Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.33, NO.5, Oct. 2023 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2023.33.5.813

사이버로핑이 조직의 정보보호 리스크에 미치는 영향

오 현 우,[1†] 김 범 수,[2] 박 재 영[3‡]
[1]금융결제원 (팀장), [2]연세대학교 (교수), [3]NH농협금융지주 NH금융연구소 (책임연구원)

Effects of Cyberloafing on Cybersecurity Risks of Organizations: The Case of a Financial Institute

Hyunwoo Oh,[1†] Beomsoo Kim,[2] Jaeyoung Park[3‡]
[1]Korea Financial Telecommunications and Clearings Institute (Manager),
[2]Yonsei University (Professor),
[3]Finance Research Institute, Nonghyup Financial Group (Senior Researcher)

요 약

조직 구성원들은 업무 시간에 사적인 목적으로 인터넷을 종종 사용하는데, 이것을 사이버로핑(cyberloafing)이라고 한다. 특정 사이버로핑(예를 들어, 웹하드, 성인 및 도박 사이트 접속)은 악성코드 감염으로 이어질 수 있기 때문에 조직의 정보보호 리스크를 증가시킬 수 있는데, 이것은 궁극적으로 조직에 상당한 피해를 줄 수 있다. 따라서, 정보보호 측면에서, 사이버로핑의 영향을 살펴보는 것은 조직 입장에서 매우 중요하다. 국내 금융기관 직원 680명의 인터넷 필터링 시스템 로그정보 118,942건을 분석한 결과, 조직 구성원이 블랙리스트 사이트에 접속할수록 악성코드 감염 가능성이 높아지는 것으로 나타났다. 즉, 조직 구성원의 사이버로핑은 조직의 정보보호 리스크를 증가시킨다. 따라서, 조직은 조직 구성원의 인터넷 사용을 적절한 방식으로 모니터링하고 통제할 필요가 있다.

ABSTRACT

Organization members often use the Internet for non-work purposes during work hours, which is called cyberloafing. Certain types of cyberloafing (e.g., webhard, adult, and gambling sites access) can be a major cause of malware infection, which can ultimately generate significant damages to organizations. It therefore is important to examine the relationship between cyberloafing and cybersecurity risks of organizations. We analyzed log data from an internet filtering system of a financial institute and found that the more employees access to blacklist sites, the higher the possibility of malicious code infection. In other words, cyberloafing increases cybersecurity risks of organizations. We suggest that organizations need to monitor and control their members' internet use in an appropriate way.

Keywords: Cyberloafing, Cybersecurity Risks, Malware, Information Security Risks, Internet Filtering System

I. 서 론

조직은 제품 생산비용 절감, 생산주기 단축, 업무 프로세스 개선 등을 위해 인터넷을 활용하고 있으며, 인터넷은 IoT(Internet of Thing), 빅데이터 등 다양한 정보통신기술과 결합되어 혁신의 원동력이 되고 있다. 하지만, 인터넷은 조직 구성원들에게 악용될 수 있다. 예를 들어, 조직 구성원들은 업무 시간에 인터넷을 업무용 목적이 아닌 개인 이메일 송·수신, 뉴스 검색, 온라인 쇼핑, 취미 생활 등 사적인 목적으로 종종 이용한다[1, 2]. 이것을 사이버로핑

Received(07. 19. 2023), Modified(08. 30. 2023), Accepted(08. 30. 2023)
* 본 연구는 오현우의 석사학위논문을 수정 및 보완하였음
† 주저자, whati@kftc.or.kr
‡ 교신저자, inyourface33@gmail.com(Corresponding author)

(cyberloafing)이라고 하는데, 기존 연구는 조직 관점에서 사이버로핑의 부정적인 영향을 살펴보았다. 예를 들어, 사이버로핑은 직원의 업무 생산성을 하락시킨다[3]. 본 연구는 이전 연구에서 거의 다루어지지 않았던 측면을 살펴보는데, 바로 정보보호 리스크이다. 즉, 조직 구성원의 사이버로핑과 조직의 정보보호 리스크 간의 관계를 규명한다.

정보보호 리스크 중 가장 빈번하게 발생하고 위험성이 높은 유형은 악성코드(malware) 감염이다[4]. 악성코드 감염은 조직에 심각한 손실을 안긴다. 예를 들어, 2011년 농협 전산망 해킹사고는 악성코드 감염으로 은행 전산망이 마비되었으며, 약 197억 원의 피해가 발생했다. 또한, 2016년 온라인 쇼핑몰 인터파크는 악성코드 감염으로 약 2,500만 건의 고객정보가 유출되었으며, 이로 인해 약 45억 원의 과징금을 부과 받았다. 이와 같이 조직 내 일부 구성원의 컴퓨터가 악성코드에 감염될 경우 해당 피해는 악성코드에 감염된 개인뿐만 아니라 조직 전체로 확산되어 대규모 손실을 야기할 수 있다[5-7].

악성코드는 일반적으로 웹하드(webhard), 성인 웹사이트 등 정보보호가 취약한 인터넷 웹사이트 또는 불법 복제된 영화 및 음악 파일에 숨겨진 형태로 유포된다[8, 9]. 조직구성원의 사이버로핑은 악성코드가 숨겨진 웹사이트나 파일에 대한 노출을 증가시켜 악성코드 감염을 유발할 수 있으며, 이것은 궁극적으로 조직에 상당한 피해를 줄 수 있다. 따라서, 조직 구성원의 사이버로핑이 조직의 정보보호 리스크에 어떻게 영향을 주는지에 대한 이해는 조직 입장에서 매우 중요하다. 하지만, 이러한 관계를 살펴본 연구는 거의 없다.

본 연구는 국내 금융기관의 인터넷 모니터링 로그 정보를 이용하여, 조직 구성원의 사이버로핑 빈도와 사이버로핑 범위가 조직의 정보보호 리스크에 미치는 영향을 살펴본다. 또한, 업무환경 특성(직무유형, 고용형태, 그리고 단위조직 규모)에 따라 조직의 정보보호 리스크가 어떻게 달라지는지 알아본다.

II. 이론적 배경 및 문헌 연구

2.1 사이버로핑(cyberloafing)

인터넷은 초창기에는 주로 군사, 학술 및 기업의 업무 목적을 위해 발전되고 사용되었으나, 최근에는 개인의 취미 활동, 사회적 관계 유지 등 개인적인 목적을 위해서도 활발하게 이용되고 있다. 이와 같이 인터넷의 업무 목적과 개인 목적의 중복된 특성으로 인해 일부 직원들은 업무 시간 중에 기업의 인터넷 자원을 사적인 목적으로 종종 이용하고 있으며, 이것을 사이버로핑이라고 한다[1, 2].

사이버로핑은 마이너 사이버로핑과 메이저 사이버로핑으로 구분된다[10]. 전자는 개인 이메일 송·수신, 뉴스 검색, 금융 거래, 온라인 쇼핑 등 비교적 심각성이 낮은 사이버로핑을 말하며, 후자는 성인 웹사이트 접속, 불법 복제된 영화 및 음악 파일 다운로드 등 다소 심각한 사이버로핑을 의미한다.

조직 구성원의 인터넷 오남용은 대리인 이론(agency theory)으로 설명될 수 있다. 대리인 이론에 따르면, 고용주와 고용인은 계약서를 통해 고용관계가 성립되지만, 불확실한 미래상황에 대한 정보의 불일치로 인해, 고용주는 고용인의 능력 및 성과를 완벽하게 감시할 수 없고, 고용인은 기대치와 다른 업무 또는 보상으로 인해 일탈 행동, 예를 들어, 사이버로핑을 하게 된다[11, 12].

