http://dx.doi.org/10.5392/JKCA.2013.13.04.389

운영 수준에서의 산업보안 관리대책 중요도 결정

Decision Making for the Industrial Security Management Measures' Importance in Operation Level

채정우*, 정진홍**
서울과학종합대학원대학교*, 서울과학종합대학원대학교 산업정보대학원장**

Jeong-Woo Chae(wiseguy21@naver.com)*, Jin-Hong Jeong(jhjeong@assist.ac.kr)**

요약

본 연구는 산업보안활동을 수행함에 있어, 운영 수준의 관리대책에 대한 전략적 우선순위 결정을 통해 합리적인 보안투자 의사결정 지원을 목적으로 하였다. 이를 위해 산업보안전문가들을 대상으로 AHP 설문조사를 시행, 분석하여 산업보안 관리대책들의 중요도와 우선순위를 결정하였다. 상위기준 비교평가에서는 'ICT서비스 사용관리'가 가장 높은 가중치(0.54)를 보였다. 하위기준은 중요도 순으로 3개 그룹으로 구분할 수 있었다. 민감도 분석결과, 'ICT시스템/통신망 접근통제'의 가중치를 2배 높이면 그 하위기준인 '운영체제 접근통제', '애플리케이션 접근통제', '유무선 네트워크 접근통제'의 전체 순위가 상위권으로 진입하였다. '물리/환경적 보안'의 가중치를 2배 높이면 그 하위기준인 '보호구역 설정 및 출입/접근통제'와 '업무설비 방재/대테러 보호 배치'는 전체 순위가 상위권으로, '전원 등 유틸리티 상시 확보'는 중위권으로 상승함을 확인할 수 있었다.

■ 중심어 : | 산업보안 | 산업스파이 | 기술유출 | 다기준의사결정 |

Abstract

This study aims to support rational security investment decision making through prioritizing on operational level of management measures strategically, in carrying out industrial security activities. For this, AHP survey is conducted against industrial security professionals and analyzed. Thereafter, the importance and the priority of industrial security management measures are determined. As a result, in a comparison evaluation among the criteria, 'ICT service management' represents the highest weight (0.54). And the sub-criteria could be divided into three groups (Group Ⅰ,Ⅱ,Ⅲ), depending on their importance. The sensitivity analysis results show that if the weight of the criterion, 'ICT systems/networks access control' is doubled, the sub-criteria, 'O/S access control', 'application access control', and 'wired/wireless network access control' are enter into top rank group. In case of the criterion, 'physical/environmental security' is doubled, the sub-criteria, 'protection zoning/access control' and 'disaster prevention on business equipment/counter-terrorism' are enter into the top rank group, 'securing utilities' is enter into the mid rank group.

■ keyword : | Industrial Security | Industrial Espionage | Technology Leakage | AHP |

접수번호 : #130311-003
접수일자 : 2013년 03월 11일
심사완료일 : 2013년 03월 28일
교신저자 : 정진홍, e-mail : jhjeong@assist.ac.kr

Ⅰ. 서론

많은 시간과 자본, 인력을 투입하여 창출한 지식정보 컨텐츠가 부실한 관리로 보호받지 못한다면, 일개 기업의 손실을 넘어 심각한 국부 유출을 야기할 수 있다. 따라서 경제적 가치가 큰 지식정보 컨텐츠는 산업기밀로 지정하여 보호를 위한 관리대책을 운용하는 것이 필요하다. 실제로 많은 조직에서 ICT보안과 물리/환경 보안업무를 수행하고 있으며, 산업기술이나 영업비밀 유출 사례를 보면 이러한 보안영역들이 내외부의 위협에 취약성을 가져 보안사고가 발생하는 것을 볼 수 있다. 그러므로 침해 위험의 영향도를 파악하고, 비용대비 효과를 고려한 보안대책을 수립하는 것이 필요하다. 그러나 보안투자는 당장의 수익으로 이어지지 않아, 조직의 존속과 발전을 보장하는 필수 요소가 아닌 매몰비용이라는 인식이 강해 과감한 투자를 꺼려하고 있다. 따라서 재원조달능력을 고려하여 보안대책 구현의 우선순위를 정한 후, 일정 비용을 지속적, 단계적으로 투자함으로써 예산상의 제약을 극복해 나가야 한다. 특히 대규모 조직에 비해 보안투자에 여력이 부족한 중소기업의 경우에는 선택과 집중을 통해 산업기밀 침해위험을 감내할 수 있는 수준으로 관리하여야 한다. 중소기업은 우리나라 기업 전체의 99%를 차지할 [7][9][12] 정도로 산업보안의 주요 주체임에도 불구하고, 기술유출 피해액이 매년 증가 추세에 있다. 중소기업의 기술유출 사고 건당 피해액은 2008년도에 평균 9억1000만원에서 2011년에는 15억8000만원으로 가파르게 늘어났다[25]. 이런 상황에도 불구하고 산업기밀 침해방지를 위한 보안투자 우선순위 결정을 지원할 마땅한 기준이 없는 실정이다. 따라서 본 연구에서는 실증을 통해 운영 차원의 산업기밀 보호대책들의 상대적 중요도를 산출하여, 산업보안활동을 위한 물적·인적자원의 투자와 배분에 대한 합리적 의사결정 근거를 제공하고자 한다.

