Research Report

연구보고서 2017-009

소프트웨어안전 정보공유체계에 관한 연구

- 해외 사례중심으로

A Study on software safety information sharing system

- Focusing on overseas cases

진회승/심미나/양민호

2018.04.

SPRi 소프트웨어정책연구소

이 보고서는 2017년도 과학기술정보통신부 정보통신진흥기금을 지원받아 수행한 연구결과로 보고서 내용은 연구자의 견해이며, 과학기술정보통신부의 공식입장과 다를 수 있습니다.

목 차

표 목 차

그 림 목 차

요 약 문

1. 제 목

소프트웨어안전 정보공유체계에 관한 연구 - 해외 사례중심으로

2. 연구 목적 및 필요성

본 연구는 SW안전 확보와 신속한 사고대응을 위한 SW안전 정보공유 플랫폼 구축이 요구됨에 따라 국내외 정보공유분석센터(ISAC, Information Sharing & Analysis Center)의 현황 및 체계를 면밀히 조사하여 SW안전 정보공유 체계 구축 및 활성화 정책 기초 자료로 활용하는데 주요 목적이 있다.

크고 작은 SW안전 사고사례가 빈번하게 발생하고 있으나, 이에 대한 분석 및 대응조치에 대한 보고서는 공개 또는 공유 되지 않는 상황이며 SW안전사고의 대부분은 SW가 가지는 본질적인 문제에서 기인하나, 산업 도메인별로 전담기관 등이 구분되어 있고 소관 부처가 별도로 지정되어 있어 그 결과의 공유가 어려운 실정이다. 이로 인해 SW안전사고와 관련한 해결과제 등을 연구하는 데 중복적 투자가 발생하고, 이는 예산 낭비로 이어질 뿐만 아니라, 효과적인 사고대응에 실패하는 결과를 초래할 수 있다. 따라서 SW안전 확보와 신속한 사고대응을 위한 SW안전 정보공유 플랫폼 구축이 요구되며, 이를 체계적으로 정착시킬 수 있는 정책적 연구가 필요하다.

3. 연구의 구성 및 범위

해외 주요국의 도메인별 정보공유체계 현황을 분석하고, 국내 정보통신 분야의 정보공유체계를 조사하고 문제점을 도출한다. 이를 위해 세부적으로 해외 분야별 공유체계 분석, ISAC의 체계, 정보공유 현황, 정보공유 기술, 구성원들의 참여 요인 요소, 운영상의 주요 이슈 등을 조사하였다. 주요 분석대상은 협의를 통해 미국과 일본의 8개를 선정하였다. 미국은 항공, 의료, 자동차, 정보기술 분야의 4개 ISAC이며, 일본은 통신 2분야, 금융, 전력 분야의 4개 ISAC이 대상이다. 국내 정보통신 분야 정보공유 체계를 분석하고 문제점을 도출한다.

정보공유체계 활성화 방안을 조사하고 시사점을 도출한다. 마지막으로 조사・분석한 결과를 바탕으로 정보공유체계 구축 및 활성화 정책 방향을 도출한다.

4. 연구 내용 및 결과

미국 산업도메인별 정보공유체계 현황을 조사한 결과, 미국의 산업도메인 중 통신, 항공, 의료, 자동차 부문은 ISAC을 운영하고 있는 대표적인 산업으로 잘 알려져 있다. 미국은 테러방지를 위해 국가안보차원에서 일찌감치 국토안보법에 근거한 국가기반보호계획의 법제화를 추진하고 이를 통해 본격적으로 중요기반보호를 위한 행정명령(PDD-63)과 국토안보행정명령(HSPD-7) 등을 통해 보호활동을 추진하고 있다. 그 일환으로 정보공유체계를 설립하고 운영하고 있다고 할 수 있다.

산업 분야 중 통신 부문의 IT-ISAC은 정부 기관과 파트너십을 갖는 비영리 조직으로 독자적으로 Threat Intelligence Platform을 구축하고 멤버쉽 등급에 따라 공유 정보 및 참여 정보를 공유한다는 특징이 있으며, 특히 다른 ISAC과 차별되는 다양한 Special Interest Groups을 운영한다. 항공 부문의 A-ISAC은 정부 파트너가 참여하는 비영리 기구로 항공 산업에 대한 사이버 위협 정보를 공유한다. A-ISAC은 공유 데이터 분석 그룹(Analyst Working Group)을 운영하며 정보공유를 위한 다양한 방식을 제공하는데, 특히 정보 공유 기술로서 TLP 표준기술을 사용함으로써 멤버 등급에 따른 차별화된 서비스를 제공한다는 특징이 있다. 의료 부문의 NH-ISAC은 보건 부문에 대한 사이버 보안 보호 및 사이버 위협을 대비하기 위한 것으로 정보 공유를 위한 커뮤니티 및 포럼을 제공하는데 특히 CYBERFIT® 보안 서비스 그룹을 제공한다. 또한 다른 ISAC가 차별화되는 독자적인 기술로 AIS(Automated Intelligence Sharing)를 사용하며 Tier에 따라서 서비스를 제공한다. 점차 중요성이 커지는 자동차 부문의 Auto-ISAC은 차량 사이버 보안 위험에 대한 정보를 공유한다. Auto-ISAC은 정보공유를 위한 커뮤니티를 제공하며 모범사례 개발을 위해 워킹 그룹을 운영하고 있다. 북미 지역의 모든 경량 차량의 99%가 Auto-ISAC의 회원일 뿐만 아니라 우리나라를 포함한 자동차 회사들이 Auto-ISAC에 회원으로 가입하고 있다는 점에서 Auto-ISAC이 의미하는 바가 크다.

