주요국의 사이버위협정보 공유체계 분석을 통한 국내 적용모델 연구

윤오준* · 조창섭* · 박정근* · 배선하** · 신용태***

요 약

최근 정부 주요인사 대상 스마트폰 해킹과 인터파크사 고객정보 탈취 등 사이버위협은 이제 우리에게 현실적인 위협으로 다가오고 있고 이러한 위협은 사물인터넷 시대 도래로 인해 더욱 고도화될 것이며 이에 대응하기 위해 민·관간 사이버위협정보 공유에 대한 체계 정립은 반드시 필요하다. 미국·일본·영국 등 주요국은 공유기구를 설치하고 관련대책을 수립·시행하는 등 사이버위협정보 공유제도를 정착시켜 나가고 있으나, 우리나라는 몇 개 기관이 공유센터를 자체 구축하여 운영하고 있고 참여기관간 정보의 제공과 공유에 있어 불균형이 존재하는 등 제도적인 미흡으로 활성화가 되지 못하고 있는 실정이다. 이에 나날이 진화하는 사이버위협에 효과적으로 대응하기 위해 정보공유체계 운영주체의 명확한 설정, 민간·공공간 협업체계 운영, 통합적이고 자동화된 시스템 구축, 면책권 부여 등 법·제도 보완 등 국내에 적용 가능한 모델을 제시하고자 한다.

A Study on the Domestic Model for Cyber Threat Information Sharing by Analyzing the Relevant Systems of Major Advacnced Countries

Yoon Oh Jun* · Cho Chang Seob* · Park Jeong Keun* · Bae Sun Ha** · Shin Yong Tae***

ABSTRACT

The recent cyber threats are becoming real threats to our lives. This gloomy situation from cyber threats necessarily demands the establishment of the cyber threat information sharing system between the public and private area. Key countries, like the US, Japan and the UK, are stabilizing the cyber threat information sharing systems by founding exclusive organizations for sharing information and setting up and implementing relevant measures. In this thesis, I would like to propose the model for cyber threat information sharing in order to cope efficiently with the ever-intensifying cyber threats. My model would include key elements for the efficient information sharing, such as the clear designation of main operator of information sharing system, the management of collaboration system between the public and private sector, the build-up of the integrated and automated system and the supplementation of legal system including the grant of privilege, and so on.

Key words : Cyber Threat, Information Sharing, Cyber Security, Hacking

투고일(2016년10월20일), 접수일(2016년12월1일)
수정일(2016년12월9일), 게재확정일(2016년12월12일)

* 숭실대학교 IT정책경영학과
** 국가보안기술연구소
*** 숭실대학교 컴퓨터학부(교신저자)

1. 서 론

지난 7월 인터넷 쇼핑몰 업체인 인터파크사가 해킹되어 2,665만여건의 고객정보가 탈취되었고[1], 이보다 앞서 지난 2월부터 국방 등 정부기관 주요인사와 일반 국민들의 스마트폰이 해킹되어 문자메시지와 통화내역 등이 절취되었으며, 국내 인터넷뱅킹 보안소프트웨어 제작업체도 해킹되어 이 제품을 사용하는 2천만 명 이상의 국민들에게 금융혼란이 발생할 우려도 있었다[2]. 또한 국제적으로는 미상의 해킹조직들이 방글라데시 중앙은행에서 8,100만 달러를 절취하는[3] 등 고도의 해킹기술을 구사하는 사이버위협은 이제 공공기관과 민간영역을 구분하지 않음은 물론 국내와 해외를 가리지 않고 동시다발적으로 발생하고 있다.

게다가 향후 사이버위협은 국민들의 스마트폰을 해킹하고 개인정보를 절취하여 금전탈취에 이용하는가 하면 사생활을 폭로하겠다며 협박에 악용하는 등 국민 개개인에게 현실적인 위협으로 다가올 것이며, 사물인터넷 시대가 도래하면서 최신 IoT 기기에 대해 지능적인 해킹수법을 동원하여 혼란을 가중시킬 것이며, 또한 국민 생활과 직결되는 국가·사회 기반시설에 대한 사이버테러도 감행하여 정부불신을 초래하고 국민들의 일상생활을 불편하게 함은 물론 생명까지도 위협하는 등 전방위적으로 국가안보와 국익을 위협하는 핵심적인 요소로 대두될 것으로 예상된다.

이에 미국 등 세계 각국들은 국가·산업기밀이나 국민의 개인정보 및 주요 기반시스템을 각종 사이버위협으로부터 보호하기 위해 대응기구 설치 등 조직정비와 법·제도적인 개선작업을 병행하는 등 적극적으로 대처해 나가고 있으며, 해외기업의 경우 시만텍·인텔 등 여러 글로벌 보안기업들이 모여 사이버위협 연대(Cyber Threat Alliance)를 결성하기도 하였으며[4], 우리나라도 북한이나 중국 등으로부터 사이버위협에 대응하기 위해 정부에서는 민간기관과 협업하여 사이버위기대응훈련 등 범 국가차원의 대비태세를 구축해 나가고 있다.

그러나 최근 사이버공격이 점점 고도화되고 심각해지면서 사이버위협정보에 대한 유관기관간 공유의 필요성을 인식하고 미래부 등 몇 개 부처에서 자체적으로 시스템을 구축하여 공유를 시도하고 있으나 통합된 운영체계나 정보시스템의 미구축, 참여기관의 의지부족, 인센티브 부여 등 법령상 유인책 미흡, 프라이버시 보장 등 개인정보 보호와 안보 및 국익과의 법익 고려 등 현실적인 문제가 해소되지 않아 그 효과에 있어서는 아직 소기의 성과를 거두지 못하고 있는 실정이다.