Ⅱ. 이론적 배경

운영 실무차원의 산업보안 관리대책을 AHP기법을 이용하여 연구한 사례를 발굴하기는 어려우므로 유사영역인 일반 정보보호분야를 중심으로 산업보안과 그 연관분야의 논의를 살펴본다. 먼저, S. Smojver(2011)는 정보보호 위험관리기법에 대한 전문가 선호도 조사를 위해 5개의 평가기준을 제시하였다. 그중 '목표 대상/정보의 상세함'의 하위기준을 위험관리방법론의 구체성에 따라 관리지침, 운영지침, 기술지침 등으로 구분하였다. AHP분석 결과, 정보보호 운영 실무에서 참고할 수 있는 '운영지침'이 가장 선호되는 선택기준으로 나타났다. 보안위험을 관리하는데 있어 추상적인 상위지침이나 기술매뉴얼 형식의 하위지침보다는 운영관리수준의 가이드라인이 보안담당자에게 가장 필요한 것으로 볼 수 있다. N. Badie, A. H. Lashkari(2012)는 컴퓨터 보안에서의 위험순위를 켄달(Kendall)의 W검증으로 산출하였다. 9개의 위험평가요소 중 '인가되지 않은 복사'와 '비인가된 접근'이 가장 위험한 것으로 나타났다. 이는 기밀정보에 대한 보호대책으로써 운영지침에 따른 접근통제관리가 우선되어야 함을 시사한다. Z. Tan, P. Li(2012)는 정보보호 위험요인의 중요도를 결정하기 위해 확률, 영향, 통제 불능성을 평가기준으로 하고 선택대안들로 기밀성 공격, 무결성 파괴, 위장 공격, 비인가 접근, 서비스 거부를 제시하였다. 평가기준 중에서는 '영향'이, 대안 중에서는 '기밀성 공격', '무결성 파괴'가 주요 위험요인으로 산출되었다. 즉, 정보자산에 대한 위협이 업무에 미칠 부정적인 영향을 파악하고, 비인가자의 기밀자산 접근통제와 암호화 등을 통한 원본 유지 등의 보안조치에 중점을 두어야 한다. I. Syamsuddin, J. Hwang(2009)는 인도네시아 전자정부 시스템에 관한 정보보호정책을 평가함에 있어 관리, 기술, 경제, 문화를 상위기준으로 하고 기밀성, 무결성, 가용성을 하위요소로 하는 모델을 AHP기법으로 분석하였는데, 정보보호 측면에서 '기술(컴퓨터 보안·유무선 네트워크 보안·인터넷 보안 등)'과 '관리(자료분류·접근통제 등)'가 상대적으로 우위에 있었으며, 정보시스템의 가용성을 보장하는 것이 가장 중요하다고 하였다. 대규모 고객 서비스를 제공하는 조직은 업무연속성 보장이 필수적이며, ICT인프라에 대한 기술적 보안관리가 뒷받침되어야 함을 보여주고 있다.

한편, 김태성·전효정(2006)은 AHP를 이용하여 현장 수요 특성에 적합한 정보보호인력 양성에 요구되는 정보보호 기술분야를 도출하였다. 그 결과, '시스템·네트워크 정보보호'부문과 '응용 정보보호'분야의 인력 양성이 가장 시급한 것으로 나타났는데, 정보보안 실무에서 이와 같은 분야의 관리대책들이 우선적으로 실행 및 개발되어야 함을 방증하는 것으로 볼 수 있다. 보안투자 기준의 우선순위 파악을 통해서도 기밀정보 보호대책의 중요도를 간접적으로 추정해 볼 수 있다. 공희경·전효정·김태성(2008)은 기업이 정보보호를 위해 투자할 경우, 기술적 측면에서의 '시스템 무결성'이 제일 중요한 기준이 된다고 하였다. 안선옥·이희조(2009)는 전략적 효과, 경제적 효과, 관리 효율성, 리스크 관리, 서비스 활용도, 업무 효율성을 평가기준으로 하는 정보보호 투자성과 분석을 통하여 '리스크 관리(데이터 보호, 개인정보 보호, 가용성 보장)'가 성과측면에서 가장 크다고 하였다. 이는 정보보호투자 자체가 목적이 아닌 정보화 투자에서도 의미가 있었다. 진찬용(2010)은 정보화 투자성과 평가를 위해 3개 수준으로 구성된 18개의 IT자산관리 평가지표로 AHP분석을 하였다. 그중 IT실무자 입장의 운용성 측면에서는 '데이터 유실'과 '시스템 유실'이 가장 중요한 지표로 나타났다. 데이터 자체의 무결성 유지와 정보시스템 해킹 방지 등을 위한 보호대책 실행은 정보화 투자에서도 그 성과를 보장한다는 것이다.

산업기술 보호를 위한 기술적 보안체계 연구로는, 김경규·최서윤·허성혜(2009)가 델파이 조사를 통하여, 예방차원의 유출 및 접근통제와 모니터링차원의 콘텐츠 모니터링과 필터링으로 구성된 산업보안기술 체계를 설계하였다. 보호대책의 중요도까지 도출한 것은 아니지만, 실제 ICT서비스 운영시 요구되는 기술적 차원의 보호체계를 제시했다는 데 의의가 있다. 장항배(2010)의 경우, 단편적인 관점을 탈피하여 중소기업 산업기술 유출방지를 위한 정보보호 관리체계를 설계하였다. 이 체계는 산업기술보호 지원역량·지원환경·기반구조와 각각의 하위항목들로 이루어지며, 관리적·물리적 보안영역을 포함하였고, 특히 내부정보 유출방지에 초점이 맞춰져 있다.

