情 報 保 護 學 會 誌
第 13 券 第 2 號, 2003. 4

# 효과적인 정보보호 교육 및 훈련을 위한 프레임워크 개발

오 창 규*, 김 종 기**

요 약

오늘날의 정보시스템 환경에서는 물리적인 접근 통제나 정보보호기술 측면에서의 통제만으로 정보자원을 효과적으로 보호하기 어렵다. 흔히 정보보호는 기술보다는 관리의 문제라고 한다. 따라서 효과적인 정보보호는 조직 구성원의 정보보호 중요성에 대한 인식을 전제로 하며, 인식을 높이기 위해서는 적절한 교육과 훈련이 수반되어야 한다. 본 연구에서는 사회심리학 관점으로부터 의사결정과정 측면과 교육 및 훈련의 효과성 측면에서 정보보호에 대한 사용자의 실제 행동과 내면화 과정을 규명하였다. 이를 토대로 조직 구성원이 지속적인 정보보호 실제 행동을 할 수 있는 정보보호 교육 및 훈련 프레임워크를 제안하고, 구성요소별 전략과 프로그램의 실행 단계를 소개하였다.

## Ⅰ. 서 론

오늘날 정보시스템 환경에서는 물리적인 접근통제나 정보보호기술 측면에서의 통제만으로는 정보자원을 효과적으로 보호하기 어렵다. 많은 조직들이 정보보호 교육이나 훈련을 실시하고 있지만, 정보보호 관련 응용프로그램이나 도구 중심으로 교육한다든지 위협에 노출되었을 때 필요한 정보보호 대책에 치중하는 경향이 많다. 물론 이들도 정보보호 교육 및 훈련에 포함되지만 정보보호 교육 및 훈련은 반드시 조직 구성원의 책임감 있는 정보보호 행동을 지속적으로 할 수 있도록 만들어져야 한다[15].

조직의 정보자원을 보호하기 위해 정보보호 기술 구현에 많은 투자를 하더라도 조직 구성원이 정보보호에 대한 충분한 인지를 하고 있지 않다면 무용지물이 될 것이다. 즉, 조직 구성원의 정보보호 중요성에 대한 인식이 전제되지 않은 상태에서 정보보호 기술 자체가 조직의 정보자원을 효과적으로 보호해 줄 수는 없다[1]. 따라서 오늘날의 정보처리 환경에 부응하는 정보보호 의식을 갖출 수 있도록 체계적이고 종합적인 정보보호 교육 및 훈련 프로그램이 있을 때 효과성은 극대화될 수 있다[12].

본 연구에서는 사회심리학 관점으로부터 개인의 의사결정과정 측면과 정보보호 교육 및 훈련의 효과성 측면에서 정보보호에 대한 사용자의 실제 행동과 내면화 과정을 밝히고자 한다. 이를 바탕으로 정보보호라는 과업의 수행도를 최대화하고 조직 구성원의 지속적인 책임 행동을 할 수 있는 정보보호 교육 및 훈련 프레임워크를 제안하고자 한다. 또한 제안된 프레임워크를 효율적으로 운영하기 위한 단계별 전략과 프로그램의 실행 단계를 소개한다.

## Ⅱ. 정보보호 인식, 교육 및 훈련의 필요성

효과적인 정보보호는 조직 구성원의 정보보호 중요성에 대한 인식을 전제로 하여 적절한 교육 및 훈련이 수반되어야 한다. 이에 본 절에서는 정보시스템의 기술적 환경의 변화 측면과 조직 구성원들의 행동 측면, 그리고 정보보호의 특성 측면에서 정보보호 인식으로부터 교육 및 훈련이 필요하게되는 이유를 살펴본다.

* 부산외국어대학교 국제통상연구소 선임연구원(cgoh@pufs.ac.kr)
** 부산대학교 경영학부 조교수(jkkim1@pusan.ac.kr)

### 1. 기술적 환경 변화 측면

조직에서 사용되는 정보시스템은 대표적인 정보보호 대상이 된다. 정보시스템의 기술적 환경 변화는 정보보호 교육 및 훈련이 사용자 중심으로 변화될 필요성을 제기하고 있다[11]. 먼저 과거 메인프레임 환경에서 정보시스템은 물리적으로 독립된 공간을 가지고 있었기에 물리적인 접근통제에 주력을 했으며, 사용자 또한 한정적이었기에 정보보호가 상대적으로 용이하였다. 그 후 보다 발전된 형태로서 다중 사용자 컴퓨팅 환경이 대두되었다. 다수 사용자가 동시에 접속하고, 물리적 접근을 통제하기가 어려우며, 공유 자원이 증가됨으로써 사용자 인증을 위한 ID와 패스워드가 요구되었다. 즉, 기술적 측면(technical security)의 정보보호 노력이 보다 많은 비중을 차지하였다.

오늘날의 정보시스템 환경은 인터넷의 광범위한 보급을 바탕으로 네트워크를 기반으로 한다. 이로 인해 조직 외부로부터의 위협이라는 새로운 요소가 대두됨으로써 종래의 보호대책만으로는 적절한 보호 수준을 유지하기 힘들게 되었다. 더욱이 정보시스템의 관리 주체가 시스템 관리자로부터 과거보다 많은 컴퓨터 지식을 보유한 사용자로 전이됨에 따라 기술적인 보안시스템의 효과성이 저해되고 있다. 이런 측면에서 볼 때 물리적인 접근통제 내지는 보안기술 측면에서의 통제만으로는 효과적으로 정보자원에 대한 정보보호를 더 이상 지속할 수 없음을 시사한다.

따라서 정보자원을 보호하기 위해 정보보호 기술 개발도 중요하지만, 조직 구성원의 정보보호에 대한 인식이나 교육 및 훈련이 매우 중요한 이슈로 등장하게 되었다. 특히 체계적인 프로그램을 통해 조직 구성원의 정보보호에 대한 행동과 태도가 무의식적으로 취해질 정도까지 되어야 하며, 효과적으로 목표를 달성하기 위해서는 구조적인 접근이 요구된다.

