Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.5, Oct. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.5.1167

국내 사이버위협 정보 공유에 영향을 미치는 요인*

김 하 영,[1†] 김 태 성[2‡]
[1](주)싸이버원, [2]충북대학교 경영정보학과

Factors that Affect Sharing Cyber Threat Information in South Korea*

Ha-Young Kim,[1†] Tae-Sung Kim[2‡]
[1]Cyberone Inc., [2]Chungbuk National University

요 약

본 연구는 우리나라 사이버위협 정보 공유의 활성화를 위해 사이버위협 정보를 제공하는 데에 영향을 미치는 요인들을 연구하였으며, 특히 제공하는 정보의 중요도에 따른 제공의도를 비교해보았다. 연구방법은 정보보호 관련 실무자들을 대상으로 정보공유시스템의 이용자 측면에서 온라인 설문 및 실증분석을 실행하였다. 연구 결과, 간단한 정보에 대해서는 오로지 최고경영자의 태도만이 정보 제공의도에 영향을 미쳤다. 반면 중요한 정보에 대해서는 최고경영자의 태도뿐만 아니라 정보평가체계, 민간화, 법적처벌 완화의 순으로 유의미한 영향을 미쳤다.

본 연구의 결과를 통해 국내 사이버위협 정보공유시스템의 문제점을 파악할 수 있으며, 개선사항의 우선순위와 정보 공유 시스템의 개선 전후 정보 제공의도의 변화를 확인할 수 있다.

ABSTRACT

The purpose of this study is to investigate the factors affecting cyber threat information provision in order to activate cyber threat information sharing in Korea. In particular, we looked at the intention to provide simple information and important information according to the importance of information. The research method was conducted on the information security practitioners' online survey in terms of users of information sharing system. And empirical analysis was conducted. As a result of the study, only the CEO's attitude influenced the intention to provide simple information. On the other hand, important information was influenced not only by the CEO's attitude but also by the information evaluation system, privatization, and mitigating legal penalties.

The results of this study can identify the problems of the cyber threat information sharing system in Korea. And we can confirm the priority of improvement and the change of information providing intention before and after improvement of information sharing system.

Keywords: Information Sharing, Cyber Threat, Intent to Provide Information

I. 서 론

최근 사이버위협은 점점 동시다발적인 공격을 목표로 하고 있으며, 공격 대상이 되는 기업 및 기관에서 단독으로 대응하는 것이 어려워지고 있다. 또한 한번 사용된 신종 공격기법은 향후에 다시 쓰이는 경

Received(06. 19. 2017), Modified(09. 26. 2017), Accepted(09. 26. 2017)
* 본 연구는 과학기술정보통신부 및 한국인터넷진흥원의 "고용계약형 정보보호 석사과정 지원사업"의 연구결과로 수행되었음 (과제번호 H2101-16-1001). 이 논문은 2015년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2015S1A5A2A01009763).
† 주저자, bj927hy@naver.com
‡ 교신저자, kimts@cbnu.ac.kr(Corresponding author)

우가 많다. 따라서 이러한 공격에 의한 피해 사례를 줄이기 위해 위협 첩보에 대한 공유가 주목을 받고 있다. White, DiCenso[1]는 국가 안보 문제를 해결하기 위해 업계와 정부의 다양한 수준 간 정보 공유 메커니즘의 필요성을 강조하였다. 그리고 사이버 보안 정보를 공유하는 것은 공유하지 않았을 때보다 저비용으로 보안 수준을 높일 수 있으며 큰 기업, 큰 산업일수록 더 가치가 있다는 것이 여러 연구를 통해 검증되었다[2-4]. 이철수[5], 김동진, 조성제[6]는 국가의 침해사고 대응을 위해 사이버위협에 대한 정보 공유가 필요함을 언급하였다. 이처럼 세계적으로 국가적 차원에서 사이버위협 정보에 대한 자발적인 공유의 필요성이 높아지고 있으며 보다 더 활발한 공유를 위해 노력하고 있다.

한편 우리나라에서는 과거 7.7 DDoS, 6.25 사이버 테러와 같은 대형 사이버 공격의 원인 중 하나로 민-관 사이버위협 정보 공유 체계의 미흡이 지목되기도 하였다[7]. 7.7 DDoS와 6.25 사이버 테러는 모두 정부, 기업을 막론하고 여러 기관에서 동시다발적으로 발생했다. 이러한 대형 공격이 발생하기 전에는 반드시 징후가 나타나기 마련이다. 만약 사고 발생 전 각 기업들이 발견한 조짐을 여러 기관과 공유 했었더라면 기업 혼자 맞서는 것이 아닌, 협력을 통해 사이버 공격에 대처할 수 있었을 것이다.

그러나 우리나라는 아직 사이버위협 정보의 공유가 활발히 이루어지고 있지 않다. 사이버 방어 협력으로 대부분의 기업들이 사이버 관련 데이터 공유를 원하지만 성공적인 모델이 없어 구체적인 방안이 요구되고 있는 상황이다[8]. 전문가들 대부분 사이버위협 정보의 공유에 대한 필요성은 공감하지만, 주로 정보를 받는 입장에 치우치기 때문이다[9]. 사이버위협 정보의 공유가 활성화되기 위해서는 정보를 받아서 잘 활용하는 것도 중요하지만, 그에 앞서 정확하고 자세한 정보가 먼저 제공되는 것이 필수적일 것이다.

따라서 본 연구에서는 우리나라 사이버위협 정보 공유의 활성화를 위해 사이버위협 정보를 제공하는 데에 영향을 미치는 요인을 분석한다. 즉 현재 운영되고 있는 사이버위협 정보 공유 시스템이 개선되어야 할 사항을 이용자 측면에서 바라보며, 개선사항들의 우선순위를 확인한다. 그리고 개선 전과 후에 사이버위협 정보 제공 의도에 변화가 있는지 알아본다.

II. 문헌 연구

2.1 사이버위협 정보 공유

정보 공유의 정의에 대한 연구는 다음과 같다. 정덕훈, 심형섭[10]은 '개인이나 조직이 활동과정에서 생산 및 획득한 각종 정보들의 단순한 공유를 넘어서서 그러한 정보를 저장·관리하는 시스템의 일부나 전부를 개방함으로써 함께 사용할 수 있도록 하는 일체의 활동'으로 정보 공유를 정의하고 있으며, 김구[11]는 '조직에서 정보 공유는 조직구성원들이 개인의 과업수행과 조직 전체 목표를 효율적으로 달성하기 위하여 개인 간, 업무 단위 간 또는 부서 간 정보를 교환하는 것이다'라고 정의하고 있다. 한상연, 강현민[12]은 정보 공유를 '정부 및 공공기관이 업무를 수행하기 위해서 보유하고 있는 정보를 정부기관과 공공기관, 공공부문과 민간부문, 기관·기업·개인 사이에 공동으로 이용하는 것'으로 정의한다. 김동욱, 윤건[13]은 정보 공유를 복수의 정보주체가 일정 정보를 공동으로 보유한 상태 혹은 보유하는 활동으로 정의하고 있다. Caffrey[14], Dawes, Prefontaine[15], Gil-Garcia et al.[16]은 '시스템의 설치, 제도적 기준의 마련, 그리고 조직 간 정보의 공동활용 등을 포함하는 개념'으로서 정보 공유를 정의하고 있다. 또한 Grant[17]는 '정보접근성에 대한 기술적 지원과 조직 인프라 구축을 통하여 정보와 지식의 활용을 극대화하여 조직역량을 강화시키는 것'으로 정보 공유를 해석하고 있다.

본 연구에서는 다양한 종류의 정보 공유 중에서도 사이버위협에 대한 공유를 다룬다. 2015년에 발의되었던 '사이버위협 정보 공유에 관한 법률안'에서는 사이버위협 정보를 '사이버위협의 발신지, 목적지, 발생일지 등 로그기록자료, 악성프로그램, 보안취약점 정보 등'으로 정의하였다[18]. 즉, 사이버위협 정보의 공유란 이러한 정보들과 같이 기업에서 발생한 사이버위협 및 침해사고와 관련한 정보들을 타 기관들과 공유함으로서 대응에 협력하는 것을 말한다. 사이버위협 정보들은 간단한 정보만 제공했을 때보다 자세하고 정확한 정보를 공유 할수록 효과는 더 높아질 것이다.

2.2 정보 공유의 문제점 및 활성화 요인

초기의 정보 공유에 관한 연구는 지식공유 분야에서 시작되었으며 지식의 변환, 수집, 분배 과정에 초

점을 두었던 것이 점차 정보 공유에 대한 영향요인에 관한 연구로 발전하였다[19].

지식공유에 대하여, 박동희, 현영란[20]은 관리기관에 대한 신뢰와 보상적 참여유인이 지식정보의 공유와 활용에 영향을 미친다는 것을 보였다. 반면 공동목표의식적 참여유인은 오히려 지식정보의 공유와 활용에 부정적인 영향을 미친다는 것을 보였다. 또한 Liu et al.[21]은 지식공유와 정보보안 투자와 관련된 두 회사의 의사결정 간의 관계를 연구했는데, 분석에 따르면 두 회사가 보유한 정보자산의 특성이 의사결정에 중요한 역할을 하며 보안 지식공유를 위해 외부의 영향이 없는 상태에서 인센티브의 특성이 필요함을 주장하였다.

반면 Bock, Kim[22], Bock et al.[23], Lin[24] 등은 많은 사람들이 지식공유의 가장 중요한 동기부여 요인으로 생각했던 보상이 지식공유에 대한 태도와 무관하다는 결과를 나타냈다.

그리고 Chen et al.[25]은 조직환경과 같은 요인이 태도에 긍정적인 영향을 미친다는 것을 보였으며, Lin[26]은 다른 사람들을 돕는 것에 대한 즐거움(기여감)과 조직적 요소 중 하나인 최고경영자의 지원이 지식공유 프로세스에 중요한 영향을 미친다는 것을 보였다.

한편 앞서 열거된 몇몇 연구들은 보상이 지식공유 의도에 무관하다는 것을 보였다. 이에 대해 Bartol, Srivastava[27]는 정보 공유에 있어서 공식적이거나 명확한 상호관계에는 보상이 유의미하지만, 비공식적이거나 불확실한 상호관계에 있어서는 보상이 큰 의미가 없다는 것을 확인했다.