물리·환경적 설계 개념을 이용한 산업보안 범죄예방과 테러방지도 연구되었다. 최진혁·박준석(2010)은 접근통제 등 물리적 보안을 중심으로, 산업보안활동의 효과성 제고를 위해 CPTED(Crime Prevention Through Environmental Design: 환경설계를 통한 범죄예방) 개념의 적용이 유용하다는 긍정적 인식이 존재함을 확인하였다. 즉, 산업보안활동에 동 개념을 적용하면 산업스파이 범죄 위험을 감소시켜 그 예방과 산업기밀 보호에 유효할 수 있음을 실증하였다. 정일훈·양진석(2010)은 CPTED의 구성요소를 물리적 요소(접근통제·감시성·영역성), 사회적 요소(신뢰도·친밀도·사회적 유대)로 나누고 AHP분석을 통해 전자가 후자보다 다소 우위에 있으며, 그중 '감시성'과 '접근통제'가 상대적으로 더 중요함을 확인하였다. 총17개의 하위요소 중에서는 '범죄대상물에 대한 접근통제'와 '공·사영역의 공간적 구별'이 높은 가중치를 보였다. 가상의 업무공간에서와 마찬가지로 현실의 업무공간에서도 산업기밀 이용에 대한 명확한 접근조건의 부여와 일반 정보와의 격리 등의 같은 관리가 필요한 것으로 해석된다. 강경연·박병직·이경훈(2011)은 초고층 건축물에 대한 차량폭발물테러 예방과 피해 경감을 위한 건축계획요소를 도출하고, 통합가중치를 각각 산정하였다. 3중 방어선 개념을 상위기준으로 하여 주변현황 및 대지조건, 1차 방어선, 2차 방어선, 3차 방어선으로 구분하고 총17개의 건축계획요소를 세부항목으로 하여 AHP분석을 하였다. 그 결과, 테러위험도에 영향이 큰 상위기준은 '주변현황 및 대지조건'과 '1차 방어선'이었고, 세부항목에서는 '해당 건축물의 인접도로에서의 이격거리', '건축물 용도', '건축물 규모', '주변 주요시설수', '도로 및 지상주차공간과 건축물 사이의 이격거리', '구조부재 노출정도'로 순으로 중요도가 높았다. 따라서 건축물 특성에 맞는 입지 선정이 가장 중요하며, 피해경감을 위해서는 위험 인자와 건축물을 충분히 이격시켜 핵심공간으로의 접근을 외곽에서부터 차단, 통제할 것을 강조하였다. 이는 산업기밀자산과 관련 시설의 방호대책 구현전략에도 적용할 수 있을 것이다.

Ⅲ. 연구방법

1. AHP기법의 활용

AHP(Analytic Hierarchy Process)는 1980년대 이후 경영과학에서 주요한 의사결정기법으로 인정받아 왔으며, 현존하는 의사결정이론 중 가장 광범위하게 활용되고 있는 이론이다[6]. AHP를 이용한 의사결정문제 해결은 다음의 5단계를 거친다[24]. ① 의사결정문제 계층화(Decision Hierarchy) ② 각 요소 간 쌍대 비교(Pairwise Comparison) ③ 상대적 가중치 산정(Estimation of Relative Weights) ④ 평가요소들의 상대적 가중치 종합(Aggregation of Relative Weights) ⑤ 평가자 일관성 검증(Verification of Consistency). 이처럼 AHP는 복잡한 평가기준을 구분하여 체계적으로 계층을 나누고, 계산과정이 명확하며, 정성적이든 정량적이든 평가항목 간의 선호도 측정이 가능하여 그 결과에 대한 일관성 측정이 가능하므로 실무적으로도 널리 이용되고 있다[11]. 따라서 본 연구는 '운영수준의 산업보안 관리대책의 실행 우선순위'를 결정하기 위하여 AHP기법을 주요 연구방법론으로 채택하였다.

2. 연구절차와 방법

본 연구에 앞서 ISO27001, KISA ISMS, PIMS의 보안영역별 통제사항들을 상호 비교 및 취합하고, 산업보안 관련 문헌들에서의 산업기밀 관리방안들과 선행연구들의 시사점 등을 종합하여 11개 영역 54개 통제사항으로 구성된 '산업보안관리 통제 프레임워크'를 도출하였다[18]. 또한 AHP 연구 설문으로 활용하기 전에 객관적 타당성을 담보할 목적으로, 산업보안 전문가들을 상대로 2회의 델파이(Delphi) 조사를 시행하였다. 그 다음 기술적(descriptive) 통계처리와 빈도분석, 전문가 의견일치 정도를 검증하기 위한 켄달(Kendall)의 W검증을 수행하여 최종적으로 확정하였다. 이중 운영수준의 보안대책인 3개 영역 17개 통제사항을 설문항목으로 하여 AHP분석을 시행하였다. 분석을 위한 계층구조는 [그림 1]과 같이 최상위계층은 연구 목표, 제1계층은 3개의 상위기준, 제2계층은 17개의 하위기준들로 구성된다.

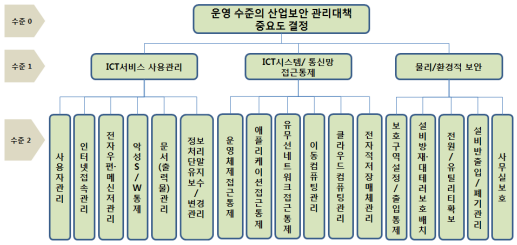

그림 1. 연구모델의 전체 계층구조

설문대상은 교수, 기업의 보안관리자, 보안 컨설턴트, 산업보안 석박사과정 재학생과 학위 취득자 등 산업보안전문가 29명으로 하였다. 설문방식은 전자우편으로 설문지를 배포하고 개별 답신을 받는 형식으로 진행하였다. 설문조사는 2013년 1월 25일부터 2월 12일까지 진행되었다. 유효한 설문응답자의 인구통계적 특성은 [표 1]과 같으며, 'SPSS 17'을 이용하여 기술적 분석과 빈도분석을 실시한 결과이다. 응답자료들은 AHP분석 프로그램인 'EC 2000'을 이용하여 가중치 산출, 일관성 여부, 그리고 민감도 분석을 하였다.

표 1. 설문 응답자의 인구통계적 특성

인적 특성		빈도(명)	백분율(%)
성 별	남	19	90.5
	여	2	9.5
	소 계	21	100
연 령	30대	7	33.3
	40대	10	47.6
	50대	4	19.1
	소 계	21	100
학 력	학사	13	61.9
	석사(수료 포함)	5	23.8
	박사(수료 포함)	3	14.3
	소 계	21	100
경력연수	10년 이하	9	42.9
	20년 이하	10	47.6
	30년 이하	2	9.5
	소 계	21	100
직 위	대리 이하	3	14.3
	부장 이하	14	66.7
	경영진 이상	2	9.5
	교수	2	9.5
	소 계	21	100

AHP기법에서는 설문응답자료의 신뢰도를 판단하기 위해 일관성 비율(CR; Consistency Ratio)을 산출한다. 일관성 비율이 0이면 응답자가 완전한 일관성을 유지하며 쌍대비교를 수행하였음을 뜻한다. Saaty는 일관성 비율이 0.1(10%)미만이면 쌍대비교가 합리적인 일관성이 있는 것으로 판단했고, 0.2(20%)이하이면 용인할 수

