정 보 보 호 학 회 지
제26권 제1호, 2016. 2

효과적인 사이버위협 정보공유체계 수립을 위한 요구사항의 우선순위 도출에 관한 연구

김 애 찬*, 이 동 훈**

요 약

공공·민간이 함께 사이버위협을 조기 탐지·전파 할 수 있는 사이버위협정보 공유체계 구축에 관한 논의가 본격적으로 진행되고 있다. 아울러 사이버위협정보의 오남용에 따른 부작용과 민감 정보유출 등 잠재적인 위협이 발생할 부작용도 존재한다. 본 연구에서는 국내외 사이버위협 정보공유 현황과 관련법규를 살펴보고, 예상되는 문제점을 규명한 뒤 이를 완화하기 위한 정책적·기술적 요구사항에 대한 우선순위를 도출한다. 연구의 결과로, 정보공유체계를 효과적으로 수립하기 위한 정책적 요구사항이 기술적 요구사항 보다 중요한 것으로 나타났다. 정책적 요구사항은 관련 법적 근거의 마련, 정보관리체계 마련 순으로 나타났으며, 기술적 요구사항은 정보 표현방식 및 전송규격 표준화, 정보 수집 방법 및 신뢰성 개선 순인 것으로 나타났다. 또한, 효과적인 정보공유체계 수립을 위해서는 국가가 주도하여 정책적 기반과 표준기술을 구축하되, 공공·민간이 적극적으로 참여하도록 유도하고 협력하여 정보공유체계를 구축해 나가는 방식이 보다 적합할 것으로 판단된다.

Ⅰ. 서 론

사이버위협은 대부분 공공분야보다 상대적으로 보안관리가 허술한 민간분야에서 대부분 발생하고 있으며, 특히 민간분야는 비용부담이나 기술부족 등으로 인하여 신속한 조치를 하지 않아 피해규모가 커지고 있다. 이와 같은 상황에서 현행 사이버위협정보 공유는 공공분야와 민간분야로 나뉘어 이루어지고 있고, 공공·민간 영역 간 사이버위협정보의 공유가 법적 근거의 부재로 이루어지고 있지 못하고 있어 사고예방에 한계가 발생하고 있다.

이에 각 조직은 사이버위협에 대한 피해확산 방지와 이에 따른 위험을 최소화하기 위해 민간을 중심으로 위협정보를 자발적으로 공유하기 시작하였고, 보다 체계적으로 정보를 수집하고 공유하기 위해 정보공유분석센터(ISAC, Information Sharing & Analysis Center)를 산업 부문별로 설치·운영하기 시작하였다. 최근 美정부는 SONY社 해킹 사건을 계기로 고도화된 사이버 위협에 보다 적극적으로 대응하기 위하여 사이버위협정보통합센터(CTIIC, Cyber Threat Intelligence Center)의 설립을 승인(`15.2)하였고, 행정명령(Executive Order, EO) 제13691호 발표(`15.2)를 통하여 민간 부문 사이버 위협정보 공유 촉진, 정보공유·분석 기구(ISAOs) 구축에 관한 내용을 지시하였다. 이와 관련된 「사이버위협정보 공유에 관한 법률」(CISA, Cybersecurity Information Sharing Act)(S.754)은 美상원 정보위원회를 통과(`15.3.17)하였는데, 이 법안은 연방정부와 민간부문의 사이버 보안 및 위협 정보공유 촉진, 공유정보의 개인 식별 가능 정보 제거, 개인정보 영향 및 이행 등에 대한 보고서 제출 의무화 등의 내용을 포함하고 있다.

최근 정부는 범국가적 사이버 위협 정보공유체계 연계를 위해 '국가 사이버 안보태세 역량 강화(`15.3.17 정부 발표)'에서 2015년 내 사이버 위협 정보 종합 수집·분석·공유 시스템을 한층 보강할 계획이라 밝힌 바 있으며, 이철우 의원 등 22인은 「사이버위협정보 공유에 관한 법률(안)」을 발의하였다(`15.5.19). 이처럼 공공·민간이 함께 사이버위협을 조기 탐지·전파 할 수 있는 체계 구축에 관한 논의는 아직 시작 단계에 있으며, 이에 효과적인 구축을 위한 관련 분야의 연구가 필요할 것으로 생각된다.