### 2. 조직 구성원 행동 측면

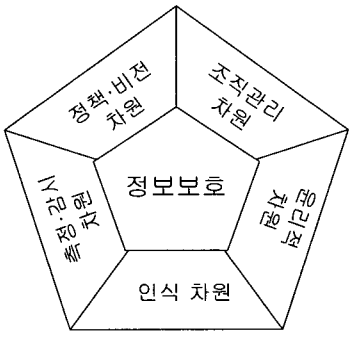
조직 구성원의 행동 측면에서 체계적인 정보보호 교육과 훈련의 필요성을 살펴보면 다음과 같다. 첫째, 조직 구성원이 수행하는 직무가 상이하다. 조직 내 다양한 업무 환경이 존재하기에 서로 상이한 종류의 직무에 적합한 정보보호 지식, 기술, 그리고 능력이 요구된다[19]. 예를 들면, 일선 업무를 수행하는 운영측면에서는 정보보호 위험에 대한 특성을 파악하고 효율적으로 관리할 수 있도록 준비해야 한다. 또한 정보보호 절차와 실행 규칙을 따라야 하는 필요성의 이해에 초점을 맞추어야 하며, 자신이 사용하는 시스템이 어떠한 위험에 노출되어 있는지를 이해해야 한다. 즉, 정보보호에 대한 보다 광범위한 지식 배양과 아울러 자신이 작업하는 특정 시스템에 적용할 수 있는 구체적인 절차와 기법이 요구된다.

반면 기술적 측면에서는 새로운 정보기술에 대한 진화방향을 탐지하고 위협을 예지함으로써 조직내 정보자원의 방어능력을 향상시키기 위한 기술 개발과 최신의 보안 기술과 제품에 대한 능력을 보유해야 한다. 즉, 보안 기술에 대한 광범위한 이해의 바탕 위에서 구체적이며 전문적인 부분에 초점을 맞춘 지식개발을 도모할 수 있는 방향으로 정보보호 교육 및 훈련이 요구된다.

둘째, 조직내 정보자원에 대한 정보보호도 직무의 한 부분이다. 정보보호가 조직 구성원 자신이 떠맡은 부가적인 임무(another assigned duty)로 간주되어서는 안된다[15]. 정보시스템 기술이 급변하는 오늘날의 상황에서 정보보호 자체를 직무의 연장선상에서 수행할 수 있어야 한다. 따라서 체계적인 정보보호 인식으로부터의 교육 및 훈련을 통해 정보자산의 보호에 대한 위협, 도구, 기술, 그리고 위험 억제 등과 관련된 내용의 최신 정보를 유지하고, 이를 실제 행동에 옮길 수 있어야 한다.

### 3. 정보보호의 다차원적 특성 측면

정보보호는 [그림 1]과 같은 다차원적인 특성으로 구성되어 있다[1]. 따라서 정보보호는 다음과 같은 특성을 포괄할 수 있는 내용의 정보보호 인식과 교육 및 훈련을 통해 단순히 정보보호 도구의 학습을 탈피한 종합적이고 체계적인 교육 및 훈련 프레임워크가 요구된다.




[그림 1] 정보보호의 다차원적 특성

첫째, 조직의 정책 및 비전 차원이 고려되어야 한다. 조직내 정보보호를 효과적으로 달성하기 위해 조직의 정보보호정책이 우선적으로 설정되어야 한다. 즉, 조직의 정책과 비전 하에서 정보보호의 근간이 되는 참조 프레임워크가 형성되어야 한다. 따라서 정보보호는 조직의 정책과 비전의 맥락에서 형성되는 속성을 가지고 있다고 볼 수 있다.

둘째, 정보보호는 조직관리 차원의 관점에서 수행되어야 한다. 인터넷의 영향으로 오늘날의 기업환경은 정보의 전송과 공유가 매우 빈번하며, 정보자산은 중요한 관리대상 자원이 되었다. 이러한 환경에서 조직이 성공하기 위한 요인 중의 하나가 조직에서 소유하는 정보자원을 얼마나 잘 관리하는가이다. 또한 정보보호는 조직의 관리통제 책임과 행동의 속성을 가지고 있다. 따라서 이를 위한 적절한 조직구조 및 구성원의 직무 권한, 조직내 효율적인 커뮤니케이션이 요구된다.

셋째, 측정 및 감시 차원을 포함하고 있다. 정보보호의 속성 안에는 조직 내부의 감사기능을 통해서 주기적으로 정보보호의 수준과 위험의 발생가능성을 측정하고 감시하는 것까지 포함된다. 정보보호 정책 및 프레임워크에 대한 측정과 이에 대한 감시를 통해 정보보호가 조직내에서 잘 관리되고 있는가를 살피는 것도 정보보호에 포함될 수 있다.

넷째, 윤리적 차원이 존재한다. 정보보호는 조직 구성원 모두의 윤리적 도덕성을 요구한다. 특히 정보보호 담당 부서 구성원이 가져야 하는 윤리적 문제는 조직의 성공적인 정보보호를 위한 필수적 요건이 된다. 따라서 정보보호에 대한 윤리적 측면은 정보보호 기법 혹은 절차가 올바르게 사용되고 해석될 수 있는 장치를 제공한다.

다섯째, 인식 차원 또한 정보보호의 특성 중의 하나가 된다. 정보보호 기술 자체가 조직의 정보자원을 보호해 줄 수는 없다. 조직의 정보자원을 보호하기 위해 정보보호 기술개발에 많은 투자를 하더라도 조직 구성원이 정보보호에 대한 충분한 인식과 인지를 하지 않고 있다면 효과적인 정보보호는 달성될 수 없다.

## Ⅲ. 사회심리학적 측면에서의 태도, 행동 의도, 실제 행동의 관계

### 1. 사회심리학적 측면에 대한 논의의 필요성

조직내 존재하는 정보자산을 보호하기 위해서는 조직 구성원의 지속적인 정보보호 행동이 요구된다. 정보보호에 대한 사용자의 행동과 내면화(internalization)는 점진적인 단계를 거치고, 장기적인 목표 달성에 초점을 맞추어야 한다[12]. 이에 본 연구에서는 이러한 과정이 무리 없이 달성될 수 있는 정보보호 교육 및 훈련 프레임워크를 개발함에 있어 다음과 같은 이유로 사회심리학 측면의 논의를 수행하였다.

첫째, 교육 및 훈련의 효과성 측면이다. 조직 구성원들에게 정보보호 교육 및 훈련을 수행하는 이유는 조직내 정보자산의 사용자와 관련된 과실을 최소화하기 위함이다. 즉, 이론적 측면에서의 강조가 아니라, 최종 사용자 관점에서 정보보호 기법, 절차 등의 효율성이 최대화 될 수 있도록 해야한다. 이때, 교육 및 훈련의 효과성을 극대화하기 위해서 개인이 저지를 수 있는 오류와 정보보호 이유에 대한 배경을 이해하고 규명함으로써 정보보호에 대한 인식과 태도부터 변경시켜야 한다[17].