사이버로핑의 선행요인을 살펴본 연구에 따르면, 업무 동기, 업무에 대한 만족도 및 조직의 정책에 대한 만족도가 사이버로핑과 관련이 있다[13-15]. Vitak et al. [16]은 인구통계학적 조사를 통해 직장에서 젊은 남성들이 개인적인 목적으로 인터넷을 더 많이 사용한다는 것을 밝혔다. Garrett and Danziger [17]는 직장에서의 일상화된 인터넷 사용과 인터넷의 효용성에 대한 인식이 조직구성원의 사이버로핑을 유발한다고 하였다. 한편, De Lara et al. [18]는 조직 내 관리자에 대한 물리적 근접성이 조직 통제에 대한 인식과 처벌에 대한 두려움을 증가시키고, 결과적으로 사이버로핑이 감소된다고 하였다. Wang et al. [19]는 개인 목적의 인터넷 사용 행동을 주변의 동료가 쉽게 볼 수 있다고 느낄 때 사이버로핑이 감소한다는 것을 밝혔다.

사이버로핑의 영향을 살펴본 연구를 보면, 사이버로핑은 조직 구성원의 업무 생산성 저하, 기업의 네트워크 자원 소모, 법적 문제 야기 등 조직 전반에 부정적인 영향을 준다[7, 20-23]. 이에 많은 기업들은 인터넷의 적절한 사용을 유도하기 위해 다양한 시도를 하고 있다[19]. 예를 들어, 기업들은 구성원들의 사이버로핑을 효과적으로 감시하기 위해 모니터링 시스템을 구축하여 활용하고 있다[24]. 또한, 기업들은 사이버로핑 모니터링 결과와 이에 따른 공식적 또는 비공식적인 제재를 결합하여 구성원들의 사이버

로핑을 억제하기 위해 노력하고 있다[25, 26].

2.2 사이버로핑과 정보보호 리스크

2019년에 발간된 세계경제포럼(WEF) 보고서에 따르면, 각 국가별 사업가를 대상으로 향후 10년 내 사업 활동에서 예상되는 기업을 위협하는 리스크에 대해 설문조사한 결과, 선진국이 다수 포함된 북미·유럽지역의 사업가들은 정보보호(사이버보안) 리스크를 향후 예상되는 최대의 리스크로 선정하였다. 이처럼 정보보호 리스크는 기업의 흥망성쇠를 가르는 중요한 열쇠 중의 하나라고 볼 수 있으며, 최근 기업에서 가장 빈번하게 발생하는 정보보호 위협은 일부 구성원의 컴퓨터를 악성코드에 감염시킨 후 이를 이용하여 기업의 중요 정보 유출, 시스템 파괴 등을 일삼는 형태이다[27].

악성코드는 악의적인 목적을 가진 공격자가 정보시스템 및 네트워크에 대한 공격을 단순화 또는 자동화하여, 개인 또는 기업의 데이터와 암호를 획득하거나, 정보시스템의 하드웨어와 소프트웨어를 손상시키는데 사용되는 소프트웨어의 일종이다[4, 28]. 악성코드에 감염된 경우 시스템의 오류나 운영체제의 충돌과 같은 일반적인 컴퓨터 문제가 발생한 것처럼 보이기 때문에 기업 및 개인은 악성코드 감염을 인지하는데 어려움을 겪는다[29]. 이로 인해 조직 내 구성원의 일부가 악성코드에 감염되는 경우 악성코드 치료에 소요되는 시간으로 인한 업무 생산성 저하, 정보시스템의 기능 손실 등으로 인해 불가피한 비용이 발생되고, 정보시스템 내에 보관된 정보의 유출 등 악성코드 감염으로 인한 피해가 확산될 수 있다[30].

악의적인 해커는 웹하드, 성인 및 도박 웹사이트 등 정보보호가 취약한 웹사이트에 악성코드를 숨겨놓거나, 악성코드가 첨부된 대량의 전자메일을 발송하는 방식으로 악성코드를 유포한다[8, 9]. 이와 같은 악성코드의 유포방식으로 인해 인터넷에 연결된 모든 정보시스템은 악성코드 감염의 대상이 될 수 있으며, 해커들은 물리적 공간의 제약 없이 세계 어느 곳에서나 잠재적인 피해자를 대상으로 악성코드를 유포하고 감염시키는 것이 가능하다[31, 32]. 즉, 악성코드 감염은 악성코드를 만든 해커와의 물리적 거리가 아닌 피해자들이 악성코드가 숨겨진 웹사이트 또는 파일에 얼마나 노출되고 근접했는지 여부에 따라 결정된다[4]. 인터넷 사용자가 정보보호 수준이 낮은 웹사이트를 통해 불법 소프트웨어 등을 다운로드하는 경우 그곳에 숨겨진 악성코드에 대한 노출이 증가될 수 있기 때문에 해커는 특정 웹사이트나 파일에 가능한 오랫동안 악성코드를 숨겨놓는 것만으로도 인터넷 사용자의 악성코드 감염을 유발할 수 있다[5, 33].

악성코드 감염을 예방하기 위한 보호수단은 물리적 보호수단(physical guardianship)과 개인적 보호수단(personal guardianship)으로 구분된다[4]. 물리적 보호수단은 침입차단시스템(firewall), 침입탐지시스템(intrusion detection system), 안티바이러스 소프트웨어(anti-virus software) 등과 같은 정보보호시스템을 구축하고 운영하는 것이다. 물리적 보호수단이 미흡한 경우 개인 또는 조직 구성원의 컴퓨터는 악성코드에 감염될 위험이 높아진다. 기업들은 악성코드 감염을 예방하기 위해 침입차단시스템, 안티바이러스 소프트웨어 등과 같은 정보보호시스템에 의존하고 있다[34, 35]. 하지만, 2011년 농협 전산망 해킹 사고와 2016년 인터파크 개인정보 유출 사고에서 볼 수 있듯이, 기술적 수단만으로 악성코드에 대응하기에는 한계가 있다. 이에 각 기업들은 정보보호 인식교육, 훈련, 처벌, 보상 등 다양한 관리적 수단을 바탕으로 조직의 정보보호 리스크를 낮추기 위해 노력하고 있다[4, 36].

개인적 보호수단은 악성코드 감염과 같은 사이버 공격의 피해를 예방하기 위한 개인별 컴퓨터 기술로 정의되며 관련 지식과 기술을 보유한 개인은 그렇지 않은 경우에 비해 악성코드의 감염 경로 등을 인식하고 적절한 컴퓨터 기술을 이용함으로써 악성코드 감염을 예방할 수 있다. 기존 연구에 따르면, 개인적 특성과 악성코드 감염 간에 밀접한 관련이 있다. 예를 들어, 인터넷에서 여가 활동을 즐기는 시간이 길수록 피싱(phishing), 악성코드 감염 등의 사이버 공격의 피해를 입을 가능성이 높다[37]. Hinduja and Patchin [38]는 초고속 인터넷을 이용하는 사람은 그렇지 않은 경우에 비해 컴퓨터 파일을 더 빈번하고 빠르게 공유할 수 있으므로 악성코드 감염 위험이 더 높다고 주장하였다. 악성코드 감염에 있어서 개인의 정보보호 인식이 중요한 역할을 하는 것으로 나타났는데, 정보보호 인식이 낮은 개인은 그렇지 않은 경우에 비해 안전하지 않은 정보보호 행동을 하므로 악성코드 감염 위험성이 더 높다[10].