또한, 정보공유의 이면에는 사이버위협정보의 오·남

* 고려대학교 정보보호대학원 정보보호학과 박사과정 (holytemple@korea.ac.kr)
** 고려대학교 정보보호대학원 교수 (donghlee@korea.ac.kr)

용에 따른 부작용 발생과 민감 정보가 유출될 수 있는 잠재적인 위협이 발생할 가능성이 존재한다. 이에 따라 정보공유센터의 원활한 업무의 수행과 민감한 정보의 노출을 방지하기 위해 적절한 정책적·기술적 방안을 수립할 필요가 있다. 본 연구에서는 사이버위협 정보공유와 관련된 국내외 법제 현황을 살펴보고, 이에 기대되는 문제점과 이를 해결하기 위한 정책적·기술적 방안을 검토하여 안전하고 효과적인 사이버위협 정보공유체계를 수립하기 위한 요구사항의 우선순위를 도출하고자 한다.

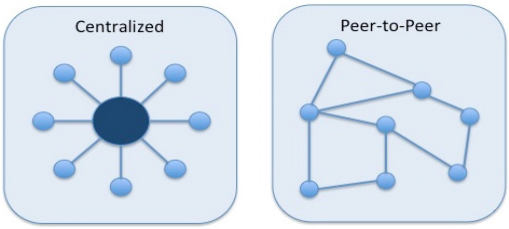
Ⅱ. 국내외 현황

2.1. 정보공유체계 유형

사이버위협정보(Cyber Threat Intelligence)란 조직의 자산에 손실 또는 잠재적인 위협이 될 수 있는 지식, 문맥, 메커니즘, 식별자에 대한 주체의 실행 가능한 조언 또는 의사결정을 지원하는 정보를 의미한다[13]. 「사이버위협정보 공유에 관한 법률(안)」에서는 정보통신망·정보통신기기 및 정보보호시스템 등에 의해 해킹, 바이러스, 서비스방해, 전자기파 등 정보통신망을 마비·파괴하거나 정보를 절취할 수 있는 행위에 관한 정보로 정의하고 있다. 대표적인 사이버위협정보는 IP(출발지, 목적지), Port, 악성코드 유포지, 해킹메일주소 등이 있다. 이러한 예를 볼 때 사이버위협정보는 개인정보 또는 금융, 신용정보와는 다른 정보이며, 수집목적이 근본적으로 다르다.

또한, 정보공유(Information Sharing)는 사이버위협정보 획득을 통한 사전예방, 사고 탐지, 사후 공동대응 등 피해확산 방지의 활동을 주목적으로 한다[11]. 사이버위협정보에 대한 정보공유를 위해 NIST는 효과적인 정보공유체계를 그림 1과 같이 제안하고 있으며[12], 우리나라는 미국의 US-CERT중심의 사이버위협 정보공유체계와 유사한 형태인 국가기관 산하 국가사이버안전센터(NCSC, National Cyber Security Center)를 중심으로 중앙집중형 정보공유체계로 구축되어 있다.

그림 1과 표 1에서 보듯 중앙집중형 체계는 초기 정보공유체계에 적합한 모형으로서 보다 효율적인 운영과 통제가 용이하며, 신속한 의사결정과 정보공유가 가능하다는 장점을 가진다. 하지만 각 산업 부문별 ISAC이 확장·증설 및 사이버위협정보의 양과 종류가 점진적으로 증가함에 따라 운영상 비효율을 증가시킨다는 단점이 있다. 이와 달리 상호교환형 정보공유체계는 효율적인 운영과 통제가 다소 떨어지나 정보 가공에 있어 상호보완적이고, 분산 환경에서 보다 활발한 정보공유가 가능하다는 장점이 있다[12].