둘째, 개인의 의사결정과정 측면이다. 개인의 실제 행동을 설명하고, 행동의 결정요인에 대한 이론적 지침으로서 사회심리학 측면에서의 의도기반 모형들이 존재한다[4]. 대표적으로 이성적 행동가설(TRA, Theory of Reasoned Action), 계획된 행동가설(TPB, Theory of Planned Behavior), 그리고 Triandis 이론, 그리고 기술수용모형(TAM, Technology Acceptance Model) 등이 있다. 이들 모형의 공통점은 의도된 실제 행동의 발생 과정을 설명하고 있는 것이다[6]. 즉, 어떤 사람의 구체화된 실제 행동은 그 행동을 수행하려는 행동 의도에 의해 결정되고, 행동 의도는 태도에 의해 결정된다고 하였다. 이러한 태도에서 행동 의도에 이르는 관계, 의도에서 실제 행동에 이르는 관계는 많은 상황에서 실증적으로 검증되어 오고 지지되어 왔다[3]. 다음 절에서 각 구성요소들에 대해 구체적으로 살펴본다.

### 2. 태도, 행동 의도, 실제 행동

태도는 특정 행동을 수행하는 것과 관련되어 개인이 긍정적 혹은 부정적으로 느끼는 감정이다[5]. 태도는 간접적이며 행동을 수반하지 않고 단지 경험을 통해 형성되는 태도와 실제 행동과의 상호작용으로부터 직접적 경험을 통해 형성된 태도로 나뉠 수 있다[18]. 전자는 효과적인 정보보호 교육 및 훈련을 달성하기 위해 사회심리학 측면에서의 의도 모형을 따라야 되는 이유를 설명한다. 후자는 이러한 교육

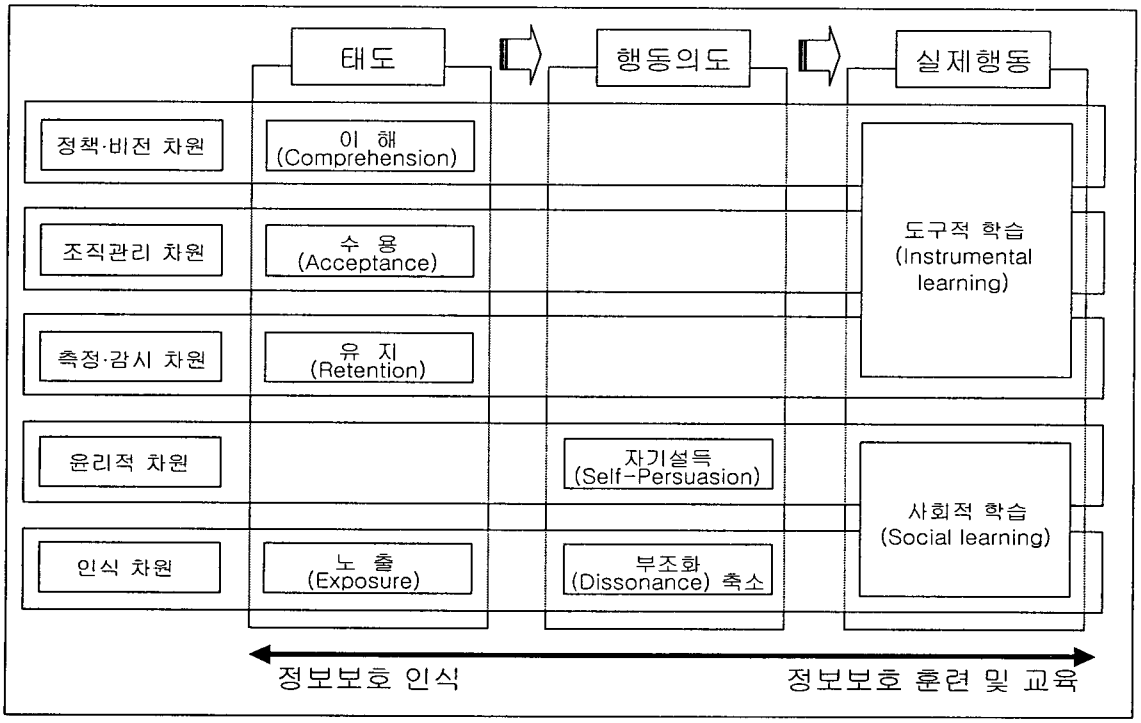
프로그램의 효과성을 극대화하기 위해 실제 행동으로부터의 피드백도 중요함을 나타낸다.

행동 의도는 어떤 행동을 수행함에 있어 개인이 상대적으로 느끼는 의지로 설명될 수 있다[16]. 개인이 특정 행동을 수행해야겠다는 의도를 가질 때 실제 행동으로 옮길 가능성은 커지게 된다. 조직에서의 정보보호는 반드시 지속적인 책임 행동이 뒤따를 때 긍정적인 정보보호 결과를 기대할 수 있다. 따라서 정보보호 실제 행동을 수행해야겠다는 의지를 부여할 수 있는 장치가 정보보호 교육 및 훈련 프로그램에 포함되어야 할 것이다.

실제 행동은 조직내 정보자산에 대한 보호를 위해 조직 구성원이 실제로 취하는 행동을 의미한다. 이때 실제 행동과 결과는 동일한 것이 아니다[6]. 즉, 어떤 행동에 대한 결과가 성공적인 것과 여러 가지 행동들 중에서 선택된 실제 행동을 취하는 것과는 별개의 속성을 가지고 있다. 예를 들면, 정보자원에 대한 보호를 위해 정보보호 행동을 한다(실제 행동)고 해서, 실제 조직의 보안이 지켜진다(결과)는 것을 의미하지는 않는다. 하지만 정보보호 교육 및 훈련의 목적이 결과를 높이기 위한 실제 행동의 강화라는 측면에서 볼 때, 본 연구에서는 정보보호 결과에 초점을 맞추기보다는 실제 행동에 초점을 맞추어 정보보호 교육 및 훈련 프레임워크를 제시하고자 한다.

