

## 직위에 따른 기업정보보호활동인식이 산업기밀유출에 미치는 영향

# Effects of the Recognition of Business Information Protection Activities in Ranks on Leaks of Industrial Secretes

Panam Choi<sup>a,\*</sup>, Seungwhoon Han<sup>b,1</sup>

<sup>a</sup> Department of protection Science, Kyungwoon University, 724-5, Gangdong-ro, Sandong-myeon, Gumi-si, Gyeongsangbuk-do, Korea

<sup>b</sup> Department of protection Science, Kyungwoon University, 724-5, Gangdong-ro, Sandong-myeon, Gumi-si, Gyeongsangbuk-do, Korea

### ABSTRACT

The objective of this study is to analyze control factors in protecting activities of business information that affects the effects of protecting leaks of industrial secretes during business security works in the ranks of staffs. A regression analysis was implemented by 36 items of protecting activities of information and 10 items of preventing industrial secretes for a total of 354 users and managers who use internal information systems in governments, public organizations, and civilian enterprises. In the recognition of protecting activities of business information that affects the prevention of controlling industrial secretes, clerks showed recognitions in physical control, environmental control, and human resource control, and software control and assistant chiefs showed recognitions in hardware control and environmental control. Also, ranks of department managers and higher levels represented recognitions in security control activities. It showed that clerks, assistant chiefs, and above department managers show effects of technical control factors on protecting activities of industrial secretes but section chiefs represent system control factors in preventing industrial secretes.

### KEYWORDS

Industrial security  
Business security  
Activities  
Industrial Secretes  
Business information protection activity  
Management security  
Technical security  
Physical security

본 연구에서는 직원들의 직위에 따른 기업보안 활동 중 산업기밀 유출 방지에 영향을 미치는 기업정보보호활동 통제요인을 분석하고자 하였다. 정부, 공공기관, 민간기업 종사자를 대상으로 내부 정보시스템에 대한 사용자 및 관리자 354 명을 정보보호활동 36문항, 산업기밀유출방지 10문항을 조사 하여 회귀분석을 실시하였다. 산업기밀 유출 통제 활동에 영향 미치는 기업정보보호활동인식으로 사원은 물리적 통제, 환경적 통제, 인적 통제, 소프트웨어통제를 대리는 환경적 통제, 하드웨어 통제, 과장은 하드웨어통제, 환경적 통제, 부장급 이상은 물리적 통제 순서로 보안통제활동 인식을 나타냈다. 사원, 대리, 부장 직위이상에서는 기술적 통제 요인이 과장 직위에서만 시스템 통제 요인이 산업기밀유출 방지 통제활동에 가장 많은 영향을 미친다고 지목하였다.

산업보안  
기업보안활동  
산업기밀  
기업정보보호활동  
관리적 보안  
기술적 보안  
물리적 보안

© 2015 Korea Society of Disaster Information All rights reserved

\* Corresponding author. Tel. 82-54-479-1358. Fax. 82-54-479-1359.

Email. whooni@hanmail.net

1 Tel. 82-10-6531-2363. Email. chlvksdka@daum.net

### ARTICLE HISTORY

Received Nov. 27, 2015

Revised Dec. 02, 2015

Accepted Dec. 07, 2015

## 1. 서론

현대·기아 자동차의 자동차 설계도면이 무더기로 중국으로 유출돼 중국 신차 개발 사업에 사용한 것으로 드러났다. 현대 기아차는 도면이 생산에 사용됐다고 가정하면 유출이 발생한 2014년을 기점으로 3년간 영업상 피해액이 700억대에 이를 것으로 추산했다. 경찰관계자는“자동차 설계 기술 등 중요 영업비밀이 국외로 유출되면서 사업의 피해뿐 아니라 국가 차원의 국부손실이 예상 된다”고 최근 언론에서 보도 하고 있다(데일리 TR, 2015.07). 이 처럼 첨단 산업기술이 해외로 유출되는 경우에는 천문학적 인 경제적 손실을 야기 한다. 뿐만 아니라 최근에 원자력발전소 도면을 온라인상에 유출시켜 사회적 혼란을 일으키는 해커나, 개인정보유출 범죄가 급증하고 사이버 범죄가 기승을 부리고 있어 정보보호나, 기밀유출 문제는 기업의 보호차원에서만이 아니라 국민의 안전과 국익보호 차원에서 접근해야 한다. 특히, 2008년도 미국발 세계 금융위기를 거치면서 국가의 경제를 회복할 수 있는 최선의 방법은 바로 기술혁신이라고, 대부분의 국가들은 절감하고 있다. 그러나 이러한 기술개발을 통한 첨단기술은 이를 쉽게 획득 하려는 경쟁국 또는 경쟁 기업의 스파이 활동인해 해외로 유출되는 사례가 빈번하게 발생하고 있다. 국가 간, 기업 간 경쟁이 심화되면서 이를 예방하기 위한 노력 또한 지속되고 있다(정구현, 2011). 이제 지식, 정보, 기술 등 무형자원이 경제적 부와 직결되는 지식정보화 사회에서 창조적 지식과 정보가 국제경쟁력의 원천이 되고 있어, 오늘날 세계 각국은 국가 간 무한 경쟁의 시대에 대처하여 핵심기술이나 산업정보 등을 보호하는 것이 매우 중요하다는 것을 인식하고 대응책 마련에 부심하고 있다.

산업사회에서 기술과 정보의 유출은 막대한 손실을 유발할 수 있기 때문에 선진국의 경우 이러한 피해에 효과적으로 대처하기 위해 국가 차원에서 법률을 제정하고 기업과 국민들에게 산업보안의 중요성을 적극적으로 홍보하고 있는 실정이다.

이제는 산업정보의 보호는 한 나라의 흥망을 좌우한다고 해도 과언이 아니라고 할 수 있다. 그러나 우리나라는 그 동안 발전과 개발 그리고 성장에만 급급한 나머지 우리의 첨단 기술과 자원을 지키고 보호하는 데는 아직 소홀히 한 측면이 있다.

산업스파이 적발건수도 급증 추세다. 경찰청에 따르면 2010년 40건(국내유출 31건, 해외유출 9건)에 불과했던 산업기술 유출사범 검거건수는 2011년 84건(국내 60건, 해외 24건)으로 늘었고, 2012년엔 140건(국내 113건, 해외 27건)으로 크게 증가했다. 2008년부터 2012년까지의 적발건수는 382건, 80%가 내부자 소행이다. 산업기밀보호센터(NISC) 기술유출 통계에 따르면 2009~2013년간 국내에서 해외로 유출된 기술유출사건은 총 209건이었다(뉴데일리 뉴스, 2014.08).