일부 연구에서 온라인 행동과 사이버 피해 간의 관계를 살펴보았다. Bossler and Holt [4]는 대학생들이 온라인에서 일탈 행동을 할수록 악성코드 희

생자가 될 가능성이 높다고 하였다. 비슷하게, Choi [5]도 대학생들의 온라인 행동과 사이버 범죄 피해와 밀접한 관련이 있다고 하였다. 하지만, 조직 관점에서 조직 구성원의 온라인 행동이 조직의 정보보호 리스크에 어떠한 영향을 주는지 살펴본 연구가 부족하다. 따라서, 본 연구는 조직 구성원들이 인터넷을 사적으로 사용하는 행동(즉 사이버로핑)이 그들의 악성코드 감염 가능성(즉 조직의 정보보호 리스크)을 높이는지 밝히고자 한다.

III. 연구가설

악의적 해커는 취약한 웹사이트 또는 불법으로 복제된 음악이나 영화파일 등에 악성코드를 숨기고 인터넷 사용자들에게 최대한 장시간 동안 악성코드를 노출하는 방식으로 악성코드를 유포한다[39]. 따라서, 인터넷 사용자들의 악성코드 감염 가능성은 악성코드가 숨겨진 웹사이트 또는 파일에 대한 근접성 및 노출 빈도에 따라 영향을 받는다[4, 28, 29]. 특히, 웹사이트가 보안에 취약할수록 악성코드 감염될 가능성이 높아진다[5, 7].

따라서, 보안에 취약한 웹사이트(예를 들어, 성인 및 도박 웹사이트)에 자주 접속하는 조직 구성원은 악성코드 감염 위험에 노출되고, 실제로 악성코드 감염으로 이어질 수 있다. 또한, 접속하는 웹사이트의 종류가 다양할수록 악성코드 감염 가능성은 높아질 것이다. 이에 아래와 같은 가설을 설정한다.

가설 1. 조직구성원의 메이저 사이버로핑 빈도와 조직의 정보보호 리스크는 긍정적인 관련이 있을 것이다.

가설 2. 조직구성원의 메이저 사이버로핑 범위와 조직의 정보보호 리스크는 긍정적인 관련이 있을 것이다.

개인 또는 조직의 구성원은 악성코드의 감염 경로 및 조치 방법 등을 인식하고 이에 따라 적절한 컴퓨터 기술을 활용하여 악성코드 감염을 막을 수 있다. 악성코드 감염을 예방하기 위한 컴퓨터 지식 및 기술은 출처가 불분명한 이메일을 열어보지 않거나, 웹사이트에서 수상한 파일을 다운로드 받지 않는 것을 말한다. 또한, 복잡한 패스워드 설정 및 주기적인 변경, 컴퓨터 운영체제의 업데이트 등의 행동을 의미한다[39]. 컴퓨터 지식 및 기술이 부족하다면, 악성코드에 감염될 가능성이 높아질 수 있다.

직무유형을 크게 IT직무와 비IT직무로 나눌 수 있다. 비IT직무를 수행하는 구성원은 소프트웨어 개발, 정보시스템 구축·운영, 정보보호 등 IT직무를 수행하는 구성원에 비해 일반적으로 컴퓨터 지식 및 관련 기술이 부족하다. 따라서, 조직의 직무유형과 조직의 정보보호 리스크와 관련이 있을 것으로 예상할 수 있다. 즉, 비IT직무인 경우에 악성코드 감염 가능성이 더 높을 것이다. 이에 본 연구는 다음과 같은 가설을 세운다.

가설 3. 조직구성원의 직무유형과 조직의 정보보호 리스크는 관련이 있을 것이다. 구체적으로, IT직무와 비교하여, 비IT직무를 담당하는 조직구성원이 조직의 정보보호 리스크를 더 높일 것이다.

김보라 등[40]에 따르면, 각 조직은 구성원들의 다양한 정보보호 인식 수준을 고려하여 조직의 목표, 구성원의 책무 등이 포함된 정보보호 정책을 수립하고 모든 구성원들이 해당 정책을 준수하도록 함으로써 조직의 정보보호 리스크를 줄이기 위해 노력하고 있다. 이에 반해 정보보호 정책은 조직의 안전을 보장하기 위해 중요한 요소 중의 하나이지만, 정보보호 정책을 수립하여 시행하는 것이 모든 구성원들이 해당 정책을 준수할 것이라는 것을 보장하지 않는다[41, 42]. 이정하와 이상용[43]에 따르면, 정보보호 정책에 대한 이해와 지식이 부족한 조직 구성원은 해당 정책을 준수하지 않게 되고, 이로 인해 정보보호와 관련하여 안전하지 않은 행동을 하게 된다. 이것은 결과적으로 조직에 해를 가할 수 있다.

고용형태는 일반적으로 내부 직원과 외주용역직원으로 구분된다. 외주용역(outsourcing)은 외부의 자원이라는 사전적 의미를 지니며, 일반적으로 비용절감 등을 목적으로 타 회사의 직원이 기업의 일부 업무를 수행한다[44]. 기업들은 정보보호 교육 및 훈련 등을 통해 외주용역직원을 포함한 전체 구성원의 정보보호 정책에 대한 이해와 인식을 제고하기 위해 노력하고 있다[45]. 하지만, 그럼에도 외주용역직원은 여전히 조직의 정보보호에 위협을 가할 수 있는 요인 중 하나로 지목된다. 외주용역직원은 정보보호 교육 및 훈련의 기회가 내부직원에 비해 상대적으로 부족하고, 이에 따라 조직의 정보보안 정책에 대한 인식이 내부직원에 비해 미흡하기 때문이다. 따라

서, 외주용역직원은 내부직원보다 악성코드에 감염될 가능성이 높다고 할 수 있다. 이에 본 연구는 다음과 같은 가설을 설정한다.

가설 4. 조직구성원의 고용형태와 조직의 정보보호 리스크는 관련이 있을 것이다. 구체적으로, 내부직원과 비교하여, 외주용역직원이 조직의 정보보호 리스크를 더 높일 것이다.

Alnuaimi et al. [46]에 따르면, 조직 내 단위조직은 개별 구성원의 특성을 넘어서는 고유한 특징을 가지고 있다. 특히, 단위조직의 크기는 일부 사회현상을 설명하기 위한 요인으로 종종 사용된다. 크기가 큰 단위조직은 작은 단위조직에 비해 감독과 통제가 어렵고, 구성원 간 원활하지 않은 의사소통 등으로 인해 구성원의 직무만족도가 상대적으로 낮다[47]. 강현[48]은 낮은 직무만족도는 조직 구성원의 정보보호 정책 준수의도에 부정적인 영향을 미치므로 단위조직의 크기가 클수록 구성원의 준수의도는 낮아진다고 주장하였다. 즉, 규모가 클수록 조직의 정보보호 리스크가 높아질 수 있다. 따라서 본 연구는 아래와 같은 가설을 설정한다.

가설 5-1. 단위조직의 규모는 조직의 정보보호 리스크와 긍정적인 관련이 있을 것이다.

한편, 조직 차원의 감시와 통제보다는 강제성은 없더라도, 구성원의 사회관계에 영향을 주는 주변 동료의 비난 등의 비공식적 제재가 오히려 구성원의 정보보호정책 준수의도에 긍정적 영향을 줄 수 있다[49]. 따라서, 부서에 동료가 많을수록 악성코드에 감염될 가능성이 낮아질 것이다. 이에 본 연구는 다음과 같은 가설을 세운다.

