https://doi.org/10.33778/kcsa.2019.19.2.059

위험커뮤니케이션 이론에 기반을 둔 정보공유 플랫폼 구조화 연구

유 지 연*, 박 향 미**

요 약

오늘날 IoT(Internet of Things)와 CPS(Cyber-Physical System) 등의 기술 발전으로 사이버와 물리적 차원의 경계가 무너지는 융합 환경이 등장하였다. 물리-사이버 간의 영향관계가 강화되면서 보다 다양하고 복잡한 형태의 위험들이 나타나고 있으며 단일 조직 혹은 정부의 자체 대응만으로는 온전히 대응해내기 어려운 상황이 되고 있다. 이로 인해 정보 공유에 기반을 둔 협력적 대응 및 적극적 방어 체계 강화를 필요로 하고 있다. 그리고 다양한 주체에 적합한 정보가 공유되고 자동 대응 할 수 있는 체계로의 전환이 요구되고 있다. 이에 본 연구는 현재의 위협 정보 수집 및 공유 중심의 체계를 개선하고 적극적이고 실질적인 사이버 방어 태세가 유지될 수 있는 정보 공유 체계 구조화를 시도하고자 한다. 이를 위해 안전 분야에서 활용되는 위험 커뮤니케이션 이론을 차용하고 행동 중심의 보안 프로세스 모델을 결합하여 새로운 플랫폼을 제안한다.

A Study on Structuring of Information Sharing Platforms Based on Risk Communication Theory

Ji-Yeon Yoo*, Hyang-Mi Park**

ABSTRACT

In this day and age physical and cyber boundaries have converged due to the development of new technologies, such as the Internet of Things (IoT) and the Cyber Physical System (CPS). As the relationship between physical system and cyber technology strengthens, more diverse and complex forms of risk emerge. As a result, it is becoming difficult for single organi zation or government to fully handle this situation alone and cooperation based on information sharing and the strengthening of active defense systems are needed. Shifting to a system in which information suitable for various entities can be shared and automatically responded to is also necessary. Therefore, this study tries to find improvements for the current system of threat information collecting and sharing that can actively and practically maintain cyber defense posture, focusing parti cularly on the structuring of information sharing platforms. To achieve our objective, we use a risk communication theory from the safety field and propose a new platform by combining an action-oriented security process model.

Keywords : Information Sharing Platform, Risk Communication Theory, SMCRE Model

접수일(2019년 6월 3일), 수정일(2019년 6월 24일), 게재확정일(2019년 6월 30일)

* 상명대학교 융합공과대학 휴먼지능정보공학과(주저자)
** 한국IT법연구원(교신저자)

1. 서 론

최근 기술이 발달함에 따라 기술로 인한 위험이 사회를 위협하는 위험사회의 징후가 나타난다. 특히 한국은 정보기술의 급진적인 발전으로 사회 전반에 걸쳐 기술의 영향력이 강화되었기 때문에 오히려 기술에 대한 불신 및 불안이 강조된다. 더욱이 오늘날 기술시스템에 의해 발생하는 위험은 더욱 복잡해지고 새로운 형태로 나타난다. 컴퓨터가 보급된 이래로 사이버 위험은 다양한 형태로 변화하고 발전하고 있으며 개인 및 기업의 컴퓨터에서 정부행정시스템 등 국가주요기반시설에까지 침해 영역을 확장하고 있다.[3][1)]

이러한 사이버 위험을 관리하고 대응하기 위해서는 정부의 정책적 노력만으로는 한계가 있으며 민간영역과의 상호 협력을 통한 위험 관리가 요구되고 있다. 그리고 상호 협력은 관련 정보 공유가 전제되어야 가능하므로 정보 공유는 사이버 위험 대응책에 있어 필수불가결한 요건이 되었다.

한편 사이버 공간과 현실 공간이 연결된 융합환경이 되면서 정보 공유 패러다임이 변화하고 있다. 현실 공간에 대한 정보기술의 영향력이 증가하고 사이버 공간과 현실 공간 간의 연계가 심화됨에 따라 사이버 위험이 다면적이고 복합적인 형태로 나타나고 있으며[2)] 사이버 위험으로 인한 현실 공간의 피해 또한 확대되고 있다.[3)] 이로 인해 사이버 위험 대응책 패러다임이 사이버 위협 대응 중심에서 현실 공간의 빠른 복구를 위한 회복탄력성(Resilience) 중심으로 변화하였다. 그리고 사회 전체시스템 차원에서 적극적인 사이버 방어(Active Cyber Defense)를 요구하고 있다. 이에 위험 및 위협 정보의 수집 및 공유 활동에 중점을 둔 기존의 정보공유 체계는 수집 및 분석된 정보에 기반을 두어 직접적인 행동 및 의사결정이 가능한 수준의 정보 공유 체계로의 확장을 필요로 한다.

한국은 사이버 위험에 대응하기 위해 공공 영역과 민간 영역에서 사이버 위협 정보를 수집・분석・공유하는 시스템을 2015년부터 구축・운영하고 있다. 다만 위협 정보 공유 활동에 초점이 맞추어져 있어 패러다임 변화로 요구되는 회복탄력성(Resilience)과 적극적인 사이버 방어(Active Cyber Defense)를 위한 체계로의 개선이 요구된다.

전술한 바와 같이 사회 전체시스템적 차원의 적극적인 방어를 요구하는 정보 공유의 패러다임 변화에 따라 단순한 정보의 수집 및 위협 정보의 공유 차원에서 더 나아가 의사 결정을 지원하고 자동적 대응 체계로의 확대가 필요하다. 특히 일차원적의 단순한 대응이 아니라 대응 활동의 일환으로 결정된 의사 결정에 대한 잠재적 영향력을 충분히 고려하여 정보를 공유해야 한다.

이에 본 연구는 시스템 사이버 위험[4)] 개념에 기초하여[16] 위험을 보다 효과적으로 대응하기 위해 등장한 위험커뮤니케이션 이론에 기반을 둔 플랫폼을 제안하고자 한다. 새로 발생하는 위험은 전문가뿐만 아니라 관련된 모든 이해관계자와 공유되어야 하므로 위험커뮤니케이션 이론과 행동 중심의 모델을 분석하여 위험에 대한 대응 행동,

1) 사이버 위험은 1988년 모리스 웜으로 인한 컴퓨터에 대한 공격을 시작으로 2007~2008년 에스토니아의 주요기반시설을 대상으로 DDoS 공격을 펼치는 Stuxnet 등의 강제적 공격 및 사이버 간첩 활동과 2013년 트위터 등의 SNS 해킹, 거짓 뉴스를 통해 주식 시장에 혼란을 야기하는 등 그 종류와 범위가 다양해지고 있다.