정보 공유의 장애요인에 대해, 왕재선, 문정욱[28]은 정보 공유 장애요인에 대한 응답자 특성별 분석을 한 결과, 기관별로는 법·제도, 직급별로는 법·제도와 조직, 직업별로는 기술적 요인들이 유의하였다. 그리고 Caffrey[14]는 정보 공유의 장애요인으로 법·제도적 정비, 예산, 프라이버시, 정보보안의 문제 등을 제시하고 있다. Aviram, Tor[29]는 정보 공유의 장애를 극복하기 위해 민간법률시스템과 정부의 개입을 주장하였다.

2.3 사이버위협 정보 공유의 문제점 및 활성화 요인

국내 보안컨퍼런스인 'NETSEC-KR2015'에서는 민간기업 간 점차 활발해지는 보안취약점 및 악성코드의 정보 공유 관련 정책과 방법 등을 두고 패널 토의를 진행했다. 사이버위협 정보 공유의 활성화 방안에 대한 패널들의 의견은 다음과 같다.

첫째, 정보의 가치에 대한 객관적 기준이 제시되어야 한다. 둘째, 정보의 가치를 평가할 수 있는 시스템이 마련되어야 한다. 셋째, 금전적인 보상체계가 필요하다. 넷째, 악성코드를 최초로 발견하고 공유하는 사람에게 보상이 있어야한다. 다섯째, 공유된 정보가 제3의 목적으로 이용되어선 안 된다. 여섯째, 어떤 정보를 공유해야 할지에 대한 기준 정립이 필요하다. 일곱째, 운영기관에서 모든 정보를 독과점으로 수집해 정보를 배부하는 방식보다는 수요자가 원하고 필요한 정보를 자유롭게 선택할 수 있도록 장터 역할을 해주는 것이 바람직하다. 여덟째, 정상 파일도 공유할 수 있는 것이 좋다. 이 밖에도 다양한 의견들이 제시되었다[30].

국내에서는 사이버위협 정보 공유 활성화에 대해 다음과 같이 연구되고 있다. 이재은, 김겸훈[19]은 과업의 특성(상호의존성, 업무프로세스의 코드화 가능성), 조직구조(공식화 수준, 조직문화), 정보 공유 시스템(시스템 활용도, 의사소통채널 구축, 공유 여건, 안전성, 정보 공유 수준)의 특징들이 국가안전관리 정보시스템의 정보 공유 정도의 요인이 될 수 있음을 보였다. 이 중 과업의 특성에 해당하는 상호의존성과 업무프로세스의 코드화 가능성, 조직구조에 해당하는 공식화 수준, 정보 공유 시스템에 해당하는 공유 여건 등은 다른 변수들에 비해 영향력이 상대적으로 높게 나타났다. 윤오준 등[31]은 우리나라의 사이버위협 정보 공유 활성화를 위해 공유절차 마련 등 법/제도 개선, 국가 차원의 통합시스템 구축, 민-관 공유협의체의 구성 및 운영이 개선되어야 함을 언급하였다. 그리고 김애찬, 이동훈[32]은 효과적인 사이버위협 정보 공유체계 수립을 위한 요구사항의 우선순위를 정책적, 기술적인 것의 순으로 도출하였다. 정책적 요구사항에서는 법적 근거의 마련과 정보관리체계 마련이 보다 중요한 것으로 확인되었다. 반면, 기술적 요구사항에서는 정보의 표현방식 및 전송규격 표준화와 정보 수집 방법 및 신뢰성 개선이 보다 중요한 것으로 확인되었다. 장홍종 등[33]은 G-ISAC의 효율적인 구축을 위해 보안관제시스템 구축 시 로그의 표준화 검토, 로그 필터링, 로그분석 기법, 보안정보제공 및 침해사고 대응과 연계/운영하는 방안 검토, 분석 팀과의 연계에 대해 고려해야한다고 주장하였다. 고성훈[34]은 정보기술 수용이론과 기술-조직-환경 프레임워크를 참조하여 환경 요인(법/제도, 신뢰, 보안), 기술 요인(정보 품질, 시스템 품질), 조직 요인(조직 능력)이 사이버 보안정보

의 유용성에 영향을 미치며 유용성이 조직간 사이버 보안 정보 공유 체계 수용의도에 영향을 미친다는 것을 보여주었다. 권유중[35]은 한국의 사이버위협 정보 공유체계 수립을 위한 고려사항으로 공유정보 품질 및 적시성 확보, 프라이버시 및 기업 평판 확보, 공유체계 원칙 및 관리, 공유 주체 간 신뢰 및 성숙도 확보, 공유 강제, 인센티브 부여를 언급하였다.

Vazquez et al.[8]은 사이버 방어 정보의 공유를 개선하기 위해 정보의 높은 품질, 명확한 관리 규칙, 인센티브, 신뢰, 인식 및 유지 등의 문제가 개선되어야함을 제안했다. Dandurand, Serrano[36]는 사이버 보안 정보 공유를 향상시키기 위해 다음과 같은 여러 개선사항들을 제안하였다. 무료 사용을 기반으로, 수용성, 확장성, 보안성 및 분산된 인프라를 제공하도록 하며, 여러 독립적인 데이터 모델 및 그들의 상관관계 구문과 의미 관리 제공이 필요하다. 또한 공유 및 개인적인 데이터 모두 보안 저장이 되어야하며 사용자 정의의 다자간 공유가 제공되어야한다. 비접속 도메인 간의 데이터 교환이 가능해야하며 인간과 기계에 대한 인터페이스가 제공되어야한다. 또한 데이터의 발생, 치밀한 사고, 검열에 대한 부담을 공유할 수 있는 도구를 제공해야한다. 정보 품질 관리 프로세스가 제공되어야 하며 합의 도달을 위한 분쟁 공개, 데이터의 지속적인 가용성 지원, 상업적인 활동이 가능해야 한다. Tosh 등[37]은 국제전기통신연합 표준화 기구인 ITU-T(International Telecommunications Union Telecommunication)에서 표준화한 사이버 보안정보 교환 프레임워크(CYBEX, Cybersecurity Information Exchange)가 사이버 공격에 대응하는 참여기업 간 공격/패치 관련 정보 공유를 용이하게 하기위해 반드시 필요하다고 하였다. 그리고 CYBEX에서의 공유를 향상시키기 위해 자신들의 수익을 얻는 것뿐만 아니라 윈-윈 상황이 될 수 있도록 가격책정 방식을 현명하게 변화시켜야 함을 보여준다.

III. 국내·외 사이버위협 정보 공유 시스템 현황

3.1 국내 사이버위협 정보 공유시스템 현황

국내에서는 민-관 기관들의 자발적인 참여에 의해 운영되는 사이버위협 정보 공유 시스템으로 ISAC(Information Sharing & Analysis Center)과 C-TAS(Cyber Threats Analysis System)가 있다.

우리나라는 2001년 제정된 「정보통신기반보호법」 제16조에 의해, 증가하는 해킹 및 사이버테러로부터 금융·통신 등 분야별 정보통신기반시설을 보호하기 위하여 정보공유·분석센터를 구축·운영할 수 있도록 지원되기 시작하였다. ISAC은 동종 업종이나 관련 분야 상호간에 사이버 상과 물리적 혹은 자연적으로 발생하는 위협과 취약점 등의 문제에 관한 정보를 분석하고, 문제를 유발하는 행위가 발생한 경우 이를 관계 기관에 신속하게 배포하여 주요기반시설에 대한 공격을 효과적으로 예방·탐지·대응할 수 있도록 하고 있다. ISAC은 현재 정보통신, 행정, 금융 분야에서 운영되고 있으며 2017년에는 에너지, 의료, 교육 분야 등에도 구축·운영 될 예정이다[38].

이러한 ISAC은 분야별로 운영되며 정보 공유가 이루어지지 않는 일반 보안관제센터와 달리, 정부 주도하에 ISAC을 중심으로 회원사간 사이버테러 공격유형 및 대처방안에 대한 정보 공유가 가능하다. 또한 개별 기관의 독자적 대처에 따른 과다비용, 인력 소모 문제가 발생하는 일반 보안관제센터와 달리, 공동대응을 통한 신속한 대처 및 효율적인 비용으로 운영이 가능하다는 장점이 있다. ISAC은 국내의 회원사간 공유만 가능한 것이 아니라 미국, 영국, 일본 등 타 국가의 ISAC과 연계를 통하여 세계적인 공유가 가능하다[39].

C-TAS는 2013년 7월 4일 발표된 '국가 사이버안보 종합대책'의 일환으로, 2014년 8월부터 한국인터넷진흥원(KISA)에 의해 운영되고 있다. C-TAS는 가장 신속하게 세계 사이버위협 정보를 수집·분석·공유하는 것을 목표로 하며 분야의 제한 없이 가입을 요청한 참여기관에 의해 정보가 공유되고 있다.

KISA는 C-TAS가 기여 기반의 정보 공유를 통해 수집 정보를 확대할 수 있도록 추진하고 있다. 원칙적으로 위협 정보를 제공하는 기관에게 정보를 공유하도록 하며 정보 제공 업체가 정보 제공 항목 및 공유의 범위를 결정할 수 있도록 했다. 그리고 권한관리, 접근통제를 통해 회원별 정보 공유 대상 및 범위를 차등화하며 단위 사업군별 정보 공유 희망 시 공유채널 제공 등 허브 역할을 수행하기 위해 노력하고 있다[40, 41].

C-TAS는 2016년 11월 기준으로, 국내 128개의 기업이 참여 중이며 최근 130여개까지 증가하고 있다[42]. 2014년 8월 30개, 2015년 2월 70여개에 비하면 참여 기업이 꾸준히 증가하고 있는 추세이다.