가설 5-2. 단위조직의 규모는 조직의 정보보호 리스크와 부정적인 관련이 있을 것이다.

본 연구의 연구모형은 아래 Fig. 1.과 같다.

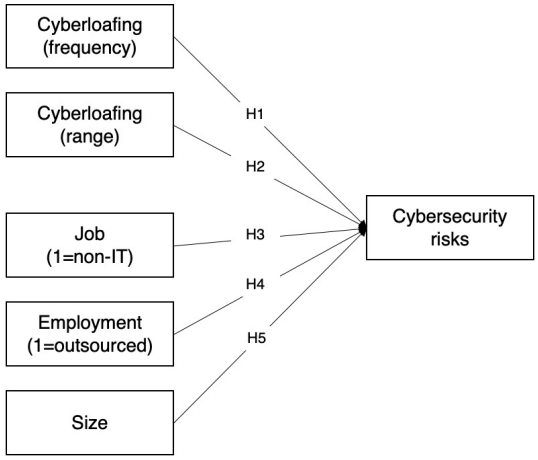

Fig. 1. Research model

IV. 연구방법

4.1 조작적 정의

본 연구는 국내 금융IT를 대표하는 금융기관의 인터넷 필터링 시스템 로그 데이터를 활용한다. 인터넷 필터링 시스템은 기업의 인터넷 통신 데이터를 실시간 분석하여 직원들의 부적절한 인터넷 사용을 모니터링하는 시스템이다[12]. 인터넷 필터링 시스템은 사이버로핑, 악성코드 유포 웹사이트 등 모니터링이 필요한 웹사이트 목록을 사전에 블랙리스트 목록으로 관리하며, 직원들이 블랙리스트 목록에 포함된 웹사이트에 접속 시 해당 접속을 차단한다. 연구대상 기관은 인터넷 필터링 시스템을 자체적으로 구축하여 운영하고 있으며, 직원들의 개인 이메일 송수신, 뉴스 검색, 인터넷 쇼핑몰 이용 등의 마이너 사이버로핑은 모니터링하지 않고, 이보다는 사안이 심각한 메이저 사이버로핑과 악성코드 유포 웹사이트 접속에 대해서만 모니터링을 실시하고 있다. 해당 기업의 구성원들이 직장 내에서 메이저 사이버로핑 관련 웹사이트나 악성코드 유포 웹사이트에 접속하려는 경우, 인터넷 필터링 시스템은 해당 웹사이트에 대한 접속을 실시간으로 자동 차단하고, 해당 웹사이트에 대한 접속이 차단되었음을 별도의 로그정보를 통해 기록을 남기고 있다.

본 연구의 종속변수인 조직의 정보보호 리스크는 연속형 변수로 조직 구성원이 악성코드에 감염될 가능성으로 정의되며, 본 연구에서는 인터넷 필터링 시스템에 의해 차단된 악성코드 유포 웹사이트 접속 건

수로 측정하였다. 차단된 악성코드 유포 웹사이트 수가 많을수록 악성코드 감염될 가능성이 올라가는데, 이것은 조직의 정보보호 리스크가 높아짐을 의미한다.

독립변수 사이버로핑 빈도는 연속형 변수로 조직 구성원이 메이저 사이버로핑과 관련된 웹사이트에 접속한 빈도로 정의되며, 본 연구에서는 인터넷 필터링 시스템에 차단된 메이저 사이버로핑 웹사이트 접속 건수로 측정하였다. 차단된 건수가 많을수록 해당 구성원은 메이저 사이버로핑 행동을 자주 하고 있음을 말한다.

독립변수 사이버로핑 범위는 연속형 변수로 게임, 웹하드, 음란물, 도박 등 해당 기관이 구분한 9개의 메이저 사이버로핑 유형 중 조직 구성원이 몇 개 유형의 웹사이트에 접속했는지로 정의되며, 본 연구에서는 인터넷 필터링 시스템에 차단된 메이저 사이버로핑 웹사이트의 유형수로 측정하였다. 차단된 메이저 사이버로핑 유형의 수가 많을수록 조직 구성원은 다양한 메이저 사이버로핑 웹사이트에 접속하고 있음을 의미한다.

독립변수 직무유형은 명목변수로 IT직무와 비IT직무로 구분된다. IT직무는 IT에 대한 지식과 기술을 기반으로 업무를 수행하는 직무의 유형으로 IT기획을 담당하는 IT기획부서, 소프트웨어 개발 및 유지보수를 담당하는 IT개발부서, 정보시스템을 구축 및 운영하는 IT운영부서, 정보보호업무를 수행하는 정보보호부서를 포함한다. 비IT직무는 업무 수행 시 IT에 대한 지식과 기술이 직접적으로 필요하지 않은 직무유형으로 사업을 기획, 추진, 관리하는 사업부서와 인사관리, 회계관리, 시설관리 등을 수행하는 지원부서를 포함한다.

독립변수 고용형태는 명목변수로 내부직원과 외주용역직원으로 구분된다. 연구대상 기관은 업무의 대부분을 기업이 자체적으로 고용한 내부직원이 수행하고 있으나, 시스템 유지·보수, 전기 및 소방설비 등 건물관리, 청소관리 등 일부 업무는 외부의 별도 용역회사와의 계약을 통해 외부에서 파견된 외주용역직원이 수행하고 있다.

단위조직 규모는 단위조직의 전체 인원수로 정의되며, 본 연구에서는 기업 내 내벽, 파티션 등 물리적으로 구분된 독립 공간에서 업무를 같이 수행하는 인원수로 측정한다.

본 연구에서 사용한 변수에 대한 조작적 정의와 측정방식을 부록에 정리하였다.

4.2 데이터 수집

본 연구는 금융IT를 주 업무로 하는 국내 금융기관의 인터넷 필터링 시스템 로그정보와 임직원 정보를 이용하였다. 해당 기관은 금융기관들의 공동 서비스를 기획, 개발 및 운용하는 업무를 수행함으로써 타 업종에 비해 높은 정보보호 수준이 요구되는 금융업종의 특성이 있으며, 동시에 IT직무를 수행하는 인력이 전체 조직의 40% 이상을 차지하고 있어 일반적인 IT 업종의 특성도 가지고 있다.

연구에 사용된 데이터는 개인정보 비식별 조치 가이드라인을 바탕으로 이름, IP정보 등 개인을 구분할 수 있는 정보가 비식별화 되었다. 즉, 임직원 식별이 불가능하다. 또한, 관련 업무 책임자의 승인 등 해당 기관의 외부 정보제공 절차를 준수하였다.

해당 기관은 인터넷 필터링 시스템을 이용하여 전체 임직원 708명의 직장 내 인터넷 사용을 모니터링하고 있으며, 본 연구는 2019년 2월 1일부터 7월 31일까지(6개월)의 로그정보가 사용되었다. 구체적으로, 총 로그정보는 128,541건이고, 이 중에서 메이저 사이버로핑 차단로그는 71,652건, 악성코드 유포 웹사이트 차단로그는 56,979건이다.