2) 이를 시스템 위험(Systemic Risk)이라 한다. 시스템 위험은 전체 시스템의 고장을 의미하며 다중변수, 종속성, 상호의존성으로 인해 예상하지 못하는 결과로 이어지는 것을 포함한다. 즉, 단순히 개별 요소의 고장이 아닌 전체 시스템의 고장으로 인한 위험을 의미한다.[15]

3) 2018년 한국에서 발생한 KT 통신장애사태는 화재사고로 인한 사고로 물리적 피해나 장애로 인해 기술적 차원에서 문제가 발생한 사례이다. 해당 사고로 인해 KT는 천 여 명 이상의 고객이 탈퇴하였고, 중앙일보 추산 약 300억 원 규모의 보상금이 소모될 것으로 보인다.

4) 시스템 사이버 위험(Systemic Cyber Risk)은 시스템 위험(Systemic Risk)에 기초하여 등장한 개념으로 국지적인 사이버 위험이 아닌 전체적인 사이버 위험을 말한다. 사이버 사고나 이상 반응으로 인해 주요기반시설 생태계의 개별 구성 요소가 서비스의 지연, 거부, 파괴, 손실과 같은 영향을 끼쳐 공공 안전, 경제, 안보 등의 생태계에 심각한 부작용을 초래하는 것을 의미한다.[17]

즉 방어적 차원의 대응을 위한 정보 공유 플랫폼을 수립하였다.

이에 본 연구의 2장은 관련하여 현재 진행된 연구와 위험커뮤니케이션 이론에 대하여 논의를 진행하며, 3장은 이에 기반을 둔 정보공유플랫폼을 제안하고, 4장에서 마무리를 짓는다.

2. 이론적 배경

사이버 위협이 복잡화되고 영역의 경계가 허물어짐에 따라 위협의 대상 범위가 확장되었다. 기존의 위험에 대한 대응활동으로서의 정보공유체계는 국가의 주도로 운영되었으나 위협이 시스템 사이버 위험(Systemic Cyber Risk)의 특성을 가지면서 정보공유의 대상이 확대되었다. 이에 본 연구는 시스템 사이버 위험에 대한 대응활동 차원의 정보공유플랫폼을 제안하기에 앞서, 사이버 보안 정보 공유와 관련한 기존의 선행된 연구를 분석하고 발전하는 위험을 명확히 인식하고 정보 공유의 당위성을 마련하고자 위험커뮤니케이션 이론을 살펴본다.

2.1 선행연구 분석

지금까지 국내에서 사이버 보안 차원의 정보 공유에 대한 연구가 꾸준히 진행되었다. 정보 공유는 점차 지능화되고 고도화되는 사이버 공격의 효과적인 예방 수단으로 인식되어 국제적 차원에서 제각기 구축되었다.[9] 사이버 위협의 예방 차원으로 등장한 정보공유는 대비 및 대응 활동을 위한 정보 수집 및 공유를 중심으로 운영되나, 공유 과정에서 민감 정보의 유출 또는 사이버 위협 정보의 오남용 등 부작용의 발생 가능성이 있다.[8] 따라서 정보의 표현방식이나 수집 방법, 전송 규격과 같은 기술적 요구사항보다 관련 법적 근거를 마련하는 등의 의사결정을 지원하는 정책적 요구사항이 중요하다.[8] 그러나 국내의 연구는 여전히 사이버 환경에서 발생하는 기술적 위험에 초점을 맞추고 기술 정보 중심의 공유체계 수립 및 공유 활동의 활성화를 위해 진행되었다.[12][10]

기술의 발전으로 고도화되는 사이버 위협은 개인의 일상과 사회, 그리고 국가까지 위협하며 그 영향력을 확대하였다. 공격이 복잡화, 다면화됨에 따라 더 이상 개인 또는 개별 조직적 차원의 대응은 효과가 미미하다. 이러한 변화는 위험의 대책으로 운용되는 정보공유체계에 대한 패러다임의 변화를 야기한다.[18][19] 기존의 정보공유체계가 적극적인 방어를 중심으로 정보의 수집 및 공유에 초점을 맞추었다면, 확장된 정보공유체계는 수집된 정보의 분석을 기반으로 의사결정의 지원 및 정보의 차별적 공유 등의 활동으로 구성된다. 특히 정보기술이 기반시설에 적용됨에 따라 사이버 물리 시스템(CPS)의 보호가 요구되며 오프라인 및 온라인과 더불어 CPS에 대한 보호의 필요성이 증가하여 융합적인 관점에서 위험에 대응해야 한다.

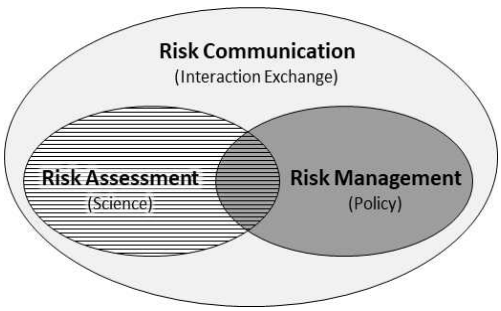
이에 본 연구는 융합 환경의 위험에 대응하기 위해 정보의 공유 활동보다 공유정보의 활용에 초점을 맞춘 강화된 정보공유체계가 필요함을 인지하였다. 이에 위험커뮤니케이션 이론을 기반으로 순환적인 정보공유체계에 대해 논의하고자 한다.

2.2 위험커뮤니케이션 이론

IT가 일상화됨과 별개로 모든 사람이 발전된 과학과 산업기술을 즉각적으로 이해하진 않는다. 특히 위험의 인식은 객관적 사실의 이해보다 개인과 사회문화의 환경을 통한 주관적 이해를 통해 이루어지므로 새로운 기술로 인한 위험 지식은 전문가들에 의해 생산되고 미디어를 통해 일반인들에게 전달된다.[15] 이 과정에서 전문가와 일반인들 간의 위험을 인식하는 범위 및 기준에서 차이가 발생하기 때문에 개인에게 정확한 정보를 제공하기 위해 위험커뮤니케이션 이론이 등장하였다.

위험커뮤니케이션은 일반적으로 위험의 평가와 관리 과정을 포함한다((그림 1) 참조). 위험 평가는 기술 기반의 자동화된 평가체계를 의미하며, 위험 관리는 정책적 차원에서의 관리를 의미한다.

따라서 위험커뮤니케이션은 평가된 위험을 정책적으로 다루고 이를 상호 교환함으로써 개선하기 위해 존재한다. 이런 관점에서 위험커뮤니케이션 이론은 정보공유 대상의 확장 및 의사결정의 지원과 자동화된 대응 체계 구축을 요하는 정보공유 패러다임의 변화에 적합하다.