〔그림 1〕 정보공유체계 유형(좌: 중앙집중형, 우: 상호교환형)

〔표 1〕 정보공유체계 장·단점 비교

구분	중앙집중형 (Centralized)	상호교환형 (Peer-to-Peer)
장점	·효율적인 운영통제 ·신속한 의사결정과 정보공유	·정보가공 및 활용도 증가 ·상호보완적 정보공유 증가
단점	·중앙집중에 따른 운영비용 증가	·운영비용 증가 ·민감정보의 유출 가능성

2.2. 현황 및 관련법규

미국의 경우 상원의원 법률안(CISA) 통과로 인하여 연방정부 소속 CTIIC를 중심으로 각 산업 부문별로 ISAC를 운영하고 있으며[2], 일본의 경우에는 경제산업성 산하의 정보보안 전문기관인 IPA(Information-technology Promotion Agency)를 중심으로 J-CSIP(Initiative for Cyber Security Information sharing Partnership of Japan)를 `11.10월에 발족하여 운영하고 있다[3]. 이는 `10.12월 경제산업성의 '사이버보안과 경제연구회'가 제기한 정보공유 필요성 제언으로부터 시작되었다. 최근에는 `14.8월 비영리사단법인으로 금융ISAC(F-ISAC)이 출범하면서, 각 부문별로 ISAC이 확대되고 있는 추세이다[2].

앞선 사례에 보듯 한·미·일 3개국은 미국 중심의 유사한 정보공유체계로 구축되고 있다. 표 2와 같이 국내는 사이버위협대응 및 정보공유체계 구축을 위해 국가안보실과 NCSC에서 전반적인 방향을 총괄하고 있으

〔표 2〕 현행 사이버위협정보 공유 관련 체계

구분	공공	민간 정보통신	금융
관련 규정	「국가사이버 안전 관리규정」 (대통령훈령)	「정보통신망 이용촉진 및 정보보호 등에 관한 법률」	「정보통신기반 보호법」, 「전자금융감독 규정」
주관	국가기관	미래창조과학부 (한국인터넷진흥원)	금융위원회 (금융보안원)
정보공유	기관별 보안관제센터를 설치·운영하고, 센터간 사이버위협정보를 실시간 공유	사이버위협 관련 통계 등 제한적 정보를 공유	

며, 각 산업 부문인 공공, 금융, 정보통신, 국방, 교육, 의료 등 주무부처별로 정보보호정책을 추진하고 있다. 부문별 법적 근거와 규약에 따라 민간 정보통신부문에서 한국인터넷진흥원(KISA) 인터넷침해대응센터(KrCert), 민간 금융부문에서 금융보안원의 통합보안관제센터·금융ISAC, 공공·정부 부문 정부통합전산센터, 경찰청 산하 사이버보안관제센터, 국방부 산하 사이버사령부 등 각 부문별 센터를 운영 중에 있다.

한편, 국내에서는 `15.5월에는 이를 효과적으로 실행하기 위한 구체적인 법안인 「사이버위협정보 공유에 관한 법률(안)」과 '16.2월 이상기 의원 등 24인이 발의한 관련 법안 「국가 사이버테러 방지 등에 관한 법률(안)」이 발의되었으나 국회 정보위원회에서 합의되지 못하여 본 회의 안건으로 상정되지 못하고 있다.

2.3. 기반 기술

미국은 연방정부 소속 CTIIC를 중심으로 항공우주(NASA), 국가안보(DHS), 국방(DOD)등의 각 부문별로 분류하여 단위를 연계한 정보공유체계를 갖고 있으며, 규격개발을 통한 사이버위협 정보공유를 추진하고 있다. 미국의 국토안보부(DHS)는 사이버 위협에 대응하기 위하여 효율적이고 안전한 정보공유체계 구축의 필요성을 인지하여 `12년부터 규격개발에 착수하였다. 미국의 국토안보부는 MITRE를 통해 `13.4월에 사이버위협정보의 전송 규격인 TAXII(Trusted Automated eXchange of Indicator Information)와 사이버위협정보 표현규격인 STIX(The Structured Threat Information eXpression)를 각각 발표하였으며, Cybox(Cyber Observable eXpression), MAEC(Malware Attribute Enumeration and Characterization)등 다양한 사이버위협정보를 표현하는 정보공유체계 기반기술을 연구하고 있다[5,6].

