情報시스템 security意識實態에 關한 比較硏究

- 韓·日 情報處理 專門要員 中心으로 -

金 榮 建[1)]

This study has carried out a comparative research on the conscious of Information Pressing Personnel of Korea and Japan. A conscious situation of Japanese based on the result 1,671 personnel of Japan Information Pressing Development Association(JIPPA) from October 3, 1994 to November 3, 1994. However these of Korean was 240 personnel from January, 1996 to May, 1996.

The conscious situation of IS(Information System) on a security related with a computer crime, in addition to that security, the security policy toward the computer crime was suggested.

Ⅰ. 序論
1.1 硏究의 目的
1.2 硏究方法 및 範圍

Ⅱ. 情報시스템의 security領域과 構成內容
2.1 情報시스템 security 槪念과 領域
2.2 情報시스템 security構成內容

Ⅲ. 情報시스템의 security實態
3.1 先進國의 IS security實態
3.2 韓國의 IS security實態

Ⅳ. security實態 意識調査
4.1 調査期間 및 對象
4.2 調査結果 및 分析
4.3 對策方案

Ⅴ. 結論
參考文獻

1) 啓明大學校 經營大學 經營情報學科 敎授

Ⅰ. 序　論

1.1 硏究의 目的

오늘날 컴퓨터 産業과 關聯된 最尖端 情報處理機器들의 비약적인 發展과 急速한 普及擴大는 國家 및 地方自治團體의 公共機關과 企業組織, 金融, 學界 및 社會 여러 分野에서 모든 情報들이 컴퓨터로 處理되고, 大量의 情報와 複雜한 情報들을 효율적으로 수집·분류·저장·검색 및 管理함으로써 個人이나 組織의 發展도 기할 수 있게 됐다.

組織에 있어서 컴퓨터 시스템의 導入 및 活用과 관련된 많은 硏究가 進行되어져 왔고, 앞으로도 계속될 것으로 展望된다. 사회 모든 조직에 있어서 發生하는 모든 情報가 컴퓨터로 處理됨으로써 컴퓨터에 의한 逆機能이 發生하고, 이것이 社會的인 심각한 問題로 대두되고 있는 實情이다. 그러나 컴퓨터 逆機能에 대한 硏究가 소홀히 되어 온 것이 事實이고 國家機密에의 接近, 私生活의 秘密侵害와 企業秘密, 其他 各種 컴퓨터 犯罪의 增加, 컴퓨터 virus 및 hacker 등의 심각한 社會問題가 提起되고 있다. 특히 高度 情報社會에 있어서 컴퓨터에 의한 가장 代表的인 逆機能은 一般的으로 컴퓨터 犯罪(computer crime)로 통칭되고, 그 逆機能[1]에는 컴퓨터 犯罪的 逆機能 以外에도 社會的 逆機能, 文化的 逆機能 및 倫理的 逆機能을 들 수 있다. 컴퓨터 犯罪의 逆機能 現狀으로는 컴퓨터의 不正操作, 誤用, 破壞, 데이터의 變造, file毁損, 情報竊盜, data不正流出, 컴퓨터 virus 등을 들 수 있고, 社會的 逆機能으로는 自動化에 隨伴되는 失業者의 誘發, 시스템 統合으로 인한 産業構造의 變動과 構造的 葛藤, 情報通信網의 돌연한 마비로 인한 社會的 混亂, 個人身上 記錄의 不正流出이나 濫用으로 인한 個人情報의 侵害現狀 등을 들 수 있다. 또한 컴퓨터에 의한 文化的 逆機能 現狀으로는 國際 情報通信網을 통해서 淨化되지 않는 外國文化의 不法流入, 國家 重要情報의 不法流出, 情報의 不法複寫로 인한 著作權 侵害, 低俗한 게임 오락에 의한 情緖的 被害를 들 수 있고, 또 컴퓨터에 의한 倫理的 逆機能 現狀으로는 電算網을 通한 低俗한 情報의 流通과 非倫理的 加害 行爲 등으로 인한 情報者의 混亂, 私設 컴퓨터 通信網(BBS : bulletin board system)을 利用한 混亂 프로그램의 商行爲, 전자사서함 프로그램을 통한 非倫理的 情報交換 및 流布 등을 들 수 있다. 이러한 逆機能 現狀을 막을 수 있는 制度的 裝置가 마련되어 있지 않을 때, 이것이 社會的으로 미치는 영향은 심각할 것으로 본다. 特히 情報化 社會로의 進展이 급속히 이루어짐으로써 企業組織의 network, 政府行政 電算網 構築, 國家정보를 저장하고 있는 data base(data bank)가 computer network system에 의한 廣域化에 대한 security對策의 確立이 절실히 필요하다고 본다.

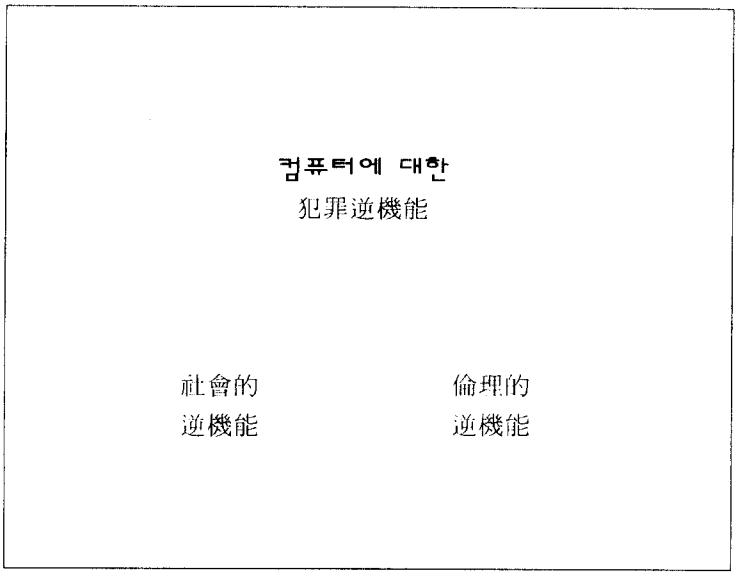
따라서, 本 論文에서 情報化 社會에로의 發展에 따른 컴퓨터 使用에 의한 逆機能 現狀과 컴퓨터 犯罪와 關聯된 情報處理要員들의 情報시스템 security 意識實態를 調査하고, 이에 對한 security對策을 提示하는데 硏究의 目的을 둔다.

註1) 國家情報化 白書(1994年), 韓國電算院, 서울, 1994, 536-537쪽.

1.2 研究方法 및 範圍

本 研究의 目的達成을 위해서 文獻的 研究方法에 의해 情報시스템의 保安(information system security)과 關聯된 內容에 關한 理論的 背景을 整理하고, 情報시스템의 利用者들인 情報處理專門要員들이 情報시스템 security에 對하여 어떤 意識을 가지고 있는지 設問紙 調査方法에 의하여 進行하고자 하며 研究範圍는 <그림 1>에서 보는 바와 같이 컴퓨터에 의한 여러 가지 逆機能 中 컴퓨터 犯罪의 源泉인 컴퓨터 犯罪의 逆機能과 關聯된 것에 限定하여 韓·日 比較 研究를 行하고, 그 結果에 따라 情報시스템 security對策을 提示하는 것으로 한정한다.

<그림 1> 컴퓨터에 의한 逆機能



Ⅱ. 情報시스템의 security領域과 構成內容

2.1 情報시스템 security 槪念과 領域

2.1.1 情報시스템 security 槪念

情報시스템의 security統制[2](information system security control)는 HW, SW 및 情報

註2) 三逸 經營經濟研究所 編, 시스템 監査 槪念, 世明書館, 서울, 1989, 237쪽

處理要員들이 예기치 못한 機器障碍(故障) 즉 事故로부터 컴퓨터 센터를 保護하고, 컴퓨터 시스템, data 또는 program의 故意, 非意識的 破壞 또는 破壞에의 노출로부터 보호하는 것, 컴퓨터와 關聯된 資産과 情報를 不法으로 變容, 流出 및 破壞에 대한 保護, 管理 잘못과 人間行爲의 잘못으로 因한 事故를 防止하는 行爲를 保安(security)[3]이라고 한다. 즉 컴퓨터 시스템에 대한 保安對策(security measure) 또는 保安統制(security control)는 HW, SW, 通信回線 등에 있어서 예기치 않은 機能障碍나 事故로부터 시스템을 保護하는 것[4]을 意味하는데, 情報시스템의 security를 低害하는 威脅要因 즉 保安事故의 原因으로는

첫째 컴퓨터 關聯機器故障 또는 物理的 原因에 의한 事故
둘째 不正行爲 및 access와 SW잘못에 의한 事故
셋째 停電 및 通信設備의 故障
넷째 시스템의 破壞
다섯째 怠業 暴動 및 人爲的 事故
여섯째 天災地變(홍수, 지진, 냉해 등) 및 不可抗力的인 狀況

등을 들 수 있다. security統制는 情報시스템의 安全性을 위협하는 것을 미연에 防止하고 可能한 한 신속히 發見하여 그로 因한 被害를 最小化하는 일련의 管理活動을 意味한다.