있는 수준이며, 이를 초과하는 경우에는 일관성이 부족한 것으로 보았다[4][13]. 연구주제의 탐색적 성격과 응답자들의 AHP기법에 대한 평가 숙련도를 감안하여, 본 연구에서는 일관성 비율 허용기준을 0.2이하로 채택하였다. 이에 따라 응답자료들의 신뢰성을 모두 확인한 결과, 전체 29명의 설문참여자 중 유효한 21명의 응답자료를 선별하였으며 나머지 8명의 응답자료는 분석대상에서 제외하였다. 그 다음, 21명 각각의 의견을 하나로 취합하였다. AHP 개발자인 Saaty는 다수의 의견을 종합하는 집단의사결정에 AHP를 적용할 경우, 개별 쌍대비교 응답결과를 기하평균(geometric mean)으로 계산하여 행렬을 구성한 후에 집단의 가중치로 산정하는 방식을 권하였다[11]. 이에 따라 21명의 개별 설문항목 평가값들의 기하평균을 구한 다음, 최종적으로 단일의 집단의견 중요도와 일관성 비율을 산출하였다.

Ⅳ. 연구 분석

1. 계층별 분석결과

1계층의 평가기준은 3개 이며, 각각의 조작적 정의는 [표 2]에 명시된 바와 같다. 일관성 비율(이하 'C.R.'로 칭함)과 가중치 산출 결과는 [그림 2]와 같다. 먼저, C.R.은 0.01로 허용 기준인 0.2이하를 만족하였다. 전체 중요도는 'ICT서비스 사용관리(0.540) > ICT시스템/통신망 접근통제(0.297) > 물리/환경적 보안(0.163)'순이다. 'ICT서비스 사용관리'의 가중치가 나머지 두 기준보다 약 2, 3배 정도 높은 것으로 나타났다.

표 2. 상위기준(1계층)의 조작적 정의

구성요소	조작적 정의
ICT서비스 사용관리	개인화된 ICT서비스를 통한 산업기밀 침해를 예방하기 위한 기술적 보호대책 (사용자 관리, 인터넷 접속관리, 전자우편 · 메신저 관리, 악성 소프트웨어 통제, 문서(출력물) 관리, 정보처리단말 유지보수 및 변경관리 등)
ICT시스템/통신망 접근통제	공용 ICT자원을 통한 산업기밀 침해 예방을 위한 기술적 보호대책 (운영체제 접근통제, 애플리케이션 접근통제, 유/무선 네트워크 접근통제, 이동(Mobile) 컴퓨팅 관리, 클라우드 컴퓨팅 관리, 전자적 저장매체 관리 등)
물리/환경적 보안	오프라인상의 실물 형태로 존재하는 산업기밀자산 보호대책 (보호구역 설정 및 접근 · 출입통제, 업무설비 방재(防災) · 대테러 보호 배치, 전원 및 유틸리티 상시 확보, 업무설비의 반출입 및 폐기 · 재사용 관리, 사무실 보호 등)

그림 2. 상위기준(1계층)의 가중치, C.R. 산정 결과

전문가들은 ICT서비스를 활용한 업무처리가 산업기밀 유출의 주요 경로가 될 수 있음을 인식하고, 이에 대한 모니터링과 통제를 매우 중요하게 여기고 있는 것으로 해석된다.

표 3. 2계층 구성요소의 조작적 정의

구성요소	조작적 정의
사용자 관리	사용자 등록 · 해지, 접근권한, 패스워드, 접속유지시간 등을 운영지침을 통해 적절하게 관리하는 것
인터넷 접속관리	업무와 무관한 유해 사이트, FTP, P2P, 웹하드 등을 차단 및 모니터링 하는 것
전자우편 · 메신저 관리	전자우편이나 메신저 등은 사내 업무용으로 제한하고, 산업기밀의 송수신 등을 적절하게 모니터링하고 관리하는 것
악성 소프트웨어 통제	바이러스, 웜, 말웨어(malware) 등에 의해 산업기밀이 저장, 처리되는 ICT시스템을 감염시키거나 네트워크로 전파되지 않도록 사전 탐지, 대응하는 것
문서(출력물) 관리	산업기밀이 포함된 문서의 출력이력을 관리하는 시스템(DRM 등)을 운용하고 출력물과 그 복사본의 활용, 폐기 등에 관한 지침을 수립하여 시행하는 것
정보처리단말 유지보수 및 변경관리	전자화된 기밀자산의 가용성 · 무결성 보장을 위해 주기적인 유지보수와 함께 변경이력을 관리하는 것. 외부 위탁시 수탁업체가 서비스수준계약(SLA)에 명시된 보안요구사항을 제대로 이행하는지 점검하고, 필요시 감사하는 것
운영체제 접근통제,	안전한 로그온 절차, 관리자 인증 등을 포함한 ICT시스템의 운영체제 접근을 통제하는 것
애플리케이션 접근통제	애플리케이션(DB, ERP, 그룹웨어, 연구개발S/W 등) 기능들에 대한 접근을 직무권한별로 제한하고, 산업기밀이 수록된 애플리케이션의 출력물은 그 반출입과 유통을 통제하는 것
유/무선 네트워크 접근통제	사용자 트래픽 및 라우팅 관리와 더불어 IPS, IDS, F/W, UTM 등의 네트워크보안시스템을 적절하게 운영, 관리하는 것
이동(Mobile) 컴퓨팅 관리	스마트폰 등 휴대용 ICT기기에 대한 내부망 연결과 공공장소에서의 사용에 대한 관리수단을 마련하여 실행하는 것
클라우드 컴퓨팅 관리	클라우드시스템과 제반 플랫폼에 대한 보호수단을 운영하는 것
전자적 저장매체 관리	DLP · 보안USB · 암호화 등을 활용하여 디지털화된 산업기밀의 반출입, 취급, 보관, 폐기 등을 관리하는 것
보호구역 설정 및 접근 · 출입통제	필요에 따라 등급별 또는 기능별 보호구역을 지정하고, CCTV와 보안 방벽(안내 데스크, 스피드 게이트, 차량출입통제소 등)을 운영하여 접근과 출입, 자산 반출입 등을 통제하고 기록하는 것
업무설비 방재(防災) · 대테러 보호 배치	건물 내외부의 생산 · 연구 · 업무지원용 ICT설비, 전력 · 통신 케이블류 등을 수재, 화재, 폭발물이나 화생방 테러 등으로부터 보호되도록 필요시 시건장치와 함께 구조적으로 안전하게 배치하는 것
전원 및 유틸리티 상시 확보	보호구역과 업무공간은 UPS 등 비상시 전원공급, 항온, 항습, 소화, 급수, 배수 등이 원활하게 이루어지도록 상시 관리하는 것
업무설비의 반출입 및 폐기 · 재사용 관리	업무용 설비의 반출입시는 안전성을 확인하고 반출입 기록을 남기고, 수명연한이나 용도목적 달성 후 폐기나 재사용에 대한 관리를 하는 것
사무실 보호	보안성을 고려한 공간 설계와 집기 배치, 책상정리(Clean desk), 이석시 정보단말 화면보호, 도청 방지 등을 통해 사무공간을 보호하는 것