이러한 측면에서 사이버안보 사고를 미연에 방지하고 예방대책을 수립하는 한편 사고 발생 시에도 체계적이고 신속한 대응조치를 취하기 위해서는 관계기관간 사이버위협정보에 대한 공유가 그 무엇보다도 중요하다 하겠다. Liu 등도 사이버위협에 대한 정보 획득을 통한 사전 예방활동과 사고 탐지 및 사후 공동대응 그리고 피해확산 방지 등을 목적으로 정보공유가 필요하다고 하였다[5]. 이에 본 논문에서는 미·일·영 등 주요국의 사이버위협정보 공유체계를 분석하고 우리나라의 현재의 공유실태를 점검함으로써 궁극적으로는 국내 실정에 바로 적용할 수 있는 사이버위협정보 공유체계의 개선 모델을 제시하고자 한다.

2. 관련 연구

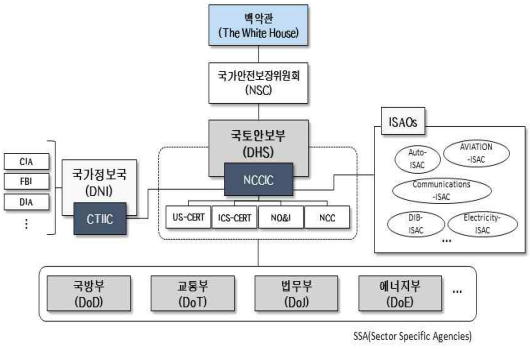
2.1 미국의 사이버위협 정보공유 체계

2.1.1 추진기구 등 법·제도[6][7][8]

미국은 2015년12월 「사이버안보법(Cybersecurity Act of 2015」을 제정하였는데 동법에는 「사이버안보 정보공유법(CISA, Cybersecurity Information Sharing Act of 2015)」과 「국가사이버안보보호발전법(NCPAA, National Cybersecurity Protection Advancement Act of 2015)」 등이 포함되어 있는데, 사이버안보 관련 정보공유를 체계적으로 규정한 CISA에는 정부기관 간 및 공공·민간 간 정보공유 절차를 마련하고, 민간주체는 사이버위협의 탐지·차단 및 이를 완화하기 위한 예방 및 방어조치를 수행하며, 국토안보부(DHS)와 법무부((DoJ)는 사이버위협에 대한 연방정부의 방어조치 절차 마련과 인권보호 방안을 확

보해야 하며, 국가정보국(ODNI)으로 하여금 사이버위협 보고서를 의회에 제출토록 하고 있으며, 특히 기관간 정보공유 과정에서 발생할 수 있는 일부 부작용에 대한 법적 면책권을 부여하고 있다.

미국의 사이버위협 정보공유 체계는 (그림 1)에서 보는 바와 같이 국토안보부와 국가정보국을 중심으로 사이버위협 정보공유 체계를 구축하여 운영 중인데 DHS는 연방사이버안보통신통합센터(NCCIC, National Cybersecurity & Communications Integration Center)를 설치하여 주요 정부기관과 민간 파트너 대상 사이버위협정보를 공유하는 창구 역할을 수행토록 하고 있고, ODNI는 정보기관을 중심으로 국가안보에 영향을 미칠 수 있는 국내외 사이버위협 정보를 수집하여 공유함으로써 공공과 민간의 효과적인 대응을 지원하고 있다.



(그림 1) 미국의 사이버위협 정보공유 체계

NCCIC는 2009년10월 CS&C(Cybersecurity & Communication) 부서 밑에 설립된 정보공유센터로 US-CERT, ICS-CERT, NO&I(NCCIC Operations & Integration), NCC(National Coordinating Center for Communications)로 구성되어 있으며 연방정부, 주·지역 정부 및 정보기관, 민간분야 등과 사이버위협정보를 24시간 공유하고 있다.

미 대통령 행정명령(Executive Order) 제13691호에 의해 설립된 정보공유분석기구(ISAOs, Information Sharing & Analysis Organizations)는 공공·민간부문을 아우르는 정보공유분석 조직으로 산업분야에 한정하지 않고 공공·민간이 모두 참여한다는 점에서 산업분야별로 구분하여 설립되어 해당분야의 구성원 중심으로 정보를 제공하는 기존의 ISAC(Information Sharing & Analysis Center)과는 다르다고 할 수 있다[9].

국가정보국(ODNI)는 오바마 대통령의 지시로 사이버안보 관련 정보를 공유하고 관계기관을 조정·감독하기 위해 2015년 2월에 사이버위협정보통합센터(CTIIC, Cyber Threat Intelligence Integration Center)를 설립하였으며, ODNI에 소속된 각 부처 및 기관은 미국의 국익에 영향을 줄 수 있는 사이버위협 및 사고와 관련된 모든 정보를 CTIIC와 공유토록 하고 있으며, CTIIC는 NCCIC, 국가 사이버범죄 합동수사 TF(NCIJTF, National Cyber Investigative Joint Task Force), 미 사이버사령부(USCYBERCOM, U.S. Cyber Command)와 협력관계를 유지하며 사이버위협관련 정보업무를 지원하고 있다.