## Ⅳ. 정보보호 교육 및 훈련 프레임워크의 제안

과업의 수행도는 개인이 가진 능력과 동기, 그리고 작업 조건(working conditions)에 의해 결정되며, 이들은 서로 상호작용 역할을 수행한다[12]. 이때 정보보호에 대한 수행도를 높이기 위해서 요구되는 작업 조건은 정보보호 기술에 해당될 수 있다. 즉, 조직내 존재하는 정보자원을 효과적으로 보호하기 위해 최신의 정보보호 기술이나 시스템을 구축할 때 정보보호를 위한 작업 조건이 훌륭하다고 볼 수 있다. 정보보호에 대한 동기는 정보보호 인식과 관련이 될 수 있다. 이러한 동기는 태도와도 밀접한 관련이 존재한다. 즉, 조직 구성원이 정보보호를 위한 지속적인 실제 행동을 수행하게끔 만들어주는 유발 요인이 될 수 있다. 개인이 가진 능력은 실제적으로 정보보호라는 행동을 취할 수 있도록 하는 교육 및 훈련에 해당될 수 있다. 즉, 정보보호를 위한 교육 및 훈련의 강도와 질이 높을 때 해당 개인은 보다 높은 수준의 정보보호를 할 수 있는 능력을 부




〔그림 2〕 제안된 정보보호 교육 및 훈련 프레임워크

여받게 되고 실제적인 정보보호 행동을 취할 수 있다.

따라서 정보보호라는 과업의 수행도를 최대화하고 조직 구성원의 책임감 있는 정보보호 행위를 할 수 있는 정보보호 교육 및 훈련이 되기 위해서는 실제 행동에 영향을 미치는 행동 의도, 그리고 그 이전 단계인 태도의 변화까지 고려된 프레임워크가 개발되어야 한다. 이에 본 연구에서는 [그림 2]와 같은 정보보호 교육 및 훈련 프레임워크를 제안하였다.

## 1. 정보보호 태도를 변화시키기 위한 전략

제안된 정보보호 교육 및 훈련 프레임워크에서 정보보호 태도를 변화시키기 위한 전략으로 노출 전략, 이해 전략, 수용 전략, 그리고 유지 전략 등을 제안하였다. 여기서 제시된 전략은 정보보호 인식 측면에 보다 주안점을 둔 전략이다. 실질적인 정보보호 행동에 앞서 정보보호에 대한 인식이 우선되어야 할 것이다.

### 1.1 노출(exposure) 전략

일반적으로 개인의 태도가 형성됨에 있어서 선택적 노출(selective exposure) 현상이 존재한다[4]. 선택적 노출이라는 것은 자신의 신념에 위배되는 메시지는 무시하는 경향을 뜻한다. 따라서 조직의 정보보호에 대한 긍정적인 태도가 형성되기 위해서는 정보자원 및 정보관리의 중요성 등에 대한 지속적인 노출을 통한 형상(形象)의 인식이 가장 먼저 요구된다. 이러한 지속적인 노출을 통해서 자신의 신념을 지지하는 메시지에 보다 긍정적인 태도가 형성되는 주의 집중(attention)이 발생할 수 있다. 주의 집중은 정보보호와 관련된 조직의 형식적인 신념과 조직 구성원 자신이 가지고 있는 내재된 신념과의 차이를 줄임으로써 정보보호에 대한 긍정적인 태도가 형성되도록 한다.

### 1.2 이해(comprehension) 전략

정보보호에 대한 노출을 아무리 많이 하더라도 정보자산 보호에 대한 기본적인 내용을 이해하고 있지 못한다면 노출을 통한 주의 집중은 발생하지 않는다. 이 때 조직에서는 정책적으로 정보보호에 대한 정보를 효과적으로 전달하기 위한 다양한 매체를 동원해야 할 필요성이 존재한다. 일반적으로 제공하고자 하는 정보가 복잡할수록 시각적 매체는 더욱 유용하며, 단순한 정보를 제공할 때는 방송 매체가 유용하다는 연구 결과가 보고된 바 있다[7]. 세계에서 가장 큰 알루미늄 생산회사인 Alcoa에서는 조직 구성원 모두가 소유하고 있는 개인용 컴퓨터의 스크린 세이버를 통해 정보보호에 대한 이해를 시킴으로써 정보보호에 대한 태도가 긍정적으로 형성된 사례가 존재한다[15].

### 1.3 수용(acceptance) 전략

정보보호의 중요성에 대한 노출과 전달하고자 하는 메시지가 아무리 다양한 형태로 제공되고 많은 정보가 제공된다고 하더라도 조직 구성원이 이를 받아들이려 하지 않는다면 정보보호에 대한 태도 변화는 발생하지 않는다. 수용 정도를 높이기 위해서는 제공되는 정보나 메시지에 대한 조직 구성원으로부터의 피드백을 적극적으로 받아들임으로써 높은 상호작용을 유지해야 한다. 또한 정보보호의 중요성에 대한 노출이 지속됨에 따라 조직 구성원의 주의 집중이 저하될 가능성도 존재한다. 이러한 단계에서 정보보호에 대한 인식을 높이기 위해 제공되는 정보의 종류나 품질에 의존하기보다는 정보제공자가 뛰어난 전문가임이 보여질 수 있도록 조직 구조 혹은 계층으로부터의 노력이 요구된다. 이러한 전문가로부터 획득된 권위의 복종은 향후 정보보호 실제 행동을 함에 있어서도 효과성이 발휘될 수 있다.

### 1.4 유지(retention) 전략

정보보호에 대한 노출, 이해, 그리고 신념의 변화로 인한 수용으로 정보보호에 대한 태도가 변하여 실제 행동으로 옮겨지기 위해서는 지속적인 태도 변화가 필요하다. 이를 달성하도록 만드는 전략이 유지 전략이다. 조직내 정보자원에 대한 중요성을 상기시키고, 제공되는 보안 정보간의 관련성을 체계적으로 규명할 수 있어야 지속적인 태도가 유지될 수 있다.

## 2. 정보보호 행동 의도를 변화시키기 위한 전략

정보보호 실제 행동을 수행해야겠다는 의지를 부여할 수 있는 장치가 정보보호 교육 및 훈련 프로그램에 포함되어야 하는데 이것이 정보보호 행동 의도를 변화시키기 위한 전략이다. 본 연구에서는 행동 의도를 촉진하기 위해 윤리적 차원과 인식 차원에

초점을 맞춘 자기 설득 전략과 부조화 축소 전략을 제안하였다.