반면, 한국·일본은 상대적으로 사이버위협 정보공유를 위한 기반기술과 시스템 이 부족하고 각 부문별 협력체계가 과도기적 성장 단계에 있어, 산업 부문 간 사이버위협 정보공유가 상대적으로 미비한 실정이다. 또한, 각 기관 별로 정보격차가 발생하거나 신뢰성 낮은 정보로 인하여 오남용 될 수 있는 잠재적인 문제에도 직면해 있다.

국내에 대표적으로 구축·운영되고 있는 KISA의 정보공유시스템 C-TAS(Cyber Threat Analysis & Sharing)는 `14.8월에 구축하여 운영하고 있으며, 민간 정보통신 사업자들과 XML기반 기술로 사이버위협정보를 공유하고 있다. KISA는 STIX를 참조하여 C-TEX라는 정보표현 방식과 전송 규격을 정의하였다. C-TAS는 포털과 쇼핑몰, 게임사, 보안 기업이 올리는 사이버위협정보를 실시간으로 공유하는 시스템으로 현재 약 100여개 민간 기업이 C-TAS를 활용 중이다. 그러나 C-TAS는 정보에 대한 민감도와 긴급도 분류 등 정보자산의 식별 및 분류에 대한 정보관리체계가 상대적으로 미흡하다는 단점이 있으며, 이에 보다 활발한 정보공유를 위해 정보의 신뢰성을 높일 수 있는 방안을 강구해야 할 것으로 판단된다.

2.4. 시사점

국내 정보공유체계는 미국의 사례와 비교하여 볼 때 다음과 같은 시사점이 있다. 첫째, 국내·외 사이버위협정보를 공유를 위한 체계적인 사이버위협 정보관리체계가 미비하여 이를 정비하고 지속적으로 개선시킬 필요가 있다. 이는 일관성 있는 사이버위협정보의 자산 식별과 정보 분류를 어렵게 만들어 효과적인 사이버위협 분석·대응을 어렵게 한다. 특히, 식별된 위협정보가 공유되지 않거나 민감한 정보가 공유되는 등 잠재적인 문제를 일으킬 가능성이 있다. 현재는 정보공유시스템 구축과 운영에 관한 기반 연구가 부족하여 기관별로 비정형 정보가 공유되고 있으며, 이로 인한 수집-분석-정보공유 프로세스의 비효율이 초래되고 있다. 이러한 문제를

해결하기 위해 수집된 정보자산에 대한 정보 분류 및 공유 기준을 마련하고, 지속적으로 개선할 필요가 있다.

둘째, 관련 법적 근거가 미비하여 원활한 사이버보안 위협대응 및 정보공유체계를 구축·운영하는 데 어려움이 생길 수 있다. 과거 2013년에 3·20 사이버테러 등이 발생하며 '국가 사이버안보 종합대책'이 마련되었고, 관련 업계에서 사이버위협정보 공유 요구가 높았다. 그러나 현재까지도 이를 체계적으로 수행할 수 있는 법적근거가 마련되어 있지 않다는 것은 향후에 안정적인 정보공유체계 운영을 어렵게 할 가능성을 남겨두는 것이다.

셋째, 공유 정보를 얼마나 신뢰할 수 있는지에 관한 판별기준이나 메커니즘, 정보공유 방식에 대한 논의가 부족하다. 신뢰되지 않은 정보의 공유는 정보공유에 참여하는 이해관계자들의 활동을 위축시키고 있으며, 이는 위협이 발생하였을 때 부정적인 영향을 미칠 가능성이 높다.