2.1.2 情報시스템의 security領域

Royal P. Fisher가 情報시스템 security에 관한 對象을 data libraries, password 및 機能的 組織(functional organization)에 한정하였으나, 컴퓨터 시스템의 導入·活用이 擴大됨으로서 情報시스템의 保安統制管理[5](security control area of information system)의 내용을 아래와 같이 要約할 수 있겠다.

첫째 情報시스템의 物理的 保安(physical security) : 火災, 洪水, 浸水, 侵入
둘째 統制와 節次(control and procedure) : 組織的 統制, 人的 統制, 作業的 統制, 接續統制 應用 開發, 其他
셋째 狀況 綜合的 計劃(contingency planning) : 일반적인 것(폭풍,지진,폭격,폭동), 基本的 서비스의 損失(냉·난방, 의사소통, 자료전달), 緊急狀況(화재경보, 일기경보, 비상경보 등), 重要한 業務의 back up, 복구(recovery)

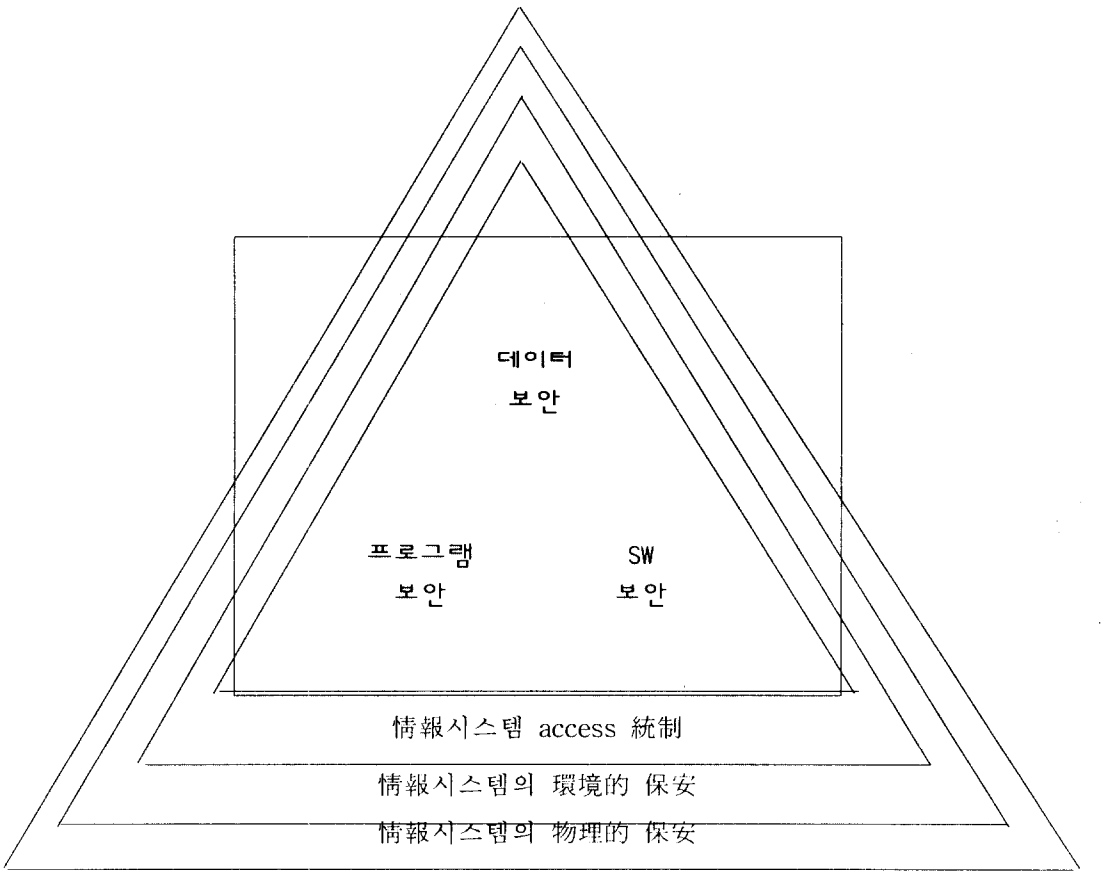
2.2 情報시스템 security 構成內容

Royal P. Fisher의 保安統制 範圍를 앞에서 提示하였지만, 一般的으로 情報시스템의 保安統制 對象[6]은 情報시스템 物理的 保安(physical security), data保安(data security) 및

註3) 安勇根·趙利男, EDP시스템 監査, 正益社, 서울, 1979, 231쪽.
註4) 申珏澈 著, 컴퓨터와 法律問題, 法榮社, 서울, 1993, 291쪽.
註5) Royal P. Fisher, Information System Security, Prentice-Hall N. J. 1984, p.43
註6) 王逸 經營經濟研究所 編, 前揭書, 서울, 237쪽.

software保安(software security)으로 細分되고 略字로는 PDS(physical data security)[7]라고도 하는데 그 構成內容을 要約하여 보면 <그림 2>와 같다.

<그림 2> 情報시스템 security構成 內容



2.2.1 情報시스템의 物理的 security

情報시스템의 物理的 security管理는 컴퓨터 hardware의 security管理를 포함하며, 物理的인 위협요인으로부터 物理的 施設 保護에 必要한 일연의 장치와 方法을 說明하는 것으로 data security을 必要로 하는 物理的 access를 統制하는 方法이다. hardware security管理上 發生할 수 있는 위협적인 문제점들을[8] 要約하면 다음과 같은 점들을 指摘할 수 있다.

첫째 不法的 access

註7) 韓國情報시스템 監査人協會, 情報시스템 監査論, 法榮社, 서울, 1990, 20쪽.
註8) 安勇根·趙利男, 前揭書, 251쪽.

둘째 process hardware의 고장
(原因으로는 ① 보호회로가 고장일 경우, ② memory의 read/write를 보호하는 회 로가 고장일 경우 ③ mode처리를 要求하는 interrupt의 무시)
셋째 process에서 情報의 漏泄
넷째 자기 tape와 disk에 기록하는 head
다섯째 通信回路에서 情報漏泄
여섯째 通信回路網의 分岐
일곱째 保安者와 漏泄
여덟째 交換者 hardware의 故障과 情報漏泄
아홉째 使用者의 I/O장치에서 情報漏泄
열째 remote에서의 情報漏泄
열 하나 使用者의 不法的 access

情報시스템의 物理的인 統制方法으로는 수위 및 안내(guard and escort), 出·入記錄簿(sign-in/sign-out register), 出入證(badge), 카드, 폐쇄회로 모니터(closed-circuit monitors), 서류세단기(paper shredders), 二重門(double-entry doors), 一方通行門(one-way emergency doors)등이 있고, 또한 保安統制計劃에는 data center의 位置에 대단히 중요하므로 관리지침으로서 원격지(remote location), 別度建物(separate building), 標識(identification utilities)統制 및 back-up施設(back-up facilities) 등을 들 수 있다.

2.2.2 情報시스템의 環境的

情報시스템의 環境的 security管理(environmental security control of information system)는 컴퓨터 시스템을 지원하는 주변환경 시스템의 信賴性을 높이기 위한 統制와 컴퓨터 關係施設의 security管理로서 情報시스템이 정지될 위험성을 줄이기 위한 일련의 조치를 意味한다. 컴퓨터 關係施設의 security管理는 電源空調施設 및 防火設備 등을 포함하며, 컴퓨터 센터의 保護를 위하여 職員訪問者, 侵入者의 出·入制限과 洪水, 地震등 自然發生에 의한 不可抗力的인 天災地變에 대한 對策도 포함한다. 컴퓨터 關係施設의 security管理 對象을 具體的으로 살펴보면 다음과 같은 것을 指摘할 수 있다.