2.1.2 정보공유 프로그램

DHS는 사이버위협 정보공유 정책으로 사이버 정보공유 및 협력 프로그램(CISCP, Cyber Information Sharing and Collaboration Program)과 국가기반시설보호계획(NIPP, National Infrastructure Protection Plan)을 시행하고 있다. CISCP는 정부·민간간 위협정보 공유를 통해 사이버위협을 사전에 예방·차단하고 대응하기 위해 DHS 산하의 NCCIC가 주도하는 정보공유 프로그램으로 CISCP 참여 파트너들은 식별된 취약점과 사이버위협정보 지표를 DHS로 전송하고, DHS는 이를 검토하고 익명으로 처리하여 CISCP 파트너들과 공유하고 있으며, 이를 위해 CISCP 분석관은 정부·산업계 파트너들과 해당 정보로부터 민감한 개인정보·기밀정보 등의 포함여부를 파악하여 정확하고(accurate), 연관성이 높고(relevant), 시의적절하며(timely), 수행 가능한(actionable) 분석정보를 생산하고 있다[10]. NIPP는 국가기반시설에 대한 정보공유를 통해 사이버위협을 예방·탐지·방어하여 주요자산·시스템·네트워크에 대한 보안취약성

을 감소시키고 공격의 파급력을 약화시키고자 DHS에서 추진하는 정책으로 기반시설을 화학, 상업시설, 통신, 제조, 댐, 응급서비스, 정보기술, 원자로·핵물질·핵폐기물, 농업, 식품, 에너지, 보건·공중위생, 금융서비스, 수자원·폐수시스템, 정부시설, 교통시스템 등 16개 부문으로 분류하여 각 부문별로 주무기관을 지정하고 관리자 역할을 부여하고 있다[11].

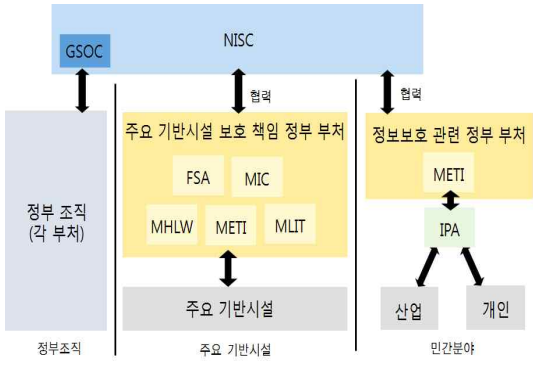
2.1.3 정보의 생산 및 전송 시스템

국토안보부(DHS)와 국립기술표준연구소(NIST)는 2012년부터 사이버위협 정보에 대한 표현 및 전송에 대한 표준화 작업을 추진해왔으며 그 결과로 표현규격인 STIX(Structured Threat Information eXpression)와 전송규격인 TAXII(Trusted Automated eXchange of Indicator Information)를 2013년10월에 공개하였다[12][13][14]. STIX는 개별조직들이 보유한 사이버위협 정보의 개념을 표준화하고 구조화하여 일관된 분석과 자동화된 해석을 가능하게 하는 표현규격으로 구성요소로는 사이버공격활동, 공격자, 공격수법, 탐지지표, 관측지표, 사고, 조치사항, 공격대상 등 8개 이다. TAXII는 STIX로 표현된 위협정보를 실시간으로 공유하기 위한 자동 전송규격으로 제공정보알림, 정보구독관리, 콘텐츠 수신, 콘텐츠 요청과 같은 4가지 서비스를 제공하며 현재 HTTP 및 HTTPS 프로토콜을 지원하며 향후에는 SMTP·SOAP 등 멀티프로토콜도 지원할 예정이다. 또한 NIST는 정보공유체계 유형을 중앙집중형(Centralized) 구조와 분산형(Peer-to-Peer) 구조를 제시하고 있는데[15], 중앙집중형 구조는 초기 정보공유체계에 적합한 모형으로 효율적인 운영과 통제가 용이하고 신속한 의사결정과 정보공유가 가능하다는 장점이 있으며, 분산형 구조는 운영과 통제가 다소 떨어지나 정보가공에 있어 상호 보완적이고 분산환경에서 보다 활발한 정보공유가 가능하다는 장점이 있으나 민감정보의 유출 가능성도 내재하고 있다[26].

한편, 미 국제전략연구센터(CSIS, Center for Strategic and International Studies)는 정부기관, 산업계, 개인정보보호 단체, 전문가 그룹 등이 참여하여 사이버위협 정보공유를 위한 기술적(technical)·구조적(structural)·법적(legal) 도전과제를 검토하여 2014년12월에 사이버위협 정보공유 노력 및 관련 법·정책 수립에 참고할 수 있는 '사이버위협 정보공유를 위한 권고'안을 발간하였다[16].

2.2 일본의 사이버위협 정보공유 체계

일본은 2014년11월에 「사이버시큐리티기본법(サイバーセキュリティ基本法)」을 제정하여 국가행정기관, 독립행정법인, 특수법인간 사이버시큐리티 관련 정보공유 등 사이버안보 확보에 필요한 시책을 마련토록 하고 있으며, 내각관방정보보안센터(NISC, National Information Security Center)를 중심으로 정부조직, 기반시설, 민간분야로 분류하여 사이버위협 관련 정보를 수집하고 공유의 범위를 확대하고 있다.



(그림 2) 일본의 사이버위협 정보공유 체계

일본의 사이버위협 정보공유 체계는 (그림 2)에서 보는 바와 같이 정부조직에 대한 정보공유는 NISC 내부조직인 정부안보운영조정팀(GSOC, Government Security Operation Coordination team)에서 정부부처 및 조직간의 정보공유 업무를 수행하고 있는데 정부기관을 대상으로 24시간 모니터링을 전담하며 사이버공격 관련 정보 수집·분석을 통해 즉각적인 대응책을 지원하고 있다[17].