우리나라는 ISMS(정보보호관리체계) 인증 의무대상 기업이 264개(미래창조과학부, 2015)이며 한국인터넷진흥원의 정보보호관리체계 홈페이지(http://isms.kisa.or.kr/)를 살펴보면 2016년 11월을

기준으로 ISMS 인증 획득 기업이 410개에 이른다[43]. 주요정보통신기반시설 역시 2015년 기준으로 공공기관 227개, 민간 127개 등 총 354개가 지정되었다[44]. 뿐만 아니라 우리나라 개인정보보호 의무적용 대상으로, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 해당하는 기업이 약 49만개 이상이며 「공공기관의 개인정보 보호에 관한 법률」 적용 기관이 약 2만 5천개, 기타 민간사업자가 310만개 이상이다. 여기에 법원 등 헌법기관, 신용정보 제공 및 이용자 관련 기업 등을 합한다면 훨씬 더 많아질 것이다[45]. 국내 사이버위협으로부터 보호받아야 할 주요 기관들이 매우 많은데, 130여개의 C-TAS 참여기관 수는 많이 부족한 편이라고 볼 수 있다. 하지만 참여기관의 수보다 중요한 것은 현재 참여하고 있는 기업들이 정보를 공유하기 위한 정보 제공이 얼마나 잘 되고 있는 지이다.

3.2 국외 사이버위협 정보 공유 시스템 현황

미국은 1998년부터 대통령 행정명령(Presidential Decision Directive-63)에 따라 ISAC이 도입되었으며 이후 핵심 인프라 부문에 대해 부문별 조직을 설립하여 위협과 취약성에 대한 정보를 공유하도록 하였다. 현재 미국의 ISAC은 자동차, 비행, 통신, 전기, 비상사태 관리 및 대응, 금융 서비스, 헬스케어, 정보기술, 국민 건강, 석유 및 천연가스, 부동산, 연구 및 교육 네트워크, 소매상 사이버 정보 공유 센터, 수자원 분야 등이 포함된 24개 분야에서 운영 중이다. 그리고 여러 주요 인프라 부문에서 상황 인식을 유지하기 위해, NCI(National Council of ISACs, http://www.nationalisacs.org/)를 통해 서로 위협 및 완화 정보를 공유 및 협력한다[46].

미국의 국토안보부(Department of Homeland Security)는 AIS(Automated Indicator Sharing) 기능을 통해 연방 정부와 민간 부문 사이에 악성 IP주소나 피싱 메일의 송신지 주소와 같은 위협 지표를 신속하게 공유할 수 있도록 하고 있다. AIS에 참여하는 업체들은 NCCIC의 DHS 관리시스템으로 연결하여 업체 인근의 서버를 통해 NCCIN과 지표를 주고받는다. 이 때, AIS를 통해 지표를 공유하는 참가자들은 자신의 신원 공개에 동의하는 경우를 제외하고 모두 익명으로 활동할 수 있다[47].

미국은 소매업 사이버 정보 공유 센터인 R-CISC (Retail Cyber Intelligence Sharing Center, https://r-cisc.org/)를 통해 소매업의 사이버 정보 공유를 활성화하기 위해 노력하고 있다[48]. R-CISC의 회원사는 핵심 회원과 준회원으로 나뉜다. 핵심 회원은 상업 서비스 및 소매 업체로, 연 매출이 일정 수준을 넘기는 업체에 한해 보안 및 위험 관리를 위한 사례를 공유할 수 있다. 준회원은 비 소매상 또는 보안 업체로, 자발적인 선택을 기반으로 정보를 공유할 수 있다.

그러나 이러한 미국의 사이버위협 정보 공유에 대한 노력에도 불구하고, 자율적인 정보 공유는 활발하게 이루어지지 않았다. 따라서 사이버위협 정보 공유에 대해 중요성을 다시 한 번 부각시키기 위해, 2015년 12월 미국 정부는 사이버보안 정보 공유법(CISA, Cybersecurity Information Sharing Act)을 통과시키면서 민간부문에서 발생한 위협 첩보를 반드시 정부에게 알리도록 의무화 하였다. 이제는 자율적인 공유뿐만 아니라 법적 강제성에 의해 사이버위협 정보를 공유해야한다.

한편 일본은 T-ISAC-J(Telecom-ISAC Japan)이라는 이름으로 통신ISAC이 운영되고 있다. T-ISAC-J는 안전하고 신뢰할 수 있는 통신 서비스를 보장하기 위해, 일본의 주요 인터넷 서비스 제공 업체가 설립한 비영리 조직이다. 11개의 Working Group(WG)과 1개의 Special Interest Group(SIG)으로 구성되어 업무를 수행하고 있다[49].

일본은 T-ISAC-J 외에도 IPA(Information Technology Agency) 기관에서 운영하는 J-CSIP (Initiative for Cyber Security Information sharing Partnership of Japan)가 있다. IPA는 사이버 공격, 특히 전자메일에 대한 대응을 위해 2011년 J-CSIP를 설립했으며, 주요 제조업체간 협의를 통해 기밀유지계약(NDA, Non-Disclosure Agreement) 내용을 구성하고 정보 공유 규칙을 개발하였다[50].

IPA는 홈페이지를 통해 J-CSIP의 운용상황을 분기별로 보고하고 있다. 가장 최근의 보고서에 의하면, 2016년 10월을 기준으로 7개 분야에서 87개의 조직이 참여하고 있다[51]. 참여 기업은 정보 제공사에 대한 정보를 익명화 하고 민감한 정보를 보호하거나 삭제하여 탐지된 사이버 공격 정보를 IPA에 제공하면, IPA가 분석정보를 추가하고 정보제공자의 승인을 얻어 공유 가능한 정보를 다시 참여기업 간에 공유한다. IPA는 필요에 따라 정보 제공사의 승인을 받아

제공된 정보의 일부를 JPCERT/CC 등과 같은 정보보안 관계기관에 제공하여 사이버 공격에 대한 대책을 협조하고 조정한다. 또한 중대한 사안이 발생한 경우 경제산업성 및 내각관방 정보보호센터(NISC, National Information Security Center)에 보고하여 해당 업무지시를 수행한다[50].

IV. 연구 방법

앞서 살펴본 바와 같이 사이버위협 정보 공유의 활성화를 위해 다양한 개선사항들이 연구되고 있다. 또한 각국에서는 여러 원인들을 고려하여 정보공유시스템을 개선시키며 운영하고 있다. 본 연구에서는 정보공유시스템 이용자들을 대상으로 한 설문을 통해 선행연구에서 제시된 특정 개선사항의 필요 정도를 알아보고자 한다. 또한 개선 후 정보 제공 의도의 변화를 알아보고, 특히 제공 정보를 간단한 정보와 중요한 정보로 구분함으로써 정보의 중요도에 따라 필요한 개선사항과 정보 제공 의도의 변화도를 파악하고자 한다.

4.1 연구 모형

본 연구에서는 사이버위협 정보 공유에 영향을 미치는 요인들을 문헌 연구 및 언론기사 등을 통하여 선정하였다. 선정된 요인들은 법적처벌 완화, 민간화, 정보평가체계, 익명성, 최고경영자 태도이다. 변수의 조작적 정의는 [표 1], 연구 모형은 [그림 1]과 같다.

'정보평가 체계'란 제공되는 사이버위협 정보들의 가치, 수준을 평가하고 분류하는 체계에 대한 개선의 필요 정도를 의미한다. 그리고 '익명성'은 사이버위협 정보를 제공하는 기업의 명칭 등 기업을 파악할 수 있는 정보의 비공개화에 대한 개선의 필요 정도를 의미한다. '법적 처벌 완화'는 사이버위협 정보를 제공하는 기업에게 법적 위반 사항에 대한 처벌을 완화함으로써 책임 부담감을 줄이는 것에 대한 필요 정도를 의미한다. '민간화'는 현재 정부 및 산하기관에 의해 주관·운영되는 사이버위협 정보 공유 시스템을 민간 기업에 의한 주관·운영 시스템으로 변경하는 것에 대한 필요 정도를 의미한다. 위의 네 가지 요인들은 각각에 대해 개선이 필요하다고 느끼는 정도를 측정한다. 이는 곧 개선의 필요성을 강하게 느낄수록 현재의 상황이 좋지 않음을 나타내므로 역채점을 하였다. 즉 설문에 대한 응답이 긍정적일수록 부정적인 의미로 채점하여 분석하였다. 마찬가지로, 설문에 대한 응답이 부정적일수록 긍정적인 의미로 채점하여 분석하였다. 마지막으로 '최고경영자 태도'는 기업 내 CEO의 정보보안에 대한 관심 및 지원 수준을 의미한다. 최고경영자의 태도는 직원이 느끼는 최고경영자의 관심도, 타기업에 비교했을 때 보안에 대한 투자 정도를 통해 측정할 수 있다.

한편 본 연구의 종속변수인 '정보 제공의도'는 응답자가 속한 기업의 사이버위협 정보를 공유시스템에 제공할 의도를 의미한다. 정보 제공의도는 간단한 정보와 중요한 정보의 두 가지로 나뉘어 측정된다. 간단한 정보는 공격 발생지IP, 공격 발생일지, 공격 기법, 악성프로그램 등의 정보와 같이, 실제 기업의 정보가 포함되지 않아서 제공하기에 부담을 덜 가질 수 있는 것을 의미한다. 반면 중요한 정보란 공격에 관한 기업의 보안 취약점, 사이버 공격으로 인한 피해, 사이버 공격으로 인한 피해 규모 등과 같이, 실제 기업 정보와 직접적으로 관련이 있어서 정보를 제공하기에 앞서 부담과 걱정이 큰 것을 의미한다.

4.2 가설 설정

4.2.1 법적처벌 완화

Bock, Kim[22], Bock et al.[23], Lin[24] 등은 보상제도가 정보 공유를 활성화 하는 데에 관련이 없음을 보이고 있다. 그러나 Bartol, Srivastava[27]는 정보 공유에 있어서 공식적이거나 명확한 상호관계 또는 비공식적이거나 불확실한 상호관계에 따라서 보상이 관여하는 정도가 다르다는 것을 알 수 있었다.

한편 김동욱, 윤건[13], 문정욱[52], 왕재선, 문정욱[28], 김은정[53], 고성훈[34], 윤오준 등[31], 김애찬, 이동훈[32], Caffrey[14]는 정보 공유의 문제점으로 법적 근거가 취약함을 말했고 Walton[54] 역시 법적 프레임과 개인정보보호/프라이버시와 같은 요인이 법제도 및 정치적 요인으로서 공유시스템 활성화에 영향을 미친다는 것을 보였다.