전체 708명의 임직원 중 임원과 업무상 목적으로 사이버로핑 및 악성코드 유포 웹사이트에 상시 접속하는 정보보호업무 관련 직원 등 총 28명을 분석 대상에서 제외하였다. 최종적으로 직원 680명의 인터넷 필터링 시스템 로그정보 118,942건을 대상으로 분석을 수행하였다. 메이저 사이버로핑 차단로그는 63,345건이고 악성코드 유포 웹사이트 차단로그는 55,597건이다. 해당 로그정보는 직원별로 취합하여 680건의 익명정보로 변환 후 분석에 이용하였으며, 해당 익명정보는 직원별 임시ID, 성별, 관리자 여부, 직무유형, 고용형태, 단위조직 규모, 메이저 사이버로핑 접속차단 건수, 차단된 메이저 사이버로핑 유형 건수, 악성코드 유포 웹사이트 접속차단 건수로 구성되어 있다.

V. 데이터 분석 및 결과

Table 1.에서 보는 바와 같이, 남성은 482명(70.9%), 여성은 198명(29.1%)으로 남성이 다소 많은 편이고, 일반직원이 563명(82.8%), 관리자가 117명(17.2%)으로 일반직원이 관리자에 비해 상대적으로 많다. 직무유형을 보면, 비IT직무가 392명

Table 1. Demographic characteristics (n=680)

		sample(%)	cyberloafing mean
Gender	Male	482(70.9)	117.67
	Female	198(29.1)	33.48
Position	Staff	563(82.8)	69.50
	Manager	117(17.2)	98.07
Job	IT	288(42.4)	126.68
	non-IT	392(57.6)	68.52
Employment	Outsourced	39(5.7)	360.00
	Internal	641(94.3)	76.92

(57.6%), IT직무가 288명(42.4%)으로 비슷한 분포를 보였다. 고용형태의 경우, 내부직원이 641명(94.3%), 외주직원이 39명(5.7%)으로 내부직원이 많은 편이다.

또한, 인구통계정보에 따른 메이저 사이버로핑 현황을 Table 1.에 제시하였다. 예를 들어, 로그정보 수집기간 6개월 동안 남성 직원의 평균 사이버로핑 빈도는 117.67건으로 여성 직원의 33.48건보다 더 많다.

수집한 인터넷 필터링 시스템 로그정보에 대한 기술통계량은 부록에 수록하였다.

5.1 가설 검정

가설 검정에 앞서 회귀분석의 기본 가정인 잔차의 독립성, 정규성, 등분산성, 선형성을 확인하였고, 연구변수 간의 다중공선성 확인을 위해 상관관계 분석을 실시하였다. Table 2.에서 볼 수 있듯이, 대부분의 변수는 절대값이 0.6 이하로 적절한 상관관계를 보여 주었으나, 사이버로핑 빈도와 범위 간 상관계수의 절대값이 0.6을 초과하여 다중공선성 진단을 추가적으로 실시하였다. 모든 요인에 대해 분상팽창지수(VIF)가 10 미만으로 다중공선성에 문제가 없는 것을 확인하였다.

조직 구성원의 메이저 사이버로핑 및 업무환경 요인이 조직의 정보보호 리스크에 미치는 영향을 알아보기 위해 다중회귀분석을 실시하였다. Table 3.에서 보는 바와 같이, 회귀모형이 적합하다고 할 수 있으며, (F=36.113, p<.001), 모형의 설명력은 26.6%이다.

다중회귀분석 결과를 보면, 메이저 사이버로핑 빈도와 메이저 사이버로핑 범위 모두 조직의 정보보호 리스크와 긍정적으로 관련이 있다(β=.149, t=3.806, p<.001; β=.248, t=4.353, p<.001). 즉, 사이버로핑 관련 웹사이트 접속 건수가 많아질수록 악성코드 유포 웹사이트 접속 건수가 많아졌다. 또한, 접속하는 메이저 사이버로핑 웹사이트 유형이 다양해질수록 악성코드 유포 웹사이트 접속 건수가 많아졌다. 즉, 메이저 사이버로핑 빈도와 범위가 증가할수록 악성코드 감염 가능성이 높아진다는 것이다. 따라서, 가설 1과 2는 모두 채택되었다.

업무환경 특성 중 하나인 조직 구성원의 직무유형과 조직의 정보보호 리스크 간의 관계는 우리의 예상대로 부정적인 관계이지만, 통계적으로 유의하지 않다. 따라서, 가설 3은 채택되지 못하였다.

업무환경 요인 중 다른 하나인 조직 구성원의 고

Table 2. Results of correlation analysis

	1	2	3	4	5	6	7	8	VIF(<10)
1	1								-
2	.486**	1							3.547
3	.492**	.844**	1						3.553
4	-.148**	-.250**	-.256**	1					1.150
5	.166**	.204**	.220**	-.070	1				1.109
6	-.087*	-.047	-.024	-.217**	.188**	1			1.343
7	.131**	.246**	.233**	-.078*	.075	-.296**	1		1.211
8	-.077*	-.024	-.039	-.091*	.096*	.362**	-.224**	1	1.178

Note. 1. Cybersecurity risks, 2. Cyberloafing(frequency), 3. Cyberloafing(range), 4. Job, 5. Employment, 6. Size, 7. Gender, 8. Position.
*: p<.05, **: p<.01.

Table 3. Results of multiple linear regression analysis

Variable	Coefficient	t-value
Cyberloafing (frequency)	.149	3.806***
Cyberloafing (range)	.248	4.353***
Job (1=non-IT)	-.103	-1.150
Employment (1=outsourced)	.431	2.299**
Size	-.164	-2.262**
F=36.113***, adjusted-R^2=.266		
**: p<.01, ***: p<.001.		

용형태는 조직의 정보보호 리스크와 긍정적으로 관련이 있다(β=.431, t=2.299, p<.01). 우리의 예상대로, 외주용역직원이 내부직원에 비해 악성코드 유포 웹사이트 접속 건수가 더 많다. 즉 악성코드 감염 가능성이 더 높다. 따라서, 가설 4는 채택되었다.

또한, 업무환경 요인 중 마지막 하나인 단위조직의 크기는 조직의 정보보호 리스크와 부정적인 관련이 있다(β=-.164, t=-2.262, p<.01). 우리가 예상한대로, 부서 규모가 커질수록 악성코드 유포 웹사이트 접속 건수가 작아진다. 즉 부서에 사람이 많을수록 해당 부서원의 악성코드 감염 가능성이 낮다. 따라서, 가설 5는 채택되었다.

VI. 결 론

6.1 연구결과 논의

본 연구는 금융기관의 인터넷 필터링 시스템 로그 데이터를 활용하여 조직 구성원의 사이버로핑 및 업무환경 특성이 조직의 정보보호 리스크에 미치는 영향을 살펴보았다. 분석결과는 다음과 같다.

첫째, 조직 구성원이 메이저 사이버로핑에 많은 시간을 소비하고 다양한 유형의 메이저 사이버로핑 관련 웹사이트에 접속할수록 악성코드 유포 웹사이트 접속할 가능성이 높아지는데, 이것은 악성코드에 감염될 가능성이 높아진다는 것을 의미한다. 이와 같은 결과는 메이저 사이버로핑과 관련된 웹사이트는 정보보호가 취약하여 해커가 악성코드를 심을 가능성이 높다는 Taylor et al. [39]의 연구와 일치한다. 또한, 악성코드가 숨겨진 웹사이트 및 파일에 대한 근접성 및 노출 빈도가 악성코드 감염에 영향을 준다는 Bossler and Holt [4]의 연구결과와도 일치한다.