(그림 1) Relationship between Risk Assessment, Risk Management and Risk Communication

지금까지 위험을 공유하기 위해 수립된 위험커뮤니케이션 이론에는 선형(Liner), 대화형(Interactive), 통신형(Transaction) 등의 다양한 모델이 존재한다. 본 연구에서는 위험커뮤니케이션 이론의 모델 중 가장 기본적이며 영향력이 있는 라스웰(G. Lassewll)의 선형모델인 SMCRE(Source, Message, Channel, Receiver, Effect)모델(1948)을 선정하여 이를 기반으로 정보공유를 위한 플랫폼을 수립하고자 한다.[13]

라스웰의 SMCRE 모델은 위험커뮤니케이션 프로세스[5]에서 정보의 수신자 특히 일반 대중이 정보를 받아들일 때 영향을 미치는 요인이 무엇인지를 확인하기 위한 가장 보편화된 모델이다.[1] SMCRE 모델은 위험커뮤니케이션의 구성요인으로 정보원(source), 메시지(message), 채널(channel), 수용자(receiver), 효과(effect) 등을 설정하였다.

다만 본 모형은 약 70여 년 전에 개발된 위험커뮤니케이션 모형(1948)으로 변화하는 기술에 따른 위험의 변화를 모두 고려하지 못한다. 따라서 본 연구는 이 SMCRE 모델을 기준으로 현대 사이버 위협에 대응하기 위한 정보 공유 플랫폼을 제안하고자 한다. 그에 앞서 라스웰 이후에 등장한 다양한 관련 모델 이론을 살펴보았다.

2.3 행동 중심의 보안 모델 분석

발전하는 기술과 이에 따른 위험에 있어 성공적인 대응을 위해 행동 중심의 대응 체계 마련이 요구된다.[7] 특히 보안 운영 차원의 사이버 위협 대응을 위해 다양한 모델이 수립되었으나 실제 운영을 위한 체계나 플랫폼은 존재하지 않는다.[7] 본 연구는 이러한 차원에서 정보 공유 플랫폼의 수립을 위해 기존의 사이버 보안 행동 모델을 분석하고자 한다. 정보나 조직의 상황 및 상태의 분석을 위해 Intelligence Cycle, OODA Loop, F3EAD, D3A, RAIM Framework 등의 프로세스 중심 모델과 ATT&CK, Diamond Model for Intrusion Analyze 등의 분석 기준 모델을 선정하였다.

2.3.1 프로세스 중심 모델

① Intelligence Cycle

일반적인 인텔리전스 사이클(Intelligence Cycle)은 4단계 혹은 5단계(Direction, Collection, Analysis and/or Processing, Dissemination)로 이루어진 순환구조의 프로세스이다. 인텔리전스 사이클은 정보를 처리하여 관련성 있고 실행 가능한 정보(Intelligence)로 전환시키는 데에 효과적이다.

Direction 단계는 비즈니스에 핵심적인 사이버 보안 위협(APT 등)의 수준을 식별하고, Collection 단계는 조직 위협정보팀의 내부 대응 사례에서 데이터를 수집, 외부 위협정보 제공업체의 제공데이터와 통합한다. Analysis 단계는 전략적 기간(6개월에서 1년) 동안 수집한 데이터를 융합 및 분석하고, Dissemination 단계는 조직을 목표로 삼은 특정 APT 위협에 대한 광범위한 위협 정보를 관련 커뮤니티로 전달한다.

5) 위험커뮤니케이션(Risk Communication)은 정보의 일방적인 전달 또는 일회적인 사건이 아닌, 시간의 경과에 따라 송신자와 수신자가 위험정보를 서로 주고받는 복잡한 과정이다.

② OODA Loop

존 보이드(John Boyd)에 의해 제시된 OODA Loop는 Observe, Orient, Decide, Act 등의 전략적 도구로 구성된다. 해당 모델은 조직이 OODA 루프를 경쟁자보다 신속하게 수행하는 것을 성공으로 보는 근본 전제를 가진다. 세계 각국과 테러 조직이 군사 전략의 일환으로 OODA 루프를 사용하며, 기업들이 경쟁이 매우 치열한 경제에서 번창하기 위한 목적으로 활용한다.

OODA 루프의 첫 번째 Observe 단계는 환경, 사람, 경쟁자, 환경에 관한 데이터 수집단계이다. 다만 데이터가 없으면 정교한 분석을 수행하기 어렵다. Orientation 단계는 수집된 데이터에 상황을 적용하여 상황 인식 데이터를 만든다. 모든 개인은 자신의 환경과 경험을 이해하는 방식이 다르기 때문에 각각의 상황에 맞는 분석이 필요하다. Decide 단계는 올바른 결정을 내리기 위해 수집된 데이터를 신중하게 평가한다. 상황에 따라 데이터를 이해하면서 행동 요령을 파악하고 그 잠재적 결과를 평가한다. Act 단계는 여러 옵션을 개발하고 평가한 후에 결정을 실현한다.

③ D3A(Detect, Deliver, Decide, Assess)

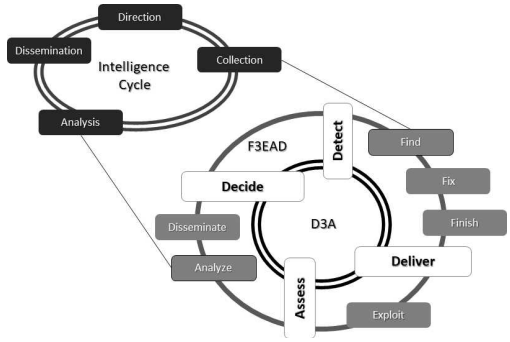
D3A방법론은 일반적으로 구성원이 공격 옵션을 사용하여 목표를 달성할 수 있는지 결정하는 데 도움을 주기 위해 사용되는 군사적 차원의 의사결정방법론이다.[5] 따라서 D3A는 작업 그룹을 대상으로 효과를 평가하기 위한 요구사항을 결정에 도움을 준다. Detect, Deliver, Decide, Assess로 단계가 구성된다.

④ F3EAD(Find, Fix Finish, Exploit, Analyze and Disseminate)

F3EAD 모델은 드론 공격 및 특수 부대 작전과 같은 치명적인 행동을 야기하는 작전 상황에서 서구 군대 내에서 사용된다.[5]

Find 단계는 본질적으로 상대의 목표물을 식별하기 위한 단계로, "누가, 무엇을, 언제, 어디서, 왜"와 같은 질문을 사용하여 상대방을 탐색한다. Fix 단계는 전 단계에서 식별된 대상을 확인하며, 수집한 정보를 다음 단계의 활동에서 사용할 기초 증거로 변환한다. Finish 단계는 앞서 생성된 증거를 기반으로 작업의 목표를 설정하는 단계이다. Exploit 단계는 마무리 단계에서 생성된 증거를 기반으로 특정 정보(예: 지표 정보)를 식별한다. Analyze 단계는 이용된 증거를 보다 광범위하게 다른 정보와 융합하여 전체적인 그림을 그린다. Disseminate 단계는 연구 결과를 주요 이해 관계자에게 최종적으로 공개한다.

대체로 Intelligence Cycle과 함께 사용하는데, Intelligence Cycle의 "Collection"단계와 F3EAD Cycle의 "Find" 단계가 맞물려 톱니바퀴처럼 돌아가며, D3A의 프로세스의 연결고리로서의 역할을 수행한다.