첫째 電源施設(electronic facilities control)
; 컴퓨터 시스템과 함께 공조시설, 人力변환장치, 照明, 엘리베이터 등 補助施設에도 信賴度가 높고 品質이 높은 電源이 要求된다.
① 입력전원양식(전압 및 주파수, 相數 및 結線, 허용변동 범위)
② 전원안전장치(過電流保護器, 자동전압조절기, 無停電原裝置(uninterruptible power supply UPS/CUCF)
③ 接地

둘째 空調施設
① 溫·濕度 許容 範圍(humidity control)
② 機械의 空調氣循環方法
③ 먼지 除去(dust control)

④ 냉·난방관리(heating and cooling control)

셋째 防火設備(file facilities control)

① 컴퓨터室 位置 및 整理

② 火災探知(컴퓨터 上下左右에 探知機 設置)

③ 火災發生(消火活動에 出動)

④ 手動消火器 作動

⑤ 固定消火器 設備

⑥ 損失管理

⑦ 消防訓練

넷째 入·出管理(I/O control)

다섯째 洪水(water control)

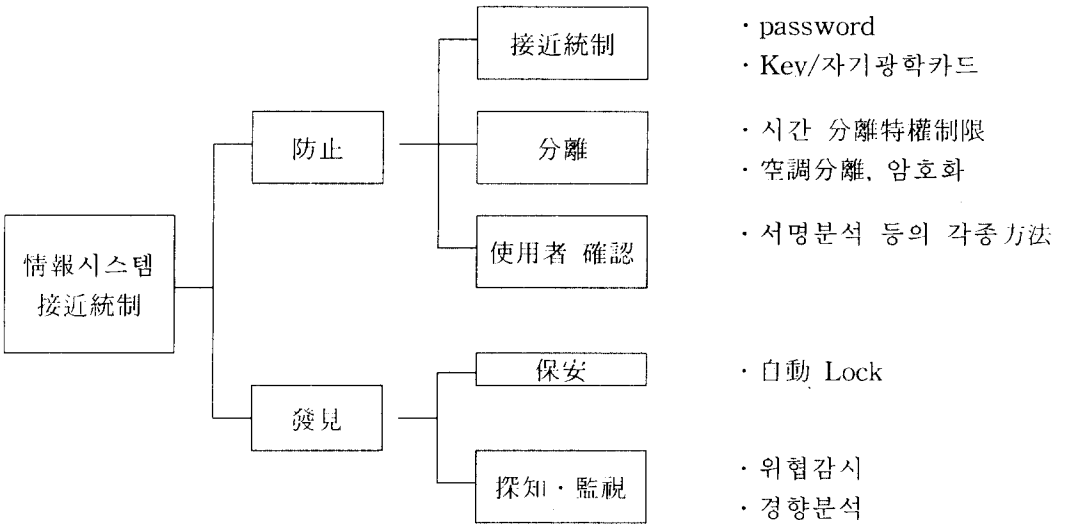
여섯째 地震

일곱째 긴급정전 관리(emergency shutdown control)

2.2.3 情報시스템의 access統制

情報시스템의 access統制는 <그림 3>과 같은 目標를 가지고 情報시스템의 保安을 지키려는 活動을 意味하며, on-line communication system을 통해 host computer에 접근하고자 할 때 시스템 使用者가 識別되어져야 한다. 시스템의 使用者 識別方法을 통해서 정보시스템의 access를 통제하고 保護할 수 있다.

<그림 3> 情報시스템 access統制方法[9]



情報시스템의 使用者 識別方法으로는

註9) 李逸 經營經濟研究所, 前揭書, 241쪽.

첫째 시스템 使用者의 所有物(열쇠, 자기 또는 광학식 카드 利用)
둘째 시스템 使用者, 個人의 知識(암호를 사용하는 方法)
셋째 시스템 使用者 個人的 特徵(체험, 지문, 음성패턴, 서명분석 및 기타의 유전적 특성) 등으로 分類되며, 使用될 수 있다.

2.2.4 情報시스템의 SW保安

情報시스템의 SW security管理(SW security of information system)는 3가지 側面에서 이루어진다.

첫째 컴퓨터 생산회사가 제공하는 SW에 대한 security管理
① operating system (OS)
② data management system(DMS)
③ utility program
④ 診斷 program
⑤ application package
⑥ teleprocessing package

둘째 시스템 使用者가 만든 SW에 대한 security管理
① 시스템 使用者가 만든 SW(예. 會計프로그램, credit check 프로그램, 각종 응용프로그램)
② data file
③ program 변경 관리

셋째 內部프로그램의 監査에 의한 security管理
① random test (정상처리 여부)
② integrated test(SW, HW의 정상여부 및 system內의 프로그램, data의 정상여부)
③ backup(도난, 재해, 기계의 고장대비)

2.2.5 情報시스템의 通信網 security[10]

컴퓨터 시스템이 資料處理시스템 또는 情報시스템으로 導入되기 前에는 部署間의 直接資料傳達을 하였으나, 오늘날에는 電話回線, 近距離通信網(local area network : LAN), 또 通信위성 system을 通해서 data나 情報를 傳達하게 됨으로 여기에 대한 保安裝置가 必要하며, 保安의 障碍의 種類 즉 通信障碍種類는 다음과 같은 것을 들 수 있다.

첫째 message의 紛失 및 變更(message loss or change)
둘째 災害나 그 밖의 攪亂(disasters and other disruptions)
셋째 保安 및 盜難(security and theft)
넷째 復源 (recovery and restart)
다섯째 誤謬處理(error handling)
여섯째 data傳送時 및 전송 중에 data에 대한 妥當性 체크(data validation or checking)

註10) 三逸 經營經濟硏究所, 前揭書, 230쪽.

이런 通信障碍를 일으킬 수 있는 通信시스템이 基本的인 構成은 다음과 같다.

첫째 terminal(단말기나 host computer간의 정보전달 매체)

둘째 modem(신호의 변조 및 복조시 사용하는 장치)

셋째 通信채널(communication channel)

넷째 通信制御 프로그램(communication control unit)

다섯째 通信制御 프로그램(communition control program) : 운영system을 통신제어 system에 적응시켜주는 software를 말함.

通信system에 security問題는 다음과 같이 4가지로 요약할 수 있다.

첫째 回線보안(line security) : 通信回線을 통한 시스템 接近을 事前에 한정시킴

둘째 傳送보안(transmission security) : data通信 中間에 가로채려는 努力을 무력화하도록함. 修行機能 및 運用可能時間의 제한 절차, 회선식별 절차의 적용, 인증절차의 適用 및 통신 log의 利用

셋째 암호화에 의한 保安(cryptographic security) : 인가를 받지 않은 자가 해독하는 것을 막고 어려운 코드로 data를 전송하는 것을 막는 것.

넷째 전자파 방출의 保安(emission security)

通信回線上의 問題가 發生하지 않도록 하거나 最小化하기 위해서 다음과 같은 統制節次를 따르는 것이 有利하다.

첫째 message 도강 system(message logging system)의 사용

둘째 message의 수령 통지

셋째 message의 연 번호부여

앞에서 情報시스템의 security 槪念, 領域 및 構成內容을 具體的으로 고찰해 보았다. 實際 先進國이나 우리나라에서 情報시스템의 security를 위한 대응책은 어떤지 具體的으로 考察하고자 한다.

Ⅲ. 情報시스템의 保安實態

3.1 先進國의 IS 保安實態

3.1.1 美國과 日本의 情報시스템 security 對策

(1) 美國[11]

美國에 있어서 情報시스템의 security에 대한 法的인 根據는 美國 勞務省 訓令 201-207

註11) 中珏澈 著, 컴퓨터와 法律問題, 法榮社, 서울, 1993, 262 쪽

에서 찾을 수 있는데, 이 法의 목적은 行政機關등의 컴퓨터 自動處理시스템과 원격 通信시스템 및 그 補助施設에 대한 安全保護對策을 樹立하는데 두고 있다. 컴퓨터 自動處理시스템이란 컴퓨터 自動處理 data(automatic data processing system : ADPS)와 遠隔處理通信시스템(telecommunication system : TCS)을 統合한 시스템을 意味하며 情報시스템의 security管理責任 즉

첫째 全職員에게 security管理에 關한 敎育 및 訓練을 實施

둘째 情報시스템 監査는 최소한 3年마다 1回 以上 정기적으로 實施

셋째 情報시스템의 危險分析[12]은 5年마다 1回 以上 實施

등 하도록 規定하고 있다. 또한 情報시스템의 security 對策은 法的 保護對策, 技術的 對策, 物理的 對策으로 區分할 수 있는데 物理的 對策이란 컴퓨터 시스템에 대한 施設環境을 적절히 設置함으로서 自然的. 偶發的, 災害를 最小化하는데 目的을 두고 있다. 이러한 정보시스템의 security대책의 一環인 立法 措置는 다음과 같다.

1) 情報시스템의 security를 위한 立法

美國의 情報시스템 Security를 위한 法的인 根據는 다음과 같다.

- 1975年 州立犯罪法(in 1975 the state criminal law)
- 1978年 the electronic fund transfer act (EFT ACT)
- 1978年 right to financial privacy act
- 1986年 연방 컴퓨터 부정 및 운용방지법(the federal computer fraud and abuse act)
- 1988年 foreign corrupt practices act

특히 美國의 情報시스템 security 關聯法은 다음과 같이 크게 4가지 領域으로 構成된다.

첫째 컴퓨터 情報資源의 保安對策 (security of information resources system)

美國 聯邦勞務省 訓令 201-207

제1조 範圍(scope of pact)

제2조 定議(definitions)

둘째 保安管理(security management)

제3조 施策(policy)

제4조 保安管理의 責任(agency security responsibilities)

제5조 保安措置要素(security program elements)

제6조 危險分析(risk analysis)

제7조 경영상의 물리적·기술적인 部門(administrative physical and technical aspects)

제8조 私生活 保護(privacy consideration)

제9조 保安 明細書(security specification)

제10조 保安明細書의 確認證明(identification of conformance to security specification)

제11조 保安檢査 및 中間評價(secuirty audit or evaluations)

셋째 데이터 處理施設의 環境, 物理的 保安裝置

(environmental and physical security of data processing facilities)

註12) 申玉澈, 上揭書, 264 쪽.