따라서 본 연구에서는 법/제도 개선 사항 중 하나로 법적 처벌 완화를 보상의 개념으로 설정하였다. 정보제공시스템에 올린 사항은 자칫 잘못하면 기업의 관리 부주의로 판단될 수 있으며 법적 위반 사항에 대한 책임을 물을 수도 있다. 이러한 점은 기업으로 하여금 정보 제공을 소홀하게 하며 소극적이게 할 것이다. 이를 반영하여, 실제로 미국에서는 사이버보안

Table 1. Operational definitions, metrics and related literature of variables

Variable	Operational definitions	Metrics	Related literature
Mitigating legal penalties*	Degree of need for reduction of liability for legal violation to information provider	• It is necessary to reduce the liability for legal violations to companies providing cyber threat information. • It is necessary for companies providing cyber threat information to reduce their responsibility for future legal violations related to the information they provide.	DHS[56], NIST[54]
Privatization*	Degree of need for change from government-led to private enterprise operating system	• It should be operated by a private enterprise. • It should be independent from government.	김민호[57], Ransbotham et al.[58]
Information evaluation system*	Degree of need for improve evaluation level of cyber threat information provided	• It is necessary to evaluate the timeliness. • It is necessary to evaluate the accuracy. • It is necessary to evaluate the importance of vulnerabilities. • It is necessary to evaluate the completeness.	Zhao, White[59], NIST[55], ENISA[60]
Anonymity*	Degree of need for anonymity of enterprise providing information	• It is necessary for the non-identification of corporate information. • Company information should not be disclosed at all. • Standards for non-identification of corporate information are needed. • Anonymity of corporate information should be guaranteed.	MNE7[61], 권유중[35]
CEO's attitude	Degree of support for the security of the CEO	• Top management's interest in information security is high. • Top management thinks that the information security is important. • Top management's support for information security is higher than other companies. • Top management is positive about sharing cyber-threat information.	Li, Lin[62], Lin[26]
Intent to provide information	Intent to provide cyber threat information	• I have intention to provide simple information about the cyber threats that companies have experienced. (Source of attack(IP) / Time of attack occurrence / Technique of attack / Malicious program) • I have intention to provide critical information about the cyber threats that companies have experienced. (Company's security vulnerability in attack / Damage due to cyber attack / Scale of cyber attack)	Ajzen[63], Ajzen[64], Bock, Kim[22]

*: Reverse scoring

정보 공유법을 통과하면서 공유를 활성화하기 위해 법적 책임에 대한 면책을 주었다[55]. 기업에서 정보를 제공한다면, 그와 관련하여 법정 위반사항이 발생하더라도 책임을 지지 않아도 되는 것이다. 즉, 정보를 제공하는 사람에 한하여 법적 처벌을 완화하여 책임을 줄여주는 것은 보상의 일종으로 볼 수 있다. 이러한 법적 처벌에 대하여 법/제도 개선이 이루어진다면 정보 제공이 활성화 될 수 있을 것이다. 따라서 본 연구에서 설정한 가설은 다음과 같다.

H1a: 사이버위협 정보를 제공한 자에게 법적 처벌이 완화되면, 간단한 사이버위협 정보 제공의도가 높아질 것이다(+).

H1b: 사이버위협 정보를 제공한 자에게 법적 처벌이 완화되면, 중요한 사이버위협 정보 제공의도가 높아질 것이다(+).

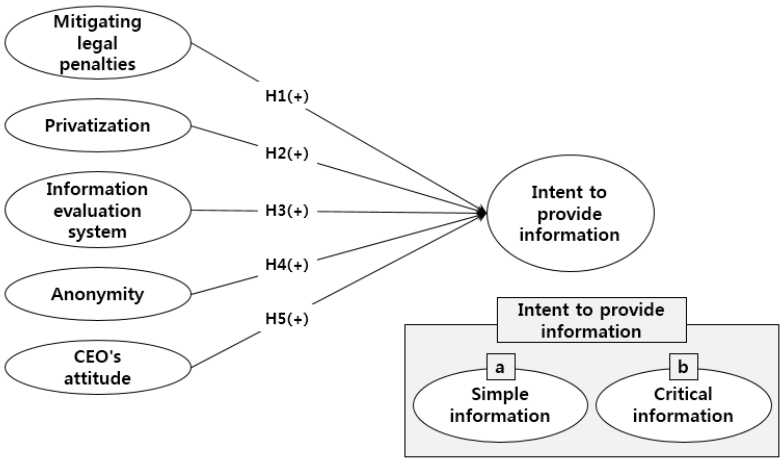

Fig. 1. Research Model

4.2.2 민간화

김민호[57]는 기능의 이전이라는 의미로 민간위탁이라는 단어를 설명했으며, 국가 또는 공공단체가 제공하던 서비스를 민간에게 위탁하여 민간이 행정 주체 또는 행정보조자의 지위에서 서비스를 제공하도록 하는 것을 언급했다. 그리고 최병선[65]은 정부의 개입이 사라져야 경제사회의 운영이 활성화됨을 주장하였다. Ransbotham et al.[58]은 보안취약점에 대하여 시장 기반 메커니즘의 효율성을 검증하였다. 시장기반 메커니즘은 공개된 취약점이 악용될 가능성은 공개 전과 비슷하지만, 악용될 수 있는 시간을 늘리고 전체 악용의 크기를 감소시켰다.

국내 보안컨퍼런스 'NETSEC-KR2015'에서는 사이버위협 정보 공유시스템이 운영기관에서 모든 정보를 독과점으로 수집해 정보를 배부하는 방식보다는 수요자가 원하고 필요한 정보를 자유롭게 선택할 수 있도록 장터 역할을 해주는 것이 바람직하다는 의견이 있었다[30]. 즉 현재 대부분 정부의 주도로 운영되고 있는 정보 공유시스템이 정부의 개입을 최소화하여 참여기관에 의해 자율적으로 운영될 필요가 있음을 뜻한다. 따라서 본 연구에서 설정한 가설은 다음과 같다.

H2a: 사이버위협 정보 공유시스템에 정부의 개입이 최소화 된다면, 간단한 사이버위협 정보 제공의도가 높아질 것이다(+).

H2b: 사이버위협 정보 공유시스템에 정부의 개입이 최소화 된다면, 중요한 사이버위협 정보 제공의도가 높아질 것이다(+).

4.2.3 정보평가체계

Dandurand, Serrano[36], 고성훈[34]은 사이버 보안 정보의 공유를 활성화하기 위해 정보 품질관리 프로세스가 개선되어야 함을 강조하며, 곧 조직간 사이버보안 정보 공유 체계 수용 의도에 영향을 미친다는 것을 보였다. 권유중[35]은 공유정보 품질 및 적시성 확보를 통해 좀 더 나은 품질의 정보를 시기적절하게 민간 측에 부가자료 형태로 제공되어야 함을 보였다. 국내 보안컨퍼런스 'NETSEC-KR2015'에서는 정보의 가치에 대한 객관적 기준이 제시되어야 함을 제안했다. 즉 제공되는 정보의 가치를 평가할 수 있는 시스템이 마련되어야 한다. 이로써 어떤 정보를 공유해야 할지에 대한 기준 정립도 필요하다[30]. 또한 위험별로 수준을 나눠주면 더욱 활용도가 높아질 것이며, 정보가 적절하게 필터링되어 고급정보화 되어야하고 정확성과 신뢰성이 밑받침이 되어야 한다[66]. 즉 정보가 체계적으로 평가됨에 따라 정보의 가치가 결정되고 공유해야할 정보의 기준이 정립될 수 있을 것이다. 그리고 정립된 기준에 따라 정보의 제공 역시 이루어질 수 있을 것이다. 따라서 본 연구에서 설정한 가설은 다음과 같다.

H3a: 제공되는 정보가 체계적으로 평가되면, 간단한 사이버위협 정보 제공의도가 높아질 것이다(+).

H3b: 제공되는 정보가 체계적으로 평가되면, 중요한 사이버위협 정보 제공의도가 높아질 것이다(+).

4.2.4 익명성

권유중[35]은 한국의 사이버위협 정보 공유체계 수립을 위한 고려사항으로 프라이버시 및 기업 평판을 확보하여 유관기관의 책임 하에 충분한 익명화를 적용할 것을 제안하였다.

미국 밴티브사의 정보보호 최고책임자(CSO, Chief Security Officer)는 위협과 보안 문제에 대한 데이터를 공유하기 위해서는 데이터의 완벽한 익명성을 보장하는 것이 중요하다고 강조하였다[67]. 즉 정보 공유시스템 내의 잠재적인 공격자로부터 정보를 제공하는 기업명을 보호할 수 있으며 평판을 확보할 수 있다면 정보 제공의도가 높아질 것이다. 따라서 본 연구에서 설정한 가설은 다음과 같다.

H4a: 사이버위협 정보 공유시스템의 익명성이 보장된다면, 간단한 사이버위협 정보 제공의도가 높아질 것이다(+).

H4b: 사이버위협 정보 공유시스템의 익명성이 보장된다면, 중요한 사이버위협 정보 제공의도가 높아질 것이다(+).

4.2.5 최고경영자 태도

김팔술 등[68], Li, Lin[62], Lin[26]은 최고경영자의 지원이 정보 공유와 관련이 있음을 보였다. 사이버위협 정보 공유시스템에 정보를 제공함으로 인해 받게 될 기업의 평판은 곧 최고경영자의 평판이 될 것이다. 따라서 정보 제공의 활성화를 위해서는 정보를 공유하는 것에 대한 최고경영자의 긍정적인 인식이 필요하며 정보보호에 대한 관심 역시 필요할 것이다. 반대로 말하면, 최고경영자가 공유에 반대한다면 기업의 사이버 위협정보를 제공할 수 없을 것이다. 따라서 본 연구에서 설정한 가설은 다음과 같다.

H5a: 정보보호에 대한 최고경영자의 관심, 지원이 클수록, 간단한 사이버위협 정보 제공의도가 높아질 것이다(+).

H5b: 정보보호에 대한 최고경영자의 관심, 지원이 클수록, 중요한 사이버위협 정보 제공의도가 높아질 것이다(+).