(그림 2) Relationship between F3EAD and D3A, and Intelligence Cycle

* Source: Reconstruction of Jimmy Gomez(2011)

⑤ RAIM Framework

RAIM 프레임워크는 2010년 능동적인 방법으로 보안 문제를 해결하기 위한 전략적 로드맵 프레임워크로서 개발되었다.[2] 주요기반시설에서 사용하는 제어시스템의 정보보안 평가를 위해 위협요소와 영향력 측면에서 회복력을 수치화한다. 시스템 특성의 식별을 핵심으로 모델링의 효과성을 저해할 수 있는 기반시설 간 상호 의존성에 대한 분석적 평가를 수행한다. 위하여 실시간 모니터링(Real time Monitoring), 이상 탐지(Anomaly Detection), 영향 분석(Impact Analysis), 완화 전략(Mitigation Strategies) 등 4가지 요소로 구성된다.

2.3.2 분석 기준 모델

① ATT&CK(Adversarial Tactics Techniques and Common Knowledge)

MITRE가 구축한 ATT&CK는 실제 조사에 토대로 구축된 전 세계적으로 접근 가능한 기반 지식이다. 민간 부문, 정부 및 사이버 보안 제품 및 서비스 커뮤니티에서 특정 위협 모델 및 방법론 개발을 위한 기초 자료로 사용된다. 초기 접근(Initial Access), 실행(Execution), 지속(Persistence), 권한 상승(Privilege Escalation), 국방 회피(Defense Evasion), 자격증명 액세스(Credential Access), 발견(Discovery), 측면 운동(Lateral Movement), 수집(Collection), 탈출(Exfiltration), 명령 및 제어(Command and Control) 등 11가지의 기준에 따라 정보를 구분한다.

ATT&CK는 기업형과 모바일 등 두 가지의 Matrix를 가진다. 기업형 Matrix에는 Windows, Mac, Linux 플랫폼에 걸친 기술이 포함되어 지식 기반 탐색에 사용한다. 모바일 Matrix는 적대적인 전술 및 장치 액세스와 관련한 기술과 장치 액세스 없이 상대방이 사용할 수 있는 네트워크 기반 효과 등 두 가지로 구분된다.

② Diamond Model for Intrusion Analysis

침입분석을 위한 다이아몬드 모델은 Adversary, Infrastructure, Capability, Victim 등 4가지 핵심 기능으로 구성된 모든 침입 활동의 기본 요소를 설정한다. 침입 분석, 측정, 테스트 가능성 및 반복성에 과학적 원리를 적용하는 공식적인 방법을 처음으로 수립하여 포괄적인 활동 문서화, 통합, 상관관계에 대한 방법을 제공한다. 네트워크 방어를 위해 지능을 실시간으로 통합하고 이벤트 간 상관관계를 자동화하여 이벤트를 분류하고 적대적인 활동을 예측할 수 있는 기회를 제공한다.

Adversary는 일반적으로 침입 활동을 수행하는 실제 해커나 사람을 의미한다. Capability는 수동적인 암호 추측 방법에서 자동화된 기술까지 포함해 침입에 사용되는 도구나 기술 등 피해자에게 영향을 미치는 모든 수단을 포함한다. Infrastructure는 침입자가 사용하는 물리적/논리적 통신 구조를 의미하며 침입자가 물리적으로 접근하는 인프라(유형 1)와 통신망을 통해 접근하는 하는 인프라(유형 2), 이러한 유형 1과 2에 대한 서비스를 제공하는 제공 업체를 포함한다. Victim은 목표 공격 대상이며 조직, 사람, 전자메일주소, IP 주소, 도메인 등이 모두 포함된다.

2.4 소결

본 연구는 정보공유 플랫폼의 구축을 위하여 위험커뮤니케이션 이론 중 가장 대표적 선형 모델인 라스웰(Lassewll)의 SMCRE모델을 분석하고 위험커뮤니케이션 이론을 기반으로 하는 방어적 차원의 정보공유 프로세스 및 기준을 선별하여 분석하였다.

Intelligence Cycle은 정보의 처리 과정이며, OODA Loop는 정보의 처리를 포함하여 의사결정 및 활동까지 포함하는 일련의 과정이다. F3EAD는 의사결정을 위한 정보 활용 체계이며, 대개 D3A와 함께 이야기된다. 분석기준으로 정보의 탐지 및 수집을 위한 ATT&CK 매트릭스가 있고, 정보 분석 시 조직내외의 환경과 조건을 분석하는 Diamond 모델이 있다. 또한 주요기반시설 SCADA 시스템의 사이버 보안 및 방어를 위한 RAIM 프레임워크도 함께 분석하였다.

본 장에서 사이버 보안 행동 중심의 모델 중 프로세스 중심의 모델을 통합·분석하여 <표 1>과 같은 결과를 도출하였다. 각 모델의 공통항목을 도출하여 탐지(Detect), 수집 및 분석(Collect and Analyze), 공유(Disseminate), 결정(Decide and Act), 영향분석(Effect Assess)으로 구성되는 정보 공유 프로세스를 도출하였다.

<표 1> Comparison of Information Processing Models

구분	A	B	C	D	E
Detect	Direction	Observe	Find	Detect	Detect
Collect and Analyze	Collect	Orient	Fix, Finish		
	Analyze		Analyze		

구분	A	B	C	D	E
Disseminate	Dissemin ate		Dissemi nate	Deliver	
Decide and Act		Decide		Decide	
		Act			Mitigation Strategies
Effect Assess				Assess	Impact Analysis

A: Intelligence Cycle
B: OODA Loop
C: F3EAD
D: D3A
E: RAIM Framework

위험은 끊임없이 발달하고 복잡해진다. 현재 상황에서 다 알 수 없는 위협 및 위험에 대응하기 위해 기존 정보 공유 차원에서 더 나아가 전체적 및 방어적 차원의 정보공유가 필요하다. 사이버 환경은 이미 모든 산업에 스며들었으며, 주요기반시설마저 사이버 기술을 활용하고 있으므로 사이버 공간에서 발생할 수 있는 모든 위험과 장애, 오류 등에 대한 조치가 필요하다. 이를 위하여 군사적, 방어적 목적을 위한 정보공유 프로세스를 사이버 차원에 적용하고, 정보공유의 파트너를 확대함으로써 다가올 미지의 복합적 위험에 대응할 수 있기를 기대한다.

3. 정보공유플랫폼의 제안

본 장에서는 2장에서 분석한 보안 모델을 통합한 형태에 기반을 두어 위험커뮤니케이션 모델과의 결합을 통해 구조화를 시도하였다. 전술한 바와 같이 본 연구는 위험커뮤니케이션 이론 중 SMCRE모델과 행동 중심의 보안 모델(프로세스 중심 모델 및 분석 기준 모델)의 요소를 분석하고 그 결과에 기반을 두어 새로운 정보공유 플랫폼을 수립하고자 한다. SMCRE 모델은 정보의 송신자가 어떤 정보를 어떤 방법으로 공유하고 공유된 정보가 어떻게 활용되는지, 그리고 그 영향력은 어떤지를 분석하기 위한 모델로 다각적 접근이 필요한 위험 대응에 적절한 구성을 가진다.