[그림 3]은 1계층 'ICT서비스 사용관리' 기준에 속하는 하위기준들의 가중치와 C.R. 산출 결과를 보여주고 있다. C.R.은 0.08로 본 연구의 기준치인 0.2이하를 만족하였다. 중요도는 '사용자 관리(0.434) > 인터넷 접속관리(0.191) > 전자우편/메신저 관리(0.128) > 악성 소프트웨어 통제(0.113) > 문서(출력물) 관리(0.073) > 정보처리단말 유지보수/변경관리(0.062)'순으로 나타났다. 여기서는 '사용자 관리'의 가중치가 다른 평가기준에 비해 상당히 비중 있게 나왔는데, ICT는 산업기밀의 유출이나 침해의 수단으로 이용될 수 있으므로 비인가자 접근통제 및 서비스 사용관리, 수요자에 대한 적정한 ICT 자원 할당 등이 우선적으로 필요한 보호대책으로 판단한 것으로 분석된다.

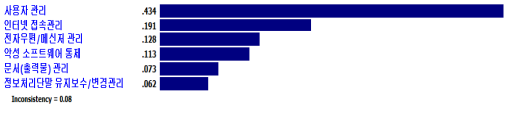

그림 3. 하위기준(2계층)의 가중치, C.R. 산정 결과(ICT서비스 사용관리)

1계층 'ICT시스템/통신망 접근통제' 기준의 2계층 구성요소 가중치와 C.R. 산정 결과는 [그림 4]와 같다. C.R.은 0.04로 본 연구에서의 허용 기준인 0.2이하를 충족하였다. 중요도는 '운영체제 접근통제(0.248) > 애플리케이션 접근통제(0.208) > 유무선 네트워크 접근통제(0.198) > 클라우드 컴퓨팅 관리(0.125) > 전자적 저장매체 관리(0.114) > 이동 컴퓨팅 관리(0.107)'순이다. 이 부문에서는 '운영체제 접근통제'의 가중치가 가장 높았다. 운영체제는 ICT서비스를 제공하기 위한 기본 플랫폼이며, 각종 정보시스템 서비스를 제어 및 관리하는 최고 권한을 가지고 있기 때문에 해킹이나 불법적인 접근 시도 등으로부터 최우선적으로 보호해야 할 대상으로 평가한 것으로 볼 수 있다. 이와 같은 맥락에서, 운영체제상에서 구동되는 업무용 응용 프로그램과 네트워크에 대한 접근통제 또한 이에 버금가는 정도로 중요시 하고 있음을 확인할 수 있다.

그림 4. 하위기준(2계층)의 가중치, C.R. 산정 결과(ICT시스템/통신망 접근통제)

[그림 5]는 1계층 '물리/환경적 보안' 부문의 2계층 구성요소들의 가중치와 C.R. 산출 결과를 보여주고 있다. C.R.은 0.04로 본 연구의 허용 수준인 0.2이하를 충족하였다. 중요도는 '보호구역 설정 및 출입/접근통제(0.417) > 업무설비 방재/대테러 보호 배치(0.211) > 전원 등 유틸리티 상시 확보(0.160) > 업무설비 반출입 및 폐기/재사용 관리(0.121) > 사무실 보호(0.092)'순이다. 여기에서는 '보호구역 설정 및 출입/접근통제'가 다른 평가기준에 비해 매우 높은 가중치를 보였다. ICT를 활용한 가상업무공간에서의 서비스 접근통제가 중요하듯이, 현실의 업무공간에서 물리적 형태로 존재하는 산업기밀과 이에 부수하는 지원시설에 대하여 그 경제적 가치와 업무에 미치는 영향에 따라 등급별 보호구역을 지정, 운용하는 것을 가장 중요하게 인식한 결과로 볼 수 있다.

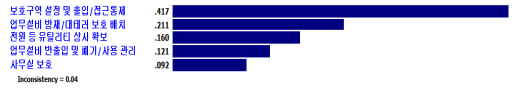

그림 5. 하위기준(2계층)의 가중치, C.R. 산정 결과(물리/환경적 보안)

평가기준의 부문별/전체 가중치와 우선순위, C.R.을 종합하면 [표 4]와 같다. 계층별 분석결과는 앞서 기술한 바와 같고, 여기서는 전체 가중치와 순위를 중심으로 논한다. 먼저, 전체 우선순위는 '사용자 관리 > 인터넷 접속관리 > 운영체제 접근통제 > 전자우편/메신저 관리 > 보호구역 설정 및 출입/접근통제 > 애플리케이션 접근통제 > 악성 소프트웨어 통제 > 유무선 네트워크 접근통제 > 문서(출력물) 관리 > 클라우드 컴퓨팅 관리 > 정보처리단말 유지보수/변경관리 = 전자적 저장매체 관리 = 업무설비 방재/대테러 보호 배치 > 이동 컴퓨팅 관리 > 전원 등 유틸리티 상시 확보 > 업무설비 반출입 및 폐기/재사용 관리 > 사무실 보호'순으로 나