둘째, 조직 구성원의 고용형태가 조직의 정보보호 리스크에 영향을 주는 것으로 나타났다. 분석결과, 외주용역직원이 내부직원에 비해 악성코드 유포 웹사이트 접속 건수가 더 많은데, 이것은 외주직원의 악성코드 감염 가능성이 더 높다는 것을 의미한다. 따라서, 외주직원이 조직의 정보보호 리스크를 증가시킬 수 있는 요인이라고 할 수 있다. 즉, 구성원의 고용형태에 따라 정보보호정책에 대한 이해와 인식이 달라지며, 이것이 결과적으로 정보보호정책 준수에 부정적인 영향을 주는 것이다[43].

셋째, 단위조직의 크기가 큰 경우에 악성코드 유포 웹사이트 접속건수가 더 낮은 것으로 나타났다. 즉, 부서에 구성원이 많을수록 정보보호 리스크가 감소한다고 볼 수 있다. 위의 가설 5 개발에서 보았듯이, 단위조직의 크기가 조직의 정보보호 수준에 미치는 영향은 다소 혼재되어 있는데, 우리의 연구결과는 이 관계가 부정적임을 말한다. 이것은 해당 기관의 정책(즉 정보보호 정책 준수를 부서 성과와 연동) 때문인 것으로 보인다. 해당 기관은 전 직원 대상으로 정보보호 점검을 정기적으로 실시한다. 구체적으로, 안티바이러스 소프트웨어 업데이트, 운영체제 패스워드 변경 등 조직 구성원의 정보보호 정책 준수 여부를 주기적으로 점검하고, 이에 대한 평가결과를 단위조직의 성과평가에 반영한다. 이러한 정책으로 인해, 만약 어느 한 구성원이 정보보호 정책을 준수하지 않을 경우(예를 들어, 웹사이트 차단 건수가 많아지는 경우) 그 구성원이 속한 단위조직의 성과평가는 낮아지고 다른 구성원들은 정책을 위반한 구성원을 비난할 것이다. 따라서, 구성원들은 인터넷을 사용하는데 있어서 서로 조심하게 된다. 이는 조직 차원의 통제보다 구성원 간의 상호 자율적인 감시가 조직구성원의 정보보호 정책 준수의도에 긍정적 영향을 준다는 기존 연구결과와 일치한다[49]. 다만, 우리가 살펴본 기관과 다른 정책 환경에서는 우리의 연구결과와 다른 결과가 나올 수 있음을 유의해야 한다.

마지막으로, 조직 구성원의 직무유형은 조직의 정보보호 리스크에 유의한 영향을 주지 않았다. 개인의 컴퓨터 지식 및 기술이 악성코드 감염을 예방하기 위한 중요한 수단이라고 인식되고 있지만, 최근 대부분의 기업들은 조직의 정보보호 리스크 관리를 강화하기 위해 구성원들을 대상으로 주기적인 정보보호 교육, 훈련 등을 실시함에 따라 직무유형과 무관하게

구성원들의 정보보호에 대한 인식 및 준수의도가 높아졌기 때문에 이러한 결과가 나온 것으로 보인다.

6.2 시사점

본 연구는 다음과 같이 학술적으로 기여한다. 첫째, 본 연구는 기존 연구와 다르게 금융기관의 로그정보를 사용했다. 이전 연구들은 주로 설문조사를 통해 조직 구성원의 사이버로핑 의도와 악성코드 감염 위험 등을 살펴보았는데, 이것은 주관적 자기보고라는 방법론적 한계점을 가진다. 설문응답과 실제 행동은 서로 다를 수 있기 때문이다. 본 연구는 조직 구성원의 사이버로핑 및 악성코드 유포 웹페이지 접속과 관련된 로그정보를 이용하여 조직 구성원의 실제 행동을 살펴보았다. 따라서, 기존 연구와 비교하여 높은 외적 타당성을 가진다.

둘째, 본 연구는 조직의 정보보호 리스크에 영향을 미치는 요인으로, 기존 연구에서 거의 다루어지지 않았던 사이버로핑을 고려하였다. 대부분의 선행 연구는 사이버로핑의 결과(consequence)로 주로 조직의 업무 생산성에 초점을 맞추었다[20, 21]. 하지만 사이버로핑은 조직의 다른 측면에도 영향을 줄 수 있다. 이에 본 연구는 조직 구성원의 사이버로핑과 조직의 정보보호 리스크 간의 관계를 규명하고자 하였으며, 금융기관의 로그정보를 활용하여 사이버로핑이 조직에 부정적인 영향을 준다는 것을 밝혔다. 본 연구는 이전 연구를 확장하여 새로운 영역을 개척했다는 점에서 학술적으로 공헌한다. 앞으로 사이버로핑의 영향을 정보보안 측면에서 다루는 연구가 활발해지기를 기대한다.

본 연구의 결과는 또한 다음과 같은 실무적 시사점을 제공한다. 첫째, 본 연구는 조직 구성원의 메이저 사이버로핑이 조직의 정보보호 리스크를 높일 수 있음을 보였다. 즉, 조직 구성원이 업무 시간에 특정 웹사이트에 접속할수록 악성코드 감염 가능성이 높아진다는 것을 확인했다. 따라서, 조직은 조직 구성원의 인터넷 사용(특히, 메이저 사이버로핑)을 모니터링하고 통제할 필요가 있다. 구체적으로, 메이저 사이버로핑은 개인의 악성코드 감염을 유발하는데, 이것은 조직을 위험에 빠지게 할 수 있으므로 정보보호 교육 등을 통해 조직의 구성원들에게 사이버로핑의 부정적 효과와 파급효과 등을 인식시킬 필요가 있다. 또한, 조직은 구성원들의 사이버로핑을 억제하기 위해 관련 모니터링을 적극적으로 실시하고 이에 따른 적절한 처벌 및 보상 체계를 마련하는 것을 검토할 필요가 있다.

둘째, 본 연구는 업무환경 특성 중 고용형태와 단위조직의 크기가 조직의 정보보호 리스크에 부정적인 영향을 줄 수 있음을 보였다. 고용형태를 보면, 외주직원인 경우에 악성코드 감염 가능성이 더 높았다. 따라서, 정보보호 담당조직은 조직구성원의 고용형태에 따라 조직의 정보보호 정책에 대한 이해와 인식이 다를 수 있으므로 조직의 정보보호 리스크를 줄이기 위해서는 구성원별 특성을 고려한 정보보호 교육 및 훈련 프로그램을 마련하고, 이에 대한 참여 기회를 늘릴 필요가 있다. 특히, 외주직원에 보다 많은 관심을 가져야 한다. 또한, 경영진은 단위조직의 크기가 조직의 정보보호 리스크에 영향을 미칠 수 있음을 고려하여 조직의 업무환경을 설계할 필요가 있다.

마지막으로, 본 연구의 대상기관과 같이, 정보보호 정책 준수가 부서 성과에 반영되는 조직인 경우에는 규모가 작은 부서에 보다 많은 관심을 기울일 필요가 있다. 우리의 연구결과에 따르면, 부서의 규모가 작을수록 정보보호 리스크(즉 악성코드 감염 가능성)가 높아지기 때문이다.

6.3 한계점 및 향후 연구방향

본 연구는 다음과 같은 한계점을 가진다. 첫째, 본 연구는 금융 업종과 IT 업종의 특성을 모두 가진 금융IT 분야를 대표하는 기관을 대상으로 진행되었다. 본 연구결과가 다른 조직에서 동일하게 나타난다고 보장할 수 없다. 향후 연구에서 다른 업종 또는 다른 유형의 기관을 대상으로 사이버로핑과 정보보호 리스크 간의 관계를 확인할 필요가 있다.