기반시설에 대한 정보공유는 NISC에서 기반시설 보호 책임을 가진 금융청(FSA), 총무성(MIC), 후생노동성(MHLW), 경제산업성(METI), 국토교통성(MLIT) 등 다른 정부부처와 협력을 통해 추진하며[18], 기

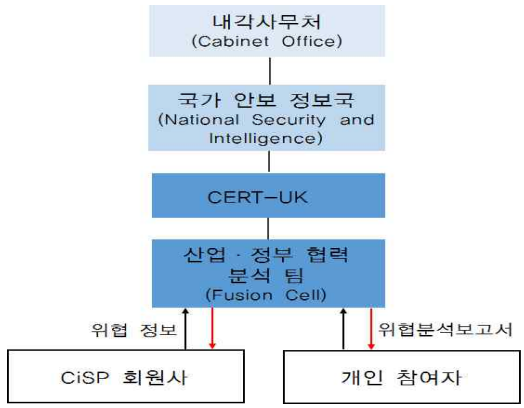
반시설 역량강화(CEPTOARs, Capability for Engineering of Protection, Technical Operation, Analysis and Response) 방안을 마련하고 통신, 금융, 항공, 전력, 가스, 수자원, 물류, 화학 등 16개 부문의 대표자들로 구성된 협의회(CEPTOARs-Council)를 구성하여 운영하고 있으며 여기에는 정부부처인 FSA, MIC, MHLW, METI, MLIT 및 IPA, JPCERT-CC가 참여하여 관련 정보를 공유하고 있다[17].

민간분야에 대한 정보공유는 경제산업성 산하의 민간분야 IT와 정보보안 관련 전문기관인 IPA(Information-technology Promotion Agency)에서 사이버안보 정보공유 체계인 J-CSIP(Initiative for Cyber Security Information sharing Partnership of Japan)를 2011년10월부터 운영하고 있다. J-CSIP 프로그램은 정부와 민간분야의 정보공유 체계로 유사한 공격의 조기탐지 및 피해 방지, 공격에 대한 방어 실시, 향후 예상되는 공격에 대한 대책 마련 등을 목표로 하고 있고, IPA로 하여금 사이버안보 관련 위협정보 수집 및 공유를 위한 배포업무를 수행토록 하고 있으며, 전력·화학업계 등 참여하는 그룹(SIG, Special Interest Group)과는 비밀유지각서를 체결하는 등 보호 조치 후 정부가 보유한 사이버안보 관련 정보를 그룹 연구자에게 제공하거나 일정기간 동안 연구자를 NISC의 특정 그룹에 투입을 가능하도록 하고 있다[8][19].

한편, 위협정보 공개와 국제협력을 위해 JPCERT/CC는 취약점 정보 알림 포털사이트인 JVN(Japan Vulnerability Notes)을 운영하고, 해외 CERT/CC와의 국제협력을 통해 수집되는 취약점 정보 및 국내 J-CSIP를 통해 수집되는 취약점 정보를 취합하여 JVN에 공개하고 있다[20].

2.3 영국의 사이버위협 정보공유 체계

영국의 사이버위협 정보공유 체계는 (그림 3)에서 보는 바와 같이 CERT-UK로 하여금 사이버안보 정보공유 프로그램(CiSP, Cyber Security Information Sharing Programme) 운영을 통해 정부와 민간간의 정보공유를 주도토록 하고 있다.



(그림 3) 영국의 사이버위협 정보공유 체계

CERT-UK의 주요 임무는 산업계·학계·정부와 정보공유 및 협력을 통한 사이버 복원력을 강화하는 것으로 내각사무처의 국가안보정보국(National Security and Intelligence) 산하로 2014년에 National CERT로 지정되었다[21]. 산업·정부 협력 분석팀(Fusion Cell)은 다양하고 광범위한 출처로부터의 사이버 위협 정보에 대한 검사와 분석을 통해 피드백을 제공하고 악성코드 및 피싱메일에 대한 맞춤형 분석, 제품과 서비스에 대한 보안경고 및 자문을 제공하는 등 CiSP 멤버의 전반적인 사이버안보 성숙도 향상을 위한 대책을 지원하고 있다.

사이버위협 정보공유 프로그램(CiSP)은 사이버위협에 대한 전반적인 인식을 향상시키고 취약점 등 정보를 공유하여 사이버위협이 산업에 미치는 영향을 최소화 하는 것이 목적이며, 정부와 산업간의 협력 이니셔티브 일환으로 정부와 산업계 전문가가 파트너십 환경 구축을 위해 상호 합의를 통해 사이버안보에 대한 정보공유 방안을 함께 설계하였다. 분야와 조직에 관계없이 안전한 동적 환경에서 사이버위협 정보를 실시간 공유하고, 공유된 정보에 대한 기밀성을 보장하며, 관련 상황보고서(CNR, CERT-UK Network Reporting)를 주기적으로 발송하여 정보를 공유토록 하고 있다. 또한 CiSP를 통해 공유되는 위협정보는 데이터 보호에 관한 법률에 의거하여 공개범위를 선정하고 보호 방안을 마련해야 한다. 이 프로그램의 참여대상은 영국에 등록된 회사 또는 법인

으로 정부부처의 지원을 받거나 기존 CiSP 참여사와 거래 또는 협력을 하는 회사가 해당되며 2016년 5월 기준으로 2,225개의 조직과 6,150명의 개인이 서비스를 제공받고 있다. 정보의 취급단계는 <표 1>에서 보는 바와 같이 정보의 중요도 및 민감도에 따라 RED, AMBER, GREEN, WHITE 등 4단계로 분류하고 단계에 따라 공유범위를 조정할 수 있다[22].

한편, 정보공유 혜택으로 안전한 환경에서 정부와 산업계간의 연대 대응이 가능하고, 사이버위협에 대한 조기 경보 서비스를 받을 수 있으며, 다른 사용자의 경험·실패·성공으로부터 교훈을 얻게 되며, 조직 요건에 적합한 모니터링 보고서 등을 통해 네트워크 보호를 위한 총체적 역량을 향상시킬 수 있다.

