인간 관점의 정보보호 연구동향 분석

김건우*, 김정덕**
*중앙대학교 일반대학원 융합보안학과
**중앙대학교 산업보안학과
e-mail: kunwoo.kim317@gmail.com, jdkimsac@cau.ac.kr

A Study on Research Trends Analysis about Human Aspect of Information Security

Kunwoo Kim*, Jungduk Kim**
*Dept. of Security Convergence, Graduate School of Chung-Ang University
**Dept. of Industrial Security, Chung-Ang University

요 약

정보기술의 발달은 조직의 업무환경에 긍정적인 영향을 주는 동시에 다양한 정보보호 위협에 따른 사고 발생 등 부정적인 영향을 미친다. 조직에서는 보안사고 예방을 위하여 다양한 노력들을 경주하고 있지만 기술적 보안 솔루션에 의존하는 경향이 있으며, 그럼에도 불구하고 보안 사고를 완벽히 예방하는 것은 불가능하다. 최근 기존의 정보보호 접근방법의 한계를 극복하기 위한 새로운 접근방법인 인간 중심 보안(People Centric Security)에 대한 관심이 증가하고 있으며, 임직원의 자발적인 정보보호 정책 준수에 대한 연구의 필요성이 제기되고 있다. 본 연구는 향후 인간 관점의 정보보호 연구의 발전을 위해 기존의 수행된 연구들을 분석하여 통합된 관점에서 연구방향을 제시하는 연구동향 분석 연구로서, 해외 4개의 저널에서 수집한 134개의 논문을 대상으로 연구 추세, 연구 주제, 연구 방법론 등을 분석하였다. 본 연구의 결과는 국내의 인간 관점에서의 정보보호 관련 연구 활성화에 기여할 수 있을 것이라 판단되며, 조직에서 임직원의 정책준수에 영향을 주는 요인들을 참고하여 정보보호 정책 수립 시 활용할 수 있을 것이다.

1. 서론

오늘날 정보기술의 급속한 발달에 따라 조직의 업무환경도 지속적으로 변화하고 있다. 임직원들은 무선인터넷과 모바일 디바이스를 활용하여 언제 어디에서든지 업무를 수행할 수 있게 되었으며, 이에 따라 조직의 업무 생산성 향상에 크게 기여하게 되었다. 하지만 기술이 발달함에 따라 APT와 같은 위협이 등장하였고, 내부정보 유출의 경로가 다양해지면서 크고 작은 보안 사고들이 매년 발생하고 있다. 이에 따라 정보보호의 중요성에 대한 인식이 증가하고 있으며, 조직들은 정보보호 수준 향상을 위해 다양한 노력을 기울이고 있다. 통계에 따르면, 정보보호 산업의 규모는 지속적으로 증가하고 있으며, 대부분의 조직들은 기술적인 정보보호 솔루션에 대한 의존도가 높은 것으로 나타났다[7]. 아무리 최신의 정보보호 솔루션을 도입하여 운용하더라도 조직 구성원들의 의식이 부족하다면 무용지물일 것이다. 즉, 사고의 원인은 인간이고 사고를 해결하는 것 역시 인간이기 때문에 기술적인 보안대책에 막대한 금액을 투자하여도 조직 구성원 개개인의 보안의식이 부족하다면 효과가 없을 것이다.

‘정보보호는 결국 인간이다.’라는 말을 언론이나 컨퍼런스 등에서 자주 들을 수 있다. 그렇다면 ‘과연 인간과 관련된 정보보호에 대한 연구는 어느 정도 수행되고 있을까?’라는 의문이 든다. 최근 정보보호 관련 연구동향 분석 결과를 보면 외부에서의 해킹공격 등 침해사고 예방 및 대응에 관한 연구가 약 40%를 차지하고 있으며, 인적보안에 대한 연구는 약 5%를 차지하고 있다[5]. 인적보안에 관한 연구의 주제는 교육 및 훈련, 인식제고, 보안서약서 징구, 입사자 및 퇴직자 관리에 대한 연구가 대부분이며, 이 결과로는 임직원이 왜 보안규정을 위반하는지, 어떠한 요인이 이러한 행동에 영향을 주는지는 판단하기 어렵다. 따라서 본 연구는 인간의 심리 및 행동과 관련된 정보보호 연구동향을 살펴보고 이에 대한 시사점과 향후 연구방향을 제시하고자 한다.