일본 산업도메인별 정보공유체계 현황을 조사한 결과, 일본은 2000년 e-Japan 구상에 따라 IT기본법을 통해 정보통신기반시설 보호정책을 추진해오고 있으며 그 일환으로 정보공유체계를 구축하고 있다. 2005년 내각관방 산하에 내각 사이버보안센터를 신설하고 정책협의회를 설치하여 본격적인 활동을 시작하였는데 2006년 책정된 제1차 사이버보안 기본계획을 통해 주요 기반의 IT장애에 대해 분야를 초월한 횡단적 보호를 표명하며 세부 목표 중 하나로 주요기반 분야의 정보공유분석기능인 셉터(CEPTOAR)를 정비하고 주요기반 연락협의회(CEPTOAR-Council) 창설을 촉진함으로써 정보공유분석기능 측면의 중대한 시발점이 되었다. 이를 시작으로 매년 정보공유 정책을 강화해가고 있으며 중요 분야의 경우는 셉터를 체계적 조직으로 구성한

ISAC을 설립하여 운영하도록 하고 있다. 2010년부터는 미국의 행정명령에 자극을 받아 민간 거버넌스를 강조한 전략을 발표하고 스마트시티, ITS를 비롯한 교통통제시스템 등의 새로운 분야까지를 포함한 구체적인 안전대책과 정보공유체제의 심화, 확충을 요구하고 있다. 또한 민관학연 등 관련 주체의 능력을 강화하고 상호협력 할 것을 강조하면서 총무성이나 경제산업성과의 구체적인 정보공유가 논의되고 있다. 일본은 산업도메인 전반에 CEPTOAR 기능을 갖추고 있는데 이들 중 특히 통신, 금융, 전력 부문은 ISAC 형태의 정보공유체계를 갖춘 대표적인 산업으로 알려져 있다.

우선 통신 부문의 텔레콤 ISAC (Telecom-ISAC)은 회원 간의 협업을 최고의 목표로 11개의 워킹그룹과 1개의 스페셜 인터레스트 그룹을 통하여 통신 분야의 사이버 위협에 대응하는 정보를 교환하며 피해를 최소화하는데 그 역할과 책임을 다하고 있다. 또한, 세부 워킹그룹을 통하여 기업 간 정보공유 체계를 이루고 있으며 기업과 기관간의 협업을 통해 정보공유를 활성화시키고 있다는 점에서 의미가 있다. 통신 부문의 ICT-ISAC은 ICT 분야 전반의 총체적 보안 확보에 기여하기 위해 ISP 사업자뿐만 아니라 방송 사업자, 소프트웨어 벤더, 정보 관련 기기 제조 사업자 등 다양한 분야로 확대하여 포괄되는 사업자들과 함께 활동하고 있다. 즉, 다양한 기업 및 단체와 협력하여 조직된 ISAC으로 정보공유 범위를 넓혔다는데 그 의의가 있다. 금융 부문의 금융ISAC (F-ISAC)은 미국의 금융 ISAC을 모델로 하여 조직 및 운영체계 면에서 매우 흡사하며 일본의 여러 ISAC 중에서 가장 완성도가 높은 조직이다. 또한 정회원과 준회원, 찬조회원 및 제휴회원 간의 정보 제공 범위에 차이를 두어 등급에 따라 양질의 정보를 제공함으로써 안전에 관한 정보를 제공함에 있어 신뢰를 갖고 있다. 전력 ISAC은 2017년 발족하였기 때문에 조직 및 운영체계 측면에서 아직 미흡하다. 향후 다른 ISAC을 참조하여 운영될 것으로 예상된다.

국내 정보통신 분야의 정보공유체계를 조사한 결과, 우리나라의 ISAC은 주요 정보통신기반 보호를 위한 분야별 근거 법률 체계를 기반으로 하여 통신, 금융, 행정 ISAC 등을 구축, 운영하고 있으며 특히 정보통신ISAC은 2002년에 설립되어 민간과 정부 이원의 재원을 통해 운영되고 있다. 기술적 지원을 명시한 정보공유분석센터 구축 운영으로는 정보공유 활성화의 한계가 있다고 분석되고 있어 최근에는 기술적 지원뿐만 아니라 재정적 지원을 법제화하는 움직임이 활발히 진행되고 있다.

정보통신ISAC은 한국정보통신진흥협회가 운영하는 조직으로 기반시설 정보보호, 취약점 분석평가, ISMS인증 업무를 수행함과 동시에 민간차원의 협의회를 운영함으로써 관련 사업자의 사이버차원의 예방활동을 강화 노력을 기울이며 지속적으로 회원가입을 권고하고 지원을 확대하고 있다. 이와 같이 기관을 중심으로 정보를 공유하는 상하체계와 협의회를 중심으로 관련 사업자간 정보를 공유하는 이원적 체계를 갖

추고 있다. 또한 국내 ISAC 기반을 위하여 C-TAS 플랫폼을 개발하고 활성화 정책을 펴고 있다. 사이버 위협정보를 체계적으로 수집해 관계기관 간 자동화된 정보공유를 수행하는 예방 및 대응 시스템을 규격화한 것으로 정보수집, 종합분석, 정보공유의 3단계로 각종 위협정보를 실시간으로 외부 기관에 전파하고 양방향 정보공유 방식으로 이해관계자간 신속한 대응 활동이 가능하도록 해준다. 한국인터넷진흥원이 운영하고 있는 C-TAS의 다양한 활용사례는 매년 증가하고 있으며 분기별로 워크샵이나 세미나를 통해 회원사에 제공되고 있다.

국내 SW안전 정보공유체계 구축 및 활성화의 문제점은 다음과 같이 세 가지로 압축하였다. 첫째 국내는 정보공유의 필요성보다는 부작용에 대한 인식이 강하다. 둘째 국내 SW안전 분야의 정보공유는 SW안전 표준이나 사고예방을 위한 관련 사고사례 정보공유 등 부분적인 정보공유에 그치는 경우가 많다. 셋째 국내의 경우 미국이나 일본에 비해 분야별 정보공유체계(ISAC)가 다소 미약하다.

