are to protect against the unauthorized access to and modification of data processing resources, unauthorized access to and modification of data files and software, and the misuse of authorized activities.

The controls relate to the physical security of the data processing department and of the areas within the data processing department ; to the security of the data files, programs, and system software ; and to the human interaction with the data files, programs, and system software. The controls that will be discussed in this paper include :

I. Risk on the computer use
II. Methods of risk counter measure
III. Role of system auditing