2. 이론적 배경

2.1 인간 관점에서의 정보보호

심리학에는 학습심리학, 사회심리학, 인지심리학 등 다양한 분야가 있으며, 분야에 따라 관점이 상이하지만 인간 행동의 원인을 규명하는 것이라는 공통적인 목적이 있다. 즉, 선천적인 생물학적 요인과 후천적인 환경적 요인이 다양한 심리적 요인에 영향을 주어 행동으로 연결되는 과정을 연구하는 것이다[1]. 따라서 정보보호 분야에서도 기술

적인 도구에 중점을 둔 연구도 중요하지만 조직의 정보보호 정책을 준수하는 행동에 영향을 주는 다양한 요인을 식별하고 이에 따른 대책에 대한 연구가 수행될 필요가 있다. 세계적인 시장조사 기관인 Gartner에서는 인간중심 보안(People Centric Security)이라는 새로운 패러다임을 제시하였으며, 강압적이고 예방 중심의 정보보호 통제가 아닌 임직원에 대한 신뢰를 기반으로 책임과 권한을 할당하고, 교육을 통해 정보보호 인식과 역량을 향상시키는 동시에 지속적인 모니터링을 통해 이상징후를 신속히 탐지하고 대응하는 접근방법의 중요성을 강조하고 있다[8]. 한편, 과거에 수행된 인간 관점의 정보보호 연구를 살펴보면, 태도, 의도, 인지와 같은 심리학적 요인을 정보보호 분야에 적용하는 해석적 연구부터 시작하여[3], 최근에는 심리적 요인에 따른 정보보호 정책 준수 행동에 대한 실증연구가 수행되었다[9]. 두 가지 측면의 연구들이 모두 의미가 있지만 향후 인간 관점의 정보보호 연구의 발전을 위해서는 기존의 수행된 연구들을 분석하여 통합된 관점에서 연구방향을 제시할 필요가 있다.

2.2 연구동향 분석

연구동향 분석은 일종의 메타분석(Meta Analysis)으로, 기존에 수행된 다양한 개별 연구들을 분석 및 종합하여 연구자들에게 통합된 관점의 연구동향을 제공하기 위한 연구 방법이다[2]. 분석 방법은 크게 기본 분석과 상세 분석으로 구분할 수 있으며, 기본 분석에는 분야별 논문 건수, 논문 게재 추세 등이 해당되며, 논문 주제, 연구 방법론, 교차분석 등이 상세 분석에 해당된다. 연구동향 분석을 위한 자료의 수집은 특정 저널이나 학술대회에 게재된 논문을 대상으로 하거나 연구검색을 위한 학술 데이터베이스를 활용하여 수집할 수 있다[4]. 검색 방법은 논문 제목, 요약, 키워드 등에 특정 용어를 입력하는 방법이 일반적이고, 이 때 전체 기간을 대상으로 하거나 특정 기간으로 한정지을 수 있다. 수집된 논문은 2~3명의 연구자가 검토하여 참고문헌의 기준을 인용하여 연구 주제, 방법론 등을 분석한다.

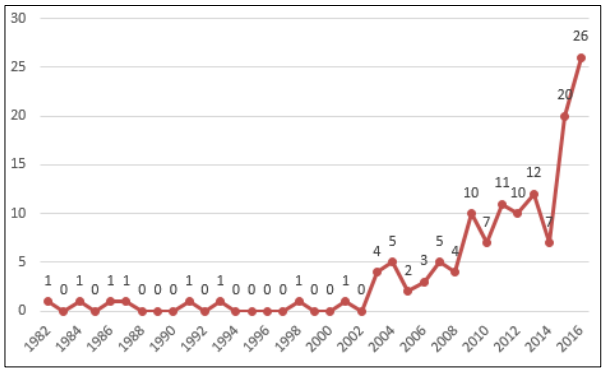
3. 연구 범위 및 방법

본 연구에서는 M.T. Dlamini 외의 연구 방법에 따라, 논문 수집을 위해 해외 4개의 저널(Computer Fraud & Security, Computers & Security, Information Management & Computer Security, IEEE Security & Privacy)을 선정하였다[6]. 선정된 저널에서 제목, 요약, 키워드에 security, human, behavior, psychology를 입력하여 인간 관점의 정보보호 연구 관련 175개의 논문을 수집하였으며, 이 중에서 행위기반 악성코드 탐지 등 인간의 행동, 심리와 관련성이 적은 논문을 제외하여 총 134개의 논문을 연구대상으로 선정하였다. 선정된 논문을 2명의 연구자가 전문을 검토하여 연구 주제와 방법론을 분류하고 교차 확인하였다. 이때 분류 기준의 객관성을 확보하기 위하여 유사분야의 분류 기준을 참고하여 분류하였다.