이러한 문제점 해결을 위하여 그간의 정보공유 활성화 정책 및 사례를 조사하였다. 미국의 사이버보안 강화를 위한 인센티브 정책에 대해 조사하였으며, 국내의 정보통신기술, 의료, 행정 분야의 정보공유를 위한 정책을 분석하였다. 재정지원을 통한 기업의 부담 해소와 자발적 참여에 대한 검토 필요, 정부의 의지와 자발적 참여사이의 균형 유지, 국내에서 효율성, 효과성 면에서 강조되는 책임의 경감 및 책임 한정, 법적 베네핏 정책을 통한 정보공유 활성화 추진의 시사점이 도출되었다.

미국과 일본의 현황 분석 결과, 크게 세 가지 정책 방향을 도출하였다.

첫째 SW안전 공유체계에 대한 인식개선이다. 정보공유 정책을 수행하는데 정보 유출에 대한 우려가 가장 큰 저해요인이 되기 때문에, 정보공유로 인한 피해보다는 정보공유에 대한 필요성 및 활용성을 강조하고 정보 유출에 대한 의심을 해소할 수 있는 방안 마련이 필요하다.

둘째 SW안전 관련 정보수집 추진 및 시스템 구축이다. 정보공유 서비스 그룹 또는 프로그램 운영을 통해 정보 수집을 확대하고, 정보 공유 표준규격을 통한 광범위한 정보공유를 실현한다.

셋째 정보공유 활성화를 위한 방안 마련이다. 체계적인 정보공유체계의 마련보다는 초기에는 기능 중심 조직을 마련한다. 자발적 참여를 위한 인센티브 정책을 마련하며, 정보 공유 사례의 발굴 및 적용이 필요하다.

5. 정책적 활용 및 기대효과

서론에서처럼 SW안전사고는 본질적인 문제에 기인하지만 산업도메인별로 소관기관이 명확하지 않고 그 결과의 공유가 어렵다. 따라서 해결과제를 연구하거나 관리하는데 예산 낭비나 효과성 문제가 제기되고 있다. 이와 같은 실정에서 국내외 정보공유분석센터(ISAC) 현황 및 체계를 조사하는 것은 그 자체로 유의미할 뿐만 아니라 SW안전 정보공유 체계의 도입 검토 시 ISAC 구축이나 활성화 정책을 위해 필수불가결한 기초 자료로 활용될 가능성이 매우 크다.

국내 정보공유체계의 문제점을 발견하고, 정보공유 활성화를 위한 해외 인센티브 정책을 벤치마킹하여, 제시한 정책방향은 국내 SW안전 정보공유체계 마련에 기여할 것으로 기대한다.

SUMMARY

The purpose of this study is to investigate the current situation of ISAC in Korea and abroad and, to utilize them as a basic data of the policy. First, we analyze the ISAC status of major foreign countries. Second, we survey the ISAC in the field of information and telecommunication in Korea. Third, we derive implications for the establishment of SW-ISAC. The four major ISACs (aerospace, medical, automotive and information technology) in US and four ISACs (communication, finance, and power) sectors in Japan are the main targets. Finally, Based on the results of the research and analysis, we draw up a policy direction for establishing and promoting an information sharing system.

The United States operates ISAC in communications, aerospace, medical, and automotive applications. In the aspect of national security, the government is promoting the legalization of the national infrastructure protection plan based on the Homeland Security Law. The United States are actively working on PDD-63 and HSPD-7 for critical infrastructure protection and are operating ISAC in earnest.

Japan will promote information and communication infrastructure protection policies through IT Basic Law. As part of that, Japan are building an information sharing system. In 2006, the first cyber security basic plan was to improve the information sharing analysis function(CEPTOAR) and promote the creation of the CEPTOAR-Council. An important area is the establishment of ISAC, which systematizes CEPTOAR.

Domestic ISAC operates communications, finance, and administrative ISAC based on the sectoral legal system to protect the major information and communication infrastructure. In particular, IT-ISAC was established in 2002 and operated by private and governmental sources. Technical support alone limits the activation of information sharing. In recent years, legislation has been underway to provide financial support as well as technical support.

As a result of analyzing the situation of the United States and Japan, three policy directions were derived.

The first is to improve awareness of the SW safety sharing system. Since the concern about information leakage is the biggest obstacle to carrying out the

information sharing policy, it is necessary to emphasize the necessity and utility of information sharing rather than damage caused by information sharing.

The second is the collection and implementation of SW safety-related information. We expand information collection through information sharing service group or program operation, and realize broad information sharing through information sharing standards.

Third, there is a plan for revitalizing information sharing. In the beginning, the government forms a function oriented organization rather than a systematic information sharing system. Incentive policy for voluntary participation about information sharing should be established, and information sharing cases should be identified and applied.

Surveys of domestic and international ISAC status are meaningful. And it will be the essential basic data when introducing SW safety ISAC. It is expected that the policy direction as a result of finding out the problems of the domestic information sharing system and benchmarking the overseas incentive policy for information sharing promotion, will contribute to the establishment of the SW safety information sharing system.

CONTENTS

제1장 서 론

제1절 연구 배경 및 필요성

크고 작은 소프트웨어 안전(이하 'SW안전') 사고사례가 빈번하게 발생하고 있으나, 이에 대한 분석 및 대응조치에 대한 보고서는 다수가 공개 또는 공유 되지 않는 상황이다. 특히 4차 산업혁명으로 인해 소프트웨어 활용이 급증하고 있으며, 소프트웨어의 복잡성과 소프트웨어에 대한 의존성으로 인한 사고 위험이 가중되고 있다. 특히 철도, 항공, 에너지, 의료 증 국민의 안전과 밀접한 분야에서 소프트웨어 오류는 치명적인 인명사고와 재산상의 커다란 손해로 이어진다. SW 안전사고 원인을 공개하고 분석함으로써 효율적인 사고 예방이 가능하나, 우리나라는 산업 도메인별로 전담기관 등이 구분되어 있고 소관 부처가 별도로 지정되어 있어, 그 결과의 공유가 어려운 실정이다.