기업정보보호활동의 개념은 최근 산업기밀 유출의 심각성에도 불구하고 국내에서는 아직까지 명확하게 정의되어 있지 않지만, 현재 기업의 입장에서 인적자원, 정보, 물리적 자산을 보호하고 회사 정보자산의 위험을 감소시키는 제반활동으로 정의(노민선·이삼열, 2010)하고 있으며, 관리적 요인과 기술적 요인, 시스템적 요인으로 분류(이상준, 2008; 정구현, 2011; 한국정보사회진흥원, 2008; 행정안전부, 2008; Holmes, 2001)되고 있다.

기업정보보호 위한 통제방식이 수립된 정보보호 요인에 의거하여 적절하게 관리되고 있는지를 확인하는 통제활동(박태완, 1997)을 관리적 요인이라고 하며, 기술적 요인은 광범위하지만 시스템 보안과 네트워크 보안 분야(Post & Kagan, 2000)를 이야기 하고 있다. 또한 시스템적 요인은 사내 지역을 제한구역, 통제구역으로 구분하여 인원의 출입, 전산매체 및 정보시스템의 사용, 반출, 반입에 대해 차등을 두어 관리 수단(Solms, 2001)을 이야기 한다.

임직원이나 사원들 개개인들은 본연의 업무를 가지고 있으며 바쁜 업무와 일정으로 인해 정보보호의 중요성을 인식하지 못하는 경우가 많아 정보보안 관리에 소홀해지기 쉽다. 그래서 정보보호 주관 부서에서는 임직원 및 협력회사 직원들에게도 정보보안 인식을 제고시키고 자발적인 보호관리 및 예방활동을 할 수 있도록 다양한 정보보호교육을 실시하기도 한다.

신입사원뿐만 아니라 직위별로 해당 직위의 수준에 맞게 정책, 인식제고, 관련 법령 및 법적 책임, 사고 사례, 임직원의 보안관리 사항, 준수사항 등으로 구성되어야 기업 보안에 대한 인식을 높여 실효성을 있는 기업정보보호활동을 통해 산업기밀 유출사태를 미연에 방지 할 수 있을 것이다.

이에 따라 산업기밀 유출 경로로서 기업 조직 내부에서의 보안 위협을 효율적으로 관리하는 것에 대한 중요성이 점차 부각되고 있으며, 민간기업에서 실질적인 보안활동이 정착되기 위한 자율적 산업보안 인식이 조직 내 문화로 형성되고, 이를 통한 해당 조직의 업무 수행에 있어서 전 구성원이 능동적으로 참여할 수 있는 구체적인 산업보안활동이 이루어져야 하며(이민형, 2013), 이를 통해 구성원들의 보안인식을 제고하고 기술유출방지의 효과를 이루기 위한 일련의 보안프로세스가 정립되어야 한다.

그러므로 본 연구에서는 직원들의 직위에 따른 기업보안 활동 중 산업기밀 유출 방지에 영향을 미치는 기업정보보호활동 통제요인을 분석하고자 한다. 각 직위에 따른 기업정보활동의 인식차이와 산업기밀 유출방지활동의 차이를 알아보고, 기업정보활동인식이 내부·외부 기밀유출통제에 미치는 영향을 분석하여 제시하고자 한다.

## 2. 연구방법

### 2.1 연구대상

본 연구의 대상은 정부와 공공기관(251명), 민간기업 종사자(103명)를 대상으로 내부 정보시스템에 대한 사용자 및 관리자를 편의적 표본추출방법을 실시하였다. 총 400부의 설문지를 배포하고 본 연구자가 직접 해당 기업과 기관을 방문하여 현장에서 부연설명 후 기재토록 한 후 바로 회수하였다. 이 중 결측치와 불성실기재 및 오류응답 표본을 제외한 후 총 354매를 본 분석에 사용하였다. 직위는 사원급 191명(54.0%), 대리급 70명(19.8%), 과장급 64명(18.1%), 부장급 이상 29명(8.2%)으로 나타났다.

Table 1. General characteristics of the study subjects

구분		빈도	백분율
성별	남자	228	64.4
	여자	126	35.6
연령	20대	75	21.2
	30대	155	43.8
	40대 이상	124	35.0
직위	사원급	191	54.0
	대리급	70	19.8
	과장급	64	18.1
	부장급 이상	29	8.2
합계		354	100.0

### 2.2 연구모형

연구모형을 위한 통제활동은 Ariss(2002), Kevin(2002)의 관리적 통제, 기술적 통제, 시스템적 통제 요인의 세 가지 요인을 사용하였다. 종속변수로는 Gerber et al.(2001)의 내부기술유출방지, 외부기술유출방지 등 두 가지 요인을 반영하였다.

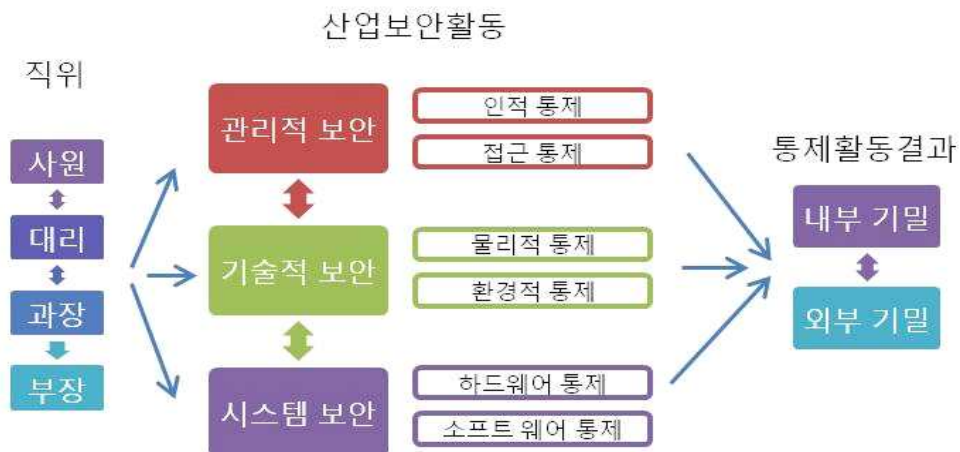


Fig. 1. Study model

### 2.3 설문지 구성을 위한 조작적 정의

#### (1) 정보보호활동

기업의 정보보호활동은 조직내 정보자산을 보호하기 위하여 조직 내에 구현한 관리장치로서 기술적, 물리적 장치뿐만 아니라 관리적 장치를 포함하여 다차원적으로 구성된다(Solms, 1996).