Ⅲ. 우선순위 도출

3.1. 요구사항 정의

본 연구는 앞장에서 언급한 시사점을 토대로 효과적인 사이버위협정보 공유체계 수립에 필요한 요구사항의 우선순위를 도출하기 위한 연구가설을 표 3과 같이 정책적 요인과 기술적 요인으로 분류하여 정의하였다. 정책적 요인은 '1. 사이버위협 정보관리체계(정보자산 식별 및 분류 관점) 마련, 2. 사이버위협정보 공유기준 마련, 3. 사이버위협정보 공유를 위한 법적 근거 마련'으로 정의한다. 기술적 요인은 '1. 사이버위협정보 수집 방법 개선, 2. 사이버위협정보 표현방식 및 전송 규격 표준화, 3. 사이버위협정보 공유채널 개선'으로 정의한다.

3.2. 도출 방법

〔표 3〕 정책적·기술적 요구사항 정의

정책적 요구사항		기술적 요구사항	
1	사이버위협 정보관리체계 마련	1	사이버위협정보 수집 방법 및 신뢰성 개선
2	사이버위협정보 공유기준 마련	2	사이버위협정보 표현방식 및 전송 규격 표준화
3	사이버위협정보 공유를 위한 법적 근거 마련	3	사이버위협정보 공유채널 개선

계층분석의사결정(AHP, Analytic Hierachy Process)은 의사결정의 계층구조를 구성하고 있는 요소간의 쌍대비교에 의한 판단을 통하여 평가자의 지식, 경험 및 직관을 포착하고자 하는 하나의 새로운 의사결정방법론이다. AHP는 목표들 사이의 중요도(Weight)를 계층적으로 나누어 파악함으로써 각 대안들의 중요도를 산정하는 기법이기도 하다[9]. 본 연구에서는 AHP분석 기법을 이용하여 국내 보안전문가 대상 34명을 대상으로 설문조사하였다. 설문은 보안업무와 관련된 공무원·공공기관 재직자 8명, 연구·유관기관 재직자 15명, 보안업체 재직자 11명을 대상으로 실시되었다.

3.3. 요구사항 도출 결과

AHP분석결과의 신뢰도를 판단하는 기준인 일관성지수(CR, Consistency Rate)의 값이 0.1보다 낮으므로(CR = 0.06) 분석은 유효한 것으로 확인되었다. 표 4의 도출 결과, 1계층은 공무원·공공기관 및 연구·유관기관 재직자 2개 집단에서 정책적 요구사항이 기술적 요구사항 보다 높은 것으로 나타났다. 정책적 요구사항(2계층) 영역에서 동일한 2개 집단에서 법적근거 마련, 정보관리체계 마련, 공유기준 마련 순으로 중요하게 생각하는 것으로 나타났으며, 보안업체에 재직하는 집단에서는 상대적으로 정보관리체계 마련을 우선시하는 것으로 나타났다. 기술적 요구사항(2계층)영역에서는 연구·유관기관 재직자 및 보안업체 재직자 2개 집단에서 정보의 표현방식 및 전송규격 표준화를 가장 중요한 요구사항이라고 응답하였고, 수집 방법 및 신뢰성 개선, 정보공유채널 개선 순으로 나타났다.

설문조사의 응답자들은 현재 재직하는 회사의 특성의 따라 중요하다고 여기는 요구사항이 상이하였으나, 전반적으로 정책적인 부분에서는 사이버위협 정보공유와 관련된 법적 근거의 마련을 중요한 요구사항으로 판단하였다. 기술적인 부분에서 정보공유의 표현방식과 전송규격을 규격화해야 하는 것을 상대적으로 더 중요시 여긴 것으로 확인된다.

Ⅳ. 관련 연구

최근까지 국내에 발표된 여러 연구는 수집된 사이버위협정보를 분석하는 방법에 초점을 두어, 어떻게 사이버위협정보를 수집하고 그에 따른 위험도를 측정할 수

있는 지에 관하여 연구하였다[15, 16, 17]. Xie (2010)는 사이버위협 분석에 초점을 두어 Bayesian 추론 기법으로 사이버위협을 예측하는 방법을 제안하였다. 즉, 분석된 정보를 어떻게 수집하여 위험을 정량화할 수 있는지에 중점을 두었는데, 본 연구는 분석된 정보를 어떻게 효과적으로 공유할 수 있는 지에 관하여 접근하고 있기 때문에 기존 연구와 비교하여 볼 때 관점은 다소 상이하다고 볼 수 있다.