4. 연구동향 분석결과

4.1 연구 추세

인간 관점에서의 정보보호 연구 논문의 게재 추세를 살펴보면 (그림 1)과 같이 2000년 초반부터 연구의 수가 증가와 감소를 반복하면서 점차적으로 증가하는 추세를 보이고 있으며 2015년부터 급증하는 것을 알 수 있다.



(그림 1) 논문 게재 추세

4.2 연구 주제

연구 주제는 오세진 외의 기준에 따라 환경적 요인, 생물학적 요인, 심리적 요인, 행동적 요인의 4가지 기준으로 분류하였다[1]. 분석 결과, <표 1>과 같이 환경적 요인(58개), 행동적 요인(32개), 심리적 요인(30개), 기타(8개), 생물학적 요인(6개) 순으로 연구가 진행되었다.

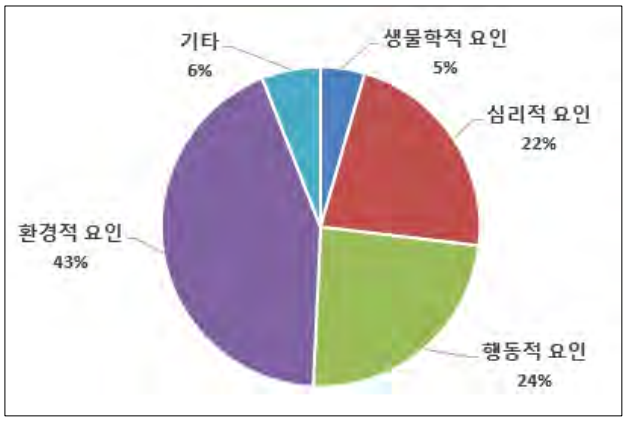
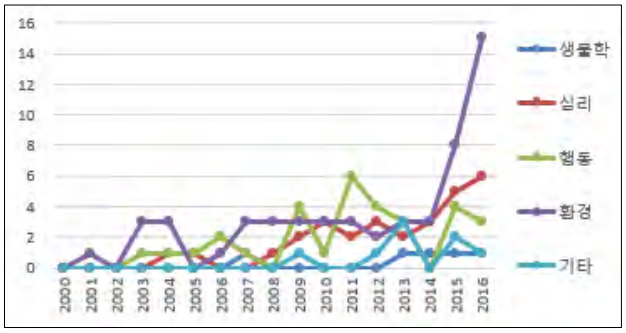


그림 2 연구 주제

환경적 요인에는 정보보호 교육, 훈련 및 인식제고, 정보보호 문화, 정보보호 투자 상벌제도에 관한 연구가 포함되며, 2000년 중반부터 사용자 친화적 보안, 스마트폰 보안정책에 대한 연구의 비중이 증가하였다. 생물학적인 요인에는 인간의 면역체계와 정보보호의 관련성을 해석하는 연구, 생체인증 방안에 관한 연구가 포함된다. 한편, 심리적 요인과 관련된 연구에는 정보보호 정책 준수 행동과 인지, 정서, 태도, 성격, 의도, 동기의 관련성을 분석한 연구가 큰 비중을 차지하고 있으며, 특히 최근에는 스마트폰 잠금 해제, 피싱 예방 및 대응방안에 대한 연구가 증가하였다. 행동적 요인과 관련된 연구에는 임직원의 실수에 의한 보안사고 감소 방안, 악의적인 행동 탐지 및 분석 방법, 행동 프로파일링이 포함된다. 끝으로 기타에는 계획된 행동이론(Theory of planned behavior), 보호동기이론(Protection motivation theory), 행동경제학 등 타 분야의 이론을 정보보호 분야에 접목한 연구가 포함된다. 이러한 연구들은 심리적 요인, 환경적 요인, 행동적 요인을 모두 적용하여 기타로 분류하였다. 또한, (그림 3)에서 알 수 있듯이 2015년도 이후 환경적 요인과 관련된 정보보호 연구가 급증하였고, 심리적 요인과 관련된 연구는 지속적으로 증가하고 있으며, 생체인증 기술의 발달에 따라 생물학적 관점의 연구가 수행되었다는 것을 알 수 있다.