제1조 施設環境 : ① 溫度와 濕度, ② 照度와 電氣施設, ③ 淸潔, ④ 職員, ⑤ 豫防對策
제2조 火災安全器 : ① 指針, ② 火災豫防
제3조 偶發的 事故 防止對策(contingency planning)
제4조 ADP施設에 관한 安全措置
제5조 ADP施設에 관한 物理的 安全

넷째 私生活 秘密保護 規程(protection of personal privacy)
제1조 목적(1974년 사생활 비밀보호법 : privan act of 1974)
제2조 用語의 定義
제3조 私生活 秘密의 保護
제4조 行政機關의 責任
제5조 利用機關의 義務
제6조 供給機關의 義務

다섯째 電話盜聽 또는 錄音記錄(listening-in or recording of telephone conversation)
제1조 適用
제2조 總則
제3조 盜聽禁止事項
제4조 許諾盜聽
제5조 行政機關의 責務
제6조 聯邦調達廳의 責任
제7조 身分證明書의 使用

(2) 日本의 情報시스템 security對策[13)]

日本에 있어서 情報시스템 security對策은 컴퓨터 犯罪를 防止하기 위해서 다음과 같은 目的으로 마련되어 졌다.

첫째 컴퓨터 시스템의 技術的 保護方法의 確立
둘째 컴퓨터 시스템의 保護를 위한 조직, 관리, 정비에 만전을 기함
셋째 情報시스템의 監査처리
넷째 社會的 法規 節次의 準備

등을 目的으로 security對策을 세웠으며, 그 內容을 具體的으로 보면 다음과 같다.

첫째 技術的 security對策
둘째 物理的 security對策
셋째 data의 技術的 保護(識別, 確認, 許可, 保全性, 分離性, data의 暗號化)
넷째 데이터의 暗號化
다섯째 其他 Security對策 : a.. 管理規則의 制定, b. 情報시스템 監査의 徹底,c. 職業倫理意識의 涵養

日本에 있어서 情報시스템의 security 對策의 具體的인 內容과 아울러 이것을 뒷받침

註13) 申珏澈, 前揭書, 280-290 쪽.

해주는 情報産業育成 基本法律 運用推移와 情報處理 促進에 關한 法律的 體系圖를 보면 <表 1>과 <表 2>와 같다.

<表 1> 日本의 정보산업 육성 기본법률 운용추이

연도	내 용
'67~'70	'전자공업진흥임시조치법'(전진법) -시험연구, 생산의 개시 합리화를 추진하기 위한 진흥계획의 책정, 국가조성, 공동행위의 제시 등을 한다
'71~'77	'특정전자공업 및 특정기계공업진흥임시조치법'(기전법) -전자공업의 시험연구, 공업생산의 개시 또는 생산의 합리화를 촉진하기 위하여 국가조성, 고도화 계획의 책정, 생활환경보전, 노력절약, 등에 도움이 될 시험연구 또는 생산의 합리화를 촉진하기 위해 같은 조치를 취 한다.
'70~'85	'정보처리진흥협의 등에 관한 법률'(정진법) -전자계산기의 이용, 프로그램의 개발을 촉진하고 그 유통을 원활히 하며 아울러 정보처리서비스업 등의 육성을 위한 조치를 취한다.
'78~'85	'특정기계정보산업진흥임시조치법'(기정법) -진흥의 대상으로서 소프트웨어를 추가하고 기계에 관한 지정요건의 일부 변경, 세제의 정비를 한다.
'85~	'정보처리의 촉진에 관한 법률'(정진법을 개편) -전산기의 이용고도화, 소프트웨어 개발촉진 등 정보처리의 고도화와 정보서비스 산업 육성을 촉진한다.

(자료 : 일본정보화백서 '88. 595面)

3.2 韓國의 IS 保安實態

3.2.1 韓國에 있어서 情報시스템 security對策[14)]

韓國의 企業組織이나 行政組織에 있어서 情報시스템에 關한 security對策은 크게 3가지 側面에서 考察할 수 있다. 즉 法的 및 制度的 security對策, 物理的 security對策 그리고 技術的 security對策 등에 關하여 간단히 考察하고자 한다.

(1) 電算網의 法的 security對策

이러한 對策方法으로서 法的인 背景을 들 수 있다. 法的背景은 高度情報化社會의 도래에 대응하기 위하여 通信技術과 컴퓨터 技術의 연계 및 均衡的 發展과 그 效率的인 利用

註14) 申珏澈 著, 前揭書, 291 쪽.

의 促進을 도모하고 電算網의 安全性, 信賴性 確保를 위해서 1986年 5월 12일 法律 第3848號 制定(電算網) 普及擴張과 利用促進에 關한 法律에서부터 始作된다.

<表 2> 日本의 정보처리 촉진에 관한 법률체계도

		전자계산기 연후 이용에 관한 지침	사업소관 장관은 사업분야에 사업자가 전자계산기의 효율적인 이용을 도모하기 위해 필요한 사항을 정한다. 예 : 공동데이터베이스, 공동정보처리센터, 전표 등 장표류의 통일
목적 : 정보처리의 촉진	전자계산기 이용고도화 계획 (법 3조)	정보처리진흥 사업협회(IPA) (법7조)	특정프로그램 위탁개발 등
			프로그램작성 효율화 업무
			정보처리 서비스업자 책임보증 정보처리 서비스업자와의 책임보증 (프로그래머 등의 기술향상에 필요한 차입금)
			임대부업무 · 공동정보처리 시스템 개발 · 프로그램 개발금 대부
			기타 · 정보처리에 관한 조사 등
		프로그램조사장 (법5조)	
		정보처리기술자시험 (법6조)	
		자금의 확보 (법4조)	일본개발은행 · 전자계산기 진흥대부 · 정비처리,통신진흥대부 · 중소기업정보화 촉진대부

1) 電算網의 安全性 確保

a. 電算網의 槪念

컴퓨터 技術과 通信技術이 연계된 network시스템을 말하되, 이 事業이란 컴퓨터 이용기술의 開發, 전산망의 구성, 유지, 보수, 전산망을 이용한 정보처리 보관 전송의무, 전산망과 관련된 기타사업

b. 保護措置 義務(同法 第22條)

c. 保護措置 內容(同法 施行令 第28條)

d. 一般遵守事項(同法 第23調)

e. 重要情報의 保護(同法 第24條)

f. 個人情報의 保護(憲法 第17條 同法 第25條)

2) 電算網의 security對策

a. 전산망법 제22조, 보안대책 수립자

b. 기본적 사항(전산망 기술기준에 관한 규칙 제14조)

c. 세부적 시행대책

기능분산(규칙 1), 발견 및 신속통보(규칙 2)

긴급복구대책(규칙 3), 식별확인 기능(규칙 4)

data SW의 손괴방지(규칙 5), 기타 보안대책(규칙 6)

3) 전산업무 보안관리

a. 기밀보호의 필요성(국가안전기획부법 제22조2호)

b. 보안관리 지침구성(전산업무 보안관리지침)

c. 전산실 보안대책(보안업무 규정 제30조 및 동시행규칙 제42조)

d. 비밀자료 입력의 관리(보안업무 규정2,4참조)

e. 보조기억장치 관리(보안법 규정 지침 5)

f. 비밀자료의 出力管理

g. 단말기 보안관리

h. 비밀자료 전송보안대책

I. word processor 보안관리

j. 출력비밀자료 보안관리

k. 보안관리의 방향

(2) 物理的 security對策

보호대상으로 HW,SW,데이터, 통신회선 운용요원 등으로 볼 수 있다. 그 대책은 data 보호의 觀點에서 제어장치를 의미하기도 한다. 그 대책의 대표적인 security法으로서

a. 식별(identification) : 단말식별번호, 신분증명서번호, 사원암호번호

b. 確認 또는 증명(authentication) : 사원 신분증의 검증, 指紋, 音色, 磁氣光學識카드

c. 許可(authorigation) : 컴퓨터 시스템의 계획대로 조작여부

d. 分離性(isolation) : 시스템 지원과 운영요원, 정보 및 시스템 사용자 등 각분야별로 책임은 명확히 한다. 서로 분리시키는 방법

e. 데이터 암호화 : 특정의 요원만이 이해할 수 있도록 program이나 데이터를 암호화하는 方法

(3) 技術的인 security對策

1) 데이터의 暗號化

a. 데이터 등 컴퓨터室에서 處理, 축적, 보관되고 있기 때문에 컴퓨터 室이나 시스템에의 接近 暗號化의 方式에 依하여 統制하는 方法을 의미한다.

b. 데이터 암호화의 기본원리

데이터 암호화 方法은 코드 암호화법과 변환 암호명이 있다. 코드암호법은 암호화

는 언어에 코드부호 또는 숫자를 맞추어 각 언어와 부호를 대응시켜 코드표를 만드는 方法, 변환암호법은 복잡한 알고리즘과 message의 2진수(0과 1의 변환)에 대하여 어려운 암호문을 작성하는 方法을 意味한다

2) 데이터 암호화의 표준화

일반적으로 많이 쓰고 있는 방식은 관용계 암호방법식으로 암호표준(DES, data encryption standards)方法이 있다.