이에 본 장에서는 SMCRE 모델 요소에 기존 모델을 적용하여 새로운 정보공유 플랫폼을 제안하고자 한다. 이를 위하여 각 요소별 대응 단계를 매치시키고 전체적인 플랫폼을 살펴볼 것이다.

3.1 SMCRE 모델 기반의 사이버 보안 정보 공유 체계 구조화

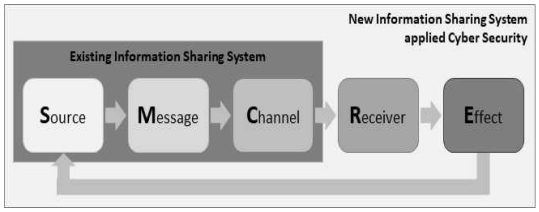
본 연구는 SMCRE 모델을 기반으로 정보 보안 모델을 적용하여 새로운 구조화를 시도하였다.

<표 2> Overview of SMCRE Model-Based Information Sharing Platform

SMCRE	Platform	Description	Note
Source	Detect	The process of detecting information through sensors, automated systems, and monitoring. Gathers the lowest level of information.	ATT&CK, Intelligence Cycle, OODA Loop, F3EAD, D3A, RAIM Framework etc.
Message	Collect and Analyze	The process of collecting the collected information through a certain step, analyzing it according to certain criteria, and storing it in the database.	Intelligence Cycle, OODA Loop, F3EAD etc.
Channel	Disseminate	The process of sharing the analyzed information with pre-linked partners.	Intelligence Cycle, F3EAD, D3A etc.
Receiver	Decide and Act	The process of utilizing shared information. Analyze the internal structure of the organization and make decisions using information appropriate to each situation and environment, and carry out activities such as policy making.	OODA Loop, D3A, RAIM Framework etc.
Effect	Effect Assess	The process of analyzing the results and impact of the activities, evaluating for improvement of the organization, and recycling the results information	D3A, RAIM Framework etc.

SMCRE 모델은 정보원(Source), 메시지(Message), 통신채널(Chanel), 수신자(Receiver), 영향(Effect)으로 구성된다. 그리고 본 연구는 2장에서 프로세스 중심의 사이버 보안 행동 중심 모델을 통합·분석하여 탐지(Detect), 분석(Collect and Analyze), 공유(Disseminate), 결정(Decide and Act), 영향분석(Effect Assess)으로 구성되는 정보공유 프로세스를 수립하였다(<표 2> 참조).

이어서 SMCRE 모델을 기준으로 현재의 정보공유체계는 분석한 결과 SMC에 미치는 수준으로 단순한 위험 정보의 수집 및 공유 차원에서 운영된다. 다만 정보 공유의 패러다임이 변화함에 따라 분석에 기반을 두어 사이버 보안 행위에 대한 의사 결정을 지원하고 그에 따른 영향을 분석하는 RE의 단계로의 확장이 요구된다. 여기서 RE 단계는 직접적인 행위에 대한 잠재적인 평가를 수행하여 그 결과를 다시 탐지 단계로 피드백 함으로써 다음 프로세스에 영향을 미치는 체계를 가진다.

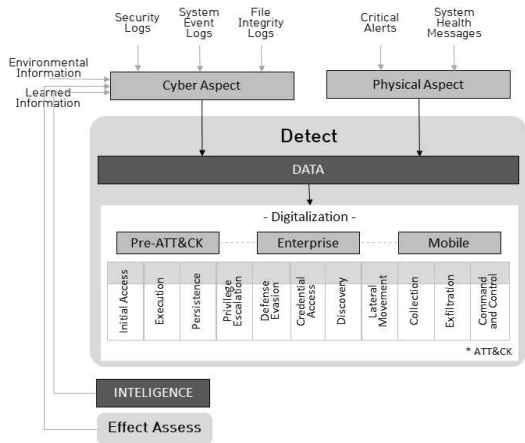


(그림 3) Comparing Existing and New Information Sharing System

따라서 본 연구는 SMCRE의 모델에 기존 보안 모델을 통합하여 도출한 프로세스를 결합하여 구조화를 시도하였다. 기존의 SMCRE 모델과 새로 구축한 정보공유 프로세스는 유사한 구조로 항목 간에 서로 매치가 가능하다(<표 2> 참조). 다음 항에서 SMCRE 모델의 요소를 기반으로 수립한 정보 공유 플랫폼의 각 단계를 살펴보고자 한다.

3.1.1 Source - Detect

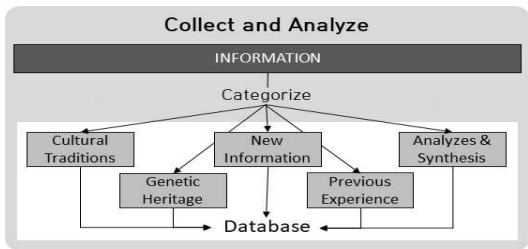
SMCRE 모델 내의 정보원은 정보의 송신자가 어떤 정보를 보낼지 정한다는 맥락에서 일반 보호 모델의 탐지나 조사에 해당한다. 여기서 탐지는 사이버적 차원과 물리적 차원을 모두 포함하며, 센서나 모니터링을 통한 데이터의 수집과 환경 정보, 기존 분석 정보 기반의 학습 정보 수집 등 모든 기초 데이터의 수집 단계를 의미한다. 이렇게 수집된 데이터는 ATT&CK와 같은 자동화 시스템을 통해 디지털화되어 사고에 따라 영역을 분류한다. 분류된 데이터는 우선순위 및 중요성을 파악하여 각 기준에 맞는 데이터로 구분한다.



(그림 4) Detect phase on platform

3.1.2 Message - Collect and Analyze

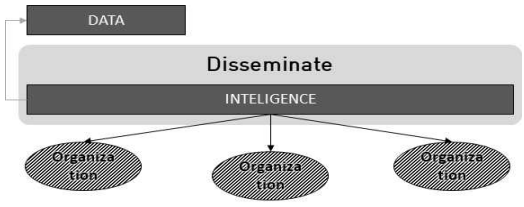
탐지 단계에서 일련의 과정을 통해 분류된 데이터는 활용을 위해 카테고리별로 다시 나뉘며 각 기준에 맞게 데이터베이스화되어 저장된다. 본 플랫폼에서는 OODA Loop의 Orient 단계에서 활용한 5가지 기준을 통해 정보를 분석하고 분석한 정보를 저장한다.