관리적 통제요인은 정보시스템에 정보보호가 구현되었음을 확인하기 위한 -보안요사항 분석 및 명세화, -메시지 인증, 암호화, -디지털 서명, -부인부채의 구현, -변경 관리 절차를 인적통제, 접근통제(Forte, 2002; Kevin, 2002)으로 조작정의 하였다. 기술적 요인으로는 정보처리 설비의 안전한 운영을 위한 - 문서화된 운영 절차 개발과 운영시설의 분리, - 시스템 수락·인수절차분리, -바이러스 통제, -데이터 백업, -매체 폐기, -전자우편 보안 통제를 물리적 통제, 환경적 통제로 정의하고(Ariss, 2002; Post & Kagan, 2000) 있으며, 시스템적 요인으로는 업무 영역 및 정보에 대한 비인가된 물리적 접근, 손실, 그리고 간섭을 예방하기 위한 물리적 보안 경계, - 물리적 출입 통제, - 기록, - 비인가자 제한, - 로그 생성, 보관, - 보안패치 규정, - 탐지시설 도입위한 통제를 하드웨어 통제, 소프트웨어 통제(ITRG:Integrated Transactions Reference Group(2003)-ISO17799)로 조작정의 하였다.

#### (2) 산업기밀 유출방지

산업기밀유출방지는 특정기업내 산업기밀이 외부로 유출되는 것을 방지 또는 예방하기 위한 제반활동으로(Gerber et al., 2001). 본 연구에서는 기업의 정보자산으로 대외보호관리되는 내·외부 기밀의 유출방지나 예방을 위한 통제 또는 관리적 결과물로서 사고감소, 정보보호 효율성 증대, 보호 만족도 향상 및 비용절감 등으로 정의(Gerber et al., 2001)라고 조작 정의 하였다.

### 2.4 측정도구의 신뢰도와 타당성 검증

#### (1) 정보보호활동

정보보호활동에 대한 36개의 문항에 대하여 요인분석을 실시한 결과 총 6개의 요인이 도출되었고, 각 요인을 구성하는 문항들의 중심개념을 바탕으로 요인 명을 부여하였다.

요인 1(12.759%)은 '환경적 통제'로 명명하였고, 요인 2(12.678%)는 '하드웨어 통제'로 명명하였으며, 요인 3(12.581%)은 '인적 통제'로 명명하였다. 요인 4(11.395%)는 '접근 통제'로 명명하였고, 요인 5(10.550%)는 '소프트웨어 통제'로 명명하였으며, 요인 6(10.251%)은 '물리적 통제'로 명명하였다. 모든 하위요인의 고유값은 1이상 값으로 나타났으며, 누적 설명력은 총 분산의 70.214%로 나타났고, 신뢰도는 최고 .933에서 .890에 위치하는 수준으로 검증 되었다.

Table 2. Validation of the information security activities

구분	성분					
	환경적 통제	하드웨어통제	인적통제	접근통제	소프트웨어 통제	물리적 통제
기술적9.	.823	.149	.125	.122	.155	.162
기술적10.	.740	.203	.208	.214	.141	.057
기술적11.	.737	.132	.140	.151	.186	.188
기술적12.	.691	.234	.184	.162	.204	.245
기술적8.	.650	.089	.177	.202	.234	.348
기술적7.	.637	.110	.311	.205	.214	.332
시스템5.	.213	.753	.225	.187	.280	.141
시스템1.	.154	.747	.193	.191	.246	.188
시스템2.	.122	.728	.262	.177	.229	.288
시스템3.	.121	.725	.208	.249	.241	.222
시스템4.	.254	.713	.168	.175	.268	.219
시스템6.	.252	.628	.201	.234	.261	.283
관리3.	.252	.204	.801	.156	.125	.173
관리6.	.095	.275	.748	.165	.225	.160
관리5.	.126	.181	.735	.192	.218	.144

구분	성분					
	환경적 통제	하드웨어통제	인적통제	접근통제	소프트웨어 통제	물리적 통제
관리1.	.099	.234	.695	.231	.133	.192
관리4.	.288	.081	.660	.264	.061	.159
관리2.	.247	.139	.652	.324	.165	.154
관리8.	.145	.095	.199	.770	.174	.156
관리10.	.162	.241	.239	.708	.207	.247
관리12.	.234	.232	.248	.690	.241	.179
관리9.	.146	.161	.289	.687	.081	.236
관리11.	.158	.253	.311	.674	.199	.244
관리7.	.387	.244	.130	.587	.129	-.040
시스템8.	.226	.279	.241	.092	.695	.271
시스템10.	.099	.334	.184	.204	.673	.158
시스템12.	.338	.225	.099	.251	.668	.076
시스템7.	.140	.358	.212	.102	.658	.193
시스템11.	.338	.150	.073	.235	.639	.107
시스템9.	.150	.242	.320	.171	.583	.283
기술적4.	.120	.309	.187	.180	.192	.722
기술적3.	.297	.179	.304	.078	.238	.671
기술적2.	.332	.215	.308	.157	.101	.637
기술적1.	.299	.320	.170	.268	.065	.615
기술적5.	.174	.208	.073	.266	.303	.608
기술적6.	.298	.238	.263	.294	.260	.515
고유값	4.593	4.564	4.529	4.102	3.798	3.690
분산설명(%)	12.759	12.678	12.581	11.395	10.550	10.251
누적설명(%)	12.759	25.437	38.019	49.413	59.963	70.214
신뢰도	.912	.933	.908	.903	.890	.895

(2) 산업기밀유출방지에 대한 타당성 검증

산업기밀유출방지에 대한 10개의 문항에 대하여 요인분석을 실시한 결과이다. 그 결과 총 2개의 요인이 도출되었고, 각 요인을 구성하는 문항들의 중심개념을 바탕으로 요인 명을 부여하였다. 요인 1(37.097%)은 '외부기밀유출방지'로 명명하였고, 요인 2(34.160%)는 '내부기밀유출방지'로 명명하였다. 하위요인의 고유값은 1이상의 값으로 나타났으며, 누적 설명력은 총 분산의 71.257%로 나타났고, 신뢰도는 최고 .902에서 .891에 위치하는 수준으로 검증 되었다.