<表 3> 한국의 전산망 안전, 보안에 관한 법령 및 기준

구분	법령 및 기준명	고시부처	공 고 일
법률	· 전산망 보급확장과 이용에 관한 법률	체신부	'86. 5. 12 '91.12. 14(개정)
	· 컴퓨터 프로그램 보호법	과기처	'89.12. 30
	· 통신비밀 보호법	체신부	'93.12. 27(공고) '94. 6. 27(시행)
	· 공공기관의 개인정보 보호에 관한 법률	총무처	'94. 1. 7(공고) '95. 1. 7(시행)
기준	· 컴퓨터 시스템 안전관리 기준	과기처	'89. 9
	· 전산망 안전 신뢰성 기준	체신부	'93. 2
지침	· 전산업무 보안관리 지침	안기부	'88. 8
	· 전산처리되는 개인정보 보호를 위한 관리지침	총무처	'91. 5
	· 행정전산망 안전관리지침	총무처	'91.10
표준	· 전산망 보안관리를 위한 기술지원서 : 총론	체신부	'93. 2
	· 전산망 보안관리를 위한 기술지원서 : 물리적보안	체신부	'93. 2
	· 국가기관전산망 패스워드 활용 표준	체신부	'93. 2

Ⅳ. security實態 意識調査

4.1 調査期間 및 對象

오늘날 情報化 社會는 社會의 모든 分野에서 情報시스템을 構築하여 活用하게 만들고 있고, network의 通信시스템 發展 및 活用 普及은 여러 가지 問題點 즉, 業務上 error, 事故, 災害 및 컴퓨터 犯罪등을 發生하게 하는 빈도를 높게 하고 있다.

이러한 情報시스템의 security을 低害하는 根本的인 原因과 그에 대한 security意識이 어떤지를 調査하였다. 勿論 論文의 目的達成을 위해서 日本의 情報시스템 保安實態調査[15]

註15) システム監査學會/(財) 日本情報處理開發協會 編, 情報セキュリテイ 意識の實態, シ

는 日本 情報處理開發協會가 調査한 內容을 再引用·說明하고, 그 內容說明의 편의를 위해서 「實態調査」로 통칭하였다. 「實態調査」는 1994年 10月 3日부터 同年 11月 30日까지 進行되었고, 設問紙調査 對象者는 同協會에 加入한 企業, 事業所 및 관공서의 情報시스템 監査部門과 被監査部門의 專門要員들을 選定하여 調査되었고, 그 現況은 조사대상자 총 4,725명중 35.7%의 1,671名(시스템 監査部門 13.5%의 640매, 被監査部門의 22.3%의 1,051매를 回收하여 分析하였다.

論者調査는 企業이나 行政組織의 情報處理要員들을 對象者로 選定하여 1996年 1月부터 4月까지 調査하였고, 全體設問紙 500매를 發送하여 그중 60.0%의 300매를 回收하여, 有效한 80.0%의 240매를 分析하였는데, 全體基礎調査 現況은 <表 4>와 같다.

設問紙 調査內容은 情報시스템 security 構成內容중 컴퓨터 犯罪와 關聯된 것으로써

첫째 情報시스템의 security關聯基準의 認知率
둘째 컴퓨터 犯罪에 대한 意識
셋째 不正行爲에 대한 意識

등으로 압축하여 調査하여 比較·說明하였다.,

4.2 調査結果 및 分析

4.2.1 情報시스템 security關聯基準의 認知率

다음 <表 5>는 컴퓨터 시스템 security基準(現 情報시스템 security對策基準, 컴퓨터 바이러스 對策基準, 및 情報시스템 監査基準)에 대하여 企業 및 組織의 情報處理 專門要員들이 어느 程度로 알고 있는가를 調査한 內容이다.

<表 5>에 있어서 實態調査의 경우 日本의 경우 컴퓨터 시스템 security對策基準은 1977年度에 策定되었는데 同 基準에 대한 認知率은 被監査部門의 專門要員의 69.3%, 監査部門의 專門要員 57.7%로 나타났는데, 被監査部門의 認知率보다는 시스템 監査部門이 11.6%로 낮은 認知率을 보이는데 問題가 指摘된다. 또 한편, 1990年度에 策定된 컴퓨터 바이러스 對策基準에 대한 認知率은 被監査部門이 54.7%, 監査部門이 46.7%로써 監査部門이 8.0%로 낮게 나타났는데, 다른 컴퓨터 바이러스 처방으로 미연에 방지할 수 있다는 理由 때문에 낮은 것으로 分析이 可能하다고 본다. 그리고 1985年度에 策定된 情報시스템 監査基準에 대한 認知率은 被監査部門이 77.3%, 監査部門은68.1%로써, 이 基準은 情報시스템 監査人을 위한 基準임에도 不拘하고 監査部門의 認知率은 낮은데 問題가 있다고 본다. 情報시스템의 被監査部門의 認知率이 높은 理由는 다음 2가지를 들 수 있겠다.

첫째 情報시스템 部門이 시스템 監査에 대하여 열심이고 主體的으로 參與한다.
둘째 시스템監査 技術者 및 監査人 資格試驗이 實施됨으로서 多數의 情報시스템 要員이 여기에 도전하기 때문이다.

ステム　　監査白書 '95-'96年, 東京, 1996, 93-104面

<表 4> 論者調査의 全體基礎 現況 (단위 : 명)

設問內容	應答內容					
성 별	남			여		
	185			55		
연 령 별	20-29세		30-39세		40세 이상	
	119		115		6	
학 력 별	고졸	전문대졸		대졸	기타(대학원)	
	22	62		148	8	
근무경력	1년 미만	2-3년		4년 이상	무응답	
	32	82		122	4	
직 책 별	일반직원	대리 및 과장		부장	전무	
	179	55		5	1	
직 무 별	SE	SA	SB	SP	AP	무응답
	62	68	9	58	2	8
총 계	240명					

<表 5> 情報시스템 security基準 認知率(多重回答)

設問 \ 基準			① 情報시스템 監査基準	② 컴퓨터 바이러스 대책기준		③ 컴퓨터 시스템 安全基準		
다음 基準에 대해서 어느 정도 알고 계십니까?	實態調査	감사부문	68.1%	46.7%		57.7%		
		피감사부문	77.3%	54.7%		69.3%		
정보시스템 보안과 다음 기준에 대하여 알고 계십니까?	論者調査		① 정보시스템 감사기준	② 컴퓨터 바이러스 기준	③ 컴퓨터 시스템 안전기준	④ 모르겠다	⑤ 무응답	計
			2/0.8	19/7.9	20/8.3	141/58.8	99/41.3	240/100

<表 5>에 있어서 論者調査는 實態調査의 結果와 아주 다른 應答率을 보이고 있음을 알 수 있다. 즉 實態調査의 경우는 정보시스템 감사기준, 컴퓨터 바이러스 기준 및 컴퓨터 시스템 안전기준에 높은 비율을 보인 반면, 論者調査의 경우는 각각 낮은 비율(정보시스템

의 감사기준 0.8%, 컴퓨터 바이러스 대책기준 7.9%, 컴퓨터 시스템 안전기준 8.3%)을 보임과 동시에 「모르겠다」(58.8%)와 「무응답」(41.3%)의 높은 비율을 보이고 있는 것은 여기에 대한 기준이 마련되어 있더라도 미비하거나 되어있지 않으며 또 잘 알려져 있지 않음을 의미하는 것으로서 여기에 대한 대책마련이 요구된다.

4.2.2 컴퓨터 犯罪에 대한 意識調査

(1) 컴퓨터 犯罪 增加與否 調査

日本의 「實態調査」에서 「금후 情報社會에 있어서 컴퓨터 犯罪는 增加한다고 생각합니까?」라는 質問에 全般的으로 多數人들은 앞으로 컴퓨터 犯罪는 增加한다고 明確히 應答했는데 그 結果는 <表 6>과 같다.

<表 6> 컴퓨터 犯罪增加與否 調査 (단위 : %)

設問 \ 應答內容 / 調査		①증가한다고 생각한다	②생각하지 않는다.	③모르겠다	④무응답	計
앞으로 컴퓨터 범죄가 증가한다고 생각하십니까?	實態調査	75.5	5.4	18.3	0.6	100.0
	論者調査	191/79.6	11/4.7	35/14.6	3/1.1	240/100.0

즉 實態調査에서는 75.7%의 應答者가 앞으로 컴퓨터 犯罪가 增加할 것으로 믿고 있고, 그것이 現實로 나타났을 때 그에 대한 對策이 마련되어져야 할 것으로 본다.

이 分野의 調査에서는 實態調査와 마찬가지로 論者調査에서도 앞으로 컴퓨터 범죄가 계속 증가하는 응답(79.6%)이 높은 비율을 보이고 있다. 兩 調査結果에 따르면 앞으로 계속되는 컴퓨터 犯罪에 대한 豫防對策이 要求된다.

앞으로 컴퓨터 犯罪가 增加한다는 見解에 따르면 더 큰 사회적 문제와 좋지 않은 파급효과를 최소로 줄이고 건전한 정보사회를 건설하기 위해서는 컴퓨터 범죄처벌이 강화 및 보완되어야 하고 공지되어야 할 것으로 본다.