V. 결과 분석

5.1 표본 특성

본 연구에서는 2016년 11월 17일부터 2016년 12월 10일까지 정보보호 관련 실무자들을 대상으로 설문을 실시하였다. 설문은 온라인을 통해 진행되었으며, 총 147부가 수집되었다. 하지만 사이버위협 정보 공유 시스템에 대하여 관심이 없거나 모르는 경우, 경력이 매우 낮은 경우, 불성실한 응답 등을 제외한 결과 43부의 설문지만이 분석에 사용되었다. 또한 설문에 대한 응답은 1점부터 5점까지 선택이 가능한 5점 척도를 이용했으며, '1'에 가까울수록 가장 부정적인 의견을 말하며 '5'에 가까울수록 매우 긍정적인 의견을 뜻한다. 한편 앞서 언급한 바와 같이, 법적처벌 완화, 민간화, 정보평가체계, 익명성은 역채점을 하였다. 유효 표본의 특성은 [표 2]와 같다.

5.2 실증 분석

본 연구에서는 요인적재값을 확인하기 위해 SPSS ver.18.0을 사용했으며 신뢰성, 타당성, 경로분석을 위해 SmartPLS 2.0 패키지의 PLS Algorithm과 PLS Bootstrapping을 이용하였다. SPSS의 요인분석은 요인적재값의 작은계수를 설정할 수 있어서 타당하지 않은 항목들을 가려내기가 쉽다. 그리고 PLS는 표본의 수가 작아도 분석이 가능하며, 표본의 분포가 정규분포에 대한 제약 조건이 없다[69]. PLS는 표본이 최소 30개 이상이면 분석이 가능하며, 표본별 적합한 분석을 위한 최소 표본 수는 가장 복잡한 변수 내에 있는 측정항목 개수의 최소 10배가 되어야 한다[70, 71]. 본 연구에서 가장 많은 측정항목을 가진 변수는 간단한 정보의 제공의도, 정보평가체계, 최고경영자 태도로 모두 4가지의 측정항목을 가지고 있다. 따라서 표본의 수 43이 측정항목4개의 최소 10배 이상을 만족하므로 PLS 분석이 가능하다. Fornell, Bookstein[72], Gefen et al.[71]은 PLS가 내생 변수의 오차를 최소화하는 방식을 채택하고 있고 형성지표에 대한 모형 구축이 가능하다고 하였다. 이러한 이유로 본 연구에서는 SPSS와 PLS 기법을 분석을 사용하였다.

내적일관성은 각 변수들에 해당하는 측정항목들 사이의 관계에 대한 신뢰도를 나타낸다. 즉, 한 변수를 측정하기 위한 항목들이 일관성이 있는지를 보여주는 검증방법이다. 내적일관성의 검증은 일반적으로 PLS의 PLS Algorithm 방식을 이용하여 복합신뢰도(Composite Reliability)와 AVE(Average Variance Extracted) 그리고 Cronbach's Alpha 측정값을 통해 이뤄진다.

분석 결과, 모든 변수들의 AVE는 Fornell,

Table 2. Characteristics of the sample

Category	Classification	Respondent
Gender	Men	42
	Women	1
	Total	43
Age	20's	5
	30's	24
	40's	10
	50's	4
	Total	43
Industry	Governments and Public Institutions	4
	IT	9
	Finance	3
	Etc.	27
	Total	43
Duty	Penetration testing	6
	Security control	8
	CPO(Chief Privacy Officer)	4
	Infrastructure	6
	Other security	19
	Total	43
Career	0-5years	7
	6-10years	22
	11-15years	8
	16-20years	4
	More than 21 years	2
	Total	43

Larcker[73], Chin[69] 등이 주장하는 기준치인 0.5 이상으로 나타났고, 복합신뢰도는 Barclay et al.[74]이 주장하는 기준치인 0.7 이상으로 나타났다. 그리고 Cronbach's Alpha는 Bernstein, Nunnally[75]이 주장한 기준치인 0.6 이상으로 나타났다. 따라서 본 모형은 높은 수준의 내적일관성을 보여주었다.

확인적 요인분석은 구성개념에 대한 요인적재값이 다른 구성개념에 대한 요인적재값보다 커야함을 나타낸다. 즉, 측정 항목에 있어서 다른 구성개념과 의미상 겹치지 않아야 한다. 확인적 요인분석은 종속변수 '정보 제공의도'의 간단한 정보와 중요한 정보에 따라 나누어 분석하였다. 분석결과, 모든 측정 문항이 본 요건을 충족하였다.

집중타당성은 각 변수의 측정항목들과 변수 사이의 관계에 대한 타당성을 나타낸다. 즉, 변수를 측정하기 위한 해당 항목들이 적절하게 구성되었는지를 보여주는 검증 방법이다[76]. 집중타당성은 일반적으로 구성개념에 대한 요인적재값과 t값으로 검증한다. 요인적재값은 SPSS를 통해 분석하였으며 t값은 PLS의 Bootstrap 방식을 이용하였다. Fornell, Larcker[73]은 측정문항의 요인적재값 기준치로 0.7 이상, t값의 기준치로 1.96 이상을 권장하였는데, 본 연구에서 모든 문항의 요인적재값이 0.7 이상, t값이 1.96 이상으로 분석되는 것으로 보아 집중타당성이 있는 것으로 나타났다.

판별타당성은 대각선 축에 표시되는 AVE 제곱근의 가장 작은 값이 다른 구성개념 간의 상관계수 중 가장 큰 값보다 큰가의 여부로 판별타당성을 검증한다[73]. 분석 결과, 간단한 정보인 경우 AVE 제곱

근의 가장 작은 값인 0.864가 구성개념간의 상관계수 중 가장 큰 값인 0.749보다 큰 값을 나타내었다. 따라서 본 모형의 구성개념은 판별타당성이 있음이 검증되었다.

마찬가지로, 중요한 정보인 경우 AVE 제곱근의 가장 작은 값인 0.772가 구성개념간의 상관계수 중 가장 큰 값인 0.577보다 큰 값을 나타내었다. 따라서 본 모형의 구성개념은 판별타당성이 있음이 검증되었다.

Chin, Gopal[77]은 PLS에서 경로모형의 설명력은 분산설명력(Explained Variance)인 R값으로 표현된다고 제시하였다. 분산설명력 역시 종속변수 '정보 제공의도'의 간단한 정보와 중요한 정보에 따라 나누어 분석하였다. 분석결과 간단한 정보의 경우 '정보 제공의도'의 R square 값은 0.14로 Falk, Miller[78]가 제시한 적정 검정력 10%를 상회하였다. 또한 중요한 정보의 경우에도 '정보 제공의도'의 R square 값은 0.16으로 검정력 10%를 상회하였다. 즉 검정력 14%와 16%로, 모형의 독립변수들이 종속변수를 충분히 설명할 수 있음을 나타낸다.

다음으로 경로계수의 유의성을 검증하였다. 경로계수의 유의수준은 일반적으로 0.01, 0.05, 0.1을 기준으로 검증하며, 이는 여러 연구를 통해 확인할 수 있다[28, 79]. 즉 오차 가능성인 유의확률이 1%, 5%, 10% 이내인 가설을 채택하는 것이며 유의확률이 낮을수록 가설이 더 정확하다고 볼 수 있다. 본 연구에서는 표본의 수가 적은 관계로 비교적 오차범위에 여유를 둔 유의수준 0.1 이하인 가설을 기준으로 채택하였다. 한편 유의수준은 경로계수 t값을 통해 확인할 수 있다. 본 연구에서는 표본의 수가 30이상인 43으로 정규분포를 따른다. 따라서 정규분포표에 의해 경로계수 t값의 절댓값이 각각 1.65, 1.96, 2.58 이상이면 유의수준 10%, 5%, 1% 이내에서 통계적으로 유의함을 확인할 수 있다.

경로계수의 유의성을 검증하기 위해 전체표본을

Table 3. Analysis of path coefficient significance (for simple information)

Hypothesis	Variable	Path coefficient	t-value	Result
H1a	Mitigating legal penalties → Intent to provide information	-0.065	0.536	Rejected
H2a	Privatization → Intent to provide information	-0.066	0.979	Rejected
H3a	Information evaluation system → Intent to provide information	-0.141	1.475	Rejected
H4a	Anonymity → Intent to provide information	-0.070	0.485	Rejected
H5a	CEO's attitude → Intent to provide information	0.208	3.476	Adopted

Table 4. Analysis of path coefficient significance (for critical information)

Hypothesis	Variable	Path coefficient	t-value	Result
H1b	Mitigating legal penalties → Intent to provide information	0.157	1.688	Adopted
H2b	Privatization → Intent to provide information	0.164	1.799	Adopted
H3b	Information evaluation system → Intent to provide information	0.220	2.385	Adopted
H4b	Anonymity → Intent to provide information	0.110	1.078	Rejected
H5b	CEO's attitude → Intent to provide information	0.242	3.444	Adopted

이용하여 구조모형에 대한 경로계수를 구하고, PLS에서 제공하는 Bootstrap 방식을 이용하여 경로계수 t값을 산출하였다. 먼저 간단한 정보에 대한 경로를 분석해보면 〔표 3〕과 같다. 경로계수 t값이 1.65보다 크게 나타난 가설 H5a가 유의확률 10% 이하로 채택되었다. 반면 가설 H1a, H2a, H3a, H4a는 경로계수 t값이 1.65보다 작게 나와 유의확률이 10%를 넘어가므로 기각되었다.

그리고 중요한 정보에 대한 경로를 분석해보면 〔표 4〕와 같다. 경로계수 t값이 1.65보다 크게 나타난 가설 H1b, H2b, H3b, H5b가 유의확률 10% 이하로 채택되었다. 반면 가설 H4b는 경로계수 t값이 1.65보다 작게 나와 유의확률이 10%를 넘어가므로 기각되었다.

5.3 사이버위협 정보제공 의도의 변화

본 연구에서는 독립변수들의 개선 전후 정보 제공의도의 변화 차이를 알아보았다. 즉 현재의 정보 제공의도와, 개선이 필요하다고 응답한 사항들이 개선되었을 때 가정 후 정보 제공의도를 측정하였다. 개선 전과 후의 정보 제공의도 측정항목은 동일하다. 응답은 5점척도로, 응답평균 역시 1에 가까울수록 더 부정적이며 5에 가까울수록 긍정적임을 나타낸다. 그 결과 〔표 5〕와 같은 결과가 나왔다.