<표 1-1> 주요 산업분야별 안전 관련 기관

분 야	담당부처	수행기관	역할
철도 분야	국토교통부	한국철도기술연구원	철도시험인증, 철도표준지정
항공 분야	국토교통부	항공안전기술원	항공기 및 항행안전시설 안전인증
원자력 분야	과기정통부, 원자력안전위원회, 산업통상자원부	한국원자력연구원, 한국원자력안전기술원	원자력 SW안전지원
의료 분야	식품의약품안전처	식품의약품안전평가원	의료기기 안전평가·인증

이로 인해 SW 안전사고와 관련한 해결과제 등을 연구하는 데 중복적 투자가 발생하고, 이는 예산 낭비로 이어질 뿐만 아니라, 효과적인 사고대응에 실패하는 결과를 초래할 수 있다.

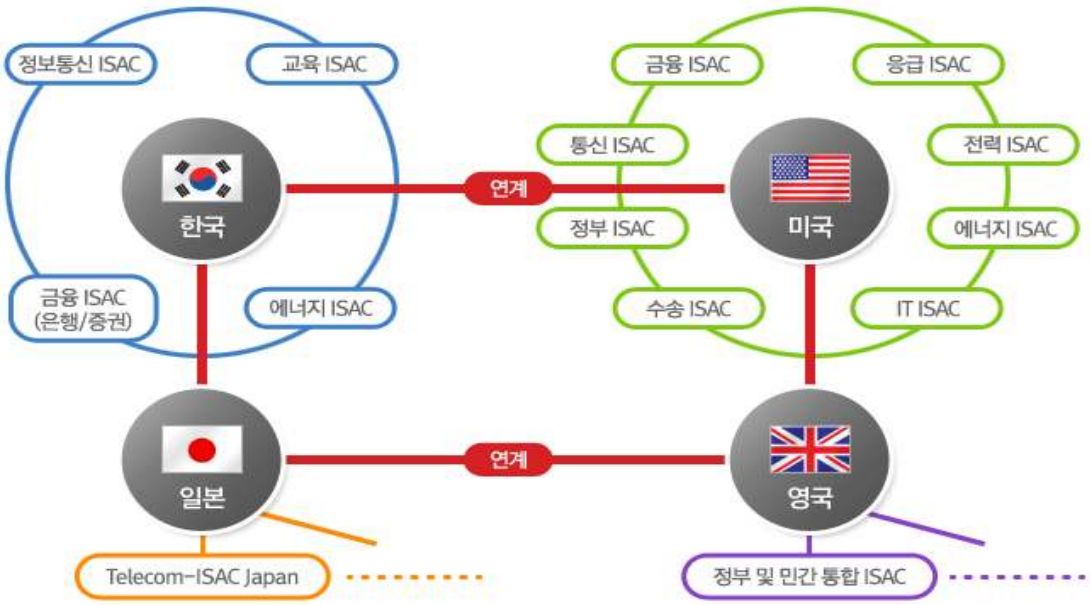
안전 필수 분야인 항공, 철도, 원자력 분야는 분야별로 안전 기술에 대한 강점을 가지고 있으며, 해외 안전 선진국에서는 각 분야의 기술이 통합되어, 표준에서도 타 도메인 표준의 기술을 차용하는 추세이다.[1)]

ISAC(Information Sharing and Analysis Center, 정보공유분석센터)이라는 조직은 각 분야별로 구성되어 있으며, 각 분야들과 해외 조직까지 연계되어 정보공유를 추진하고 있다.

1) 박태형, 진회승 외(2016), 소프트웨어 안전 산업 동향 조사, pp.76

미국의 경우, 대표적으로 통신, 항공, 의료, 자동차 분야에서 IT-ISAC, Aviation-ISAC, National Health-ISAC, Auto-ISAC의 사례를 살펴볼 수 있었다. 일본의 경우에도 통신 분야를 중심으로 금융, 전력 분야에서 Telecom-ISAC, IT-ISAC, F-ISAC, JE-ISAC과 같은 대표 사례를 찾아볼 수 있었다. 미국이나 일본 모두 주로 각국의 중요 인프라를 보호할 목적을 띠고 국가기반시설보호를 위한 법률이나 행정명령을 통해 시행되고 있다고 할 수 있다. 미국은 행정명령을 기반으로 사이버위협 정보공유를 위한 표준 규격을 마련하고 이를 정보공유를 위한 보다 체계적인 플랫폼을 갖추고 있다고 할 수 있다. 이에 반해 일본은 표준규격을 갖추고 시작한 것은 아니었으나 미국의 규격을 도입하여 자국의 규격으로 보완하여 적용하고 있으며 미국보다 늦었음에도 불구하고 오히려 최근 사이버안보 관련 법을 제정함으로써 강력하게 보호체계를 갖춰나가고 있다.

[그림 1-1] 국내외 ISAC간 연계도



자료: 정보공유분석센터(ISAC) 홈페이지

또한 우리나라는 미국, 일본을 비롯하여 영국 등 EU국가들과 각국의 정보공유체계끼리 상호 연계하여 보다 활발하고 신속한 예방 및 대응 활동이 이루어지기를 희망하고 있다. 국내외 ISAC들은 [그림 1-1] 와 같이 상호 협력체계를 갖추고 긴밀히 협조하고 있다. 그러나 ISAC의 경우는 국가기반시설의 사이버공격에 대한 정보공유가 주목적이다.

<표 1-2> 국외 ISAC 구축 및 운영 현황

구분	설립	운영주체	회원사	주요기능	재원조달
미국 통신ISAC	'00.03	NCC (국가통신 조정센터)	정부기관, 민간기관	- NS(National Security)/EP(Emergency Preparedness) 통신 서비스 - 정보공유 및 분석 등	민간 + 정부
미국 ISAC-Council	-	-	미국내 ISAC 연합	- 정부 및 각 분야별 협조와 의사소통 체계 확립 - ISAC간 사고 데이터 및 분석 정보의 공유 - ISAC 공동의 R&D 등 수행	정부
일본 통신ISAC	'05.02	데이터통신협회	민간기관	- 회원사간 침해사고에 대한 대응방안 정보공유 - Cyber Clean Center - BGP Monitoring - Trace Back Project - SoNAR(Society of Network Abuse Response)	민간 + 정부
유럽 ISAC	-	영국, 스웨덴 등	-	- 기본적인 ISAC 기능 수행 - 글로벌 ISAC 설립 및 미국 ISAC-Council과 협력을 통한 정보공유 추진	민간 + 정부

자료: http://www.isac.or.kr/intro/intro01.jsp Home > 정보통신ISAC > ISAC 현황

따라서 SW안전 확보와 신속한 사고대응을 위한 SW안전 정보공유 플랫폼 구축이 요구되며, 이를 체계적으로 정착시키고 활성화할 수 있는 정책적 연구가 필요하다. 이를 위해 현재 법제화되어 체계적으로 운영되고, 각 부문간, 국가간 정보공유를 추진하고 있는 국가 인프라 보호 목적의 ISAC을 국외 정보공유체계의 조사·분석의 대상으로 선정했다.