표 4. 전체 및 계층별 가중치 산출 결과와 우선순위

1계층 평가항목	1계층 가중치	2계층 평가항목	2계층 가중치		순 위	
			Local	Global	Local	Global
ICT서비스 사용 관리	0.540	사용자 관리	0.434	0.234	1	1
		인터넷 접속관리	0.191	0.103	2	2
		전자우편/메신저 관리	0.128	0.069	3	4
		악성 S/W 통제	0.113	0.061	4	7
		문서(출력물) 관리	0.073	0.039	5	9
		정보처리단말 유지보수/변경관리	0.062	0.034	6	11
ICT시스템/통신망 접근통제	0.297	운영체제 접근통제	0.248	0.074	1	3
		애플리케이션 접근통제	0.208	0.062	2	6
		유무선 N/W 접근통제	0.198	0.059	3	8
		이동 컴퓨팅 관리	0.107	0.032	6	14
		클라우드 컴퓨팅 관리	0.125	0.037	4	10
		전자적 저장매체 관리	0.114	0.034	5	11
물리/환경적 보안	0.163	보호구역 설정 및 출입/접근통제	0.417	0.068	1	5
		업무설비 방재/대테러 보호 배치	0.211	0.034	2	11
		전원 등 유틸리티 상시 확보	0.160	0.026	3	15
		업무설비 반출입 및 폐기/사용관리	0.121	0.020	4	16
		사무실 보호	0.092	0.015	5	17

타났다. 17개의 평가기준 중 '사용자 관리(0.234)'가 운영수준에서 가장 중요한 산업보안 관리대책으로 평가되었다. 산업기밀의 유통과 보관, 활용 등의 도구로서 ICT서비스를 이용하는 사용자는 잠재적 침해자가 될 수 있으므로, 이에 대한 관리를 가장 먼저 실행해야 할 보호조치로 인식한 것으로 보인다. 평가기준들은 가중치의 비중에 따라 세 그룹으로 구분되었다. 제1그룹은 10~20%대의 높은 가중치를 보인 '사용자 관리', '인터넷 접속관리'이며, 제2그룹은 5~7%대인 '운영체제 접근통제', '전자우편/메신저 관리', '보호구역 설정 및 출입/접근통제', '애플리케이션 접근통제', '악성 소프트웨어 통제', '유무선 네트워크 접근통제'이고, 제3그룹은 3%대 이하인 '문서(출력물) 관리', '클라우드 컴퓨팅 관리', '업무설비 반출입 및 폐기/재사용 관리', '전자적 저장매체 관리', '정보처리단말 유지보수/변경관리', '이동 컴퓨팅 관리', '전원 등 유틸리티 상시 확보', '업무설비 방재/대테러 보호 배치', '사무실 보호'이다. 따라서, 중요도가 높이 평가된 제1그룹의 관리대책 구현에 조직 역량과 자원을 우선적으로 집중시키고, 보유하고 있는 산업기밀 관련 실물자산의 규모를 감안하여 중요도가 상대적으로 낮게 평가된 2그룹과 3그룹의 관리대책들을 순차적 또는 선별적으로 구현하는 방식으로 산업보안활동에 투자를 해야 할 것이다.

2. 민감도 분석결과

민감도 분석(Sensitivity Analysis)은 평가기준의 가중치를 변화시킬 때 평가대안의 우선순위가 어떻게 변동하는지 관찰하는 것이다[8]. 본 연구는 1계층 평가기준들의 가중치 변화에 따라 2계층 산업보안 관리대책들 간의 순위 변동 추이를 파악하기 위해 민감도 분석을 실시하였다. 즉, 중요도가 가장 높게 나타난 1계층 'ICT서비스 사용관리'의 가중치를 고정시키고 나머지 두 기준의 가중치를 변화시켰을 때, 2계층 산업보안 관리대책들의 중요도 순위의 변동을 살펴보았다. [그림 6]은 민감도 분석 시행 전의 평가요소들의 초기 가중치를 보여주고 있다.

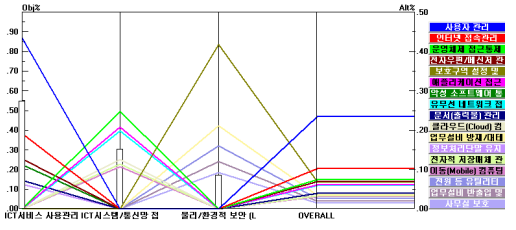

그림 6. 민감도 분석 전 평가요소들의 가중치

먼저, [그림 7]처럼 'ICT시스템/통신망 접근통제'의 가중치를 초기 수준보다 두 배 높이면 그 하위기준인 '운영체제 접근통제'는 전체 순위가 3→1위로, '애플리

케이션 접근통제'는 6→3위로, '유무선 네트워크 접근통제'는 8→4위로 상승되어 우선시 되어야 할 보호대책으로 전환되었다. '클라우드 컴퓨팅 관리', '전자적 저장매체 관리', '이동 컴퓨팅 관리' 등 하위권에 머물러 있던 것들도 중위권으로 진입되는 것을 확인할 수 있었다. ICT인프라의 성숙도나 활용도가 상대적으로 높은 조직은 산업기밀보호에 이처럼 변형된 모델을 적용해야 할 것이다.

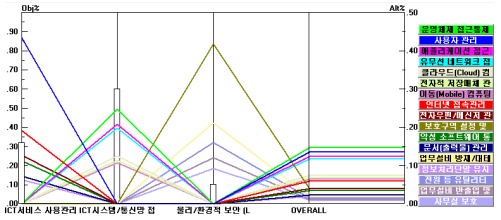

그림 7. 'ICT시스템/통신망 접근통제' 가중치 증가시 민감도 변화 결과

그 다음, [그림 8]과 같이 '물리/환경적 보안'의 가중치를 처음보다 두 배 높이면 그 하위기준인 '보호구역 설정 및 출입/접근통제'는 전체 순위가 5→2위로, '업무설비 방재/대테러 보호 배치'는 16→4위로, '전원 등 유틸리티 상시 확보'는 15→7위로 향상되어 보호대책으로써의 중요도가 매우 높아지는 것을 확인하였다. 현물처럼 물리적인 형상을 갖춘 기밀자산을 상대적으로 많이 보유한 조직에서는 이러한 변경 모델을 산업보안 운영 업무에 적용해야 할 것이다.