먼저 개선 전, 간단한 정보와 중요한 정보 모두 '보통'과 가까운 수치를 나타냈다. 하지만, 간단한 정보는 평균이 3.28로 긍정적인 응답을 보였으며 중요한 정보는 평균이 2,56으로 부정적인 응답을 보였다. 개선 후에는 간단한 정보와 중요한 정보 모두 긍정적인 응답을 보였다. 간단한 정보가 중요한 정보보다 긍정적인 응답이 더 높은 것을 볼 수 있다.

제공의도의 변화차이를 살펴보면, 간단한 정보는 개선 전보다 개선 후 0.69만큼 증가했지만 중요한 정보는 1.19만큼 증가했다. 수치상으로 중요한 정보의 의도 변화량이 간단한 정보 의도변화량의 2배 가까이 증가했다. 뿐만 아니라 중요한 정보는 부정적인 응답에서 긍정적인 응답으로 변화했으며 간단한 정보와의 의도 차이가 개선 전 0.72에서 0.22로 감소하였다.

5.4 결과 논의

본 연구의 결과는 다음과 같다. 간단한 정보에 대해서는 오로지 최고경영자의 태도만이 정보 제공의도에 영향을 미쳤다. 반면 중요한 정보에 대해서는 최고경영자의 태도뿐만 아니라 법적처벌 완화, 민간화, 정보평가체계가 영향을 미쳤다. 이는 간단한 정보를 제공하기 위해서는 최고경영자의 태도 외에는 큰 요인이 필요하지 않는 것으로 볼 수 있다. 즉 최고경영자가 정보보호에 대한 관심과 지원이 있고 공유에 긍정적이라면 간단한 정보를 제공하는 것은 어렵지 않은 것으로 보인다. 또한 최고경영자의 태도는 간단한 정보와 중요한 정보에 모두 유의미한 것으로 보아 정보를 제공함에 있어서 꼭 필요한 요소임을 알 수 있다. 그러나 중요한 정보를 제공하기 위해서는 법적처벌 완화, 민간화, 정보평가체계, 최고경영자의 태도의 영향을 받는다. 즉 현재 사이버위협 정보 공유 시스템에 참여하고 있거나 관심이 있는 사람들은 법적처벌과 정부의 관리로부터 자유로워지길 희망하며 기술적으로 더 체계화되고 조직적으로 정보보호에 대한 관심 및 투자가 증가하기를 바란다고 볼 수 있다.

〔표 6〕은 경로계수의 절댓값을 확인하여 유의미한 요인들의 우선순위를 매겨보았다. 최고경영자의 태도는 간단한 정보와 중요한 정보에서 모두 1순위를 차지했다. 최고경영자의 태도는 정보를 제공함에 있어, 반드시 필요할 뿐만 아니라 가장 필요한 요소임을 볼 수 있다. 중요한 정보의 제공의도에서는 최고경영자의 태도에 이어 정보평가체계, 민간화, 법적처벌 완

Table 5. Change in intention to provide information before and after improvement (average response)

Before/After improvement	Intent to provide simple information	Intent to provide critical information	Difference in offer of (simple information - critical information)
Before improvement	3.28	2.56	0.72
After improvement	3.97	3.75	0.22
Difference in Intention to Provide	+ 0.69	+ 1.19	0.5

Table 6. Priority of valid variables

Ranking	Intent to provide simple information		Intent to provide critical information	
	Path coefficient (absolute value)	Variable	Path coefficient (absolute value)	Variable
1	0.208	CEO's attitude	0.242	CEO's attitude
2	-	-	0.220	Information evaluation system
3	-	-	0.164	Privatization
4	-	-	0.157	Mitigating legal penalties

Table 7. Significance probability of valid variables

Hypothesis	Path	t-value
H1b	Mitigating legal penalties → Intent to provide information (critical)	1.688*
H2b	Privatization → Intent to provide information (critical)	1.799*
H3b	Information evaluation system → Intent to provide information (critical)	2.385**
H5a	CEO's attitude → Intent to provide information (simple)	3.476***
H5b	CEO's attitude → Intent to provide information (critical)	3.444***

* $p<0.1$, ** $p<0.05$, *** $p<0.01$.

화의 순으로 필요성이 높다.

기업이 사이버위협 정보 공유 시스템에 참여하고 정보를 제공하기 위해서는 기업 내부적으로 최고경영자의 관심과 긍정적인 인식이 가장 중요하며 그밖에는 정보 공유 시스템이 가지고 있는 문제로서 제공되는 정보의 평가체계 및 분류체계부터 이루어져야 함을 알 수 있다. 또한 중요한 정보를 제공함에 앞서 간단한 정보를 제공하게 함으로써 정보 제공의 참여도를 높이기 위해 기업의 최고경영자에게 정보보호의 중요성을 알리고 사이버위협 정보 공유에 대한 적극적인 홍보가 필요하다.

그리고 정보 제공이 활성화되고 안정화되기 시작하면, 정보 공유 시스템에 대한 정부의 개입을 줄이고 법적 개선을 위한 노력을 해야 할 것이다.

한편 익명성은 간단한 정보, 중요한 정보에 대해 모두 기각된 것으로 보아 사이버위협 정보 공유 시스템에서 정보를 제공하는 데에 있어서 크게 관련이 없는 것으로 볼 수 있다.

본 연구에서는 유의수준 기준을 0.1로 하여 채택된 가설들의 유의확률에 차이가 있다. 유의확률이 1%인 경우에는 t값이 2.58 이상이며, 유의확률이 5%인 경우에는 경로계수 t값이 1.96이상이다. 그리고 유의확률 10%인 경우에는 경로계수 t값이 1.65 이상이어야 한다.

정보 제공에 있어 반드시, 가장 필요한 요소인 최고경영자의 태도는 유의확률이 1% 이하가 나왔다. 그리고 정보평가체계는 유의확률이 5% 이하이며 법적처벌 완화와 민간화는 10% 이하임을 확인할 수 있다[표 7].

마지막으로, 본 연구에서는 설문 응답평균을 통해 독립변수들의 개선 전후 정보 제공의도의 변화 차이를 알아보았다. 정보 공유 시스템이 많이 개선될수록 간단한 정보보다 중요한 정보 제공의도의 증가폭이 올라가며 기업에서 제공하는 정보의 종류와 수준이 높아질 수 있음을 짐작 할 수 있다.

VI. 결 론

김상오, 윤선희[80], 송장근, 김광석[81], 김문중, 권기환[82], Javadi et al.[83], Lin[26]은 지식 및 정보 공유가 개인 또는 조직의 성과에 긍정적인 영향을 미친다고 주장하고 있다. 또한 Gordon et al.[2], Gar-Or, Ghose[4]는 사이버 보안 정보의 공유가 경제적으로 매우 효과적임을 강조하고 있다. 이렇게 정보를 공유하는 것은 다양한 측면에서 이익이 될 수 있음을 알 수 있다.

본 연구에서는 사이버위협 정보를 공유하기 위해, 사이버위협 정보의 중요도에 따라 공유시스템에 정보

를 제공하는 요인을 살펴보았다. 그 결과 간단한 정보의 제공과 중요한 정보의 제공 모두 최고경영자의 태도의 영향을 가장 크게 받았다. 그리고 중요한 정보는 최고경영자의 태도 다음으로 정보평가체계, 민간화, 법적 처벌 완화의 순으로 영향을 받았다. 또한 요인들의 개선 전/후 정보 제공의도의 변화를 살펴봤을 때, 정보 공유 시스템이 점점 개선될수록 간단한 정보보다 중요한 정보 제공의도의 증가폭이 올라가며 기업에서 제공하는 정보의 질이 높아질 수 있을 것으로 확인되었다.

본 연구는 다음과 같은 시사점을 제공한다. 학술적으로는 '정보 제공'에 초점을 맞춤으로써 실질적인 정보 공유의 활성화 요인을 확인하였다. 정보 공유 참여자는 정보를 제공하는 입장과 활용하는 입장으로 나눌 수 있는데, 정보 공유가 활성화되기 위해서는 무엇보다 정보를 제공하는 것이 뒷받침 되어야하기 때문이다. 또한 기존의 연구들과 다르게 제시된 요인으로, '민간화'를 통해 정보제공 의도를 높일 수 있음을 보였다. 비록 현재는 정보 공유의 초기단계여서 정부의 개입이 부득이하겠지만, 향후에는 철저히 기업과 민-관의 공유가 정부로부터 독립되어 자율적으로 이루어져야할 것이다.

실무적으로는 첫째로, 국내 사이버위협 정보 공유 시스템의 문제점을 파악할 수 있으며 개선해야할 우선순위를 제공한다. 그리고 이에 따라 개선 방안을 마련할 수 있을 것이다. 둘째로, 단순히 정보 제공 요인만을 파악한 것이 아니라 실제 기업에서 정보 공유 시스템의 개선 전과 후에 정보 제공의도의 변화를 파악할 수 있다.

본 연구에는 몇 가지 한계점이 있다. 먼저, 표본수가 부족하여 정보 공유시스템의 종류별로 정보 제공 요인을 자세하게 파악하지 못하였다. 현재 시스템별 특징과 개선되어가는 현황에 따라 요인이 다르게 작용할 수 있다. 그리고 업종별로 정보 제공의도와 요인을 파악하지 못했다. 기업의 업종에 따라 역시 요인이 다르게 작용 할 수 있을 것이다. 따라서 향후 표본을 더 수집하고 특징을 분류하여 요인을 분석해볼 필요가 있다.

궁극적으로, 사이버위협 정보 공유의 활성화를 위해 국내 정보 공유 시스템의 운영 현황을 주기적으로 보고할 필요가 있다. 미국과 일본의 경우, 홈페이지 등을 통해 주기적으로 정보 공유 시스템의 운영 현황을 보고하고 있다. 국내에서는 C-TAS의 경우, 분기별로 정보 공유 세미나가 열리지만 보다 더 체계적이고 정확한 정보를 제공하는 보고가 필요하다. 또한 적극적인 홍보를 통해 사이버위협 정보 공유 시스템의 존재부터 알릴 필요가 있다. 운영 현황에 대한 정확한 정보가 제공되어야 국내 시스템의 활성화에 대해 보다 더 정확한 연구가 진행될 수 있을 것이다.

References

[1] G.B. White and D.J. DiCenso, "Information sharing needs for national security," Proceedings of Hawaii International Conference on System Sciences, IEEE, 2005.