(2) 컴퓨터 犯罪處理與否 調査

컴퓨터 犯罪處理에 대한 法處理方法에 대해서는 양조사에서 모르겠다는 應答者를 보이고 있다. <表 6>에서 보이는 바와 같이 앞으로 設問調査에 依하면 앞으로 컴퓨터 犯罪가 계속적으로 增加할 것이고, 컴퓨터 犯罪의 新種手法이 出現하므로 現行 컴퓨터 犯罪處罰法으로 可能한지 여부에 대하여 調査한 結果는 <表 7>과 같다.

現行 刑法으로 컴퓨터 犯罪處理가 充分하다고 생각하는 사람은 5.9%에 불과하지만 充分하지 않다고 생각하는 應答者가 33.0%에 이른다는 것은 기존의 컴퓨터 犯罪處理法 이외에도 보장되어 져야 한다는 結果에 注目할 만한 價値가 있다고 본다.

<表 7> 컴퓨터 犯罪處理與否 調査 (단위 : %)

設問 \ 應答內容 / 調査		① 생각한다	② 생각하지 않는다	③ 모르겠다	④ 무응답	計
컴퓨터 범죄에 대응되는 현행 刑法으로 充分하다고 생각합니까?	實態調査	5.9	33.0	60.4	0.8	100.0
	論者調査	23/9.5	56/23.3	130/54.5	31/12.7	240/100.0

4.2.3 컴퓨터 不正行爲에 대한 犯罪意識

컴퓨터 不正行爲에 대한 犯罪意識調査는 여러 가지로 생각할 수 있으나, 여기에서 다음과 같은 內容으로 한정하여 조사하였다,.

첫째 市販SW를 不正 複寫行爲
둘째 data와 program의 무단사용 여부
셋째 data나 program의 공개 여부
넷째 컴퓨터의 不正使用 與否
다섯째 컴퓨터 바이러스의 傳達行爲 與否
여섯째 他社시스템의 侵入 與否
일곱째 業務時間外 컴퓨터 게임 遂行 與否

(1) 市販SW를 不正 複寫하는 行爲

市販되고 있는 SW를 通常 個人, 企業 혹은 敎育機關들의 復數使用 許可자緖者 契約에 근거하여 運用되고 있으므로 使用許可를 받지 않은 者가 그런 SW를 複寫해서 運用하는 것이 明確히 著者權의 侵害이다. 著作權의 侵害 例示를 具體的으로 提示하여 program 著作權을 保護받도록 되어 있다. 市販SW 複寫使用 與否에 관한 設問內容은 <表 8>과 같다.

<表 8> 市販SW 複寫使用 與否 (단위 : 명 / %)

設問 \ 應答內容 / 調査		①특히문제가 되지 않는다	②문제가 된다	③계고,훈고, 주의처분및징계,면직대상	④형법상의 범죄행위이다	⑤모르겠다	⑥무응답	計
市販SW를 복사해서 사용하는데 대하여 어떻게 생각합니까?	實態調査	131/8.0	747/47.2	196/12.4	429/27.1	54/3.4	27/1.7	1584/100
	論者調査	12/5.0	131/54.6	23/9.4	6.0/25.1	7/3.1	7/2.8	240/100

동 設問에 있어서 47.2%에 해당하는 747명은 市販SW를 複寫해서 사용하는 것은 問題가 되는 것으로 응답했고, 27.1%의 429名은 刑法上 犯罪行爲로 認識하고 있다는 點에 注

目이 된다.

市販SW 複寫使用에 대해서 實態調査와 論者調査에서도 사회적으로 問題가 되고, 법적 징계 처분의 대상이 되며, 나아가 형사처벌의 대상이 된다고 인식하고 있는 점은 컴퓨터 범죄와 처리를 위한 處罰法이 마련되면 어느 정도 컴퓨터 범죄예방에 많은 도움을 줄 수 있다는 증거로 해석이 된다. 물론 컴퓨터 범죄는 다수인 보다는 소수가 문제가 되기 때문에 이 소수의 응답(각각 8.0, 5.0%)에 注目할 必要가 있다고 본다.

(2) data와 program의 無斷使用 與否

<表 9>은 컴퓨터 犯罪와 關聯된 設問으로써 實態調査에 있어「데이터」나 프로그램을 無斷使用했을 때「問題가 된다」고 應答한 結果는 27.3%의 432명,「戒告, 訓戒, 注意處分 및 징계의 대상이 된다」고 응답한 結果는 44.0%의 716명 그리고 刑法上의 犯罪行爲로 認識하는 것은 22.5%의 353명에 이르고 있는데, 응답자중 93.8%의 1,501명은 무단사용자체가 問題가 되고, 컴퓨터 犯罪로 認識하고 있다는 點에 注目이 된다. 論者調査에서는 實態調査와는 약간 다른 응답을 보이고 있다.「데이터」나 program 복사에 대해서 특히 문제가 되지 않는다는 데 35.6%의 비율로 보이는데 특히 주목이 된다. 즉 실태조사 응답자보다는 論者調査에서의 응답자가 문제의식을 덜 느끼는데 문제가 있다는 점이고, 앞으로 컴퓨터 범죄 발생의 높은 가능성을 안고 있다는 점으로 지적할 수 있다. 따라서 컴퓨터 犯罪問題의 發生은 극소수에 의해서 發生하기 때문에 이것도 管理의 對象이 된다는 點이다. 따라서 data나 program은 情報시스템 資産으로써의 價値를 가지고 있음을 인정하고 이런 資産을 管理하는데 필요한 對應策이 要求된다.

<表 9> data 및 program 無斷使用 與否 (단위 : 명/ %)

設問 \ 應答內容 / 調査		①특히문제가 되지 않는다	②문제가 된다	③계고,훈고,주의처분및징계, 면직대상	④형법상의 범죄행위이다	⑤모르겠다	⑥무응답	計
데이터나 프로그램 무단사용에 대해서 어떻게 생각합니까?	實態調査	22/1.4	432/27.3	716/44.0	353/22.5	50/3.2	27/1.7	1584/100
	論者調査	85/35.6	66/27.5	61/25.5	12/5.1	8/3.3	7/3.0	240/100

(3) data나 program의 公開 與否

<表 10>에 있어서 이 設問에 대한 見解는 사람에 따라 다를 수 있다. 이것을 機密情報란 觀點에서 公的 組織情報와 個人情報를 훔쳐보는 行爲는 分明히 問題가 되며 또 system에 侵入하는 行爲에 이르게 되기 쉽다는 點에서 문제가 된다.

<表 10>에서 보는 바와 같이 實態調査에서 data나 program을 훔쳐보는 행위에 대한 設問調査에서도「훔쳐보는 것 자체가 문제가 된다」고 응답한 結果는 85.6%의 564명,「

戒告, 訓告, 注意處分 및 懲戒對象이 된다」고 應答한 結果는 42.3%의 670명의 비율로 나타났다. 또 한편으로는10.9%의 173명은 刑法上의 犯罪行爲로 認識하고 있다는데 注目이 된다. 물론 論者調査에서도 「데이터」나「프로그램」, 정보에 대해서 機密度 順位를 정해서 管理를 한다면, 훔쳐보아서는 안돼는 情報가 明確히 되어질 수 있고, 엄밀한 管理를 함으로써 問題發生의 原因을 事前에 豫防할 수 있을 것으로 생각된다. 훔쳐보는 행위에 대한 인식조사에서 응답자중 56.7%가 문제가 된다고 응답했고, 23.5%가 법률적 범죄행위 내지 징계처분의 대상이 된다는 높은 인식을 하고 있다는데 注目이 된다.

<表 10>「데이터」나「프로그램」의 公開 調査 (단위 : 명/ %)

設問 \ 應答內容	調査	①특히문제가 되지 않는다	②문제가 된다	③ 계고,훈고, 주의처분 및 징계,면직대상	④형법상의 범죄행위이다	⑤모르겠다	⑥무응답	計
데이터나 프로그램을 훔쳐보는 것에 대해 어떻게 생각하십니까?	實態調査	102/6.4	564/35.6	670/35.6	118/14.9	45/2.8	30/1.9	1584/100
	論者調査	13/5.4	136/56.7	30/12.3	27/11.2	30/12.5	5/1.9	240/100

(4) 컴퓨터의 不正使用 與否

自己가 屬한 會社의 computer를 使用해서 情報를 處理하는 것은 問題가 되며 바로 情報處理要員의 職業管理 問題가 된다고 본다. 自己가 屬한 會社의 컴퓨터를 許可없이 利用했을 때의 컴퓨터 犯罪意識을 調査한 結果는 <表 11>과 같다.