Table 3. Validation for the industry secrets leak prevention

구분	성분	
	외부	내부
외부 7.	.807	.281
외부 6.	.807	.283
외부 8.	.805	.283
외부 9.	.797	.344
외부 10.	.757	.271
외부 3.	.212	.829
외부 4.	.193	.817
외부 2.	.398	.763
외부 1.	.401	.743
외부 5.	.386	.703
고유값	3.710	3.416
분산설명(%)	37.097	34.160
누적설명(%)	37.097	71.257
신뢰도	.902	.891

## 2.4 자료처리

자료 분석 방법으로 수집된 자료의 통계처리는 데이터 코딩(Data Coding)과 데이터 크리닝(Data Cleaning)과정을 거쳐, SPSS(Statistical Package for Social Science) 17.0 통계 패키지 프로그램을 활용하여 분석하였다. 기업내부 보안통제활동, 산업기술유출방지에 대한 인식을 알아보고, 연구대상자의 사회인구학적 특성과 직위에 따른 차이가 있는지를 알아보기 위하여 일원변량분석(One way ANOVA)을 실시하였으며, 사후검정으로 Duncan test를 실시하였다. 각 직위에 따라 산업기술 유출 방지에 영향을 미치는 보안통제활동 인식을 알아보기 위해 선형회귀분석을 실시하였다.

## 3. 연구 결과

### 3.1 직위에 따른 기업정보보호활동 인식

Table 4. Corporate information security awareness activities, the difference

구분	관리적 활동		기술적 활동				시스템적 활동		전체					
	인적 통제		접근 통제		물리적 통제		환경적 통제				하드웨어 통제		소프트웨어 통제	
	M	SD	M	SD	M	SD	M	SD	M	SD	M	SD		
사원급	3.63	.755	3.52	.784	3.53	.750	3.58	.828	3.55	.882	3.63	.786	3.57	.664
대리급	3.54	.747	3.48	.719	3.48	.689	3.46	.856	3.52	.752	3.59	.702	3.51	.612
과장급	3.62	.866	3.46	.744	3.51	.828	3.56	.826	3.49	.883	3.59	.920	3.54	.722
부장급 이상	3.42	.924	3.17	.882	3.48	.904	3.26	.885	3.43	1.049	3.51	.887	3.38	.773
F-value(p)	.715(.544)		1.787(.149)		.108(.955)		1.424(.235)		.213(.887)		.231(.875)		.769(.512)	

직위에 따른 기업정보보호활동 인식 차이를 분석한 결과 관리적 활동의 하위요인 인적통제(F=.715, p=.544)과 접근통제(F=1.787, p=.149), 기술적 활동요인의 하위요인 물리적 통제(F=.108, p=.955)와 환경적 통제(F=1.424, p=.235), 시스템적 활동의 하드웨어통제(F=.213, p=.887)와 소프트웨어 통제(F=.231, p=.875), 모두에서 사원, 대리, 과장, 부장급 이상의 기업 정보보호활동인식 차이는 나타나지 않았다.

### 3.2 직위에 따른 산업기밀유출통제활동

Table 5. The difference between industrial secrets spill control activities

구분	내부기밀유출방지		외부기밀유출방지		전체	
	M	SD	M	SD	M	SD
사원급	3.54	.742	3.63	.695	3.58	.662
대리급	3.47	.794	3.68	.758	3.58	.686
과장급	3.53	.825	3.67	.791	3.60	.743
부장급 이상	3.46	.823	3.57	.798	3.51	.759
F-value(p)	.177(.912)		.215(.886)		.106(.956)	

직위에 따른 산업기밀 유출 통제 활동차이를 분석한 결과 내부 기밀 유출 방지(F=.177, p=.912)와 외부 기밀 유출방지(F=.215, p=.886) 모두에서 사원, 대리, 과장, 부장급 이상의 산업기밀유출 통제 활동의 차이는 나타나지 않았다.

### 3.3 직위에 따른 기업정보보호활동인식이 내부기밀유출 통제 활동에 미치는 영향

Table 6. Corporate information security awareness activities impact on leaked confidential internal control activities

내부 통제활동		B	표준오차	$\beta$	t	P	
사원	1 (constant)	1.514	.186		8.141	.000	
	환경적 통제	.568	.051	.631	11.167	.000***	
	R=.631 R2=.398 F(p)=124.711(.000)						
	2 (constant)	.998	.209		4.759	.000	
	환경적 통제	.405	.059	.452	6.861	.000***	
	인적 통제	.301	.065	.306	4.643	.000***	
	R=.678 R2=.460 F(p)=79.915(.000)						
	3 (constant)	.868	.212		4.092	.000	
	환경적 통제	.315	.068	.352	4.606	.000***	
	인적 통제	.227	.070	.231	3.225	.001**	
	물리적 통제	.203	.081	.206	2.515	.013*	
	R=.691 R2=.477 F(p)=56.893(.000)						
대리	1 (constant)	1.635	.328		4.980	.000	
	환경적 통제	.531	.092	.573	5.763	.000***	
	R=.573 R2=.328 F(p)=33.213(.000)						
과장	1 (constant)	1.036	.275		3.768	.000	
	하드웨어 통제	.715	.076	.765	9.342	.000***	
	R=.765 R2=.585 F(p)=87.274(.000)						
	2 (constant)	.387	.273		1.418	.161	
	하드웨어 통제	.457	.085	.489	5.370	.000***	
	환경적 통제	.435	.091	.435	4.778	.000***	
	R=.835 R2=.698 F(p)=70.418(.000)						
	3 (constant)	.116	.297		.392	.697	
	하드웨어 통제	.373	.093	.399	4.028	.000***	
환경적 통제	.394	.091	.394	4.335	.000***		
접근 통제	.204	.100	.184	2.041	.046*		
R=.847 R2=.717 F(p)=50.772(.000)							
부장	1 (constant)	1.318	.463		2.847	.008	
	물리적 통제	.617	.129	.677	4.784	.000***	
R=.677 R2=.459 F(p)=22.884(.000)							

직위에 따른 기업정보보호활동인식이 내부기밀유출 통제 활동에 미치는 영향을 알아보기 위해 다중회귀분석을 단계 선택(Stepwise)으로 실시하여 산업기밀유출통제활동의 하위요인인 내부기밀유출 통제에 가장 큰 영향을 미치는 기업정보보호활동인식의 하위 변수를 순서대로 선택한 결과 사원에서는 첫 번째 단계에는 환경적 통제( $\beta=.631$ )인 것으로 나타났다. 그 설명력은 39.8%( $R^2=.398$ )인 것으로 나타났다. 두 번째 단계에는 환경적 통제( $\beta=.452$ )와 인적 통제( $\beta=.306$ )가 선택되었으며, 그 설명력은 46.0%( $R^2=.460$ )인 것으로 나타났다. 세 번째 단계에서는 환경적 통제( $\beta=.352$ ), 인적 통제( $\beta=.231$ ), 물리적 통제( $\beta=.206$ )가 선택되었으며, 그 설명력은 47.7%( $R^2=.477$ )인 것으로 나타났다.