사실, 미국에서는 민관이 협력하여 사이버위협정보를 정량화하고 위험을 측정하기 위한 프로젝트가 지속적으로 운영되고 있으며, 이에 대표적인 사례는 CVE(Common Vulnerability Exposures)와 이를 점수화하여 관리하기 위한 시스템인 CVSS(Common Vulnerability Scoring System)를 꼽을 수 있다[1, 4].

Gordon (2003)는 보안업계에서 정보공유의 중요성을 경제학적인 관점에서 강조하였으며[8], 이에 Cavelty (2007), Hausken (2007)는 사이버위협으로 발생 가능한 위험확산 방지와 예방을 위해 지속적인 정보공유 활동을 수행하는 것은 경제적인 이득이 있다고 설명하면서 범정부차원의 정보공유의 중요성을 논의하였다[7, 10].

더욱이 2010년 이후 사이버위협정보 공유에 관한 논의가 계속되면서 FS-ISAC등 부문별 정보공유센터가 설치되기 시작하였고, 이와 관련하여 US-CERT에서는 MITRE를 통하여 STIX와 TAXII 등을 연구 완료하였다[5]. 2014년 전후로 미국은 이와 관련된 기반 기술을 각 부문별 정보공유센터에 구축 완료하여 사이버위협정보를 상시에 공유하고 있으며, 분석·공유기술을 지속적으로 연구하고 있다.

Ⅴ. 결 론

본 연구에서는 사이버위협에 대한 피해확산 방지와 위험을 최소화하기 위한 정보공유체계를 수립하는 과정에서 필요한 정책적·기술적 요구사항들을 정의하였다. 요구사항들의 우선순위를 살펴볼 때 정책적 요구사항이 기술적 요구사항에 비하여 보다 중요하게 여기는 것으로 나타났으며, 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.

이를 종합하여 볼 때 사이버위협정보의 효과적인 분석과 공유를 위해서는 선결적으로 이를 추진하기 위한 법적 근거의 마련과 운영에 관한 지침과 기준이 만들어져야할 것이다. 또한, 수집된 정보들의 표준화된 저장과 전송이 이루어질 때 분석과 관리가 용이하여 정보공유의 그 효율성을 향상시킬 수 있다. 결론적으로 우리나라

〔표 4〕 요구사항 우선순위 도출 결과

	공공부문 재직자(8)		연구·관련기관 재직자(15)		보안전문업체 재직자(11)	
Level 1	1	정책적 요구사항 (0.75)	1	정책적 요구사항 (0.60)	1	기술적 요구사항 (0.63)
	2	기술적 요구사항 (0.25)	2	기술적 요구사항 (0.40)	2	정책적 요구사항 (0.36)
Level 2 정책적 요구사항 (정보관리체계/공유기준/ 법적근거)	1	법적 근거 마련 (0.62)	1	법적 근거 마련 (0.46)	1	정보관리체계 마련 (0.54)
	2	정보관리체계 마련 (0.25)	2	정보관리체계 마련 (0.34)	2	법적 근거 마련 (0.36)
	3	공유기준 마련 (0.13)	3	공유기준 마련 (0.20)	3	공유기준 마련 (0.10)
Level 2 기술적 요구사항 (정보수집 방법 및 신뢰성 /표현방식 및 전송규격 표준화/정보공유채널)	1	수집 방법 및 신뢰성 개선(0.50)	1	표현방식 및 전송규격 표준화(0.47)	1	표현방식 및 전송규격 표준화(0.46)
	2	표현방식 및 전송규격 표준화(0.25)	2	수집 방법 및 신뢰성 개선(0.4)	2	수집 방법 및 신뢰성 개선(0.36)
		정보공유채널 개선 (0.25)	3	정보공유채널 개선 (0.13)	3	정보공유채널 개선 (0.18)

는 사이버위협정보 공유체계 구축에 적극적으로 나서고 있는 미국의 기반 정책과 기술을 차용하되 국내 상황에 걸맞게 발전해 나가야 한다는 것을 의미하며, 공공·민간이 협력하여 신뢰성 있는 정보를 공유할 때 보다 나은 사이버위협 정보 공유체계를 수립할 수 있을 것이라 기대한다.