### 2.1 자기 설득(self-persuasion) 전략

실제적 행동이 발생하기 위해서는 자신의 태도 변화에 대한 이유를 제공해야 한다. 이러한 이유가 합당하다고 생각될 때, 변화된 태도가 실제 행동을 유발시킬 수 있게 된다. 즉, 어떤 상황에서 어떤 행동을 왜 할 수밖에 없는가를 설명하는 귀착(attribution)이 요구되며, 이러한 자기 귀착(self-attribution)이 개인의 행동 의도를 결정짓게 만든다[7]. 따라서 정보보호의 인식에 대한 태도가 실제 행동으로 옮겨지기까지의 중간 단계로서 물질적이거나 정신적인 보상 등으로 자신의 정보보호 행동을 취하는 당위성을 설명하는 자기 설득(self-persuasion) 전략이 요구된다. 이 때, 정보보호에 대한 윤리적 차원에서의 접근이 보다 효과적인 자기 설득을 달성하도록 만든다.

### 2.2 부조화(dissonance) 축소 전략

부조화라는 것은 개인이 가지고 있는 신념이나 태도와 보여지는 실제 행동간의 불일치를 의미한다. 이러한 부조화는 개인의 긴장을 야기하고, 긴장을 줄이기 위해 행동을 변화하도록 만든다. 모든 사람이 금전적인 이유나 보안 위협 등과 같은 이유로 인해 자신의 행동 변화를 정당화하지는 않는다[7]. 따라서 이러한 부조화는 개인의 태도변화가 실제적인 행동으로 그대로 옮겨지기 전까지 매우 중요한 역할을 수행한다. 즉, 매우 큰 유인책은 즉각적인 실제 행동의 변화를 야기할 수는 있다. 하지만 궁극적으로 태도의 변화를 통해서 실제 행동의 변화가 온 것이 아니기에 지속적인 정보보호 행동을 한다고 기대할 수는 없다. 따라서 효과적이며 지속적인 실제 정보보호 행동을 유지하기 위한 정보보호 교육 및 훈련 프로그램이 되기 위해서는 태도의 변화로부터 실제 행동의 변화가 발생할 수 있도록 부조화를 줄이는 방향으로 구성되어야 한다.

## 3. 정보보호 실제 행동을 변화시키기 위한 전략

조직내 정보자산에 대한 보호를 위해 조직 구성원이 실제로 취하는 행동을 강화할 수 있는 전략으로 도구적 학습 전략과 사회적 학습 전략을 제시하였다.

### 3.1 도구적 학습(instrumental learning) 전략

정보보호를 달성할 수 있는 실질적인 도구를 학습함으로써 실제 정보보호 행동을 취하도록 하는 것이다. 이러한 도구를 학습함에 있어 크게 두 가지 기법이 존재한다[9]. 첫째, 자발적 학습(operant learning)으로서 교육에 대한 결과로 인해 발생하는 행동이 정당할 경우 구체적인 보상을 통해 정보보호 행동을 강화하는 방식이다. 둘째, 형상 학습(shaping)으로서 도구에 대한 교육 결과의 수준을 낮은 수준에서 시작하여 점차 높은 수준으로 전이하는 방식이다. 즉, 처음엔 기대된 정보보호 행동과 유사한 행동을 하더라도 보상이 존재하지만, 시간이 지날수록 보다 구체적인 정보보호 행동과 기대 행동을 할 때 보상이 주어지는 방식이다. 이 때, 정보보호 행동으로 인한 보상은 물리적인 보상에 치중하는 것이 아니라 다른 조직 구성원들에게 보여질 수 있는 보상이 되어야 한다. 그렇게 됨으로써 정보보호에 대한 조직 전체적인 동기 부여가 발생되는 피드백이 형성될 수 있다.

조직내 정보 자산과 정보시스템의 정보보호를 위한 도구로서 [표 1]과 같은 내용에 대한 교육 및 훈련이 요구된다[8]. 이 때 사람들은 자신이 베푼 호의에 대해 물질적으로나 정신적으로 보상받기를 원하는 경향이 존재한다. 이를 상호관계(reciprocity)로 정의 내릴 수 있는데, 효과적인 정보보호 교육 및 훈련을 달성하는데 있어 이를 적용할 수 있다. 예를 들면, 처음에는 많은 수의 정보보호 실행 과업을 요청하고 점차 직무에 필요한 핵심 요구사항만을 남기고 그 수를 줄인다면, 상대적 보상심리에 의해 정보보호 행동은 더욱 강화될 것이다.

[표 1] 정보보호 교육 및 훈련에서 요구되는 내용

| 분 야 | 내 용 |
|---|---|
| 기술적 측면 (technical security) | 컴퓨터 및 네트워크 보안, 아키텍처, 구성(configuration), 침입탐지, 방화벽, 표준화, 로그인 관리 |
| 관리적 측면 (administrative security) | 정보보호 정책, 위험관리, 개인사용자 보안, 보안인식 훈련 |
| 운영적 측면 (operational security) | 정보보호 처리 및 절차, 패스워드 관리, 헬프 데스크 운용 |
| 물리적 측면 (physical security) | 서버 및 네트워크 영역, 사무실의 보안관리 |

### 3.2 사회적 학습(social learning) 전략

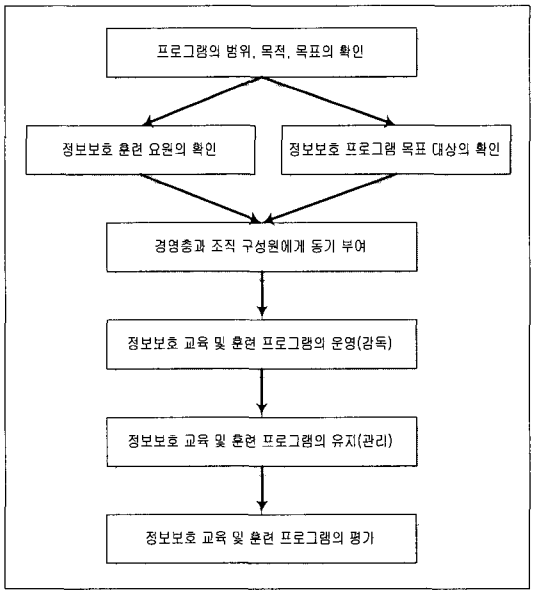
사회적 학습은 사회심리학 측면에서 볼 때, 개인의 관점으로 모든 것이 결정되고 행동으로 옮겨지기보다는 오히려 집단의 관점으로 자신의 생각과 행동이 결정된다는 것이다[11]. 이러한 사회적 학습을 통해 정보보호에 대한 실제 행동이 설명될 수 있다.