대리에게서는 환경적 통제( $\beta=.573$ )인 것으로 나타났으며, 그 설명력은 32.8%( $R^2=.328$ )인 것으로 나타났다. 과장에게서는 첫 번째 단계에는 환경적 통제( $\beta=.765$ )인 것으로 나타났다. 그 설명력은 58.5%( $R^2=.585$ )인 것으로 나타났다. 두 번째 단계에는 환경적 통제( $\beta=.489$ )와 인적 통제( $\beta=.435$ )가 선택되었으며, 그 설명력은 68.8%( $R^2=.698$ )인 것으로 나타났다. 세 번째 단계에서는 환경적 통제( $\beta=.399$ ), 인적 통제( $\beta=.394$ ), 물리적 통제( $\beta=.184$ )가 선택되었으며, 그 설명력은 71.7%( $R^2=.717$ )인 것으로 나타났다. 이외 하위요인은 역할성향을 설명하는데 도움을 주지 못해 채택되지 않았다. 부장에게는 물리적 통제( $\beta=.677$ )인 것으로 나타났으며, 그 설명력은 45.9%( $R^2=.459$ )인 것으로 나타났다. 이외 하위요인들은 내부기밀유출 통제 활동을 설명하는데 도움을 주지 못해 채택되지 않았다.

### 3.4 직위에 따른 기업정보보호활동인식이 외부기밀유출 통제 활동에 미치는 영향

Table 7. Impact on corporate information security awareness activities outside leaked confidential control activities

외부 통제활동		B	표준오차	$\beta$	t	P
사원	(constant)	1.575	.189		8.336	.000
	물리적 통제	.582	.052	.629	11.112	.000***
	R=.629 R2=.395 F(p)=123.467(.000)					
	(constant)	1.342	.200		6.695	.000
	물리적 통제	.444	.069	.480	6.468	.000***
	소프트웨어 통제	.198	.066	.224	3.023	.003**
	R=.651 R2=.423 F(p)=68.961(.000)					
	(constant)	1.199	.210		5.699	.000
	물리적 통제	.377	.075	.407	4.999	.000***
	소프트웨어 통제	.160	.068	.181	2.370	.019*
	인적 통제	.143	.069	.155	2.064	.040*
	R=.660 R2=.436 F(p)=48.191(.000)					
대리	(constant)	1.253	.321		3.901	.000
	하드웨어 통제	.689	.089	.684	7.727	.000***
	R=.684 R2=.468 F(p)=59.703(.000)					
	(constant)	.892	.318		2.802	.007
	하드웨어 통제	.504	.100	.500	5.032	.000***
	환경적 통제	.293	.088	.332	3.340	.001**
R=.737 R2=.544 F(p)=39.887(.000)						
과장	(constant)	1.483	.292		5.071	.000
	하드웨어 통제	.627	.081	.699	7.704	.000***
	R=.699 R2=.489 F(p)=59.349(.000)					
	(constant)	1.300	.298		4.357	.000
하드웨어 통제	.411	.131	.459	3.143	.003**	
소프트웨어 통제	.260	.126	.303	2.074	.042*	
R=.723 R2=.523 F(p)=33.405(.000)						
부장	(constant)	1.329	.418		3.179	.004
	물리적 통제	.643	.117	.728	5.519	.000***
R=.728 R2=.530 F(p)=30.463(.000)						

직위에 따른 기업정보보호활동인식이 외부기밀유출 통제 활동에 미치는 영향을 알아보기 위해 다중회귀분석을 단계 선택(Stepwise)으로 실시하여 산업기밀유출통제활동의 하위요인인 외부기밀유출 통제에 가장 큰 영향을 미치는 기업정보보호활동인식의 하위 변수를 순서대로 선택한 결과 사원에서는 첫 번째 단계에는 물리적 통제( $\beta=.629$ )인 것으로 나타났다. 그 설명력은 39.5%( $R^2=.395$ )인 것으로 나타났다. 두 번째 단계에는 물리적 통제( $\beta=.480$ )와 소프트웨어 통제( $\beta=.224$ )가 선택되었으며, 그 설명력은 42.3%( $R^2=.423$ )인 것으로 나타났다. 세 번째 단계에서는 물리적 통제( $\beta=.407$ ), 소프트웨어 통제( $\beta=.181$ ), 인적 통제( $\beta=.155$ )가 선택되었으며, 그 설명력은 43.6%( $R^2=.436$ )인 것으로 나타났다.

대리에게서는 첫 번째 단계에는 하드웨어 통제( $\beta=.684$ )인 것으로 나타났다. 그 설명력은 46.8%( $R^2=.468$ )인 것으로 나타났다. 두 번째 단계에는 하드웨어적 통제( $\beta=.500$ )와 환경적 통제( $\beta=.332$ )가 선택되었으며, 그 설명력은 54.4%( $R^2=.544$ )인 것으로 나타났다. 과장에게서는 첫 번째 단계에는 하드웨어 통제( $\beta=.699$ )인 것으로 나타났다. 그 설명력은 48.9%( $R^2=.498$ )인 것으로 나타났다. 두 번째 단계에는 하드웨어적 통제( $\beta=.459$ )와 소프트웨어 통제( $\beta=.303$ )가 선택되었으며, 그 설명력은 52.3%( $R^2=.523$ )인 것으로 나타났다. 부장이상에서는 물리적 통제( $\beta=.728$ )인 것으로 나타났으며, 그 설명력은 53.0%( $R^2=.530$ )인 것으로 나타났다. 이외 하위요인들은 내부기밀유출 통제 활동을 설명하는데 도움을 주지 못해 채택되지 않았다.