<표 1> CiSP 정보취급 단계

단 계	내 용
RED	지정된 참여자에 한해서 제한적 공유
AMBER	지정된 그룹/조직 내 참여자와 공유될 수 있으나 정보의 출처를 밝히지 않음
GREEN	CiSP 참여자는 모두 공유 가능
WHITE	CiSP 참여자 외에도 공개와 배포 가능 (저작권 또는 공개제한 없음)

2.4 우리나라의 정보공유 운영실태[6]

우리나라는 사이버위협을 모니터링하면서 해킹을 탐지하여 차단하고 수집된 관련정보를 분석하여 공유하기 위해 행자부·미래부·금융위 등 정부부처별로 시스템을 각각 구축하여 운영하고 있다. 행자부는 2011년2월 정부통합전산센터에 사이버위협정보 공유센터를 구축하였고[23], 미래부는 2014년8월에 사이버위협정보분석・공유시스템(C-TAS)을 한국인터넷진흥원에 구축하여 현재 110여개의 민간기관들과 함께 운영하고 있다. C-TAS는 정보의 수집(저장, 통합 프로파일링), 분석(위협탐지, 연관분석), 공유 등 3단계의 프로세스로 구성되어 있으며 기업이 C-TAS 가입 홈페이지에서 가입을 신청하면 KISA에서 일정기준에 따라 심사하여 가입을 승인함으로써 신청기업의 가입이 이루어지며 이후 서비스는 무료로 제공받게 된다[4][24]. 한편, 국가사이버안전센터에서도 2015년 하반기 중앙부처 대상으로 정보공유시스템을 구축하여 운영하고 있으며 특히, 실무자 차원의 보안취약점 등 기술적 위협정보 공유뿐만 아니라 부처의 고위공직자들을 대상으로 북한 등에 대한 고급의 종합적인 위협정보나 국내외 언론이나 연구소가 제기하는 현안사항에 대한 판단정보도 제공하고 있다고 한다.

또한, 「정보통신기반보호법」 제16조에 따라 주요 정보통신 기반시설을 보호하기 위하여 취약점 및 침해요인과 그 대응방안에 관한 정보 제공과 침해사고가 발생하는 경우 실시간 경보·분석체계를 운영하는 등 정부차원에서 민간주도의 ISAC 설치를 권고하고 있고, 현재 금융·통신·행정 ISAC 등이 운영 중이며 미래부는 2017년까지 에너지·의료·교육 등 다른 분야로 점차 확대 구축할 계획이다[25].

그러나 사이버위협정보 공유에 대한 필요성을 인정하여 나름대로 체계를 구축해가고 있으나 부처별 또는 분야별로 제각각 구축하여 운영함으로써 효율적이고 체계적인 정보공유가 되지 않고 있다. 즉, 정보공유에 있어 국가기관은 국가기관끼리, 민간분야는 민간기관끼리 침해사고 현황이나 탐지규칙 등 최소한의 사이버위협 정보를 개별적이고 단편적으로 공유하고 있어 통합된 공유체계가 아직 미흡한 실정이다. 또한, 공유체계에 스스로 가입되거나 가입 승인만 받으면 무료로 서비스를 이용할 수 있기 때문에 정보의 제공은 기관의 의지에 달려있으므로 정보의 제공과 공유가 제대로 이루지지지 않고 있으며 정보의 가치에 대한 객관적인 기준이 없어 정보 제공에 대한 피드백이 부족하고 보상도 없어 공유가 활성화되지 못하는 상황이 지속되고 있다.

따라서 민·관이 함께 하는 국가차원의 정보공유 체계 내에서 참여기관간의 정보제공 서비스에 대한 불균형 해소방안 마련과 함께 사이버위협을 사전에 예측하고 이를 통한 예방적인 보안활동과 사고 발생시 유기적인 공조 대응활동의 한계를 극복하기 위해서는 관계기관간의 사이버위협정보 공유를 활성화하기 위한 체계적이고 효율적인 당근·채찍 방안 강구가 긴요

하다 하겠다.

한편, 김애찬 등은 효과적인 정보공유체계를 수립하기 위한 요구사항의 우선순위 도출 연구에서 정책적 요구사항이 기술적 요구사항보다 보다 더 중요하게 나왔으며, 정책적 요구사항의 경우 관련 법적근거의 마련, 정보관리체계 마련 순이고, 기술적 요구사항은 정보 표현방식 및 전송규격 표준화, 정보수집 방법 및 신뢰성 개선 순으로 나타났으며 궁극적으로는 국가가 주도하여 정책적 기반과 표준기술을 구축하되 공공·민간이 적극적으로 참여하도록 유도하는 방식을 제시하였으며[26], 또한 박상돈 등은 국가차원의 정보공유시스템 구축시 공공기관간, 민간기관간 그리고 공공과 민간을 아울러 정보공유가 원활히 이루어질 수 있도록 부문별 구분 없이 정보수집·분석 역량을 갖춘 기관이 책임지는 정보공유 체계를 수립하고 정보공유를 활성화하기 위한 제도적 보완도 필요하다고 제안하였다[27].

3. 국내 적용 가능한 공유모델

우리나라의 사이버위협정보 공유체계 수립을 위해 미국·일본·영국의 사이버위협정보 공유 추진기구, 운영방법, 민·관 협력시스템 등 운영실태 분석을 통해 국내에 적용 가능한 공유 모델로 정보공유체계 운영주체의 명확한 설정, 민간·공공간 협업체계 운영, 통합적이고 자동화된 시스템 구축, 면책권 부여 등 법·제도 보완 등 방안을 제시하고자 한다.