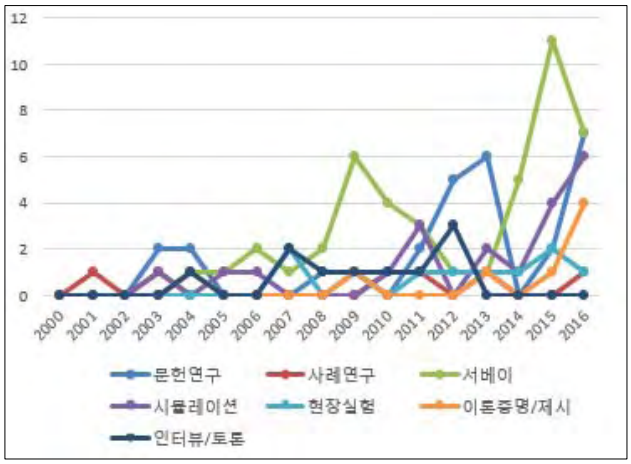
(그림 3) 연도별 연구 주제

4.3 연구 방법론

수집된 논문에서 사용된 연구 방법론을 M. Silic과 A. Back의 기준을 참고하여 분류하였으며[5], 본 연구에서는 <표 1>과 같이 7개의 연구 방법론으로 비교하였다. 분석 결과, 서베이가 가장 많이 사용되었으며, 문헌연구, 시뮬레이션, 인터뷰, 이론증명/제시, 현장실험, 사례연구 순으로 사용된 것을 알 수 있다. 또한, (그림 4)의 연도별 연구 방법론 사용 추세를 살펴보면, 서베이, 문헌연구는 사용 빈도가 증가와 감소를 반복하고 있고, 시뮬레이션이나 이론증명/제시 방법은 점증하는 것을 알 수 있다. 한편, 정성적 연구 중 인터뷰/토론의 경우 2000년 중반부터 지속적으로 사용되었으나 2012년 이후 감소추세임을 알 수 있다.

<표 1> 연구 방법론 비교

구분	연구 수	백분율(%)
서베이	45	33.58
문헌연구	30	22.39
시뮬레이션	20	14.93
인터뷰/토론	11	8.21
이론증명/제시	10	7.46
현장실험	10	7.46
사례연구	8	5.97
총계	134	100



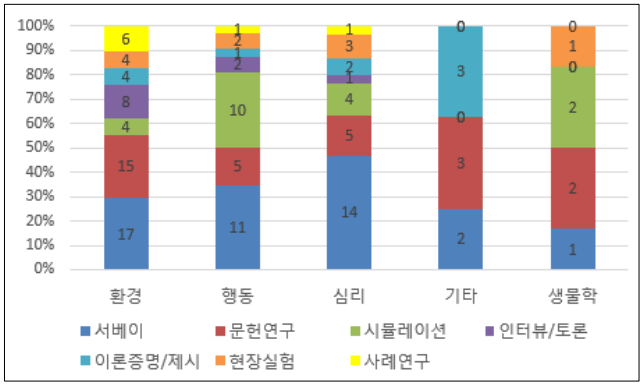
(그림 4) 연도별 연구 방법론

4.4 연구 주제와 방법론의 교차분석

인간 관련 정보보호 연구에 대한 보다 상세한 분석을 위하여 <표 2>, (그림 5)와 같이 연구 주제와 연구 방법론의 교차분석을 실시하였다. 우선, 서베이의 경우 심리, 환경, 행동적 요인과 관련된 주제의 연구에 많이 사용되었으며, 특히 정보보호 교육, 문화 등 환경적 요인에 해당되는 연구는 문헌연구, 인터뷰와 같은 정성적 방법도 높은 비중으로 사용되었다. 이상행동 탐지와 같은 행동적 요인에 대한 연구는 주로 모니터링 시스템 구현과 관련성이 높으며, 시뮬레이션 방법이 가장 많이 사용되었다. 한편, 심리학, 경제학 등에서 사용되는 이론을 정보보호 분야에 접목한 연구에서는 문헌연구, 이론증명, 서베이와 같은 방법들이 사용되었다는 점을 시사한다.