### 3.5 직위에 따른 기업정보보호활동인식이 통제 활동에 미치는 영향

Table 8. Corporate information security awareness activities impact on the control activities

	외부 통제활동	B	표준오차	$\beta$	t	P
1	(constant)	1.504	.172		8.735	.000
	물리적 통제	.589	.048	.668	12.347	.000***
	R=.668 R2=.446 F(p)=152.460(.000)					
	-----					
2	(constant)	1.278	.171		7.489	.000
	물리적 통제	.382	.064	.433	5.995	.000***
	환경적 통제	.267	.058	.335	4.634	.003***
	R=.709 R2=.503 F(p)=95.225(.000)					
3	(constant)	1.063	.179		5.922	.000
	물리적 통제	.290	.068	.329	4.234	.000***
	소프트웨어 통제	.224	.058	.281	3.878	.000***
	인적 통제	.191	.060	.218	3.215	.002**
R=.727 R2=.529 F(p)=70.081(.000)						
4	(constant)	.970	.182		5.342	.000
	물리적 통제	.242	.071	.275	3.405	.001***
	환경적 통제	.193	.059	.242	3.268	.001***
	인적 통제	.162	.060	.185	2.687	.008***
	소프트웨어 통제	.130	.060	.155	2.168	.031***
R=.735 R2=.541 F(p)=54.774(.000)						
1	(constant)	1.725	.257		6.701	.000
	환경적 통제	.535	.072	.668	7.400	.000***
R=.684 R2=.468 F(p)=54.753(.000)						
2	(constant)	1.118	.290		3.850	.007
	환경적 통제	.374	.080	.466	4.664	.000***
	하드웨어 통제	.331	.091	.363	3.630	.001***
R=.733 R2=.537 F(p)=38.869(.000)						
1	(constant)	1.260	.232		5.437	.000
	하드웨어 통제	.671	.064	.797	10.406	.000***
R=.797 R2=.66 F(p)=108.287(.000)						
2	(constant)	.862	.249		3.458	.001
	하드웨어 통제	.513	.078	.610	6.596	.000***
	환경적 통제	.266	.083	.296	3.198	.002**
R=.830 R2=.688 F(p)=67.318(.000)						
1	(constant)	1.421	.400		3.551	.001
	물리적 통제	.597	.113	.718	5.264	.000***
R=.718 R2=.516 F(p)=27.713(.000)						

직위에 따른 기업정보보호활동인식이 기밀유출 통제 활동에 미치는 영향을 알아보기 위해 다중회귀분석을 단계선택 (Stepwise)으로 실시하여 산업기밀유출통제활동에 가장 큰 영향을 미치는 기업정보보호활동인식의 하위 변수를 순서대로 선택한 결과 사원에서는 첫 번째 단계에는 물리적 통제( $\beta=.668$ )인 것으로 나타났다. 그 설명력은 44.6%( $R^2=.446$ )인 것으로 나타났다. 두 번째 단계에는 물리적 통제( $\beta=.433$ )와 환경적 통제( $\beta=.335$ )가 선택되었으며, 그 설명력은 50.3%( $R^2=.503$ )인 것으로 나타났다. 세 번째 단계에서는 물리적 통제( $\beta=.329$ ), 환경적 통제( $\beta=.281$ ), 인적 통제( $\beta=.218$ )가 선택되었으며, 그 설명력은 52.9%( $R^2=.529$ )인 것으로 나타났다. 네 번째 단계에서는 물리적 통제( $\beta=.275$ ), 환경적 통제( $\beta=.242$ ), 인적 통제( $\beta=.185$ ), 소프트웨어 통제( $\beta=.155$ )가 선택되었으며, 그 설명력은 54.1%( $R^2=.541$ )인 것으로 나타났다. 대리에게는 첫 번째 단계에는 환경적 통제( $\beta=.668$ )인 것으로 나타났다. 그 설명력은 46.8%( $R^2=.468$ )인 것으로 나타났다. 두 번째 단계에

는 환경적 통제( $\beta=.466$ )와 하드웨어 통제( $\beta=.363$ )가 선택되었으며, 그 설명력은 53.7%( $R^2=.537$ )인 것으로 나타났다. 과장에게서는 첫 번째 단계에는 하드웨어 통제( $\beta=.797$ )인 것으로 나타났다. 그 설명력은 66%( $R^2=.660$ )인 것으로 나타났다. 두 번째 단계에는 하드웨어적 통제( $\beta=.610$ )와 환경적 통제( $\beta=.296$ )가 선택되었으며, 그 설명력은 68.8%( $R^2=.688$ )인 것으로 나타났다. 부장이상에서는 물리적 통제( $\beta=.718$ )인 것으로 나타났으며, 그 설명력은 51.6%( $R^2=.516$ )인 것으로 나타났다. 이외 하위요인들은 내부기밀유출 통제 활동을 설명하는데 도움을 주지 못해 채택되지 않았다.

#### 4. 논의

전경련 산업본부와 산업기밀보호센터, 한국산업기술보호협회 등 유관단체들은 우리나라가 최근 10년간 산업스파이로 인해 입은 직간접 피해액이 최대 600조에 달하는 것으로 나타났다고 추정했다. 해마다 60조원씩 피해를 입는 꼴로 2014년 GDP 1200조의 5%를 넘는 어마어마한 규모다. 기관마다 400조~600조까지의 편차가 있지만 산업 기술 유출에 따른 피해액 산정을 정확히 계산하기 어려운 점과 국가 경쟁력 타격 등 유무형의 피해까지 고려할 경우 그 규모는 짐작조차 쉽지 않다(뉴테일리 뉴스, 2014.08).

산업기밀유출 문제를 개인의 윤리 도덕이나 기업의 개별적 상황으로 치부하기엔 국가적 손실이 너무 크다. 더구나 중국과 동남아 쪽에 한정됐던 유출 사례가 최근엔 대만 러시아 독일 일본 미국 등으로 확산되고 있다.

최근 다변화되고 있는 다양한 산업기밀유출사고에 기인한 시급한 현안에 비추어 볼 때, 안전하게 내부 조직의 정보와 시스템을 보호하기 위해서는 기술적인 측면보다 제도적 또는 관리적 측면과 시스템적 관점에서 효과적인 기업정보보호 활동을 위한 체계를 수립하고 이를 조직 구성원들이 실행할 수 있는 속성을 찾아 점목시킴으로써 자사에 맞는 체계를 실행하는 것이 필요하다. 이러한 체계는 기업정보보호활동에 대한 기술적(Technical), 관리적(Management), 제도적(Institutional) 경로를 통해 발전 되어 오고 있다(Solms, 2000; 2006).