3.1 정보공유체계 운영주체의 명확한 설정

최근의 사이버공격은 국가·공공기관은 물론 이들 기관보다는 상대적으로 보안이 허술한 민간기관을 침투한 다음 대상기관을 공격하는 우회적인 전술을 구사하고 있다. 그렇기 때문에 기존의 국가·공공기관이 보유한 위협정보와 민간분야에서 탐지하고 수집한 정보를 원활히 공유하기 위해 민・관이 합동으로 참여하는 국가차원의 사이버위협정보 공유센터를 설립하여 조기에 정착시켜 나가야 할 것이다.

지난 5월30일 이철우 의원이 대표 발의한 「국가사이버안보에 관한 법률안」제11조에는 국가차원의 사이버위협정보를 효율적으로 공유하고 관리하기 위하여 국가정보원으로 하여금 국가사이버위협정보공유센터를 구축·운영토록 하고 있으나[28], 지난 9월1일 입법예고된 정부안의 「국가 사이버안보기본법안」제11조에는 공유센터를 국무조정실에 두도록 하고 있어 국민들에게 혼선을 초래하는가 하면 정부기관간 운영주체를 두고 갈등이 있음을 암시하고 있다. 공유센터는 법안 추진과정에서 시민단체 등이 국정원의 권한 강화 내지 민간사찰 우려 등을 제기한 것에 대한 정무적 판단이 작용한 것으로 보이나 사이버위협이 국가안보와 국익의 핵심요소도 대두되고 있는 작금의 엄중한 현실을 직시해봤을 때 정치적인 타협의 대상이 되어서는 안되며, 또한 「정부조직법」 상 부처간 임무·기능을 고려해 보더라도 경제·사회 분야의 정책이나 갈등 조정 등을 주 임무로 하는 국무조정실의 역할보다는 국내외 정보를 취급하고 안보업무를 수행하는 국정원의 역할에 가깝다고 판단되어지므로 국정원에 두는 것이 바람직할 것으로 보인다.

한편, 관련 연구에서도 살펴본 대로 미국도 국가안보를 다루고 정보를 종합하는 국가정보국(ODNI) 밑에 CTIIC를, 국토안보부에 NCCIC를 두고 두 기관을 연계한 사이버위협 정보공유 체계를 구축함으로써 기관간 원활한 정보공유를 유도하고 있는 사실 또한 우리에게 시사하는 바가 크다 하겠다.

3.2 민간·공공간 협업체계 운영

현재 각급기관별로 위협정보를 자체적으로 수집하여 활용하거나 유관기관들과 일부 제한적으로 공유를 하고 있는 실정이나 기관간 정보공유에 대한 불신이 아직 남아 있어 실질적으로 유용한 정보에 대해서는 공유가 원활하지 못한 상황이 지속되고 있다. 정부기관 내에서는 국정원이 국가·공공기관을 대상으로 각급기관의 보안관제센터로부터 수집된 위협정보를 실시간 제공하면서 탐지규칙을 개발하여 지원하고 있는 것으로 알려져 있고, 미래부(한국인터넷진흥원)는 정보통신서비스제공자(ISP)나 정보보호업체와 연계하여 악성코드와 보안취약점 등을 공유하고 있으며, 금융위(금융보안원)는 은행・증권 등 금융사를 대상으로 피

싱사이트 등 침해시도 정보를 제공하고 있으며, 행자부(정부통합전산센터)는 일부 공공기관이나 보안업체와 관련정보를 공유하고 있다. 이는 각급기관들이 보유중인 위협정보가 양적으로 크게 차이가 있는데다 질적으로는 수준차가 상당히 커 기관간 정보공유에 대한 신뢰가 구축되지 않아 정부공유를 주저하면서 원활히 진행되지 않고 있는 것으로 보인다.

따라서 민·관간 원활한 위협정보 공유를 위해서는 국가・공공기관, 민간업체 및 연구소 등 제반 사이버 대응 요소가 참여하는 '민·관 사이버위협 정보공유 협의체'를 구성하여 제대로 운영하여야 한다. 이 협의체를 통해 민간을 포함한 국가차원의 위협정보 공유체계나 제도적 보완 방안 등을 논의하여 개선할 필요가 있으며 이를 활성화하기 위해 미래부, 행자부, 금융위, 국정원 등 정부차원에서도 유관기관간 실무적 협력을 통해 공유하는데 있어 방해 요소를 과감히 제거해 나가고 한편으로는 행정적이고 재정적인 지원을 강화해야 할 것이다. 해당기관의 자발적 참여를 유도하기 위해 참여기관 입장에서도 자사의 정보를 대부분 제공하면서 반대급부로 협의체에서 공유되는 모든 정보를 수혜 받을 수 있다는 신념을 가지고 최대한 동참하는 노력을 보여야 할 것이다.

3.3 통합적이고 자동화된 시스템 구축

현재 우리의 정보공유시스템은 각급기관이 필요에 의해서 제각각 구축하여 운영하면서 민간・공공기관간 통합된 공유체계가 미흡하여 사전에 위협을 예측하거나 이를 통한 차단활동이나 위기경보 발령 등 유기적인 대응이 곤란한 실정이다. 또한 시스템 구축·운영 측면에서도 처음에 기관별 별도의 시스템으로 구축되었으므로 나중에 서로 다른 시스템을 연계할 경우 통합하는데 상당한 기술적인 어려움이 우려되고 있다.