제2절 연구 목적

SW안전 확보와 신속한 사고대응을 위한 SW안전 정보공유 플랫폼 구축이 요구됨에 따라 국내외 정보공유분석센터(ISAC, Information Sharing & Analysis Center)의 현황 및 체계를 면밀히 조사하여 SW안전 정보공유 체계 구축 및 활성화 정책 기초 자료로 활용하는데 본 연구의 목적이 있다.

이에, 국내외 주요국의 도메인별 정보공유체계 현황을 분석하고 SW안전 정보공유체계 구축을 위한 시사점을 도출하고자 하며, 세부적으로는 국내외 SW안전 관련 분야별 기존

정보공유체계 분석, ISAC의 체계, 정보공유 현황, 정보공유 기술, 구성원들의 참여 요인 요소, 운영상의 주요 이슈 등을 조사하고자 한다.

제3절 연구 내용

SW안전 정보공유 체계 구축을 위해 국내 정보공유체계 현황을 분석한다. 국내 정보통신 분야의 정보공유체계에 대한 정보통신 ISAC의 체계(조직 구성 형태, 운영방식 등), 정보통신 ISAC의 정보공유 현황(정보공유 방식, 정보공유 범위 등), 정보통신 ISAC의 정보공유 기술(정보교환 기술 표준, 정보 교환 기술 등), 기관·산업체 참여 유인 요소를 조사 분석한다. 분석한 결과를 토대로 현재까지 운영상의 주요 이슈를 도출하고 시사점을 분석한다.

이론적 배경으로 SW안전의 정의 및 범위, 정보공유체계의 정의 및 유형에 대해 조사한다.

해외 주요국(미국, 일본)의 도메인별 정보공유체계 현황을 분석한다. 정보공유체계에 대한 법적 근거에 대해 조사한다. 해외 주요국의 ISAC들의 현황(ISAC의 종류·산업 도메인 등) 조사하고, 가능한 해외 주요국의 SW안전과 관련된 정보공유 체계를 분석한다. 해당 ISAC의 체계, 정보공유 현황, 정보공유 기술 등에 대해 조사한다. 미국의 경우는 통신, 항공, 의료, 자동차 부분의 정보공유체계에 대해 분석하고, 일본의 경우는 통신, 금융, 전력 부분의 정보공유체계에 대해 분석한다. 정보 교환을 위한 표준과 정보 등급을 대한 표준을 포함하여 정보공유 규격 및 표준에 대해 정리한다.

국내 정보통신 정보공유체계 현황을 분석을 분석하고, 해외 사례와 비교하여 문제점을 분석한다.

국내외 정보공유체계 활성화를 위한 정책 및 사례에 대해 조사하고 분석한다. 정보공유 활성화를 위한 인센티브 정책과 법제화에 대해 확인하고, SW 안전 정보공유체계 구축 및 활성화를 위한 정책 방향을 제시한다.

제4절 연구 방법 및 범위

국내외 정보공유체계에 대해 분석하기 위해 국내외 ISAC 관련 보고서, 논문, 보도자료 등 문헌을 참조하여 법적근거, 조직형태, 운영활동, 정보공유 방식, 정보공유 기술 등 9가지 기준에 의해 분석한다. 또한 웹 검색을 통해서 국내외 ISAC 운영 및 관련 기관 사이트를 조사한다.

각국의 주요 ISAC 목록 및 조사·분석 대상은 다음과 같다.

다음은 미국과 일본의 산업도메인별 주요 ISAC 또는 정보공유체계 목록이다. 협의를 통해 그 중 8개 ISAC(미국 4개, 일본 4개)을 주요 대상으로 선정하고 세부 분석하였으며, 그 외에는 기타로 분류하여 간략하게 정리하였다.

<표 1-3> 주요 ISAC 목록 및 조사·분석 대상

국가	도메인	ISAC
미국	통신	COMMUNICATIONS ISAC
	항공	**AVIATION ISAC**, Global Aviation Safety Network(GAIN)
	의료	**National Health ISAC**, HEALTHCARE READY
	자동차	**AUTOMOTIVE ISAC**
	국방	DEFENSE SECURITY INFORMATION EXCHANGE
	비상 관리 및 대응	EMERGENCY MANAGEMENT AND RESPONSE ISAC
	정보 기술	**INFORMATION TECHNOLOGY ISAC**
	소매	RETAIL CYBER INTELLIGENCE SHARING CENTER
일본	통신	**Telecom ISAC, ICT-ISAC**
	금융	**F-ISAC**
	전력	**JEC-ISAC**
	자동차	Auto-ISAC
	원자력	JE-ISAC

(참고사항) 목록 중 굵은체로 표시한 것이 조사·분석 대상임

정보 공유 체계에 대해 법적근거, 조직형태, 운영활동, 정보공유 방식, 정보공유 기술 등 8가지 기준에 의해 분석한 결과를 기반으로 안전 정보 공유 체계 마련 및 활성화 방안에 대해 연구한다.