본 연구에서 산업 정보 유출 방지를 위한 기업정보보호활동 요인으로 관리적, 기술적, 시스템적 요인(Ariss, 2002; Kevin, 2002)을 선정하여 회사에서 각자 맡은 직위에 따라 산업기밀유출 통제활동 활동 즉 내부기술유출방지, 외부기술유출방지(Gerber et al; 2001)에 미치는 영향을 알아보자 하였다. 산업기밀 유출 방지활동에 영향을 미치는 기업정보보호활동 통제 요인을 분석한 결과 직위에 따른 기업 정보보호활동 인식요인과 산업기밀유출 통제 활동의 차이를 검증한 결과 사원급, 대리급, 과장급, 부장급 이상은 통계적으로 유의한 차이가 나타나지 않았다( $p<.05$ ). 이는 모든 직위에서 기업 정보보호 활동 인식 요인( $M=3.5$ )이 높은 수준을 유지 하고 있으며, 산업기밀 유출 통제 활동( $M=3.56$ )도 높은 것으로 나타났다. 즉, 모든 직위가 기업 정보보호활동 인식요인과 산업기밀유출 통제 활동에서 높은 수준에서 비슷하게 유지되는 것으로 보인다.

직위에 따른 정보보호활동 인식요인이 산업기밀유출 통제 활동에 미치는 영향을 검증한 결과 먼저 내부기밀유출방지에 있어서는 사원은 환경적 통제, 인적 통제, 물리적 통제가 대리는 환경적 통제 그리고 과장은 하드웨어, 환경적 통제, 접근통제, 부장이상은 물리적 통제가 통계적으로 유의한 정(+)의 영향을 미치는 것으로 나타났다( $p<.05$ ). 즉, 산업 기밀 유출 방지 통제 활동의 내부 요인인 교육참여, 업무만족, 효율증대, 사고감소, 책임인식을 높이는데 사원(환경)과 대리(환경)는 기술적 활동 요인을 중요시 하였으며, 과장(하드)은 시스템적 활동요인 그리고, 부장이상의 직위(물리)에서는 기술적 활동요인이 가장 많은 영향을 미친다고 하였다. 모든 직위에서는 기술적인 요인을 중요시 하였지만, 과장 직위에서만 시스템요인의 하드웨어 통제 요인을 내부 통제활동 결과에 최우선적으로 영향을 미치는 요인으로 지목하였다. 또한 외부기밀유출 통제 활동에 있어서 사원은 물리적 통제, 소프트웨어 통제, 인적 통제가 대리는 하드웨어 통제, 환경적 통제 그리고 과장은 하드웨어, 소프트웨어 통제, 부장이상은 물리적 통제가 통계적으로 유의한 정(+)의 영향을 미치는 것으로 나타났다( $p<.05$ ).

산업 기밀 유출 방지 통제 활동의 외부 요인인 위협에 대한 안정감, 부담, 경각심, 보안정책관리, 비용 절감을 높이는 데 사원(물리)은 기술적 활동 요인 대리(하드)와 과장(하드)은 시스템적 활동요인을 중요시 하였으며, 부장이상의 직위(물리)에서는 기술적 활동요인이 가장 많은 영향을 미친다고 하였다. 사원과 부장이상의 직위는 물리적 요인, 대리(하드)와 과장은 시스템 요인을 외부 통제활동 결과에 최우선적으로 영향을 미치는 요인으로 지목하였다.

내부 기밀과 외부 기밀 합한 산업기밀 유출 통제 활동요인은 사원은 물리적 통제, 환경적 통제, 인적 통제, 소프트웨어 통제가 대리는 환경적 통제, 하드웨어 통제 그리고 과장은 하드웨어 통제, 환경적 통제, 부장이상은 물리적 통제가

통계적으로 유의한 정(+)의 영향을 미치는 것으로 나타났다( $p < .05$ ). 내부 기밀과 외부 기밀 합한 산업기밀 유출 통제 활동요인은 내부 요인과 같이 사원(환경)과 대리(환경)는 기술적 활동 요인을, 과장(하드)은 시스템적 활동요인 그리고, 부장이상의 직위(물리)에서는 기술적 활동요인이 가장 많은 영향을 미친다고 하였다. 이러한 결과 사원, 대리, 부장 직위 이상에서는 기술적 통제 요인이 산업기밀유출 방지 통제활동에 가장 많은 영향을 미친다고 판단했으나, 과장 직위에서는 시스템 통제 요인을 지목하였다고 요약할 수 있다.

물리적, 기술적, 관리적 이 3가지 정보보안 수준을 바탕으로 한 선행연구에서는 최고 경영층의 정보 보안 의식 수준이 높으면 조직의 물리적, 기술적 정보보안 수준도 높으며, 직원들의 정보보안 의식 수준이 높으면 조직의 기술적 정보보안 수준도 높다는 결과가 나왔다. 그러나 직원의 정보보안 의식이 높아도 물리적 보안, 관리적 보안과는 관계가 없다는 결과가 나왔으며, 업종에 따른 보안 의식도 관련이 없는 것으로 나타났다(정해철·김현수, 2000). 이는 기술적 정보보안 수준의 중요성을 강조한 연구로 본 연구에서는 과장급 이외에는 직위에서 모두 기술적 통제 요인을 지목하여, 같은 의미 결론을 도출하였다.

또한 최근 많은 연구에서 불법 산업기밀유출을 예방하고 방지하기 위해서는 관리적 차원뿐만 아니라 정보보호기술적 차원의 속성, 정보 사용자 인증 등의 시스템적 기술이 요구되고 있다고 주장하고 있다. 특히 정보유출 방지방면 정보기기, 네트워크기를 중심으로 그 중요성을 지적하고 있다(남기효 외, 2009; 박성욱·이상호, 2008; Brian, 2005; Dan, 2005; Raul & Rich, 2006). 즉 시스템적 기술에 중요성을 주장하여 본 연구에서 나타난 과장 직위에서 중요시 생각하는 시스템 통제 활동 요인의 생각과 같은 주장의 연구라고 할 수 있다.