<表 11> 컴퓨터 不正使用行爲 意識調査 (단위 : 명/ %)

設問 \ 應答內容	調査	①특히 문제가 되지 않는다	②문제가 된다	③ 계고,훈고, 주의처분 및 징계,면직대상	④형법상의 범죄행위이다	⑤모르겠다	⑥무응답	計
소속회사의 컴퓨터 사이용에 대해 어떻게 생각하십니까?	實態調査	74/4.7	481/30.4	876/55.2	88/2.4	38/2.4	27/1.7	1584/100
	論者調査	12/5.1	71/29.6	21/8.6	37/15.4	85/35.6	14/5.7	240/100

<表 11>에서 보는 바와같이 實態調査에 있어서 自社의 컴퓨터를 私用에 利用했을 때 懲戒對象(戒告, 訓告, 注意處分 및 懲戒)이 된다고 응답한 結果는 55.3%의 876명,「問題가 된다」고 응답한 結果는 30.4%의 481명, 刑法上의 犯罪行爲가 된다고 응답한 結果가 5.6%의 88명으로서 自社의 컴퓨터 私用에 대한 컴퓨터 犯罪意識은 대단히 높은 수준으로 나타났다.

또 한편으로 論者調査에서는 응답자중 29.6%가「컴퓨터」不正使用行爲가 문제가 된다고 응답했으며 징계처분이 형법상 범죄행위로 인식하는데는 實態調査에서보다 낮은 應答率을 보였고,「모르겠다」고 응답한 비율은 35.6%에 이르고 있는 점이 實態調査와 큰 差異點을 나타내고 있다. 會社의 컴퓨터 不正使用에 대한 犯罪意識은 낮으며 公私를 區別하는 水準도 낮은 것으로 나타났다. 따라서 職業倫理 敎育이나 情報倫理 敎育을 통해서 이 問題를 解決하는 對策이 要求된다고 본다.

(5) 컴퓨터 바이러스의 傳染行爲 意識調査

컴퓨터 바이러스(computer virus) 發生件數는 어느 나라를 막론하고 增加一路에 있으며 情報시스템의 security에 害할 수 있는 위협성이 큰 要因으로 指目되고 있다.

이점을 고려하여 큰 被害를 입지 않기 위해서 여러 가지 側面을 검토하여 對策을 세울 必要性이 있다고 본다. <表 12>는 컴퓨터 바이러스 傳染行爲 意識에대해 調査한 結果이다.

實態調査에서는 컴퓨터 바이러스를 傳染시키는 行爲에 대해서 應答者 中 73.5%의 1,164명은 壓倒的으로 犯罪行爲라고 應答했다. 論者調査에서도 實態調査와 마찬가지로 컴퓨터 바이러스 傳染行爲가 문제(49.4%)가 될 뿐만 아니라, 刑法上의 문제(24.6%)가 된다고 높은 응답을 했는데, 그 반면에 모르겠다는 응답(20.5%)이 높게 나타난 것은 컴퓨터 바이러스 영향이 얼마나 큰 문제를 유발하고 그 미치는 파장이 얼마나 큰지를 교육을 통해서 여기에 대한 인식도를 높여 가야 할 것이다.

<表 12> 컴퓨터 바이러스 傳染行爲 意識調査 (단위 : 명/ %)

設問 \ 應答內容	調査	①특히 문제가 되지 않는다	②문제가 된다	③ 계고,훈고, 주의처분 및 징계,면직대상	④형법상의 범죄행위이다	⑤모르겠다	⑥무응답	計
컴퓨터 바이러스 전염행위에 대해서 어떻게 생각하십니까?	實態調査	3/0.2	64/4.0	249/15.7	1164/73.5	78/4.9	26/0.6	1584/100
	論者調査	5/2.0	119/49.4	7/3	59/24.6	49/20.5	1/0.5	240/100

(6) 他社시스템의 侵入行爲 意識調査

通信시스템인 network의 發展에 따라서 他社 system에 侵入하는 컴퓨터 犯罪行爲가 社會的인 큰 問題로 提起되고 있다. 通信回船을 通해서 不正하게 접속하여 system에 侵入하는데는 여러 가지 해커의 問題가 제기된다. <表 13>은 他社시스템 侵入에 대한 犯罪意識을 調査한 結果이다.

他社의 시스템에 侵入하는 行爲에 대한 應答結果는 實態調査에서 바이러스를 傳染시키는 행위와 마찬가지로 응답자 중 78.5%의 1,244명은 대단히 높은 율의 犯罪行爲로 認識하고 있는데 注目이 된다. 論者調査에서는 他社의 system 침입이 문제가 된다고 인식하고

<表 13> 他社시스템의 侵入行爲 意識調査 (단위 : 명/ %)

設問 \ 應答內容	調査	①특히 문제가 되지 않는다	②문제가 된다	③ 계고,훈고, 주의처분 및 징계,면직대상	④형법상의 범죄행위이다	⑤모르겠다	⑥무응답	計
他社의 시스템 침입에 대하여 어떻게 생각하십니까?	實態調査	1/0.1	80/5.1	149/9.4	1244/78.5	86/5.4	24/1.5	1584/100
	論者調査	6/2.6	136/56.7	38/15.9	37/15.4	13/5.4	10/4.0	240/100

있는 응답율은 56.7%에 이르고 있고, 또 징계나 형법상 범죄행위(31.3%)로 높은 인식을 하고 있다는 것은 職業倫理 敎育이나 情報倫理 敎育을 통해서 이와 유사한 컴퓨터 犯罪는 어느 정도로 예방할 수 있다는 가능성을 제시하는 것으로 볼 수 있다. 또 한편으로 法律的, 制度的 裝置의 보완이나 강화를 통해서 그 예방의 가능성이 높다는 것을 보여준다. 特히 他社의 시스템에 侵入하는 行爲는 정보의 도둑질, 정보파괴, 정보를 훔쳐보는 것이 可能하므로 家宅侵入과 유사한 犯罪로 認識하고 있다는 點이다. 高度의 情報社會에 있어서 家宅侵入보다도 他社의 시스템 侵入防止가 重要하다고 많은 사람들이 認識하고 있다는 것은 健全한 思考方法으로 생각된다.

(7) 業務時間外 컴퓨터 게임 實行에 대한 意識調査

<表 14>는 컴퓨터 業務時間外 休息時間이나 業務終了 後에 自社의 컴퓨터를 가지고 게임을 즐기는 행위에 대한 犯罪意識을 調査한 結果이다.

<表 14> 業務時間外 컴퓨터 게임 實行 意識調査 (단위 : 명/ %)

設問 \ 應答內容	調査	①특히 문제가 되지 않는다	②문제가 된다	③계고,훈고, 주의처분 및 징계,면직대상	④형법상의 범죄행위이다	⑤모르겠다	⑥무응답	計
업무시간외에 회사의 컴퓨터를 이용해서 게임을 하는데 대하여 어떻게 생각하십니까?	實態調査	439/27.7	622/39.3	389/27.6	26/1.6	71/4.5	37/2.3	1584/100
	論者調査	85/35.6	60/25.1	74/30.7	5/2.1	12/5.0	4/1.5	240/100

實態調査에서 應答者 中 27.7%의 439명은「特히 問題가 되지 않는다」고 應答했는데, 이것은 自社의 公用 컴퓨터를 私用인 오락을 위해 사용한다는 公·私區別에 問題가 있다고 본다. 그러나 65.5%의 1,037명은 刑法上의 컴퓨터 犯罪가 된다고 응답했는데 상당한 犯罪意識을 느낀다는데 注目이 된다. 그러나 論者調査에서는 업무시간의 會社의 컴퓨터를 가지고 game을 하는 것에 대해서 35.6%의 응답자가「특히 문제가 되지 않는다」고 응답

했는데 이것도 공·사를 구별할 수 있는 意識水準이 낮다는 것을 의미한다고 본다. 그러나 이에 못지 않게 「문제(25.1%)가 되거」나 「징계(30.7%) 대상이 된다」고 응답했으나 「刑法上의 범죄행위」로는 인식하지 않고 있다는 점이다. 私用을 통해서 자기회사로 하여금 컴퓨터 사용료를 부담하게 하는 그 자체는 職業 倫理的인 問題로 지적할 수 있겠다. 시간외 會社의 컴퓨터로 게임을 행하는 것은 특히 問題가 되므로 上位階層의 情報管理者로부터 使用許可를 得한 후에 게임을 하는 것이 바람직하다. 이 점을 고려하지 않을 때 各種게임用 SW를 通해서 컴퓨터 바이러스가 감염될 수 있거나 시스템 自體를 破壞할 수 있는 계기가 되기 때문에 充分한 注意를 하지 않으면 안된다.

4.3 對策方案

情報시스템의 security對策方案으로 다음 2가지로 提示하여 說明하고자 한다.

4.3.1 情報시스템 security에 대한 制度的對應策

컴퓨터 不正行爲에 대한 情報處理 專門要員의 컴퓨터 犯罪意識을 調査한 <表 7, 8 ,9, 10, 11, 12, 13, 14>에서 보는바와 같이 컴퓨터 犯罪行爲에 대한 應答은 「問題가 되거나」 또는 「징계대상 및 刑法上의 犯罪行爲」라고 應答한 높은 비율을 보이고 있다. 이와 같은 問題를 豫防하는 事前措置로써 다음 <表 15>에서 「직업윤리교육이나 정보윤리교육을 통해서 컴퓨터 犯罪를 豫防하는데 도움이 되는가?」라는 設問에 대하여 직업윤리교육은 77.1%*185명) 정보윤리교육은 89.6%(215명)의 높은 비율을 보이고 있다.