[2] L.A. Gordon, M.P. Loeb and W. Lucyshyn, "Sharing information on computer systems security: An economic analysis," Journal of Accounting and Public Policy, 22(6), 461-485, 2003.

[3] E. Gal-Or and A. Ghose, "The economic consequences of sharing security information," In Economics of Information Security, 95-104, Springer US, 2004.

[4] E. Gal-Or and A. Ghose, "The economic incentives for sharing security information," Information Systems Research, 16(2), 186-208, 2005.

[5] Chul-soo Lee, "National security system for countering information incidents," Review of Korea Institute of Information Security and Cryptology, 15(1), 33-40, 2005.

[6] Dong-jin Kim and Sung-je Cho, "An analysis of domestic and foreign security vulnerability management systems based on a national vulnerability databases," Internet and Information Security, 1(2), 130-147, 2010.

[7] Oh-jun Yoon, Kwang-yong Bae, Jae-hong Kim, Hyung-jun Seo and Yong-tae Shin, "A study on measures for strengthening cybersecurity through analysis of cyber-attack response," Convergence Security Journal, 15(4), 71-78, 2015.

[8] D.F. Vázquez, O.P. Acosta, C. Spirito, S. Brown, and E. Reid, "Conceptual framework for cyber defense information shar-

ing within trust relationships," Proceedings of International Conference on Cyber Conflict, IEEE, 2012.
〔9〕 Boannews, "Just talk about a lot of information, why it is not working properly", 20 June 2016.
〔10〕 Duke-hoon Jeong and Hyoung-seop Shim, "A study on information sharing system for information application on the public institutions," Journal of Finance & Knowledge Studies, 3(1), 223-235, 2005.
〔11〕 Gu Kim, "A study on weights of intentions to share information among officials by AHP," Korean Society of Public Administration, 15(3), 207-228, 2004.
〔12〕 Sang-yun Han and Hyun-min Kang, "Enhancing information sharing activities in local government," The Korea Local Administration Review, 21(1), 97-122, 2007.
〔13〕 Dong-wook Kim and Kun Yoon, "A study on information sharing: focusing on creative commons license," Journal of Koran Association for Regional information Society, 13(4), 53-74, 2010.
〔14〕 L. Caffrey, Information Sharing between & within Governments, The International Council for Technology in Government Administration, London, 1998.
〔15〕 S.S. Dawes and L. Prefontaine, "Understanding new models of collaboration for delivering government services," Communications of the ACM, 46(1), 40-42, 2003.
〔16〕 J.R. Gil-Garcia, C. Schneider, T.A. Pardo and A.M. Cresswell, "Interorganizational information integration in the criminal justice enterprise: preliminary lessons from state and county initiatives," Proceedings of Hawaii International Conference on System Sciences, IEEE, 2005.
〔17〕 R.M. Grant, "Toward a knowledge-based theory of the firm," Strategic Management Review, 17(52), 109-122, 1996.
〔18〕 Cheol-u Lee, Proposal for Cyber Threat Information Sharing Act, 2015.
〔19〕 Jae-eun Lee and Gyum-hun Kim, "An analysis of the information sharing determinants in the NDMS," Modern Society and Administration, 17(1), 155-185, 2007.
〔20〕 Tong-hee Park and Young-ran Hyun, "Sharing and utilization of knowledge and information among nonprofit organizations through public web portal: case study of culture portal of national knowledge information system," Modern Society and Administration, 21(3), 1-33, 2011.
〔21〕 D. Liu, Y. Ji and V. Mookerjee, "Knowledge sharing and investment decisions in information security," Decision Support Systems, 52(1), 95-107, 2011.
〔22〕 G.W. Bock and Y.G. Kim, "Breaking the myths of rewards: An exploratory study of attitudes about knowledge sharing," Proceedings of Pacific Asia Conference on Information Systems, 2001.
〔23〕 G.W. Bock, R.W. Zmud, Y.G. Kim and J.N. Lee, "Behavioral intention formation in knowledge sharing: examining the roles of extrinsic motivators, social-psychological forces, and organizational climate," MIS Quarterly, 29(1), 87-111, 2005.
〔24〕 H.F. Lin, "Effects of extrinsic and intrinsic motivation on employee knowledge sharing intentions," Journal of Information Science, 33(2), 135-149, 2007.
〔25〕 S.S. Chen, Y.W. Chuang and P.Y. Chen, "Behavioral intention formation in knowledge sharing: examining the roles of KMS quality, KMS self-efficacy, and organizational climate," Knowledge-Based Systems, 31(1), 106-118, 2012.

[26] H.F. Lin, "Knowledge sharing and firm innovation capability: an empirical study," International Journal of Manpower, 28(3/4), 315-332, 2007.
[27] K.M. Bartol and A. Srivastava, "Encouraging knowledge sharing: The role of organizational reward systems," Journal of Leadership & Organizational Studies, 9(1), 64-76, 2002.
[28] Jae-sun Wang and Jung-wook Moon, "The attitude on information sharing between public agencies: Focusing on the perception of civil servants in central government," Journal of Korean Association for Regional Information Society, 16(1), 1-34, 2013.
[29] A. Aviram and A. Tor, "Overcoming impediments to information sharing," Alabama Law Review, 55, 231, 2004.
[30] Boannews, "Truth and falsity of information sharing for malicious code and security vulnerability," 25 Apr. 2015.
[31] Oh-jun Yoon, Chang-seob Cho, Jeong-keun Park, Hyung-jun Seo and Yong-tae Shin, "A study on the improvement model for invigorating cyber threat information sharing," Convergence Security Journal, 16(4), 25-34, 2016.
[32] Ae-chan Kim and Dong-hoon Lee, "A study on the priority of requirements for establishing effective cyber-threat information sharing system," Review of Korea Institute of Information Security and Cryptology, 26(1), 61-67. 2016.
[33] Hong-jong Jang, In-jae Park and Jung-hyun Lee, "A study on implementation of information sharing and analysis center for e-government," Proceeding of The 2001 Fall Conference of the Korea Information Processing Society, 2001.
[34] Seong-hun Go, "A study on factors motivating cyber security information sharing for responding preemptively to cyber terror threat of national organizations," Doctoral Dissertation, Soongsil University, 2015.
[35] You-joong Kwon, "Study on North Korea's cyber warfare capability and response strategy of South Korea," Master Dissertation, Korea University, 2014.
[36] L. Dandurand and O.S. Serrano, "Towards improved cyber security information sharing," Proceedings of International Conference on Cyber Conflict, IEEE, 2013.
[37] D. Tosh, S. Sengupta, C. Kamhoua, K. Kwiat and A. Martin, "An evolutionary game-theoretic framework for cyber-threat information sharing," Proceedings of IEEE International Conference on Communications, 2015.
[38] Boannews, "Sharing Security Threat Information ISAC, What is the most urgent reason for the medical field?", 11 Sep. 2016.
[39] Information Sharing Analysis Center, http://www.isac.or.kr/.
[40] KISA(Korea Internet & Security Agency), "Conference on information sharing of cyber incidents," 2014.
[41] KISA(Korea Internet & Security Agency), "Conference on information sharing of cyber incidents," 2015.
[42] HelloT Advanced News, "Pay attention to the fourth industrial revolution platform, 'security'", 30 Sep. 2016.
[43] ISMS / PIMS / G-ISMS certification, http://isms.kisa.or.kr/.
[44] Ministry of Science, ICT and Future Planning, Key Policies for Information Protection, 2016.
[45] Ministry of Government Administration and Home Affairs, Understanding the Personal Information Protection Act: Focusing on What is Different from the Present, 2011.
[46] National Council of ISACs, http://www.n

ationalisacs.org/.
〔47〕 US-CERT(AIS), http://www.us-cert.gov/ais/.
〔48〕 R-CISC, https://r-cisc.org/.
〔49〕 Telecom-ISAC Japan, https://www.telecom-isac.jp/.
〔50〕 IPA, Cyber Information Sharing Initiative (J-CSIP) FY 2012 Activity Report, 2013.
〔51〕 IPA, Cyber Information Sharing Initiative (J-CSIP) Operational Status 〔July-September 2016〕, 2016.
〔52〕 Jung-wook Moon, "Factors of success and failure of information sharing in the public sector: Focused on cognition survey of public officials," Korea Information Society Development Institute, 19(6), 1-17, 2007.
〔53〕 Eun-jeong Kim, "Analyzing the determining factors of electronic information sharing in korean government using the structural equation model," Korean Public Administration Review, 38(4), 125-145, 2004.
〔54〕 R.E. Walton, Up and Running: Integrating Information Technology and the Organization, Boston, MA: Harvard Business School Press, 1989.
〔55〕 NIST, Guide to Cyber Threat Information Sharing, 2014.
〔56〕 HSAC, Info-sharing Final Report, 2005.
〔57〕 Min-ho Kim, "A study on entrusting public service to private sector and privatization of public corporations," Korean Public Land Law Association, 25(1), 267-285, 2005.
〔58〕 S. Ransbotham, S. Mitra and J. Ramsey, "Are markets for vulnerabilities effective?," MIS Quarterly, 36(1), 43-64, 2012.
〔59〕 W. Zhao and G. White, "Designing a formal model facilitating collaborative information sharing for community cyber security," Proceedings of Hawaii International Conference on System Sciences. IEEE, 2014.
〔60〕 ENISA(European Network and Information Security Agency), Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches," 2015.
〔61〕 MNE7(Multi-national Experiment 7), "Information sharing framework outcome 3," Cyber Domain Objective, 2013.
〔62〕 S. Li and B. Lin, "Accessing information sharing and information quality in supply chain management," Decision Support Systems, 42(3), 1641-1656, 2006.
〔63〕 I. Ajzen, "The theory of planned behavior," Organizational Behavior and Human Decision Processes, 50(2), 179-211, 1991.
〔64〕 I. Ajzen, From Intentions to Actions: A theory of Planned Behavior, Berlin Heidelberg: Springer, 1985.
〔65〕 Byeong-seon Choi, "Government-led economic and social administration and administrative ethics," Korean Journal of Public Administration, 39(4), 81-111, 2001.
〔66〕 Etnews, "Cyber threat information 'Need to secure reliability'," 30 Nov. 2015.
〔67〕 ITWorld Korea, "CSO wants to share cyber threat information, but does not want law," 24 Sep. 2015.
〔68〕 Pal-sul Kim, Kwan-soo Hong and Byoung-chan Lee, "Antecedents and relationship effectiveness of information sharing within supply chains," Journal of Business Research, 19(4), 273-307, 2004.
〔69〕 W.W. Chin, "The partial least squares approach to structural equation modeling," Modern Methods for Business Research, 295(2), 295-336, 1998.
〔70〕 Jin-chun Lee, "Structural equation modelling for small samples: component-based SEM vs. covariance-based SEM," Journal of Decision Science, 16(1), 77-95, 2008.
〔71〕 D. Gefen, D.W. Straub and M.C.