그래서 사이버위협정보를 서로 다른 기관과 상호 공유하거나 자동적으로 교환을 확산시키기 위해서는 국가차원의 체계적이고 통합적인 공유시스템의 구축이 무엇보다도 중요하다고 할 것이다. 우선적으로 각 급기관이 부문별로 구축한 위협정보 공유시스템을 상호 연동시킴으로써 관련정보가 소통되고 공유되도록 보완하여야 한다. 중장기적으로는 정부의 예산과 인력 운용의 효율성·경제성 등을 고려하여 어느 한 부처가 중심이 되어 통합적인 시스템을 새로 구축하는 방안도 적극 검토해볼 가치가 있으며 이를 운영하는 과정에서 기존의 시스템과의 연계 방안 등 기술적인 대책도 고려해야 할 것이다.

아울러 사이버위협정보 공유체계가 원활히 운영되도록 하기 위해서는 공유할 정보가 가치있는 양질의 수준을 유지해야 하는데 이를 위해서는 수집, 분석, 검증 등 모든 과정에 걸쳐 관련기술이 개발되고 적용되어야 할 것이다. 이를 위해서는 많은 양의 수집된 탐지정보로부터 일차적으로 핵심적인 위협요소를 분류, 식별, 분석할 수 있는 기술과 다양한 국내외 사이버안보 위협에 대해 위협의 강도나 성격 등을 조기에 판단하여 대응하기 위해 자동적으로 판별하고 분석할 수 있는 기술을 우선 개발하여야 한다. 또한 위협수준을 정확하게 판단하기 위해서는 과거의 사고사례나 실제 공격과의 관계 등 이력을 비교할 필요가 있는데 공격IP나 공격기법, 해킹의 경유지, 악성코드 등의 위협정보가 상호 어떤 관계를 맺고 있는지를 비교분석하는 기술 개발도 필요하다.

3.4 면책권 부여 등 법·제도 보완

사이버위협정보를 민간기관과 공공기관이 상호 공유함으로써 사전에 대책을 강구할 필요가 있고 한편으로는 사고 발생시 긴급한 조치를 취하여 피해 확산을 차단하기 위해서라도 정보공유는 반드시 필요하다. 하지만 대통령훈령인 「국가사이버안전관리규정」이나 「정보통신기반보호법」등에 정보공유 근거가 규정되어 있으나 국가・공공 영역이나 기반시설 등 특정분야로 한정되어 있어 산업기술 보유기업이나 방산업체 등 다른 민간분야와의 공유는 미흡한 실정이다. 또한, 정보공유 대상이나 목록(내용)이 불명확하고 공유정보에 대한 보안기준이 설정되어 있지 않아 공유를 꺼리고 있어 정보의 질적 수준이 낮은 편이다.

사이버위협정보 공유에 대한 인식이 점차 개선되고 있어 이를 더욱 활성화하기 위해서는 관련 법률을 제

정하여 국가기관은 물론 주요 기반시설 등 국가·사회 운영에 필수적인 기관들로 하여금 정보공유를 강제하여야 하며 이를 위해서는 국회에 계류되어 있는 이철우의원 대표발의 「국가 사이버안보에 관한 법률안」이나 지난 9월 정부가 입법예고한 「국가 사이버안보 기본법안」이 조속히 통과되어 시행되어야 한다. 아울러 최근 사이버위협이 동시다발적이고 대규모로 발생하는 만큼 분야별 필수기관의 범위를 확대하기 위해 세제상 특례 등 인센티브를 부여하는 유인책 강구가 필요하다. 그리고 민간기관이 정보공유 참여기관에 위협정보 제공과 공유활동 수행 과정에서 발생한 사건이나 소송 등에서 민·형사상 법적 책임을 면제해주거나 완화시켜 주는 등 참여기관에 대한 보호장치를 마련해야 하고 한편으로는 위협정보의 수집·탐지·전파 등에 대한 전반적인 공유절차와 공유정보의 목적외 이용 금지나 의도적 유출시의 처벌 등 위협정보의 구체적 취급지침을 수립하는 것도 필요하다.

또한, 점차 지능화되고 위협이 현실화되고 있는 상황에서 정부기관과 민간기관간 공동대응 필요성에 대한 공감대를 발전시켜 기관간 원활한 정보공유가 지속될 수 있도록 실무적 차원에서 정보공유의 원칙, 참여기관의 역할, 공유정보의 범위·대상, 공유대상 정보의 등급화, 공유기관간 접근권한 차등화 등에 대한 기준이나 가이드라인 제정이 시급하다.

4. 결 론

본 논문에서는 최근 국내외에서 금융기관 해킹, 스마트폰 자료 절취 등 사고가 지속 발생하고 있고 향후에도 이와 유사하거나 한층 진화된 사이버위협이 예상되어 이에 대응하기 위한 방안으로 정부와 민간기관이 공동으로 사이버위협정보를 적극적으로 공유할 필요가 있음을 제기하였다. 이를 위해 미국·일본·영국 등 주요국이 정보공유 추진기구를 설치하고 대책을 수립·시행하는 등 사이버위협정보 공유제도를 살펴보고 우리나라 현재의 운영실태를 비교하면서 국내 상황에 적용할 수 있는 방안들을 연구하였다. 그 동안 우리나라는 부처별로 필요성에 의해 일부 공유센터를 구축하여 운영하고 있으나 제도적 지원 미흡으로 활성화가 되지 못하고 있는 실정이다. 이에 점차 고도화되는 사이버위협에 효과적으로 대응하기 위해 정보공유체계 운영주체의 명확한 설정, 민간·공공간 협업체계 운영, 통합적 자동화 시스템 구축, 면책권 부여 등 법·제도 보완 등 국가차원의 개선모델을 제시하였으며 향후 우리나라를 대상으로 하는 각종 사이버위협이 발생하더라도 이 모델의 올바른 적용을 통해 대규모 사고를 미연에 방지하거나 사고 발생시 피해를 최소화하여 사이버안보 수준 향상에 기여할 수 있을 것이다. 향후 연구에서는 관계기관간 사이버위협정보 공유를 활성화하는 것이 사고를 미연에 방지하는 등 예방활동과 사고발생시 조사·복구 등 사후대응 측면에 유용한 지 여부를 실증적으로 연구하여 궁극적으로는 우리의 사이버안보 체계 강화에 일조하고자 한다.