조직내에서 정보보호 교육 및 훈련을 직접적으로 제공받지는 않더라도 조직 구성원은 정보보호에 대한 영향을 받는다. 즉, 자신의 동료가 정보보호 행동으로 인하여 보상을 받는 경우 자신이 유사한 보상을 받기 위해 정보보호에 대한 실제 행동을 취하도록 만드는 것이 정보보호를 위한 사회적 학습 전략이다. 예를 들면, 동료가 패스워드를 안전하게 관리를 한다던가 데이터 백업을 주기적으로 하는 행동을 보게 되는 경우 자신의 행동 또한 유사하게 취하게 된다. 따라서 정보보호에 대한 실제 행동을 조직 구성원이 하기 위해서는 물리적인 도구의 학습도 중요하지만 타인으로부터의 사회적 학습 또한 병행되어야 한다. 이러한 사회적 학습을 통해 조직 전반에 걸친 정보보호 문화가 형성될 수 있다.

그리고 정보보호 문화 측면에서 조직 구성원의 정보보호 실제 행동은 조직의 압력으로부터도 형성 가능하다. 일반적으로 권위에 대한 복종은 개인의 행동을 설명해 주는 사회법칙이 된다[7]. 이 때 명령을 부여한 사람이 특정 분야의 전문가일 경우 이러한 경향은 더욱 뚜렷해진다. 또한 명령이 전달되는 상황도 개인의 행동을 설명하는 중요한 요인이 된다. 따라서 조직 구성원이 정보보호 행동을 하도록 만들 때, 정보보호 교육을 담당하는 사람이 보안 분야의 전문가이면서 적절한 조직의 압력이 존재할 때 보다 강화된 행동이 도출되며 긍정적인 방향으로의 사회적 학습이 달성될 수 있다.

## V. 정보보호 교육 및 훈련 실행 단계

정보보호 교육 및 훈련 프로그램이 효과적이 되기 위해서는 적절한 계획, 구현, 유지, 그리고 정기적인 평가가 이루어져야 한다. [그림 3]은 NIST에서 제시한 정보보호 교육 및 훈련 프로그램 실행 단계이다[13].




[그림 3] 정보보호 교육 및 훈련의 실행 단계

### 1. 프로그램의 범위, 목적, 그리고 목표의 확인

정보보호 교육 및 훈련 프로그램을 개발하기 위한 첫 단계로서 프로그램의 범위, 목적, 목표를 정하는 것이다. 이 때 프로그램의 범위는 정보시스템을 사용하는 모든 이에게 훈련을 제공하는 것이며, 전체 조직이 되거나 하위 조직 단위가 될 수도 있다. 특정 시스템을 사용하기 위해 직접적으로 관련된 훈련을 사용자들에게 해주어야 하기에, 보다 세분화된 프로그램으로 대규모 조직 차원의 프로그램을 보충할 수도 있다. 또한 조직 구성원에게만 요구되는지 아니면, 해당 시스템을 사용하는 외적인 사용자에게도 요구되는지에 대한 범위가 명확해야 한다.

일반적으로 정보보호 교육 및 훈련 프로그램의 전체적인 목적은 정보보호 책임에 대한 조직 구성원의 인지를 증대함으로써 정보 자원에 대한 보호를 할 수 있는 적절한 수준을 달성하는 것으로 요약될 수 있으며, 보다 세분화된 목적도 세워야 한다. 목표는 조직이 가지고 있는 특정 목적을 충족시키는 정도로 정의될 수 있다.

### 2. 정보보호 훈련 요원의 확인

조직내 교육부서, 컴퓨터 보안 스텝, 혹은 외부 교육서비스 계약자 등과 같이 정보보호 교육 및 훈련을 수행할 수 있는 요원들은 다양하다. 어떤 대안이 선택되든지 간에 훈련 요원은 컴퓨터 보안 이슈, 원칙, 기술에 대해 충분한 지식을 가지고 있어야 되며, 자신이 가지고 있는 정보와 생각을 효과적으로 전달할 수 있어야 한다.

### 3. 정보보호 프로그램 목표 대상의 확인

자신의 직무를 수행하는데 있어 모든 사람이 동일한 수준 혹은 종류의 정보보호를 필요로 하지는 않는다. 따라서 정보보호 교육 및 훈련 프로그램은 정보보호 프로그램의 목표 대상을 개인과 그룹으로 구분 지으며, 해당 대상에게 요구되는 정보를 발췌하고, 관련 없는 정보는 생략함으로써 최상의 결과가 도출될 수 있도록 구성되어야 한다. 기능에 의한 분류를 하든, 시스템과의 관련성에 의한 분류를 하든 간에 정보보호 교육 및 훈련 프로그램의 목표 대상자를 구분 짓는 것은 프로그램의 효과성을 높이는데 중요한 요인이 된다.

다음은 목표 대상을 구분하기 위한 기준을 예로 든 것이며, 조직 규모에 따라 유동적인 분류가 가능하다.

첫째, 정보보호에 대한 인식 수준에 따른 구분으로서 목표 대상자가 가지고 있는 인식수준에 따라 나누어 질 수 있다. 이 때 효과적인 구분이 되기 위해서는 조직 구성원이 컴퓨터 보안 절차를 얼마나 잘 따를 수 있는가와 어떻게 자신의 직무에 컴퓨터 보안을 적용할 것인가에 대한 이해가 요구된다.

둘째, 과업 혹은 직무에 따른 구분으로서 목표 대상자는 데이터 제공, 처리, 사용하는 사람에 따라 그룹화 될 수 있다.

셋째, 특정 직무 범주에 따른 구분을 살펴보면, 조직에서는 직무에 따라 조직 구성원을 할당하며, 각각의 직무 범주는 서로 상이한 책임권한을 가지기에 이에 따른 훈련이 요구된다. 예를 들면, 일반 관리자, 기술 관리자, 어플리케이션 개발자 혹은 보안 담당자 등과 같은 직무범주에 따라 목표 대상자도 구분되는 것이다.