<표 2> 연구 방법론-주제 교차분석

구분	환경	행동	심리	기타	생물학	총계
서베이	17	11	14	2	1	45
문헌연구	15	5	5	3	2	30
시뮬레이션	4	10	4	0	2	20
인터뷰/토론	8	2	1	0	0	11
이론증명	4	1	2	3	0	10
현장실험	4	2	3	0	1	10
사례연구	6	1	1	0	0	8
총계	58	32	30	8	6	134



(그림 5) 연구 주제-방법론 교차분석

5. 결론

본 연구는 인간 관점의 정보보호 연구동향을 분석하기 위하여 기존에 수행된 연구들을 분석하여 향후 발전방향을 제시하고자, 해외 4개의 저널에 개제된 논문 134개를 대상으로 연구 추세, 주제, 방법론을 중심으로 정량적인 분석을 시도하였다. 인간 관점에서의 정보보호 연구는 점차 증가하는 추세이며, 연구 결과 도출된 시사점을 정리하면 첫째, 예방적 보호대책 보다는 임직원에 의한 정보유출 등 보안사고의 신속한 탐지 및 대응이 중요해짐에 따라 이상행동에 대한 탐지 및 분석 연구가 지속적으로 증가할 것으로 예상된다. 둘째, 기존의 정보보호에 대한 부정적 인식을 전환하기 위해서는 사용자의 편의성을 고려한 정보보호 접근방법에 대한 연구가 수행될 필요가 있다. 셋째, 인간의 심리와 행동을 정량적으로 분석하는 것에는 한계가 존재하므로, 임직원들의 행동을 변화시키기 위한 요인들을 식별하고 이에 필요한 정보보호 대책을 수립하기 위한 사례연구, 인터뷰 등 정성적인 연구가 수행될 필요가 있다.

끝으로 본 연구는 연구 주제를 분류하는 과정에서 연구자의 주관적인 판단이 일부 존재한다는 점, 해외 연구동향만을 분석하였다는 점, 분석 대상을 주제와 방법론으로 제한하였다는 연구의 한계가 존재한다. 하지만 종합적인 관점에서 정량적인 분석을 통해 인간 관점의 정보보호 연구 주제를 식별하고, 연구동향을 파악하였다는 의의를 가지며, 국내의 인간 관점에서의 정보보호 관련 연구 활성화에 기여할 수 있을 것이라 판단되며, 조직에서 임직원의 정책 준수에 영향을 주는 요인들을 참고하여 정보보호 정책 수립 시 활용할 수 있을 것으로 기대된다. 끝으로 서베이와 같은 정량적 연구와 사례연구 등 정성적 연구를 결합하여 심도 깊은 함의를 도출할 수 있는 통합방법 연구가 수행된다면 학계와 산업분야에 기여할 수 있을 것이라 판단된다.

참고문헌

[1] 오세진 외. “인간행동과 심리학”. 학지사. 2010.

[2] 장항배, 산업보안 연구동향 메타적 분석 연구, 한국산업보안연구학회, 2010.

[3] M.E. Thomson, R. von Solms, “Information Security Awareness Educating Your Users Effectively” Information Management & Computer Security, Vol. 6, Iss. 4, pp. 167 - 173. 1998.

[4] Mi-Hwa Kang, Tae-Sung Kim. “Research Trends in Information Security Economics: Focused on the Articles Presented at WEIS” Journal of The Korea Institute of Information Security & Cryptology, Vol. .25, No .6, pp. 1561-1570, 2015.

[5] M. Silic and A. Back, “Information Security: Critical Review and Future Directions for Research” Information Management & Computer Security, Vol. 22, Iss. 3, pp. 279-308, 2014.

[6] M.T. Dlamini, J.H.P. Eloff, and M.M. Eloff, “Information Security: The Moving Target” Computers & Security, Vol. 28, No. 3-4, pp. 189-198, 2009.

[7] R. Contu, C. Canales, and L. Pingree. “Forecast: information security worldwide 2012-2018” Gartner, G00264279, 2014.

[8] T. Scholtz. “People centric security strategy” Gartner, G00249357, 2013.

[9] T. Sommestad, H. Karlzén and J. Hallberg, “The sufficiency of the theory of planned behavior for explaining information security policy compliance” Information & Computer Security, Vol. 23 Iss. 2 pp. 200-217, 2015.