<表 15> 職業倫理敎育 및 情報倫理敎育의 必要性 認識 (단위 : 명/%)

設問 \ 應答內容		①필요하다	②필요없다	③모르겠다	計
컴퓨터 범죄에방을 위해 직업윤리교육 및 정보윤리교육이 필요하다고 생각하십니까 ?	직업윤리 교육	185/77.1	39/16.2	16/6.7	240/100
	정보윤리 교육	215/89.6	16/6.7	9/3.8	240/100

이러한 應答結果로 미루어 볼 때 직업윤리교육과 정보윤리교육이 필요할 것으로 본다.

<表 16>은 컴퓨터 犯罪處罰法 制定을 통해서 컴퓨터 犯罪를 어느 정도 豫防할 수 있는지 與否를 묻는 質問에 40.8%의 98名은 「막을 수 있다」고 응답했으나 47.8%의 115名은 「막을 수 없다」고 응답했는데, 法律的 制定만으로 컴퓨터 犯罪를 豫防하기는 부족하므로 여기에 대한 홍보와 교육을 통해서 豫防할 수 있는 措置가 要求된다.

<表 17>은 컴퓨터 犯罪處罰法의 制定에 대해 情報處理 專門要員의 認識與否 묻는 內容으로서 應答者 中 43.8%의 105名은 制定되어 있음을 認識하고 있으나, 37.9%의 91名은 그렇지 못한 結果를 보여주고 있다. 컴퓨터 犯罪 誘發性이 높고 그것이 現實로 나타난 危險이 있으므로 앞으로 증가가 예측되는 컴퓨터 犯罪豫防의 對備策이 要求된다.

<表 16> 컴퓨터 犯罪處罰法을 통한 犯罪豫防 與否 (단위 : 명/%)

應答內容 / 設問	①막을 수 있다	②막을 수 없다	③모르겠다	計
컴퓨터 犯罪處罰法 制定을 통해서 컴퓨터 犯罪를 막을 수 있다고 봅니까 ?	98/40.8	115/47.8	27/11.3	240/100

<表 17> SW산업보호를 위한 data보호법 및 privacy법 제정의 필요성 (단위 : 명/%)

應答內容 / 設問	①막을 수 있다	②막을 수 없다	③모르겠다	計
SW산업보호를 위해서 data보호법 및 privacy법의 제정이 필요하다고 생각하십니까 ?	215/89.5	10/4.2	15/6.3	240/100

<表 18>은 SW産業保護를 위해서 data保護法이나 privacy法 制定의 必要性을 묻는 質問에 89.5%의 215名으로 나타났고, 또 現實的으로 情報處理 現場에서는 그 必要性을 정실히 느끼고 있다고 볼 때 SW産業保護對策이 要求된다.

이러한 情報시스템의 security를 위해서 제도적 대응책으로서

첫째 職業倫理(企業倫理)와 情報倫理의 制度的 强化

둘째 컴퓨터 犯罪處罰法의 弘報 및 敎育訓練 强化

셋째 컴퓨터 犯罪處罰法의 强化 및 補完

넷째 SW産業保護를 위한 data보호법과 privacy제정 등이 촉진되어야 할 것이다.

또 다른 한편으로는 情報시스템 security을 위한 一般的 對備策으로

첫째 컴퓨터 犯罪의 科學的 搜査能力 向上을 위한 法律的 및 制度的인 對應策에 관한 持續的인 硏究

둘째 情報시스템의 security對策基準, 監査基準 및 virus對策基準이 策定 및 實施의 制度化

셋째 情報시스템의 security對策 專門家 育成 및 確保

넷째 情報處理 專門要員의 身元調査를 통한 積極的인 管理의 制度化 등을 提示하고자 한다.

V. 結 論

오늘날 情報産業과 關聯된 最尖端 情報處理 機器들의 發展과 그 活用의 擴大는 날로 더

해 갈 뿐만아니라 情報處理 機器의 利用者의 숫자가 增加 一路에 있고, 社會 모든 分野의 業務處理는 더욱 便利하게 되고, 그 文化生活의 水準도 점차로 높아지고 있음은 周知의 事實이다.

그만큼 組織에 있어서 業務處理나 生活이 便利함이 뒤따르는 반면에, 그 부작용으로서 여러 가지 심각한 社會問題, 즉 컴퓨터 犯罪的 逆機能, 社會的 逆機能, 文化的 逆機能 및 情報 倫理的 逆機能이란 社會的 問題를 야기시키고 있다. 뿐만 아니라 이런 問題들이 앞으로 社會全般에 걸쳐 미치는 影響은 심각할 것으로 展望되고, 그 被害도 대단히 큰 것으로 豫想된다. 本 論文에서는 앞으로 到來할 21C의 健全한 情報化 社會 또는 情報社會 建設이란 前提下에 컴퓨터 關聯 情報處理機器 活用에 의한 逆機能 中 컴퓨터 犯罪的 逆機能에 焦點을 두고 情報시스템의 security에 關한 간단한 理論的 背景을 說明하고 情報시스템의 security對策實態가 어떤지 先進國(美國, 日本)과 韓國을 中心으로 考察했고, 實際 여기에 대한 情報處理 專門要員들의 意識狀態가 어떤지를 韓·日 專門要員들을 對象으로하여 調査하여 比較·分析하였다. 그 結果에 依하면 情報시스템의 security에 대한 이들의 意識實態는 設問 問項에 따라 類以한 應答率를 나타내기도 하고, 또 다른 差異點도 나타내기도 하였다.

綜合的으로 볼 때 정보시스템의 security를 위한 制度的 裝置와 基準設定이 未備하다는 것을 알 수 있었다. 따라서 情報處理 機器의 發展과 그 利用擴大에 걸맞는 措置가 절실히 要求되며, 그에 따른 敎育도 必要하다고 본다. 이러한 措置들이 이루어지고 補完됨으로써 健全하고 信賴할 수 있는 21C 情報化 社會의 建設리 可能할 것이며 보다 安全하고 便利한 高度의 情報社會 建設을 위한 努力과 持續的인 硏究가 進行되어져야 할 것으로 본다.

參 考 文 獻

1. 國內文獻

申珏澈 著, 컴퓨터와 法律問題, 法榮社, 서울, 1993.

三逸經營經濟硏究所 編, 시스템 監査 槪論, 世明書館, 서울, 1989.

李撥天 著, 職業倫理, 螢雪出版社, 大邱, 1990.

李允植 著, 行政情報體系論, 法榮社, 서울, 1994.

柳長善 著, 企業倫理, 法文社, 서울, 1990.

安勇根・趙利男 共著, EDP시스템 監査論, 正益社, 1979.

韓國電算院, 國家情報化 白書(1994年), 서울, 1994.

韓國情報시스템 監査人協會 編, 情報시스템 監査槪論, 法榮社, 서울, 1990.

2. 外國文獻

宇佐美 博 著, システム監査の 技法, 日刊工業新聞社, 東京, 1986.

宇佐美 博と富山茂 著, システム監査の 手法と 實務, 日刊工業新聞社, 東京, 1994.

前川良博 著, 情報處理と職業倫理, 日刊工業新聞社, 東京, 1989.

宮川公男 編著, システム監査基準, 中央經濟社, 東京, 1987.

日本公認會計協會 編, 監査方法, 中央經濟社, 東京, 1988.

システム監査學會/(財)日本情報處理開發協會 編, 情報セサュリテイ意識の實態, システ 監査 白書 '95 '96年, 東京, 1996.

Brenda Sutton, The Legitimate Corporation, Essential Reading in Business Ethics & Corporate Govenmance, Black-well, Massachusetts, 1993.

Brian Harvey, Henk van Lutik, European Case book on Business Ethics, Prentice-Hall, N.Y. 1994.

Ernest A. Kallman, John P. Grillo, Ethical Decision Making and Information Technology, McGraw-Hill, N.Y. 1993.

H. Wedekind, Gibt es eine Ethik der Informatik? Springer-Verlag Berlin, Band 10 Heft 6, 1987.

Joseph W. Weiss, Business Ethics, Wadeworth Publishing Co. California, 1994.

K.M.Jackson, J. Hruska, Dom R. Parker, Computer Security Reference Book, ERC press, Florida, 1992.

P. Schefe, Zehn Gebote für die Informatik, Informatik, Springer-Verlag, Berlin, Band 14 Heft 4, 1991.

Paul M. Minus, The Ethics of Business in global Economy, Kluwer Academic Publishing, Boston, 1993.

R. Capurro, Ethik und Informatik, Informatik, Springer-Verlag, Berlin, Band 13, Heft 6, 1990.

Robin Snell, Developing Skills for Ethical Management Champman & Hall, N.Y. 1993.

Ronald M. Green, The Ethical Manager, Macmillan College Publishing Co, N.Y. 1984.

Royal P. Fisher, Information System Security, Prentice-Hall, N.Y. 1984.
Thomas R. Piper · Mary C. Gentile, Can Ethics be Taught ?, HBS, Massachusetts, 1993.
Tom L. Beauchamp & Norman E. Bowie, Ethical Theory and Business, Prentice-Hall, N.Y. 1988.