둘째, 본 연구는 조직의 정보보호 리스크를 악성코드 감염 가능성(악성코드 유포 웹사이트 접속 건수)으로 측정하였다. 조직의 정보보호 리스크에는 악성코드 외에도 해킹, 디도스 공격 등 다양한 위협이 존재한다. 또한, 정보보호 리스크에는 조직구성원의 정보보호에 대한 인식 등 다양한 내적요인이 영향을 줄 수 있는데, 우리는 시스템 로그정보만 활용하였다. 따라서, 향후에는 다양한 정보보호 리스크를 측정하여 연구결과를 비교 및 분석하고, 설문조사 연구를 병행하여 조직 구성원의 내적요인이 미치는 영향을 추가적으로 살펴본다면 보다 정확한 분석이 이루어질 수 있을 것이다.

셋째, 본 연구는 사이버로핑과 정보보호 리스크

간의 관계를 규명하는 것에 초점을 맞추었다. 하지만, 사이버로핑이 정보보호 리스크에 미치는 영향은 특정 요인에 따라 달라질 수 있다. 따라서 향후 연구에서는 이 관계를 조절하는 요인을 찾는 것이 중요하다.

마지막으로, 최근 모바일 기기를 이용한 사이버로핑이 새로운 문제로 떠오르고 있다. 이와 같은 유형의 사이버로핑을 전통적인 사이버로핑과 구별하기 위해 모바일 사이버로핑(mobile cyberloafing)이라고 부른다[50]. 전통적인 사이버로핑은 기업의 인터넷 자원을 이용하므로 기업의 모니터링이 용이한 반면, 모바일 사이버로핑은 이와 다른 별도의 인터넷채널을 이용하므로 조직에서 해당 행동을 모니터링하기 어렵다. 또한, 모바일 기기를 업무에 이용하는 사례가 증가함에 따라 조직 구성원의 모바일 기기가 악성코드에 감염되어 고객정보 유출 등의 보안사고가 발생할 수 있다. 그럼에도 불구하고, 모바일 사이버로핑이 조직의 정보보호 리스크에 미치는 영향에 대한 연구가 거의 이뤄지고 있지 않으므로 이와 관련한 연구가 진행된다면 조직에게 의미 있는 시사점을 제공할 수 있을 것이다.

부록. 변수 설명 및 기술통계

변수	조작적 정의	측정방식	평균 (표준편차)	최소값	최대값
정보보호 리스크	악성코드 감염 가능성	인터넷 필터링 시스템에 차단된 악성코드 유포 웹사이트 건수	13.88 (25.28)	0	230
사이버로핑 빈도	메이저 사이버로핑 웹사이트 접속 빈도	인터넷 필터링 시스템에 차단된 메이저 사이버로핑 웹사이트 접속 차단 건수	93.15 (347.47)	0	4,770
사이버로핑 범위	메이저 사이버로핑 웹사이트 접속 범위	인터넷 필터링 시스템에 차단된 메이저 사이버로핑 웹사이트 접속 차단 유형(카테고리) 수	1.62 (1.37)	0	7
단위조직 크기	구성원이 소속된 단위조직 크기	같은 물리적 공간에서 근무하는 인원수(명)	10.46 (9.62)	1	43
직무유형	조직구성원 직무유형	IT 관련 업무를 수행하는 IT 부서에 속하는지 그렇지 않은지로 구분	0.58 (0.49)	0	1
고용형태	조직구성원 고용형태	내부직원인지 외주직원인지로 구분	0.06 (0.23)	0	1

References

[1] V. K. Lim, "The IT way of loafing on the job: Cyberloafing, neutralizing and organizational justice," Journal of organizational behavior, vol. 23, no. 5, pp. 675-694, June 2002.

[2] B. Liberman, G. Seidman, K. Y. Mckenna and L. E. Buffardi, "Employee job attitudes and organizational characteristics as predictors of cyberloafing," Computers in Human behavior, vol. 27, no. 6, pp. 2192-2199, Nov. 2011.

[3] G. W. Bock and S. L. Ho, "Non-work related computing (NWRC)," Communications of the ACM, vol. 52, no. 4, pp. 124-128, April 2009.

[4] A. M. Bossler and T. J. Holt, "On-line activities, guardianship, and malware infection: An examination of routine activities theory," International Journal of Cyber Criminology, vol. 3, no. 1, pp. 400-420, January - June 2009.

[5] K. S. Choi, "Computer crime victimization and integrated theory: An empirical assessment," International Journal of Cyber Criminology, vol. 2, no. 1, pp. 308-333, January - June 2008.

[6] C. D. Marcum, "Identifying potential factors of adolescent online victimization for high school seniors," International Journal of Cyber Criminology, vol. 2, no. 2, pp. 346-367, July - December 2008.

[7] T. J. Holt, J. van Wilsem, S. van de Weijer and R. Leukfeldt, "Testing an integrated self-control and routine activities framework to examine malware infection victimization," Social Science Computer Review, vol. 38, no. 2, pp. 187-206, April 2020.

[8] E. R. Leukfeldt, "Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization," Cyberpsychology, Behavior, and Social Networking, vol. 17, no. 8, pp. 551-555, July 2014.

[9] E. R. Leukfeldt, E. R. Kleemans and W. P. Stol, "A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists," Crime, Law and Social Change, vol. 67, no.1, pp. 21-37, Feb. 2017.

[10] L. Hadlington and K. Parsons, "Can cyberloafing and Internet addiction affect organizational information security?," Cyberpsychology, Behavior, and Social Networking, vol. 20, no. 9, pp. 567-571, Sep. 2017.

[11] K. M. Eisenhardt, "Agency theory: An assessment and review," Academy of management review, vol. 14, no. 1, pp. 57-74, Jan. 1989.

[12] J. Glassman, M. Prosch and B. B. Shao. "To monitor or not to monitor: Effectiveness of a cyberloafing countermeasure," Information & Management, vol. 52, no. 2, pp. 170-182, March 2015.

[13] J. Chalykoff and T. A. Kochan, "Computer aided monitoring: Its influence on employee job satisfaction and turnover," Personnel Psychology, vol. 42, no. 4, pp. 807-834, Dec. 1989.

[14] A. Urbaczewski and L. M. Jessup, "Does electronic monitoring of employee internet usage work?," Communications of the ACM, vol. 45, no. 1, pp. 80-83, Jan. 2002.

[15] G. S. Alder and M. L. Ambrose, "Towards understanding fairness judgments associated with computer performance monitoring: An integration of the feedback, justice, and monitoring research," Human