본 연구에서는 조사에 앞서 SW안전 정보공유체계를 포함하여 크게 세 가지 유형의 정보공유체계를 조사 대상의 목표로 정하고 조사에 착수하였으며, 이후 분석과정에서 다음과 같은 다양한 분석 기준을 설정하였다. 예상과 같이 현재까지는 SW안전 정의에 부합하는 유사한 형태의 SW안전 정보공유체계 사례는 찾아보기 어려웠다. 따라서 분석을 위한 기준에서는 산업도메인별 특성에 따라 안전관련 일반정보를 공유하는 형태, 특히 안전을 위협하는 보안 위협정보를 공유하는 형태, 이와 더불어 새롭게 논의되는 SW안전 정보를 공유하는 형태의 3 가지로 유형을 구분하여 조사 분석을 수행하였다. 이들 3 가지 유형의 의미는 다음과 같이 구분할 수 있다.

① 산업도메인별 안전관련 일반정보를 공유: 품질 또는 신뢰성 측면에서 소프트웨어 안전을 위한 정보를 공유하는 형태

② 산업도메인별 보안 (위협)정보 공유: 궁극적으로는 안전을 목표로 하며 특히 관련 보안 위협에 대응하기 위한 정보를 공유하는 형태

③ 산업도메인별 SW안전 정보 공유: 품질은 기본이고 소프트웨어 안전 부분의 문제를 회피할 수 있는 메커니즘을 구현하기 위한 정보 공유 즉, 소프트웨어 안전은 기능요구사항 뿐만 아니라, 안전 요구사항에 대한 정보를 공유하는 형태

따라서 본 연구에서는 각국의 정보공유체계 조사·분석을 위한 세부 유형을 다음의 9가지 항목에 따라 구분하고, 이를 기준으로 각국의 산업도메인 및 정보공유체계별 현황을 정리하고 특징을 비교·분석하였다.

<표 1-4> 정보공유체계 조사·분석 기준

No	구분	유형	의미
1	관련 분야	1) 일반 분야	정보공유체계의 정보 특성상 특정산업의 일반정보를 공유 대상으로 하는 경우
		2) 보안 분야	정보공유체계의 정보 특성상 보안(위협)정보를 주요 공유 대상으로 하는 경우
		3) SW안전 분야	정보공유체계의 정보 특성상 SW안전정보를 주요 공유 대상으로 하는 경우
2	법적 근거	1) 법령 근거	법령(법률, 시행령)에 의해 설립 및 운영

No	구분	유형	의미
		2) 그 외 방법	법령 근거 없이 다양한 자율적 방법으로 운영
3	재원 조달	1) 정부	정부 주도로 정부 재원을 통해 운영
		2) 민간	민간 주도로 회원사 회비, 사업수익 등으로 운영
		3) 정부 + 민간	정부 재원을 기반으로 운영하되, 민간 회원사가 협의회를 구성하여 병행 활동
4	조직 형태	1) 일반 정보공유체계	ISAC이 아닌, 다양한 형태로 정보공유 활동을 수행하는 형태 또는 체계
		2) 산업도메인별 대표 ISAC	특정 산업도메인을 대표하는 하나 이상의 ISAC을 설립하여 운영하는 형태
		3) 기관 또는 기업의 자체 ISAC	특정 기관 또는 기업이 자체적으로 ISAC을 구성하고 운영하는 형태
5	운영 활동	1) 일반	특정 내부 조직 없이 운영
		2) 커뮤니티	정보공유체계 내 특정 주제 기반의 조직 운영
		3) 스터디 그룹	커뮤니티와 같이 특정 주제를 기반으로 운영되지만 문제 해결 방안을 모색하기 위해 운영되는 운영 활동
		4) 표준화	특정 주제에 대한 문제 해결 방안 및 절차 등을 표준화하기 위한 활동
6	정보 공유 방식	1) 시스템	자체 개발 시스템을 통하여 정보를 공유
		2) 이메일	전자메일을 통하여 정보를 공유
		3) 인쇄물	정기간행물 등을 통하여 정보를 고유
		4) 온라인 토의	Webex 또는 다양한 온라인 토의 도구를 통하여 워크숍(컨퍼런스) 개최 및 정보 공유
		5) 워크숍(컨퍼런스)	오프라인 모임을 통하여 정보를 공유
7	정보 공유 기술	1) 표준 규격 또는 기술	표준화 된 규격 또는 기술을 이용하여 정보 공유
		2) 독자 규격 또는 기술	각 도메인 또는 조직에서 정의한 규격 또는 기술을 이용하여 정보 공유
8	정보 공유 범위	1) 멤버십 별	ISAC 또는 조직에서 멤버십의 종류에 따라 공유되어지는 정보공유 범위가 상이
		2) 정보 유형별	도메인 일반정보, 보안정보, SW안전정보 등 정보 유형에 따라 공유되는 범위가 상이
		3) 운영 활동별	운영활동의 형태에 따라 정보공유 범위가 상이

제2장 이론적 배경

제1절 SW안전

1. SW안전의 정의

IEEE 표준 1228-1994에 따르면 소프트웨어의 안전이란 소프트웨어 위험요소 제거를 통해 소프트웨어 오류로 인한 시스템의 사고를 예방하는 것이다.[2] 2016년 연구조사(소프트웨어정책연구소)에서[3], SW안전이란, “인명이나 재산상 피해를 주는 사고 발생을 회피하기 위한 능동적인 방안(Safety Mechanism/Functional Safety)을 포함한 개념”으로 정의하였다. 2015년 조사에서는 SW안전을 품질과 동일한 개념으로 보는 관점과 소프트웨어 품질과는 확연히 구별되는 것으로써 소프트웨어로 인하여 발생하는 인명이나 재산의 사고를 회피하는 방안(Safety Mechanism)으로 보는 관점이 주를 이루었다. 소프트웨어 안전은 수용할 수 있는 만큼의 사고 위험을 가지도록 소프트웨어의 기능을 구현함으로써 보장된다. 이를 위해서는 소프트웨어 품질이 좋아야 하고 보안도 유지되어야하기 때문에 SW안전은 품질, 보안 개념과 혼용하여 쓰이기도 한다.