참 고 문 헌

[1] CVE, https://cve.mitre.org/

[2] FS-ISAC, https://www.fsisac.com/

[3] IPA J-CSIP, http://www.ipa.go.jp/

[4] NVD CVSS, https://nvd.nist.gov/

[5] STIX Project, https://stixproject.github.io/about/

[6] Barnum, Sean. “Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX).” MITRE Corporation, 2012.

[7] Cavelty, Myriam Dunn. *Cyber-security and threat politics: US efforts to secure the information age.* Routledge, 2007.

[8] Gordon, Lawrence A., Martin P. Loeb, and William Lucyshyn. “sharing information on computer systems security: An economic analysis.”, *Journal of Accounting and Public Policy* 22(6), pp.461-485, 2003.

[9] Harker, Patrick T. Analytic hierarchy process. Vol.113. Pergamon, 2003.

[10] Hausken, Kjell. “Information sharing among firms and cyber attacks.” *Journal of Accounting and Public Policy* 26(6), pp.639-688, 2007.

[11] Liu, Charles Zhechao, Humayun Zafar, and Yoris A. Au. “Rethinking fs-isac: An it security information sharing network model for the financial services sector.” *Communications of the Association for Information Systems* 34(1), 2014.

[12] NIST Special Publication 800-150: *Guide to Cyber Threat Information Sharing (Draft)*, 2014.

[13] Rob McMillan, *Definition: Theat Intelligence, Gartner,* May 2013.

[14] Xie, Peng, et al. “Using Bayesian networks for cyber security analysis.” Dependable Systems and Networks (DSN), *2010 IEEE/IFIP International Conference on. IEEE*, 2010.

[15] 김기영, 임선희, 김종현. "사이버 위협 사전인지를 위한 위협 정량화 기술." *정보보호학회지* 22(8), pp.15-20, 2012.

[16] 김성원, et al. "네트워크 기반의 실시간 위험관리를 위한 위험분석 및 평가 방법연구." *한국정보과학회 한국컴퓨터종합학술대회 연구집* 34(1), pp.29-34, 2007.

[17] 이기혁, 이철규. "사이버 환경에서의 침해사고대응을 위한 위험도 산정 및 실시간 경보생성에 대한 연구." *정보보호학회지* 18(5), pp.112-124, 2008.

〈저 자 소 개〉

김 애 찬 (Aechan Kim)
정회원

2009년 2월 : 서울과학기술대학교 산업정보시스템공학과 졸업(공학사)
2009년 3월~2011년 6월 : 육군 정보체계운용장교
2014년 2월 : 고려대학교 정보보호대학원 금융보안학과(공학석사)
2014년 3월~현재 : 고려대학교 정보보호대학원 정보보호학과 박사과정
2014년 2월~2015년 4월 : 금융보안연구원 근무
2015년 4월~현재 : 금융보안원 대리
관심분야 : Network Security, Pattern Recognition, Machine Learning

이 동 훈 (Dong Hoon Lee)
종신회원

1983년 2월 : 고려대학교 경제학과 졸업
1987년 12월 : Oklahoma University 전산학과(공학석사)
1992년 5월 : Oklahoma University 전산학과(공학박사)
1992년 8월 : 단국대학교 전자계산학과 전임강사
1993년 3월~1997년 2월 : 고려대학교 전산학과 조교수
1997년 3월~2001년 2월 : 고려대학교 전산학과 부교수
2001년 2월~현재 : 고려대학교 정보보호대학원 교수
관심분야 : 암호프로토콜, 암호이론, USN 이론, 키 교환, 익명성 연구, PET 기술