Resource Management Review, vol. 15, no. 1, pp. 43-67, March 2005.
[16] J. Vitak, J. Crouse and R. LaRose, "Personal Internet use at work: Understanding cyberslacking," Computers in Human Behavior, vol. 27, no. 5, pp. 1751-1759, Sep. 2011.
[17] R. K. Garrett and J. N. Danziger, "On cyberslacking: Workplace status and personal Internet use at work," CyberPsychology & Behavior, vol. 11, no. 3, pp. 287-292, June 2008.
[18] P. Z. M. De Lara, D. V. Tacoronte, and J. M. T. Ding, "Do current anti cyberloafing disciplinary practices have a replica in research findings?," Internet Research, vol. 16, no. 4, pp. 450-467, Aug. 2006.
[19] J. Wang, J. Tian and Z. Shen, "The effects and moderators of cyber-loafing controls: an empirical study of Chinese public servants," Information Technology and Management, vol. 14, no. 4, pp. 269-282, June 2013.
[20] D. Malachowski, "Wasted time at work costing companies billions," San Francisco Chronicle, vol. 11, no. 3, Nov. 2005.
[21] A. L. Blanchard and C. A. Henle, "Correlates of different forms of cyberloafing: The role of norms and external locus of control," Computers in human behavior, vol. 24, no. 3, pp. 1067-1084, May 2008.
[22] K. Askew, J. E. Buckner, M. U. Taing, A. Ilie, J. A. Bauer and M. D. Coovert, "Explaining cyberloafing: The role of the theory of planned behavior," Computers in Human Behavior, vol. 36, pp. 510-519, July 2014.
[23] L. Cheng, W. Li, Q. Zhai and R. Smyth, "Understanding personal use of the Internet at work: An integrated model of neutralization techniques and general deterrence theory," Computers in Human Behavior, vol. 38, pp. 220-228, Sep. 2014.
[24] J. A. Conger and R. N. Kanungo, "The empowerment process: Integrating theory and practice," Academy of management review, vol. 13, no. 3, pp. 471-482, July 1988.
[25] J. C. Ugrin and J. M. Pearson, "Exploring Internet abuse in the workplace: How can we maximize deterrence efforts?," Review of Business, vol. 28, no. 2, pp. 29-41, Winter 2008.
[26] C. A. Henle, G. Kohut and R. Booth, "Designing electronic use policies to enhance employee perceptions of fairness and to reduce cyberloafing: An empirical test of justice theory," Computers in Human Behavior, vol. 25, no. 4, pp. 902-910, July 2009.
[27] S. Furnell, "Cybercrime: vandalizing the information society," *International conference on web engineering,* Berlin, Heidelberg: Springer Berlin Heidelberg, June 2003.
[28] M. Dodel and G. Mesch, "Cyber-victimization preventive behavior: A health belief model approach," Computers in Human behavior, vol. 68, pp. 359-367, March 2017.
[29] T. J. Holt and A. M. Bossler, "Examining the relationship between routine activities and malware infection indicators," Journal of Contemporary Criminal Justice, vol. 29, no. 4, pp. 420-436, Nov. 2013.
[30] T. J. Holt and A. M. Bossler, Cybercrime in progress: Theory and prevention of technology-enabled

offenses, 1th Ed., Routledge, Dec. 2015.
[31] E. Chien, "Malicious threats of peer-to-peer networking," Symantec White Paper, 2003.
[32] M. Yar, "The Novelty of 'Cybercrime' An Assessment in Light of Routine Activity Theory," European Journal of Criminology, vol. 2, no. 4, pp. 407-427, Oct. 2005.
[33] T. J. Holt and H. Copes, "Transferring subcultural knowledge on-line: Practices and beliefs of persistent digital pirates," Deviant Behavior, vol. 31, no. 7, 625-654, Aug. 2010.
[34] J. M. Hagen, E. Albrechtsen and J. Hovden, "Implementation and effectiveness of organizational information security measures," Information Management & Computer Security, vol. 16, no. 4, pp. 377-397, Oct. 2008.
[35] J. L. Spears and H. Barki, "User participation in information systems security risk management," MIS quarterly, vol. 34, no. 3, pp. 503-522, Sep. 2010.
[36] M. A. Sasse, Usability and trust in information systems. Edward Elgar, 2005.
[37] E. R. Leukfeldt and M. Yar, "Applying routine activity theory to cybercrime: A theoretical and empirical analysis," Deviant Behavior, vol. 37, no. 3, pp. 263-280, March 2016.
[38] S. Hinduja and J. W. Patchin, "Cyberbullying: An exploratory analysis of factors related to offending and victimization," Deviant behavior, vol. 29, no. 2, pp. 129-156, Feb. 2008.
[39] R. W. Taylor, E. J. Fritsch, J. Liederbach, M. R. Saylor and W. L. Tafoya, Cyber crime and cyber terrorism. New York, NY: Pearson, 2019.
[40] Bo-ra Kim, Jong-Won Lee and Beom-Soo Kim, "Effect of Information Security Training and Services on Employees' Compliance to Security Policies," Informatization Policy, 25(1), pp. 99-114, March 2018
[41] L. Cheng, Y. Li, W. Li, E. Holm and Q. Zhai, "Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory," Computers & Security, vol. 39, pp. 447-459, Nov. 2013.
[42] T. Gundu and S. V. Flowerday, "Ignorance to awareness: Towards an information security awareness process," SAIEE Africa Research Journal, vol. 104, no. 2, pp. 69-79, June 2013.
[43] Jeong-Ha Lee and Sang-Yong Tom Lee, "A Study on the Factors for Violation of Information Security Policy in Financial Companies: Moderating Effects of Perceived Customer Information Sensitivity," Journal of Information Technology Applications and Management, 22(4), pp. 225-251, Dec. 2015
[44] Jeong-Ha Lee and Sang-Yong Tom Lee, "Violations of Information Security Policy in a Financial Firm : The Difference between the Own Employees and Outsourced Contractors," Information Systems Review, 18(4), pp. 17-42, Dec. 2016
[45] J. D'Arcy, A. Hovav and D. Galletta, "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach," Information

systems research, vol. 20, no. 1, pp. 79-98, March 2009.
〔46〕 O. A. Alnuaimi, L. P. Robert and L. M. Maruping, "Team size, dispersion, and social loafing in technology-supported teams: A perspective on the theory of moral disengagement," Journal of Management Information Systems, vol. 27, no. 1, pp. 203-230, Summer 2010.
〔47〕 P. M. Muchinsky and M. L. Tuttle, "Employee turnover: An empirical and methodological assessment," Journal of vocational Behavior, vol. 14, no. 1, pp. 43-77, Feb. 1979.
〔48〕 Hyun Kang, "Effects of Job Satisfaction and Organizational Commitment on Security Policy Compliance Motivation in Relation to Organizational Culture," Korean Journal of Industry Security, 5(2), pp. 167-199, Dec. 2015
〔49〕 A. C. Johnston, M.. Warkentin and M. Siponen, "An enhanced fear appeal rhetorical framework," MIS quarterly, vol. 39, no. 1, pp. 113-134, March 2015.
〔50〕 A. Sheikh, M. S. Atashgah and M. Adibzadegan, "The antecedents of cyberloafing: A case study in an Iranian copper industry," Computers in Human Behavior, vol. 51, pp. 172-179, Oct. 2015.

〈저자소개〉

오 현 우 (Hyunwoo Oh) 정회원
2021년 2월: 연세대학교 정보대학원 정보시스템학 석사
2001년 12월~현재: 금융결제원 정보보호부 팀장
〈관심분야〉 정보보호, 프라이버시, 정보보안 정책

김 범 수 (Beomsoo Kim) 종신회원
1990년 2월: 서울대학교 경영학 학사
1992년 2월: 서울대학교 경영학 석사
1999년 2월: University of Texas at Austin 경영학 박사
1999년~2002년: University of Illinois at Chicago 조교수
2002년~현재: 연세대학교 정보대학원 교수
〈관심분야〉 ICT의 효과적 활용, 데이터 거버넌스, 프라이버시, 개인정보보호

박 재 영 (Jaeyoung Park) 정회원
2012년 8월: 숭실대학교 정보통신전자공학부
2017년 2월: 연세대학교 정보대학원 정보시스템학 석사
2021년 8월: 연세대학교 정보대학원 정보시스템학 박사
2021년 9월~2022년 7월: 연세대학교 정보대학원 박사후 연구원
2023년 6월~현재: NH농협금융지주 NH금융연구소 책임연구원
〈관심분야〉 프라이버시, 개인정보보호, 디지털 금융, 데이터 사이언스