넷째, 컴퓨터 지식 수준에 따른 구분은 다음과 같다. 컴퓨터에 관한 지식 수준이 높은 전문가는 컴퓨터 보안 관리와 같은 한가지 이슈 보다는 기술 정보까지 포함된 교육 프로그램이 훨씬 가치 있다고 생각한다. 반면 컴퓨터 초보자는 기초적인 소개부터 시작하는 훈련 프로그램으로부터 더 많은 이득을 얻을 수 있다.

다섯째, 사용되는 기술 혹은 시스템의 종류에 따른 구분으로서 기존 제품 혹은 어플리케이션에 사용되는 정보보호 기술은 계속적으로 변한다. 따라서 어플리케이션 사용자는 해당 어플리케이션의 특정 부분에 대한 훈련을 받을 수 있도록 해야하며 이에 따라 교육 프로그램 수강 대상자가 나뉠 수도 있다.

### 4. 경영층과 조직 구성원에 대한 동기 부여

경영층과 조직 구성원의 적극적인 지원과 참여는 정보보호 교육 및 훈련 프로그램을 성공적으로 이행하기 위한 주요 요인 중의 하나다. 조직을 위해서 관리자와 조직 구성원의 정보보호 교육 및 훈련 프로그램 참여를 유도하기 위해 동기를 유발할 수 있는 방안이 고려되어야 한다.

먼저 경영층으로부터 동기를 유발하는 것은 정보보호에 대한 인식 수준을 얼마나 높이는 가에 달려있다. 즉, 정보자산에 대한 보호를 통해 줄일 수 있는 손실이 무엇인가를 명확하게 인지시킬 수 있어야 한다. 이를 통해 정보보호 교육 및 훈련 프로그램을 개발하고 확대하기 위해 사용되는 자원을 지속적으로 확보할 수 있게 된다.

그리고 단지 경영층에게만 동기를 부여하는 것으로는 충분치 않다. 조직 구성원도 정보보호로 인한 이득과 자신의 직무와 어떠한 관련성이 존재하는지를 알아야 한다. 이 때 적절한 교육 및 훈련을 통해서만이 자신이 사용하는 정보자원의 중요성을 이해시킬 수 있다.

### 5. 정보보호 교육 및 훈련 프로그램의 운영(감독)

정보보호 교육 및 훈련 프로그램을 운영함에 있어 몇 가지 중요한 고려사항은 다음과 같다. 첫째, 가시성(visibility)이다. 해당 프로그램이 성공하기 위해서는 가시성이 있어야 하기에 프로그램 개발의 첫 단계에서부터 높은 가시성을 달성하기 위한 노력을 해야 한다.

둘째, 교육 및 훈련 기법으로서 해당 프로그램에서 사용되는 교재는 일관되며 수강대상자의 요구에 맞도록 작성되어야 한다. 또한 직장내 훈련(on-the-job training)도 병행할 수 있는 기법 중의 하나가 된다.

셋째, 교육 및 훈련 주제로서 정보보호와 관련된 주제는 단일의 교육과정에서 배울 수 있는 것 이상의 이슈가 존재하지만, 수강대상자의 요구사항에 기반을 둔 주제가 선정되어야 한다.

넷째, 교육 및 훈련 교재 측면을 살펴보면, 일반적으로 훈련 교재의 품질이 높을수록 수강대상자가 호의적으로 채택할 가능성은 높아지지만 그만큼의 비용도 따른다. 이 때 훈련 교재를 수정하는 비용이 새로 만드는 것보다는 저렴하기 때문에 만일 다른 조직에서 사용한 훈련 교재를 채택한다면 비용은 최

소화될 수 있다.

다섯째, 교육 및 훈련 프리젠테이션으로서 빈도(정기적으로 할 것인지 아니면 필요할 때마다 할 것인지), 프리젠테이션의 길이(일반적인 경우라면 20분 정도), 그리고 프리젠테이션의 스타일(공식적인 프리젠테이션인지 아니면 비공식적인 토의인지, 컴퓨터 기반의 훈련인지 아니면 담화형식인지) 등과 같은 요인들을 고려해야 한다.

### 6. 정보보호 교육 및 훈련 프로그램의 유지(관리)

정보보호 분야는 계속적으로 바뀌는 분야이기에 컴퓨터 기술과 정보보호 요구사항에 맞추어 지속적인 변화에 대한 노력을 기울여야 한다. 만약 인터넷 망에 연결하는 것과 같이 조직의 환경을 바꾸려고 하거나, 새로운 어플리케이션 사용을 시작하거나 할 때, 단순히 조직의 요구사항에만 맞춘 정보보호 교육 및 훈련 프로그램은 비효과적인 결과를 낳을 수도 있다. 마찬가지로 정보보호 인지 프로그램 역시 법이나 조직의 정책이 변경된다면 무용지물이 될 수도 있다. 예를 들면, 기존의 인지 프로그램의 범주에서 조직의 이메일 사용에 따른 새로운 정책에 대한 정보보호 인지를 부여할 수는 없는 것이다. 정보보호 훈련 및 교육 프로그램이 최신의 정보를 제공하지 않는다면 조직의 구성원은 해당 프로그램을 도외시할 가능성이 높아지며 정보보호의 중요성에 대한 지각은 낮아질 수 있다.

### 7. 정보보호 교육 및 훈련 프로그램의 평가

정보보호의 인식과 교육 및 훈련 프로그램의 효과성에 대한 평가를 내리는 것은 어렵다. 그럼에도 불구하고 얼마나 많은 정보를 계속 유지해야 할 지, 어느 정도까지 조직내 정보자원에 대한 보호가 이루어져야 하는지, 정보자산을 보호하기 위한 태도는 어느 정도까지 유지해야 할 지에 대한 평가는 수행되어야 한다. 그러한 평가에 대한 결과는 문제를 규명하고 해결하는 실마리를 제공한다. 이 때, 적용될 수 있는 평가 기법으로서 수강대상자의 평가 이용, 교육교재로부터의 시험, 조직 구성원들의 권고된 정보보호 절차 이행 정도, 정보보호 프로그램이 수행되기 이전과 이후에 보고된 정보시스템 보안사고 종류와 빈도수의 확인 등이 있으며, 이들은 서로 병행되어 사용될 수도 있다.