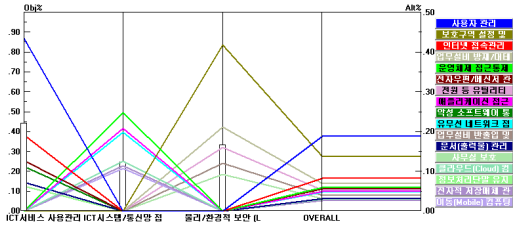

그림 8. '물리/환경적 보안' 가중치 증가시 민감도 변화 결과

V. 결론

본 연구는 산업보안활동에 있어, 운영 수준의 관리대책에 대한 전략적 우선순위 결정을 위해 델파이 조사로 객관적 타당성이 검증된 관리대책들을 AHP기법으로 분석하였다. 상위기준(1계층) 간 비교평가에서는 'ICT서비스 사용관리'가 54.0%로 가장 중요도가 높았으며, 'ICT시스템/통신망 접근통제' 29.7%, '물리/환경적 보안' 16.3%의 순서로 나타났다. 따라서 개인화 된 ICT서비스가 산업기밀 침해의 통로나 수단이 되지 않도록 실제 운영 차원의 산업보안활동에서 우선적으로 관리되어야 함을 확인할 수 있었다. 'ICT서비스 사용관리'의 하위기준에서는 '사용자 관리'가, 'ICT시스템/통신망 접근통제'에 대한 하위기준에서는 '운영체제 접근통제'가, '물리/환경적 보안'에 대한 하위기준에서는 '보호구역 설정 및 출입/접근통제'가 가장 중요한 관리대책으로 평가받았다. 전체 관리대책들의 중요도는 '사용자 관리 > 인터넷 접속관리 > 운영체제 접근통제 > 전자우편/메신저 관리 > 보호구역 설정 및 출입/접근통제 > 애플리케이션 접근통제 > 악성 소프트웨어 통제 > 유무선 네트워크 접근통제 > 문서(출력물) 관리 > 클라우드(Cloud) 컴퓨팅 관리 > 정보처리단말 유지보수/변경관리 = 전자적 저장매체 관리 = 업무설비 방재/대테러 보호 배치 > 이동(Moblie) 컴퓨팅 관리 > 전원 등 유틸리티 상시 확보 > 업무설비 반출입 및 폐기/재사용 관리 > 사무실 보호'순으로 나타났다. 이들은 가중치에 따라 중요도가 높은 제1그룹(사용자 관리, 인터넷 접속관리), 보통 정도인 제2그룹(운영체제 접근통제, 전자우편/메신저 관리, 보호구역 설정 및 출입/접근통제, 애플리케이션 접근통제, 악성 소프트웨어 통제, 유무선 네트워크 접근통제), 상대적으로 낮은 제3그룹(문서(출력물) 관리, 클라우드 컴퓨팅 관리, 업무설비 반출입 및 폐기/재사용 관리, 전자적 저장매체 관리, 정보처리단말 유지보수/변경관리, 이동 컴퓨팅 관리, 전원 등 유틸리티 상시 확보, 업무설비 방재/대테러 보호 배치, 사무실 보호)으로 구분할 수 있었다. 따라서 조직 특유성, 재원조달능력, 산업기밀의 존재형태 등을 고려하여 자체 보안 역량에 걸맞게, 우선순위가 높은 제1그룹의 관리대책들부터 순차적 또는 선별적으로 시행하면서 점진적으로 확대해 나가는 전략을 세워야 한다. 다음으로 민감도 분석결과, 'ICT시스템/통신망 접근통제'의

가중치를 초기치보다 2배 높이면 '운영체제 접근통제', '애플리케이션 접근통제', '유무선 네트워크 접근통제'의 전체 순위가 상위권으로 진입함을 확인하였다. '물리/환경적 보안'의 가중치를 처음보다 2배 높이면 '보호구역 설정 및 출입/접근통제'와 '업무설비 방재/대테러 보호 배치'는 전체 순위가 상위권으로, '전원 등 유틸리티 상시 확보'는 중위권으로 상승함도 볼 수 있었다. 그러므로 어떤 상위기준에 비중을 더 둘 것인가에 따라 탄력적으로 관리대책을 선별하여 운용하여야 할 것이다.

본 연구의 시사점으로는 먼저, AHP기법을 통한 운영수준에서의 산업보안 관리대책 간 상대적 중요도 산정을 통해 보안 자원 투자결정에서의 합리적인 판단근거를 마련하였다. 둘째, 민감도 분석으로 부가적인 응용모델들을 제시하여 조직에 특유한(specific) 산업보안 관리대책을 실행하도록 지침을 제시하였다. 셋째, 산업보안 인증체계 구축의 기초자료로 활용 가능한 탐색적 연구로서 의미가 있다고 본다. 전략적 성격의 조직·제도 차원이 아닌 운영수준의 보안관리대책은 기존 정보보호관련 인증체계들의 통제사항과 공통되는 점이 있으나 산업보안전문가들의 시각에서 그 상대적 중요도를 실증하였다. 연구의 한계점과 향후 과제로는 첫째, 학문적 태동기에 있는 산업보안의 특성상 전문가 풀(pool)이 다소 부족하여 완전한 일반화에는 어느 정도 한계가 있다. 동 분야의 통섭적 지식과 경험을 겸비한 전문인력들이 일정 수준 배출되면 이들을 대상으로 추가 연구가 필요하다. 둘째, 개별 관리대책들에 대한 구체적인 측정지표(metric)가 만들어져야 한다. 셋째, 우선순위는 평가자들의 경험적 판단에 의해 산출된 결과이므로 실제 산업별 내지 조직별 현장업무 특성이나 그에 따른 보안관리대책의 중요도 차이 등을 본 연구결과와 비교, 검증하는 사례연구가 수행되어야 한다.