그러나 최근에는 이와 더불어 ‘사람의 생명 및 건강에 직간접적으로 연관되어야만 SW안전’이라고 정의하면서 경제적·재산상의 손해 등은 SW안전이 아닌 신뢰성 문제로 보아야 한다는 의견도 제시되고 있다. 그러나 국제적으로 통용되는 개념은 안전을 지키기 위해 위험으로부터 지켜야 하는 것은 사람의 생명, 재산, 환경의 세 가지 요소가 포함되어 있으며,[4] 이를 위해서는 SW의 품질요소와 보안요소가 검토되어야 한다.

2015년 국내 SW안전 분야 사업의 기업 부분의 인식 조사[5]에서는 SW안전의 개념을 추상적이고 일반적으로 인식하면서 35%의 비율로 안전, 품질, 보안을 구분한 반면, 2016년 동일조사[6]에서는 SW안전을 보안 관점으로 인식하는 비율이 50%에 달하였으며, 분석, 설계, 회피 메카니즘의 공학 관점으로 이해하는 비율도 40%에 달하였다. 안전, 품질, 보안의 상관관계에 대해서는 다양한 해석이 있으나 안전 문제를 품질 문제와 구분하면서도 점점 보안 문제와는 구분하지 않는 경향을 띠는 것으로 이해할 수 있다.

---

2) 진회승 외(2016), 소프트웨어 안전 분야 재직자 역량 제고를 위한 교육 커리큘럼 개발에 관한 연구, pp.7
3) 소프트웨어정책연구소(2016), 소프트웨어 안전(Safety) 산업 동향 조사, pp.93, 2016.12.
4) IEEE SA - 1228-1994 - IEEE Standard for Software Safety Plans
5) 소프트웨어정책연구소(2015), 소프트웨어 안전(Safety) 산업 동향 조사, pp.131, 2015.8.
6) 소프트웨어정책연구소(2016), 소프트웨어 안전(Safety) 산업 동향 조사, pp.131, 2016.12.

SW안전에 대해 주의할 점은 소프트웨어 자체로만은 위험하지 않으며 하드웨어와 소프트웨어가 융합되어 있을 때, 하드웨어와 소프트웨어의 복합적인 원인으로 사고가 일어난다는 것이다. 하드웨어의 오류에 의해 소프트웨어의 동작이 잘못되거나. 소프트웨어의 오류로 인한 하드웨어의 오동작이 일어나서 사고가 일어나게 되므로, SW안전을 고려할 때는 그 도메인의 지식이 고려되어야 한다. 그러나 소프트웨어의 오류를 방지하는 매카니즘과 기술은 동일하며, 이는 여러 도메인에 걸쳐서 같이 적용된다.

한편 해외의 경우에는 안전에 관한 표준을 토대로 산업도메인별로 SW안전 개념이 어느 정도 정립되어 있는 것으로 파악된다. SW안전 관련 선진국 활동에 관한 현황 보고서에 따르면 산업 도메인별로 최소 한 개 이상의 SW안전 표준이 존재한다. 다만, 소프트웨어가 실제로는 전자전기시스템을 포함하는 제품 내에서 동작되는 관계로 법제도적 관점에서 SW안전 표준으로 별도의 요구사항을 제시하고 있는 것은 아니다. 즉, 전기전자 부품, 시스템 또는 제품 수준에서 이들을 안전하게 만들기 위한 항목으로 법, 제도 및 표준에 포함되어 규정화하고 있으며 정부기관 및 인증기관 등을 통해 적용되고 있다.

산업도메인별 표준을 살펴보면, 자동차의 국제표준인 ISO26262는 사고발생 시 제조물책임법 하에 SW안전 최신 기법 적용 여부를 증명하기 위한 기준으로 업체들이 자발적으로 이를 준수하는 사후 규제의 성격이다. 철도의 경우, 미국은 화물 운송 및 저속 운속 중심의 AREMA(American Railway Engineering and Maintenance-of-Way Association) 표준을, 유럽은 고객 운송 및 고속 운송 중심의 EN50128 표준을 사용한다. 항공의 경우, 우주항공, 국방, 상용항공으로 표준이 구분되는데, 상용항공의 경우는 미국의 RTCA(Radio Technical Commission for Aeronautics)와 유럽 EUROCAE(European Organization for Civil Aviation Equipment)의 공동연구로 개발된 표준을 적용한다. 원자력의 경우, 국제표준이 있으나 각국이 자국에 맞는 표준과 안전등급을 정의하여 사용하고 있다. 그러나 산업도메인별 산업 특성을 고려한 SW안전 표준은 국제전기기술위원회(IEC, International Electrotechnical Commission)에서 작성한 산업에 적용되는 규칙인 국제표준 IEC61508의 정립 이후, 이를 근간으로 SW안전이 필요한 산업에 대한 자체적 안전표준으로써 제정된 것이다.[7)]

이러한 현황을 비추어 볼 때, SW안전에 대한 개념 정의도 국제표준인 IEC61508의 정의와 함께 각 산업도메인별 특성에 따라 살펴보아야 한다. IEC61508((E/E/PE or E/E/PES, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems)은 전기/전자/프로그램 가능한 전자 안전 관련 시스템의 기능 안전에 대한 표준을 목적으

7) 소프트웨어정책연구소(2015), 소프트웨어 안전(Safety) 산업 동향 조사, pp.10-14, 47-50, 2015.8.

로 작성된 것이다. 여기서 기능 안전(Functional Safety)이란, “E/E/PE 안전 관련 시스템의 정확한 기능, 다른 기술 안전 관련 시스템과 외부적인 위험 감소 설비에 의존하는 제어 대상 장비(EUC, Equipment Under Control)와 EUC를 제어하는 시스템 관련된 부분적 또는 전반적인 안전” 으로 정의된다.[8] 즉, SW안전 관련 산업의 근간이 되는 표준은 SW 안전을 구체적으로 정의하고 있지 않고 시스템이나 장비의 기능 측면의 안전을 다루고 있음을 알 수 있다. 부가적으로 IEC61508은 SW안전의 4개 위험레벨(Risk Class)을 정의하고, 시스템개발 시 안전기능의 목표수준(SIL, Safety Integrity Level)을 제공함으로써 위험을 관리하기 위한 가이드를 제시하고 있으며, 다양한 산업도메인별 표준에서 이를 적용하고 있다.[9] 상기와 같은 이유로 산업도메인별 SW안전은 주로 기능적 측면의 안전으로 이해할 수 있을 것이다.