참고문헌

[1] 미래부, “인터파크 개인정보 유출 침해사고 조사 결과 - APT(지능형 지속 위협) 공격으로 개인정보 유출 발생”, 보도자료, 2016.8.31.

[2] 국정원, “국가사이버안전 대책회의 결과 - 北, 정부 주요인사 수십명 스마트폰 해킹”, 보도자료, 2016.3.8.

[3] 이상렬, “희대의 중앙은행 해킹 사건”, 중앙일보, 2016.3.16

[4] 민세아, “위협정보 공유한다는 C-TAS, 얼마나 알고 있나요?”, 보안뉴스, 2015.12.9.

[5] Charles Zhechao Liu, 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(2), 2014.1

[6] 윤오준 등, “사이버위협정보 공유 활성화를 위한 관리적·기술적 개선모델 연구”, 한국융합보안학회 논문지 제16권 제4호, 2016.6

[7] 김소선, “미국 사이버위협 정보공유 동향 및 시사점”, 월간 Cyber Security Issue 1분기 동향, 한국인터넷진흥원, 2015.5.8

[8] 박철민 등, “국외 사이버위협 정보공유의 체계 조

사", INTERNET & SECURITY FOCUS, 한국인터넷진흥원, 2014.1
[9] 정대상, "미 오바마 대통령, 사이버위협 정보공유 행정명령 발동", KISTI 미리안 글로벌동향브리핑, 2015.2.25.
[10] DHS, Cyber Information Sharing and Collaboration Program (CISCP), https://www.dhs.gov/ciscp
[11] DHS, National Infrastructure Protection Plan (NIPP) 2013 : Partnering for Critical Infrastructure Security and Resilience, https://www.dhs.gov/publication/nipp-2013
[12] STIX, https://www.stixproject.github.io/
[13] TAXII, https://www.taxiiproject.github.io/
[14] Sean Bamum, "Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIXTM)", MITRE Corporation, 2014.2.20[15] NIST, Special Publication 800-150 "Guide to Cyber Threat Information Sharing, 2014.10
[15] NIST, Special Publication 800-150 "Guide to Cyber Threat Information Sharing, 2014.10
[16] Denise E. Zheng, James A. Lewis, "Cyber Threat Information Sharing - Recommendations for Congress and the Administration," A Report of the CSIS Strategic Technologies Program, 2015.3
[17] Hiroshi Kawaguch, "Cybersecurity Strategy in Japan", Japan Security Operation Center, 2015.1
[18] Information Security Policy Council, "The Basic Policy of Critical Information Infrastructure Protection 3rd Edition", 2014.5
[19] IPA J-CSIP, http://www.ipa.go.jp
[20] JPCERT/CC, https://www.jpcert.or.jp/
[21] CERT-UK, https://www.cert.gov.uk/
[22] CERT-UK, "Cyber security information sharing partners terms and conditions", 2013.8
[23] 김정완, "정부통합전산센터, 사이버위협 정보공유 시스템 본격 가동", 보안뉴스, 2011.2.17.
[24] 윤현기, "미래부-KISA, 사이버위협 정보분석·공유시스템(C-TAS) 가동", IT DAILY, 2014.8.11.
[25] 미래부, "정보보호 패러다임 대전환을 위한 K-ICT 시큐리티 발전 전략 발표", 보도자료, 2015.4.21.
[26] 김애찬 등, "효과적인 사이버위협 정보공유체계 수립을 위한 요구사항의 우선순위 도출에 관한 연구", 정보보호학회지 제26권 제1호, 2016.2
[27] 박상돈 등, "사이버안보 추진체계의 제도적 개선과제 연구", 한국융합보안학회 논문지 제13권 제4호, 2013.9
[28] 이철우, "국가 사이버안보에 관한 법률안", 의안번호 32, 2016.5.30

[著者紹介]

윤 오 준 (Oh-jun Yoon)
1990년 2월 서울대학교 학사
2013년 8월 건국대학교 정보통신 대학원 석사
2015년 3월 숭실대학교 IT정책경영 학과 박사과정
email : ojyoon27271@naver.com

조 창 섭 (Chang-Seob Cho)
1992년 2월 동국대학교 학사
2015년 3월 숭실대학교 IT정책경영 학과 석박사 통합과정
2000년~ (주)이글루시큐리티 부사장
email : cscho@igloosec.com

박 정 근 (Jeong-keun Park)
1993년 2월 전북대학교 학사
2015년 2월 한양대학교 경영전문 대학원 석사
2015년 3월 숭실대학교 IT정책경영 학과 박사과정
email : Jeong.keun.park@sap.com

사진생략

배 선 하 (Sun-ha Bae)
2007년 2월 한양대학교 학사
2009년 1월 한국과학기술원 전기전자 공학과 석사
2009~2012 LIG 넥스원 연구원
2015년~ 국가보안기술연구소 기술원
email : sunhabae@nsr.re.kr

신 용 태 (Yong-tae Shin)
1985년 2월 한양대학교 학사
1994년 2월 美아이오아대학교대학원 컴퓨터공학과 석·박사
1994년 美미시간주립대 교수
1995년~숭실대학교 컴퓨터학부 교수
email : shin@ssu.ac.kr