참 고 문 헌

[1] 강경연, 박병직, 이경훈, "국내 고층 건축물의 차량폭발물테러 위험도 분석 연구", 대한건축학회지, 제27권, 제11호, pp.125-133, 2011.

[2] 공희경, 전효정, 김태성, "AHP를 이용한 정보보호 투자 의사결정에 대한 연구", Journal of Information Technology Applications & Management, 제15권, 제1호, pp.139-152, 2008.

[3] 김경규, 최서윤, 허성혜, "산업기술 보호를 위한 기술적 보안의 탐색적 연구", 한국항행학회논문지, 제13권, 제1호, pp.120-125, 2009.

[4] 김승렬, 김창식, 곽기영, "AHP기법을 이용한 몽골지역을 방문하는 한국인 국외관광객의 여행상품 선택에 관한 연구", 관광·레저연구, 제22권, 제3호, pp.451-465, 2010.

[5] 김태성, 전효정, "AHP를 이용한 정보보호인력 양성 정책 분석", 한국통신학회논문지, 제31권, 제5B호, pp.486-493, 2006.

[6] 김형근, 노창균, "AHP를 이용한 안전관리체제 실행지원 모듈 개발방향에 관한 연구", 해양환경안전학회지, 제10권, 제1호, pp.23-28, 2004.

[7] 남재성, "중소기업의 산업기밀 유출범죄 피해실태와 대책 - 법·제도적 방안을 중심으로 -", 한국공안행정학회보, 제46호, pp.45-75, 2012.

[8] 민혜성, 원갑연, "AHP를 이용한 패밀리 레스토랑의 서비스 수준 연구", 외식산업학회지, 제1권, 제1호, pp.41-70, 2005.

[9] 박춘식, "일본 중소기업 정보보호 대책 가이드라인 동향", 한국정보보호학회논문지, 제20권, 제1호, pp.19-30, 2010.

[10] 안선옥, 이희조, "AHP 기반 Security ROI를 활용한 정보보호 투자성과 분석 연구", 2009년도 한국멀티미디어학회 춘계학술발표논문집, 제12권, 제1호, pp.575-578, 2009.

[11] 여규동, 김길호, 이상원, "AHP 가중치 도출을 위한 쌍대비교의 수정비율 개발", 국토연구, 제71권, pp.25-46, 2011.

[12] 이규안, "중소기업 첨단기술 유출사고의 문제점과 디지털 포렌식을 이용한 해결방안", 한국전자통신학회 2011 추계종합학술대회지, 제5권, 제2호, pp.43-47, 2011.

[13] 이종영, 홍기권, 조규식, 한중근, "AHP기법에 의

한 토사사면 조사항목 평가", 제35회 대한토목학회 정기 학술대회, pp.1824-1827, 2009.
[14] 장항배, "중소기업 산업기술 유출방지를 위한 정보보호 관리체계 설계", 한국멀티미디어학회논문지, 제13권, 제1호, pp.111-121, 2010.
[15] 정덕영, 정병수, "대학 내 산업보안활동 활성화 방안", 한국콘텐츠학회논문지, 제10권, 제5호, pp.314-324, 2010.
[16] 정일훈, 양진석, "환경설계(CPTED)를 활용한 도시범죄 예방에 관한 연구", 한국생활환경학회지, 제17권, 제4호, pp.434-446, 2010.
[17] 진찬용, "AHP 기법을 이용한 IT 자산관리에 관한 연구", 산업경제연구, 제23권, 제6호, pp.3093-112, 2010.
[18] 채정우, 정진홍, "산업보안 관리체계를 위한 보안통제 프레임워크 구성에 대한 연구", 한국공안행정학회보, 제50호, pp.295-338, 2013.
[19] 최진혁, 박준석, "CPTED 전략이 산업보안의 효과성 향상에 미치는 유용성에 관한 실증연구", 한국경찰학회보, 제12권, 제2호, pp.283-320, 2010(5).
[20] I. Syamsuddin and J. Hwang, "The Application of AHP to Evaluate Information Security Policy Decision Making," International J. of Simulation Systems Science and Technology, Vol.10, No.4, pp.46-50, 2009.
[21] N. Badie and A. H. Lashkari, "A new Evaluation Criteria for Effective Security Awareness in Computer Risk Management based on AHP", J. of Basic and Applied Scientific Research, Vol.2, No.9, pp.9331-9347, 2012.
[22] S. Smojver, "Selection of Information Security Risk Management Method Using Analytic Hierarchy Process (AHP)," Proceedings of the 22nd Central European Conference on Information and Intelligent Systems, pp.119-126, 2011.
[23] Z. Tan and P. Li, "Group Decision-Making Information Security Risk Assessment Based on AHP and Information Entropy," Research J. of Applied Sciences, Engineering and Technology, Vol.4, No.15, pp.2361-2366, 2012(8).
[24] T. L. Saaty, *The Analytic Hierarchy Process*, McGraw-Hill, 1980.
[25]http://news.heraldcorp.com/view.php?ud=201302120000176&md=20130215004947_AN

저 자 소 개

채 정 우(Jeong-Woo Chae) 정회원

- 2002년 9월 ~ 2012년 6월 : 한국전력공사 ICT운영센터
- 2010년 8월 : 서울과학종합대학원대학교 산업보안MBA(경영학석사)
- 2012년 9월 : 서울과학종합대학원대학교 경영학 박사과정 수료(산업보안 전공)

<관심분야> : 산업보안정책, 산업보안 컴플라이언스, 산업스파이

정 진 홍(Jin-Hong Jeong) 정회원

- 1993년 2월 : 한양대학교 법학과(법학박사)
- 2009년 2월 : 국가정보원 산업기밀보호센터(처장/실장)
- 2009년 3월 ~ 현재 : 서울과학종합대학원대학교 산업정보대학원장

<관심분야> : 산업보안법령, 산업보안관리실무