Boudreau, "Structural equation modeling and regression : Guidelines for research practice," Communications of the AIS, 4(7), 1-79, 2000.

〔72〕 C. Fornell and F.L. Bookstein, "Two structural equation models: LISREL and PLS applied to consumer exit-voice theory," Journal of Marketing Research, 19(4), 440-452, 1982.

〔73〕 C. Fornell and D.F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error," Journal of Marketing Research, 18(1), 39-50, 1981.

〔74〕 D. Barclay, C. Higgins and R. Thompson, "The Partial Least Squares (PLS) approach to causal modeling: Personal computer adoption and use as an illustration," Technology Studies, 2(2), 285-309, 1995.

〔75〕 I.H. Bernstein and J.C. Nunnally, Psychometric Theory, New York: McGraw-Hill, 1994.

〔76〕 Seo-il Chae, Social Science Research Methodology, B&M Books, 2005.

〔77〕 W.W. Chin and A. Gopal, "Adoption intention in GSS: Relative importance of beliefs," ACM SigMIS Database, 26(2-3), 42-64, 1995.

〔78〕 R.F. Falk and N.B. Miller, A Primer for Soft Modeling, University of Akron Press, 1992.

〔79〕 Dong-man Lee and Hyun-sun Park, "The effects of individual psychological and social motivation factors on information sharing intention through social media," The Journal of Internet Electronic Commerce Research, 11(2), 1-21, 2011.

〔80〕 Sang-oh Kim and Sun-hee Youn, "A study on the effects of preceding factor of information sharing, information sharing and risk information sharing on supply chain performance," Journal of The Korean Production and Operations Management Society, 18(4), 117-146, 2007.

〔81〕 Jang-gwen Song and Gwang-suk Kim, "The performance formation model through information sharing: The effect of asset specificity and information sharing on SCM(Supply Chain Management) performance," Journal of The Korean Production and Operations Management Society, 21(1), 101-121, 2010.

〔82〕 Moon-jung Kim and Gee-Hwan Kwon, "The effect of transactive memory system, knowledge sharing and knowledge application on performance," Korean Corporation Management Review, 63(1), 249-267, 2015.

〔83〕 M.H.M. Javadi, N.D. Zadeh, M. Zandi and J. Yavarian, "Effect of motivation and trust on knowledge sharing and effect of knowledge sharing on employee's performance," International Journal of Human Resource Studies, 2(1), 210-221. 2012.

부록

Table A1. Internal consistency analysis

Dependent variable	Variable	AVE	Composite Reliability	Cronbach's Alpha
Simple Information	Mitigating legal penalties	0.914	0.955	0.906
	Anonymity	0.725	0.911	0.943
	Privatization	0.752	0.858	0.687
	CEO's attitude	0.855	0.959	0.944
	Information evaluation system	0.843	0.955	0.937
	Intent to provide	0.759	0.926	0.895
Critical Information	Mitigating legal penalties	0.809	0.893	0.906
	Anonymity	0.851	0.958	0.943
	Privatization	0.596	0.720	0.687
	CEO's attitude	0.835	0.953	0.944
	Information evaluation system	0.832	0.952	0.937
	Intent to provide	0.863	0.950	0.920

Table A2. Confirmatory factor analysis

Metrics	Factor loading value						
	1	2	3	4	5	6	7
(Simple_Info)Intent_1	-0.054	-0.076	0.208	0.887	0.133	0.038	0.302
(Simple_Info)Intent_2	0.118	-0.235	0.089	0.740	0.314	0.212	0.211
(Simple_Info)Intent_3	-0.053	-0.048	0.004	0.868	0.148	-0.041	0.162
(Simple_Info)Intent_4	-0.192	-0.113	0.123	0.823	0.142	0.162	0.137
(Ciritical_Info)Intent_1	0.072	0.108	0.158	0.121	0.854	0.184	0.127
(Ciritical_Info)Intent_2	0.135	-0.111	0.034	0.322	0.869	0.037	0.204
(Ciritical_Info)Intent_3	0.057	-0.163	0.068	0.334	0.881	0.096	0.062
CEO's attitude_1	-0.020	-0.131	0.935	0.129	-0.008	-0.033	-0.056
CEO's attitude_2	-0.023	-0.139	0.913	0.103	-0.077	-0.009	-0.089
CEO's attitude_3	-0.222	-0.197	0.876	0.108	0.153	-0.074	-0.377
CEO's attitude_4	-0.022	0.004	0.896	0.059	0.212	0.044	-0.006
Mitigating legal penalties_1	0.793	0.211	-0.140	-0.217	0.199	0.323	0.203
Mitigating legal penalties_2	0.864	0.206	-0.106	-0.147	-0.025	-0.134	-0.016
Privatization_1	0.199	0.833	-0.082	-0.269	0.349	0.295	0.307
Privatization_2	0.296	0.702	-0.013	-0.057	0.049	0.198	0.013
Anonymity_1	0.023	0.153	0.040	0.032	0.104	0.893	0.059
Anonymity_2	0.031	0.052	-0.085	0.200	-0.058	0.894	0.082
Anonymity_3	0.028	0.054	-0.009	-0.129	0.108	0.884	0.067
Anonymity_4	0.025	0.234	-0.028	-0.014	0.067	0.879	0.124
Information evaluation system_1	0.173	0.072	-0.068	-0.075	-0.044	0.056	0.920
Information evaluation system_2	0.144	0.094	-0.088	-0.140	-0.050	0.016	0.911
Information evaluation system_3	-0.010	-0.058	-0.164	-0.092	-0.090	-0.128	0.780
Information evaluation system_4	0.207	-0.048	-0.121	-0.034	-0.049	-0.039	0.901

Table A3. Intensive feasibility analysis

Variable	Metrics	Factor loading value	t-value (Simple/Critical)
Intent to provide (Simple_Info)	Simple_Info_1	0.887	59.84
	Simple_Info_2	0.740	17.21
	Simple_Info_3	0.868	21.90
	Simple_Info_4	0.823	25.10
Intent to provide (Critical_Info)	Critical_Info_1	0.854	28.10
	Critical_Info_2	0.869	53.45
	Critical_Info_3	0.881	79.07
CEO's attitude	CEO's attitude_1	0.935	59.75 / 7.088
	CEO's attitude_2	0.913	36.96 / 6.506
	CEO's attitude_3	0.879	75.59 / 8.693
	CEO's attitude_4	0.89	44.21 / 9.632
Mitigating legal penalties	Mitigating legal penalties_1	0.793	17.34 / 3.987
	Mitigating legal penalties_2	0.864	22.83 / 3.352
Privatization	Privatization_1	0.833	7.48 / 3.895
	Privatization_2	0.702	5.04 / 2.596
Anonymity	Anonymity_1	0.893	4.44 / 8.288
	Anonymity_2	0.894	2.98 / 8.833
	Anonymity_3	0.884	4.52 / 9.135
	Anonymity_4	0.879	4.77 / 10.119
Information evaluation system	Information evaluation system_1	0.920	29.72 / 5.582
	Information evaluation system_2	0.911	43.30 / 5.768
	Information evaluation system_3	0.780	14.14 / 5.575
	Information evaluation system_4	0.901	28.43 / 5.753

Table A4. Discriminant validity analysis (simple information)

Variable	Intent to provide (Simple_Info)	Mitigating legal penalties	Anonymity	Privatization	CEO's attitude	Information evaluation system
Intent to provide (Simple_Info)	0.871	0	0	0	0	0
Mitigating legal penalties	-0.221	0.956	0	0	0	0
Anonymity	-0.187	0.572	0.851	0	0	0
Privatization	-0.215	0.358	0.320	0.867	0	0
CEO's attitude	0.277	-0.217	-0.093	-0.165	0.925	0
Information evaluation system	-0.270	0.340	0.282	0.492	-0.267	0.918

Table A5. Discriminant validity analysis (critical information)

Variable	Intent to provide (Critical_Info)	Mitigating legal penalties	Anonymity	Privatization	CEO's attitude	Information evaluation system
Intent to provide (Critical_Info)	0.929	0	0	0	0	0
Mitigating legal penalties	0.164	0.899	0	0	0	0
Anonymity	0.159	0.577	0.923	0	0	0
Privatization	0.139	0.360	0.238	0.772	0	0
CEO's attitude	0.233	-0.201	-0.102	-0.120	0.914	0
Information evaluation system	-0.144	0.303	0.255	0.358	-0.243	0.912

〈저자소개〉

김 하 영 (Ha-Young Kim) 정회원
2015년 2월 : 충북대학교 정보통신공학부 학사
2017년 2월 : 충북대학교 정보보호경영학과 석사
2017년 3월~현재: 싸이버원 컨설팅사업본부 정보보호컨설턴트
〈관심분야〉 정보보호 컨설턴트, 정보보호 인력, 사이버 정보 공유

김 태 성 (Tae-Sung Kim) 종신회원
1997년 2월: KAIST 산업경영학과 박사
1997년 2월~2000년 8월: 한국전자통신연구원 정보통신기술경영연구소 선임연구원
2005년 1월~2006년 2월: Univ. of North Carolina at Charlotte 방문교수
2010년 7월~2012년 7월: Arizona State University 방문연구원
2000년 9월~현재: 충북대학교 경영정보학과 교수, 보안경제연구소장, 보안컨설팅융합전공 주임교수, 일반대학원 정보보호경영전공 주임교수, 국가정보원 보안관리실태평가 자문 및 평가위원, 행정안전부 전자정부 민관협력포럼 자문위원, 국방부 사이버보안 자문위원, ISMS/PIMS 인증위원회 위원
〈관심분야〉 정보통신과 정보보호 분야의 경영 및 정책 의사결정