(그림 5) Collect and Analyze phase on platform

3.1.3 Chanel - Disseminate

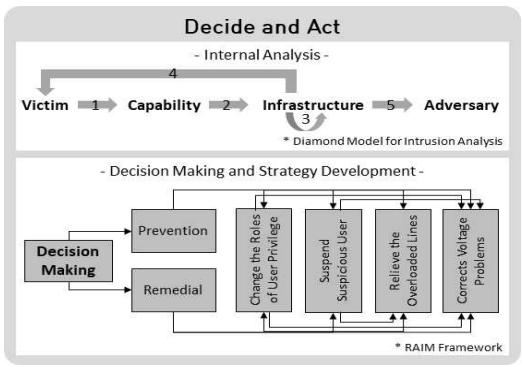
데이터베이스에 저장된 정보는 활용을 위해 정제된 데이터로 해당 정보가 필요한 각 조직 및 파트너에게 전송된다. 이 단계에서 분석된 정보는 다시 초기의 탐지 단계로 보내져 다른 기초 자료를 분석하기 위한 기준으로도 활용된다.



(그림 6) Disseminate phase on platform

3.1.4 Receiver - Decide and Act

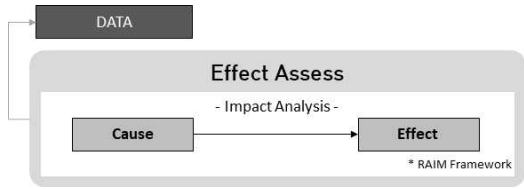
전송 단계를 통해 조직으로 전달된 정보는 조직 내부 환경 및 상황, 요소에 대한 분석을 진행한 후, 분석 결과와 정보를 결합하여 의사결정을 수행한다. 본 플랫폼 중 조직별 자체 상황 분석은 침해분석을 위한 다이아몬드 모델의 프로세스를 기반으로 이루어지며 위험의 피해자와 역량, 위험 대상, 공격자 등을 분석한다. 이렇게 분석한 조직의 상황에 따라 예방과 처리를 위한 의사결정을 수립하고, 일환으로 대응, 완화 등의 전략을 수립하여 수행한다. 이러한 분석 및 의사결정, 전략의 수행은 정보를 전달받은 조직별로 이루어진다.



(그림 7) Decide and Act phase on platform

3.1.5 Effect - Effect Assess

이렇게 각 조직별로 수행한 전략 등에 대한 결과를 요인과 영향력으로 구분하여 상관관계를 분석하고, 그 결과를 다시 최초 단계의 데이터 수집 및 수집된 데이터의 분석 시에 활용한다. 이는 발생한 사고의 영향력이나 발생가능성이 높은 위험의 영향력 등을 평가하고 분석한다.



(그림 8) Phase of Effect Assessment on Platform

3.2 새로운 플랫폼 제안

전술한 바와 같이 위험커뮤니케이션 이론 중 SMCRE 모델의 요소를 기반으로 새로운 정보공유 플랫폼을 수립하였다. SMCRE 모델은 선형적 모델로 단방향성이 강한 모델이므로 사이버 보안 운영을 위한 프로세스 중심의 행동 모델을 분석해 도출한 정보공유 프로세스(탐지-수집 및 분석-공유-의사결정-영향분석)와의 결합을 통해 일련의 프로세스를 포함하여 플랫폼을 수립하였다. 해당 플랫폼은 새로 나타나는 위험 및 위협에 대한 대응이 원활하도록 군사적 차원에서 국가의 보호를 위한 행동 모델을 분석하여 적용하였으므로 변화하는 정보공유 패러다임에 적합하다. 제안된 플랫폼은 정보의 탐지부터 수집 및 분석, 공유, 의사결정, 행동, 평가로 구성된 체계이며 학습 정보를 재공유하고 새로운 데이터에 대한 기준으로 제시함으로써 지속적인 발전 가능성을 보장함으로써 보안(security) 차원에서 더 나아가 적극적 방어(active defense) 차원의 정보공유가 가능하다.((그림 9) 참조)

기존의 정보공유체계를 SMCRE 모델에 적용하여 분석한 결과 정보원(S)은 위협 정보를 제공하

는 정보 제공자이며 메시지(M)는 전달받은 정보의 형태와 종류를 의미한다. 채널(C)은 정보공유를 위해 오픈되는 공유채널로 일종의 정보 간 터미널의 역할을 수행한다. 수용자(R)는 정보를 전달받아 분석하는 대상으로 현재의 정보공유체계에서는 조직의 내부에 해당하고 영향(E)은 분석의 결과로 나타나는 영향을 의미하며 마찬가지로 조직 내부적 차원에서 활용된다. 이러한 결과를 보았을 때 현재의 정보공유체계는 SMCRE 모델 중 SMC의 단계에 머문다. 이는 단순히 위협정보의 공유에 있어 공유 활동에 초점을 맞추어 운영되는 것으로 판단되며, 정보공유 패러다임의 변화에 못 미치는 체계로 개선이 필요하다. 특히 수용자(R)와 영향(E)은 내부적 차원에서 수행되고 있으나 변화한 정보공유 패러다임에 따르면 체계화를 통해 관계자와 함께 정보를 공유하여 그 영향의 인지가 필요하다.

SMCRE 차원에서 현재 정보공유체계와 새로운 정보공유체계에 대한 비교 분석을 통해 기존의 정보공유와 새로운 정보공유를 식별하였다. 기존의 정보공유 패러다임은 위협 정보 수집과 공유를 중심으로 마련된 체계이나 새로운 정보공유의 패러다임은 적극적 사이버 방어(ACD) 차원의 위협 대응과 의사결정 중심을 중시하는 체계이다.

이에 본 장에서 수립한 정보공유 플랫폼은 융합 환경의 위험에 대응하기에 적합한 정보공유체계로, 적극적인 사이버 방어 차원의 정보공유가 가능한 형태이다.