## Ⅵ. 결 론

본 연구에서 조직내 정보시스템 및 정보자원에 대한 정보보호를 효과적으로 수행하고, 조직 구성원들이 지속적인 책임 행동을 할 수 있도록 만들기 위한 정보보호 교육 및 훈련을 위한 프레임워크를 제안하였다.

먼저 정보보호 교육 및 훈련의 필요성을 정보시스템의 기술적 환경 변화 측면과 조직내 조직 구성원들의 행동 측면, 그리고 정보보호의 특성 측면에서 살펴보았다. 또한 정보보호 교육 및 훈련의 효과성 측면과 개인의 의사결정과정 측면에서 정보자산을 보호하는 조직 구성원의 지속적인 정보보호 행동은 점진적 단계를 거치며 장기적인 목표 달성에 초점을 맞추어야 함을 규명하였다. 효과적인 정보보호 교육 및 훈련이 되기 위해서는 실제 행동에 영향을 미치는 행동 의도, 그리고 그 이전 단계인 태도의 변화까지 고려된 프레임워크가 개발되어야 한다. 본 연구에서는 사회심리학적 측면에서 태도와 행동 의도, 그리고 실제 행동과의 관련성을 통해 정보보호라는 과업의 수행도를 최대화하고 조직 구성원의 지속적인 책임 행동을 할 수 있는 정보보호 교육 및 훈련 프레임워크를 제안하였다.

제안된 프레임워크에서 정보보호의 특성인 정책 및 비전 차원, 조직관리 차원, 측정 및 감시 차원, 윤리적 차원, 그리고 인식 차원에 따라 개인의 정보보호에 대한 태도, 행동 의도, 그리고 실제 행동 단계별 전략을 소개하였다. 그리고 이를 효율적으로 운영하기 위한 프로그램의 실행 단계를 나타내었다. 사회심리학 측면에서 본 행위 이론에 따르면 조직내 정보보호 이슈와 관련된 태도 및 행동 의도를 형성함에 있어 자유방임주의 방식의 리더십이나 경영관리 혹은 관례로서 주어진 지침에만 엄격히 따르도록 프로그램을 운영하는 것은 오히려 부적절한 결과를 초래할 수 있음을 경고하고 있다[2]. 따라서 제안된 프레임워크내에서 조직의 특성과 환경에 맞는 대처도 요구된다.

## 참 고 문 헌

[1] B. Solms, "Information Security—A Multi-dimensional Discipline," *Computers and Security*, 20(6), pp. 504-508, 2001.

[2] C. C. Wood, "Information Security A-

wareness Raising Methods," *Computer Fraud and Security Bulletin*, pp. 13-15, June 1995.

[3] E. Klein, "Image Theory Decision Making Biases Applied to the Technology Acceptance Model," *Unpublished Ph.D. Dissertation*, University of Houston, December 1999.

[4] E. B. Swanson, "Measuring User Attitudes in MIS Research: A Review," *OMEGA*, 10, pp. 157-165, 1982.

[5] F. D. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly*, 13(3), pp. 319-340, September 1989.

[6] I. Ajzen, T. J. Madden, "Prediction of Goal-Directed Behavior: Attitudes, Intentions, and Perceived Behavioral Control," *Journal of Experimental Social Psychology*, 22, pp. 453-474, 1986.

[7] J. Greenberg, R.A. Baron, *Behavior in Organizations*, Allyn and Bacon, Boston, MA. 1993.

[8] K. Peters, "Establishing and Managing an Information Assurance Program," Iowa University, 2002. http://www.itd.state.ia.us/security.

[9] M. Wilson, S. I. Pitcher, J. D. Tressler, J. B. Ippolito, "Information Technology Security Training Requirements : A Role- and Performance-Based Model," *NIST Special Publication 800-16*, April 1998.

[10] M. B. Desman, *Building an Information Security Awareness Program*, AUERBACH, 2001.

[11] M. E. Thomson, R. Solms, "Information Security Awareness: Educating Your Users Effectively," *Information Management and Computer Security*, 6(4), pp. 167-173, 1998.

[12] M. T. Siponen, "A Conceptual Foundation for Organizational Information Security Awareness," *Information Management and Computer Security*, 8(1), pp. 31-41, 2000.

[13] NIST, "An Introduction to Computer Security: The NIST Handbook," *NIST Special Publication 800-12*, 1999.

[14] NSTISS, "Information Systems Security (INFOSEC) Education, Training, and Awareness," *National Security Telecommunications and Information Systems Security*, NSTISSD No. 500, 1993.

[15] P. Spurling, "Promoting Security Awareness and Commitment," *Information Management and Computer Security*, 3(2), pp. 20-26, 1995.

[16] P. M. Bentler, G. Speckart, "Models of Attitude-Behavior Relations," *Psychological Review*, 86(5), pp. 452-464, 1979.

[17] P. S. Dowland, S. M. Furnell, H. M. Illingworth, P. L. Leynolds, "Computer Crime and Abuse: A Survey of Public Attitudes and Awareness," *Computers and Security*, 18(8), pp. 715-726, 1999.

[18] R. P. Bagozzi, "Attitudes, Intentions, and Behavior: A Test of Some Key Hypotheses," *Journal of Personality and Social Psychology*, 41(4), pp. 607-627, 1981.

[19] S. F. Barnett, "Computer Security Training and Education: A Needs Analysis," *Proceedings of the 1996 IEEE Symposium on Security and Privacy*, pp. 26-27, 1996.

## 〈著 者 紹 介〉

**오 창 규 (Changgyu Oh)**
**정회원**

1996년 8월 : 부산대학교 경영학부 졸업
1999년 2월 : 부산대학교 경영학과 석사
2002년 8월 : 부산대학교 경영학과 박사
2001년 3월~2003년 2월 : 부산외국어대학교 국제통상지역원 전임강사(강의전담)
2003년 3월~현재 : 부산외국어대학교 국제통상연구소 선임연구원
관심분야 : 조직내 정보기술채택, 정보시스템 보안관리

**김 종 기 (Jongki Kim)**
**정회원**

1987년 : 부산대학교 경영학과 학사
1988년 : Arkansas State University, MBA
1992년 : Mississippi State University, Ph.D. in MIS
1993년 3월~1998년 12월 : 국방정보체계연구소 선임연구원
1999년 3월~현재 : 부산대학교 경영학부 조교수
관심분야 : 정보시스템 보안관리, 전자상거래, 프로젝트 관리