하지만, 기업의 정보보호 활동은 인적·물적·시스템적 요소의 상호 연계된 복합적 양상으로 병행되어야 효과 극대화시킬 수 있으므로, 보안의 위험성을 조기에 예방하기 위해서는 각자 직위의 업무를 전문적이며, 체계적으로 역할과 책임 소재를 명확히 설정하는 효율적인 관리가 요구되며, 기업의 여건과 환경에 맞는 기업보안 정책을 수립하고, 관리적, 기술적, 시스템 적으로 통합된 보안관리시스템을 책정하여 운행해야 할 것이다.

## 5. 결론 및 제언

본 연구는 직원들의 직위에 따른 기업보안 활동 중 산업기밀 유출 방지에 영향을 미치는 기업정보보호활동 통제요인을 분석한 본 연구의 결론은 다음과 같다.

첫째. 내부기밀유출 통제 활동에 영향 미치는 기업정보보호활동인식으로 사원은 환경적 통제, 인적통제, 물리적 통제를 대리는 환경적 통제, 과장은 하드웨어통제, 환경적 통제, 접근 통제. 부장급이상은 물리적 통제 순서로 나타났다.

둘째. 외부기밀유출 통제 활동에 영향 미치는 기업정보보호활동인식으로 사원은 물리적 통제, 소프트웨어통제, 인적 통제를 대리는 하드웨어 통제, 환경적 통제, 과장은 하드웨어통제, 소프트웨어 통제, 부장급이상은 물리적 통제 순서로 나타났다.

셋째. 산업기밀 유출 통제 활동에 영향 미치는 기업정보보호활동인식으로 사원은 물리적 통제, 환경적 통제, 인적 통제, 소프트웨어통제를 대리는 환경적 통제, 하드웨어 통제, 과장은 하드웨어통제, 환경적 통제, 부장급이상은 물리적 통제 순서로 나타났다.

이상의 연구결과를 종합해 보면, 사원, 대리, 부장 직위이상에서는 기술적 통제 요인이 산업기밀유출 방지 통제활동에 가장 많은 영향을 미친다고 판단 하였으며, 과장 직위에서만 시스템 통제 요인을 지목하였다. 따라서 과장 직위에서 정보유출 방지에 있어 시대적 흐름을 가장 빠르게 인식하는 것으로 생각된다. 하지만 기업의 정보활동은 상호연계된 복합적 양상을 가지고 있으므로 조직원들이 수궁할 수 있는 기업 보안활동과 제도 적용을 통해 조직원들의 역할 인식과 회사에 대한 신뢰도를 높일 수 있는 방안이 필요하며, 회사의 환경에 맞는 기업보안정책과 체계 구축이 하여야 한다.

## References

- Ki-Hyo Nam · Hyung-Suk Kang · Ji-Ho Gil · Sung-In Kim(2009). "Internal information leakage prevention (DLP) technology trends". 『Week Technology Trends』 . No. 1413.
- Min-Sun No · Sam-Yeol Lee(2010). "Factors assessment of the security capabilities of the SME industry". 『Korea Public Administration Review』 . Vol44, No. 3.
- Sung-Uk Park · Sang-Ho Lee(2008). "An Analysis on Information Security Industry in Korea : An Input-Output Analysis". 『Industrial Innovation』 . Vol24, No. 3.
- Tae-Wan Park(1997). 『Information Systems Security Supervision』 . Korea Computerization Agency.
- Min-Hyeong Lee(2013), A Study on the Developmental Activation Plan of Local Medium and Small Firms - Focussed on Industrial Security . Korea Local Government Studies, Vol.15, No. 2, pp141-159.
- Sang-Jun Lee(2008). Assessing the accounting errors of the job relevance of skills. HoSeo University Graduate School.
- Gu-Hun Jung(2011). "Effect of Information Security Management and Control Activities for Proprietary Information Leakage Prevention on Information Asset Protection Performance". Ph.D. Diissertation, KookMin University Business IT Graduate School.
- Hae-Chul Jung · Hyun-Soo Kim(2000). "Relationship between consciousness and organization of information security and information security level of the organization". 『Journal of Information Technology Applications & Management』 . Vol7, No. 2.
- Korea Information Society Development Institute(2008). 『National Informatization White Paper』 . Korea Information Society Development Institute.
- MOPAS(2008). 『Privacy medium-term Master Plan』 . MOPAS.
- New Daily News. 'Industrial espionage damage 年 60 80% an inside job jo bomb technology delivered' Aug 25th, 2014.
- Daily TR. 'Hyundai Kia's design leaked a bunch of drawings China'. July 22th, 2015
- E-Daily. 'Group opposing nuclear power, nuclear power figures released ... "I sell in other countries," Cash requirements ". Aug 3th, 2015.
- Ariss, S. S. (2002). Computer Monitoring: Benefits and Pitfalls Facing Management. Information & Management, Vol39, No.7, pp. 553-558.
- Brian, E. B. (2005). Worldwide Outbound Content Compliance 2005-2009 Forecast and Analysis: IT Security Turns Inside Out. Internet Data Center(IDC).
- Dan, Y. (2005). InfoWatch: A Multi-layered Approach for Information Leakage Detection and Prevention. Internet Data Center(IDC).
- Forte, S. (2002). Vulnerability Management: One Problem, Several Potential Approaches. Network Security, Vol5, pp. 11-13.
- Gerber, M., Solms, R., Overbeek, P. (2001). Formalizing Information Security Requirements. Information Management and Computer Security, Vol9, No.1, pp. 32-37.
- Holmes, D. (2001). E-Gov: e-Business Strategy for Government. London: Nicholas Brealey Publishing.
- Kevin, S. H. (2002). The Digital Security Debate: How to Manage Risk?, Secure Business Quarterly, First Quarter.
- Post, G. & Kagan, A. (2000). Management Tradeoffs in Anti-virus Strategies. Information & Management, Vol37, No.1, pp. 13-24.
- Raul, E. P. & Rich, M. (2006). Magic Quadrant for Content Monitoring and Filtering and Data Loss Prevention. Gartner RAS Core Research Note.
- Solms, B. (1996). Information Security Management: The Second Generation. Computer and Security, Vol15, No.4, pp. 281-288.
- Solms, B. (2001). Corporate Governance and Information Security. Computers and Security, Vol20, No.3, pp. 215-218.
- Kwon, Y. T., Yoon, M. O., Choi, H. C., The Comparative Study on the Perception of Business Activities about Disaster Preparedness between Korea and Japan, Journal of The Korean Society of Disaster Information, Vol 9, No.4