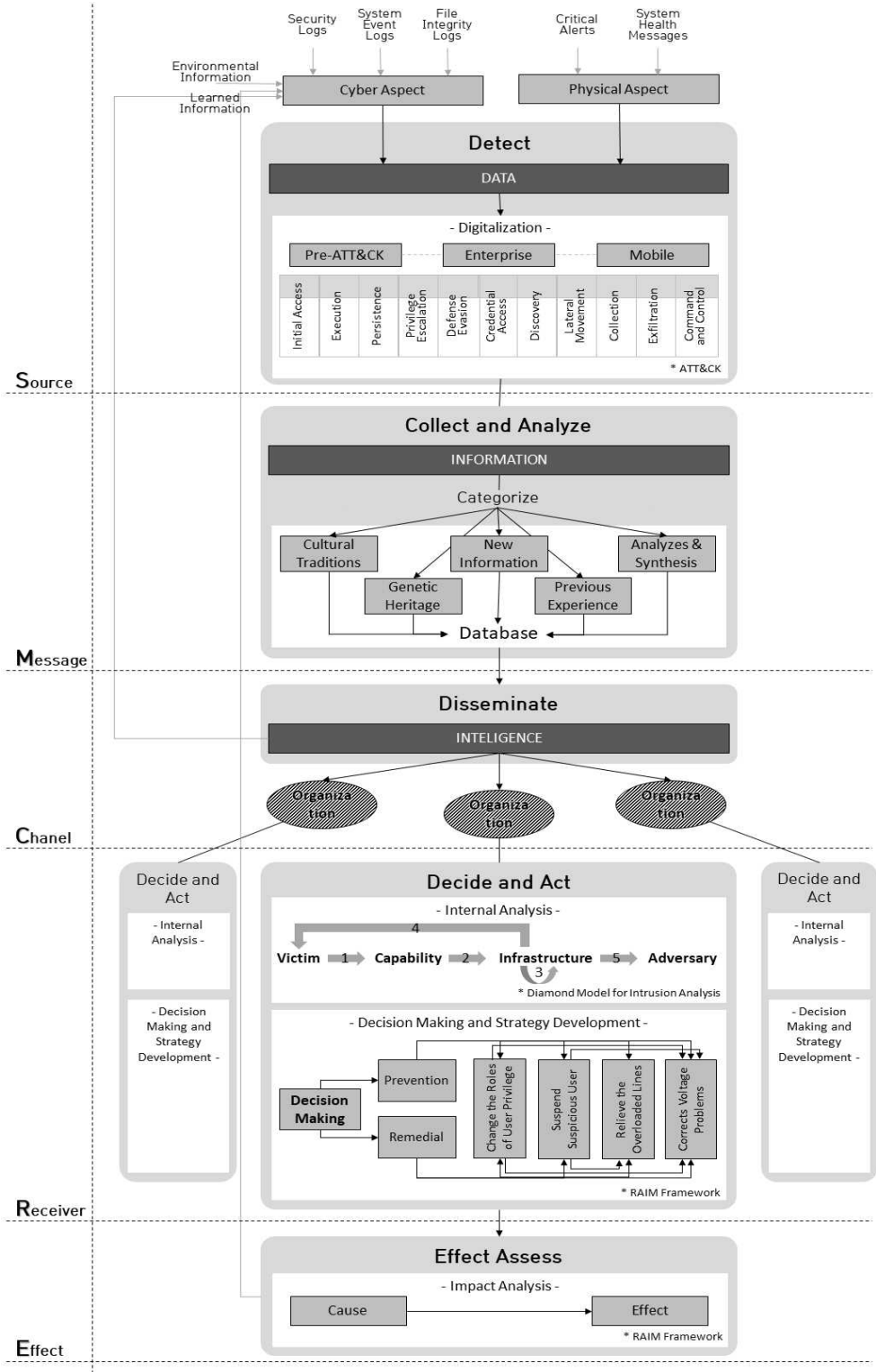
3.3 소결

이번 장에서 수립한 정보공유 플랫폼은 현존하는 사이버 위협 정보 공유 플랫폼과는 차이가 있다. 현재 정보공유플랫폼은 사이버 영역에 한정되어 있으나 본 연구에서 제안하는 플랫폼은 물리적 영역까지 고려하는 등 융합 환경에 적합하며 단순한 공유 차원에서 끝나는 것이 아니라 공유된 정보를 토대로 조직의 상황에 맞게 의사결정을 하고 전략 및 정책을 수립 및 시행하며 그에 대한 영향평가를 통해 지속적으로 개선될 여지를 가진다. 즉 대응 활동을 초점으로 구성되었다. 정보공유 플랫폼을 구성하는 행동 모델들은 보안적 차원에서 더 나아가 안전과 보호를 위한 활동을 포함한다. 새로운 위험에 대응하는 것은 국가의 사회나 경제적 차원의 안보와 연결되기 때문에 실제로 공유된 정보를 활용하는 것이 중요하다.

본 연구에서 기반 모델로 활용한 Lasswell의 SMCRE 모델은 선형(linear) 모델로 비교적 단순한

<표 3> Comparing Existing Model and New Information Sharing Model

	Existing System	New Model System
S	Information about sender providing risk and threat information	(Detect) Digitize and classify for automated analysis of information analyzed and collected based on the source of information such as cyber and physical aspects
M	Type and kind of information (qualitative/quantitative characteristics of message, whether it is forced/recommended, simplified technical information, etc.)	(Collect and Analyze) Collected information is processed and uniformly classified into the same form through digitization, and converted into a database for easy sharing of information
C	Shared channel opened for information sharing(Information terminal)	(Disseminate) It is possible to share information in the database at all times and provide lessons derived from analysis as a new information source
R	Internal Performance	(Decide and Act) Using shared information as the basis of decision making through organization's internal analysis system, linking to actual prevention and response activities through strategy establishment
E	Internal Performance	(Effect Assessment) Analyze the correlation between the results of the action and the factors and influence, and use the analysis results as a new source of information



(그림 9) Information Sharing Platform

구조로 되어 있으며 정보의 접근에 한계가 있어 구체적인 적용을 위한 추가적인 분석이 요구된다.

이에 본 연구는 SMCRE 모델을 기반으로 사이버 위협 정보의 공유 플랫폼을 구축하여 각 단계별 자동화 및 분석 프로세스를 적용함으로써 해당 모델의 효용성을 강화하고자 한다. 본 연구에서 제안하는 정보 공유 플랫폼은 공유되고 수집된 정보의 자동화 분류 체계 및 분석 체계를 통해 해당 정보가 필요한 조직으로 신속하게 분석된 정보를 전달하고 조직 자체적인 분석 및 의사결정 프로세스를 통해 실제 행동 및 영향 분석으로 이어지는 일련의 프로세스이며, 각 단계에서 분석된 결과를 새로운 정보원으로 활용하여 순환적인 구조를 가진다.((그림 9) 및 <표 3> 참조)

4. 결 론

본 연구는 발전하는 기술에 따른 위험의 변화를 전체적인 관점에서 파악하고 대응하기 위하여 Systemic Cyber Risk를 중심으로 새로운 위험을 인지하였다. 따라서 복잡화되고 다양해지는 새로운 위험은 더 이상 개인 혹은 단일 조직적 차원에서의 대응 조치로는 보호하기 어려워짐을 확인하였으며, 이에 대응하기 위해 위험커뮤니케이션 이론을 기반으로 모두가 협력하여 신속한 대응 플랫폼을 구축하고자 진행되었다.

위험커뮤니케이션 이론을 기반을 둔 모델 중 SMCRE 모델의 요소를 도출하여 보안 운영을 위한 행동 중심 모델들을 재배치, 새로운 정보공유 플랫폼을 구축하였다. S-탐지, M-분석, C-공유, R-의사결정, E-영향 평가로 구성된 이 플랫폼은 현존하는 사이버 위협 정보공유체계와는 달리 방어적 차원으로 접근하는 행동 중심의 플랫폼으로 조직의 상황을 분석하여 준비와 대응에 초점을 맞춘다.

연구의 결과로서 제시하는 정보공유플랫폼을 통해 기존 형태인 Top-down 보다 실제적으로 해당 기관이 협력할 수 있는 구조가 필요하다. 특히 단순히 정보공유 수준에서 그치는 것이 아닌 각 기관이 활용할 수 있는 정보를 공유플랫폼에 탑재하고 전달하는 구조로 만들어져야 한다. 또한 기존의 사이버 위협 정보를 공유하는 차원에서 더 나아가 국가 안보를 위한 수준으로 발전하여야 한다. 다가오는 공격에 대한 대응뿐만 아니라 사전에 대비하고 후속 조치를 통해 지속적으로 정보를 분석하고 공유해야 한다.

참고문헌

[1] Businesstopia, “Lasswell Model of Commication”, Dec 29th 2015. https://www.slideshare.net/businesstopia/laswell-model-of-commication (Search: 2018.12.03.)

[2] Chee-Wooi Ten, Govindarasu Manimaran, and Chen-Ching Liu, "Cybersecurity for Critical Infrastructures: Attack and Defense Modeling", IEEE Transactions on Systems, Man, and Cybernetics - Part 1: Systems and Humans, Vol.40, No.4, Jul 2010.

[3] DTCC, “Cyber Risk - A Glbal Systemic Threat”, Oct 2014.

[4] Earl Guzman, “Basic Linear Communication Models: Lasswell, Shannon and Weaver”, Jul 15th 2015. https://www.slideshare.net/EarlGuzman/lasswell-shannon-weaver (Search: 2018.12.03.)

[5] Gomez, Jimmy A., "The Targeting Process: D3A and F3EAD", Small Wars Journal, Jul 16th 2011.

[6] Han Sang-Kook., “Improvement of National Information Sharing System by Security Environment Change: Focusing on US Information Society Case,” Konkuk University Graduate School of Public Administration, Feb 2013. (한상국, “안보환경 변화에 따른 국가정보 공유 체계 개선 방향 : 미국 정보공동체 사례를 중심으로,” 건국대학교 행정대학원, 2013.)

[7] Ismael Valenzuela, “Intelligence-Driven Defense:

Successfully Embedding Cyber Threat Intel in Security Operations", SANS Blue Team Summit, 2018.

[8] Kim Ae-Chan, and Lee Dong-Hoon, "A Study on the Priority of Requirements for Establishing Effective Cyber-threat Information Sharing System," Journal of the Korea Institute of Information Security and Cryptology, Vol.27, No.5 :61-67, 2016. (김애찬, 이동훈, "효과적인 사이버위협 정보 공유 체계 수립을 위한 요구사항의 우선순위 도출에 관한 연구," 한국정보보호학회, 26(1), p.61-67, 2016.)

[9] Kim Dong-Hee, Park Sang-Don, Kim So-Jeong, and Yoon Oh-Jun, "A Study on Establishment of Cyber Threat Information Sharing System Focusing on U.S. Cases," Convergence Security Journal Vol.17, No.2 :53 - 68, 2017. (김동희, 박상돈, 김소정, 윤오준, "사이버 위협정보 공유 체계 구축방안에 관한 연구 - 미국 사례를 중심으로 -," 한국융합보안학회 융합보안논문지, 17(2), p.53-68, 2017.)

[10] Lim Won-Sick, Yoon Myung-Keun, and Cho Hark-Su, "KOSIGN: Cyber Threat Information Sharing System from Information Protection Products," Korea Institute of Information Security and Cryptology, Vol.28 No.2 :20-26, 2018. (임원식, 윤명근, 조학수, "KOSIGN:정보보호제품 관점의 사이버위협정보 공유 체계," 한국정보보호학회 28(2), p.20-26, 2018.)

[11] NSA CSS(National Security Agency Central Security Service), "Active Cyber Defense (ACD)", Aug 1st 2014. https://apps.nsa.gov/iaarchive/programs/iad initiatives/active-cyber-defense.cfm

[12] Park Ji-Baek, Choi Byoung-Hwan, and Cho Hark-Su, "Promoting sharing of cyber threat information," Journal of The Korean Institute of Communication Sciences, Korea Institute Of Communication Sciences, Vol.35 No.7 :41-48, 2018. (박지백 ,최병환 ,조학수, "사이버 위협정보의 공유 활성화 방안," 한국통신학회, 정보와 통신, 35(7), p.41-48, 2018.)

[13] Song Hae-Ryong, Cho Hang-Min, Lee Yoon-Kyung, and Kim Won-Je, "A Study on the Conceptualization, Structural Analysis and Domain Establishment of Risk Communication," Dispute Resolution Studies Review, Dankook Center for Dispute Resolution, Vol.10, No.1 :65-100, 2012. (송해룡, 조항민, 이윤경, 김원제, "위험커뮤니케이션의 개념화, 구조 분석 및 영역 설정에 관한 연구", 단국대학교 분쟁해결연구소, 분쟁해결연구, 10(1), 2012.)

[14] SRC(Systemic Risk Center), "System Risk", http://www.systemicrisk.ac.uk/systemic-risk(Search: 2018.10.05.)

[15] START, "Understanding Risk Communication Theory: A Guide for Emergency Managers and Communicators", May 2012.

[16] WEF "Part 1: Global Risks 2014: Understanding Systemic Risks in a Changing Global Environment", Jan 2014. and G. G. Kaufman and K. E. Scott, "What Is Systemic Risk, and Do Bank Regulators Retard or Contribute to It?" in Independent Review Vol.7, No.3 :371 - 391, 2003.

[17] WEF, "Understanding Systemic Cyber Risk", Oct 2016.

[18] Yoon Oh-Jun, Cho Chang-Seob, Park Jeong-Keun, Bae Sun-Ha, and Shin Yong-Tae, "A Study on the Domestic Model for Cyber Threat Information Sharing by Analyzing the Relevant Systems of Major Advanced Countries," Convergence Security Journal, Vol.16, No.7 :101-111, 2016. (윤오준, 조창섭, 박정근, 배선하, 신용태, "주요국의 사이버위협정보 공유 체계 분석을 통한 국내 적용모델 연구," 한국융합보안학회 융합보안논문지, 16(7), p.101-111. 2016.)

[19] Yoon Oh-Jun, Cho Chang-Seob, Park Jeong-Keun, Seo Hyung-Jun, and Shin

Yong-Tae, “ A Study on the Improvement Model for Invigorating Cyber Threat Information Sharing” Convergence Security Journal, Vol.16, No.4 :25-34, 2016. (윤오준, 조창섭, 박정근, 서형준, 신용태, “사이버위협정보 공유 활성화를 위한 관리적·기술적 개선모델 연구,” 한국융합보안학회 융합보안논문지, 16(4), p.25-34. 2016.)

〔저자소개〕

유 지 연 (Ji-Yeon Yoo)
2012년 2월 고려대학교 정보경영공학과 박사
2014년 ~ 현재 상명대학교 휴먼지능정보공학과 조교수
email : yooo@smu.ac.kr

박 향 미 (Hyang-Mi Park)
2017년 2월 상명대학교 지식보안경영학과 석사
2017년 ~ 현재 한국IT법연구원 선임연구원
email : aymi0103@gmail.com