2. SW안전의 범위 및 유형 분류

1) 산업도메인별 SW안전의 범위

산업 전반에 적용되는 SW안전의 일반적 정의는 산업의 특성에 따라 구체화되고 위험이 평가되므로 산업도메인별로 다루어지는 SW안전의 범위를 살펴봄으로써 이후 관련 산업에서 정보공유의 요구사항을 이해하는데 도움이 될 것이다. 해외 SW안전 관련 산업의 국제표준으로써 자동차, 철도, 원자력, 기계와 같은 산업도메인은 기본규격인 IEC61508을 기초한 개별 표준을 통해 SW안전을 다루고 있으며, 항공이나 의료와 같은 분야는 자체 산업의 기준을 마련하고 표준으로 사용하고 있다.

SW안전 요구사항에 있어서 자동차의 경우는 구체적인 법적요구사항이 표현되어 있지 않으나 자동차, 자동차 시스템, 자동차 부품 차원에서 안전을 제시하고 있다. ISO26262를 통해 자동차 전기/전자 시스템 안전(Functional Safety)을 다루고 있는데 표준제정 이전에는 소프트웨어 개발을 주로 자동차 산업 소프트웨어 신뢰성 협회 가이드라인이 적용되었다. 특히 MISRA C는 자동차 산업에 사용되는 임베디드 시스템 소프트웨어의 안전성, 호환성, 신뢰성 향상을 위한 C언어 코딩표준으로 볼 수 있다.

철도의 경우, IEC62279를 통해 철도 어플리케이션에 대한 IEC61508의 해석을 제공하는데 철도 제어와 보호를 위한 커뮤니케이션, 신호 및 처리시스템에 대한 소프트웨어 개발

8) 소프트웨어정책연구소(2015), 소프트웨어 안전(Safety) 산업 동향 조사, pp.10
9) IEC 61511, IEC61513(Nuclear), IEC62061(Machinery), EN50128/EN50129(Railway), EN50402(Fixed gas), ISO26262(Automotive)

요구사항을 포함하고 있다. 또한 자체 절차, 분석 방법과 문서를 통해 인증 요구사항을 제시하고 있다.

원자력의 경우, ISO61513을 통해 원자력발전소의 안전 관련 중요시스템의 장치와 제어 요구사항 및 권고사항을 제공한다. 컴퓨터 기능과 설계 요구사항에 대한 규정 준수 방법으로 표준을 적용하고 있으며, 시스템을 단순하게 안정성/비안정성으로 분류하고 있다. 더불어 IEC61513의 참고문서인 IEC60880을 통해 카테고리A 기능을 수행하는 I&C 시스템(Instrumentation and Control, 기계와 제어)의 소프트웨어 부분에 대한 문제해결을 위한 표준을 제공하고 있다.

항공의 경우, DO-178C 표준은 항공전자시스템에서 사용되는 안전 필수 소프트웨어의 안전성에 관한 지침이다. 기술적 지침이긴 하나 항공전자 소프트웨어 시스템을 개발하기 위한 사실상의 표준이다. 연방항공관리국(FAA, Federal Aviation Administration)이 인증을 위한 기술표준요구(TSO, Technical Standard Order)를 명시할 때, 소프트웨어가 항공 환경에서 신뢰성 있게 수행 가능한지를 확인하기 위한 지침으로써 사용한다.

<표 2-1> 산업도메인별 SW안전의 의미 및 요구사항

구분	관련 표준	SW안전의 의미 및 요구사항
자동차	Automobile Software - ISO26262	- 자동차 전기/전자 시스템 안전(Functional Safety)을 위하여 IEC61508을 근간으로 제정한 표준 - 차량용 시스템의 계통적 고장(Systematic Failure)과 우발적 고장(Random Failure)에 대해 회피 또는 제어를 위한 방법과 조치 정의
	MISRA C	- 자동차 산업에 사용되는 임베디드 시스템 소프트웨어의 코드 안전성, 호환성, 신뢰성 향상을 위한 C프로그래밍 언어 개발 가이드라인 즉, 코딩 표준을 정의
철도	Railway Application - IEC62279 - EN50128	- IEC62279는 철도 어플리케이션에 대한 IEC61508의 해석을 제공 - EN50128은 철도 산업에 관련된 유럽의 안전 관련 소프트웨어 표준으로 안전한 소프트웨어 개발을 위한 방법론, 원칙, 방안 등을 규정
원자력	Nuclear Power Plants - ISO61513	- 원자력발전소의 안전시스템에서 사용하는 장치와 제어에 대한 요구사항에 대한 표준 및 권고사항을 제공 - SIL 개념을 사용하고 있지 않으나 심각도에 따라 안전 기능을 분류하고 안전기능 수준에 따라 시스템 클래스를 정의하여 안전 목표를 관리
	IEC60880	- IEC SC45A문서 중 IEC61513의 참고문서로서 카테고리A 기능을 수행하는 I&C 시스템의 소프트웨어 부분의 문제 해결을 위한 표준문서로써 컴퓨팅 시스템의 하드웨어 부분은 IEC60987에서 다룸

구분	관련 표준	SW안전의 의미 및 요구사항
기계	Machinery - ISO62061	- IEC61508 표준의 기계 특화된 시스템 구축에 대한 표준
항공	DO-178C	- 항공전자시스템에서 사용되는 안전 필수 소프트웨어의 안전성을 취급하는 가이드임과 동시에 항공전자 소프트웨어 시스템 개발을 위한 사실상 표준 - 즉, 항공기 시스템과 장비의 소프트웨어 부분이 감항성(airworthiness) 인증 요구사항을 준수하는지 여부를 검증하는 소프트웨어 개발 표준 - 안전평가 프로세스, 위해도 분석으로 결정된 레벨을 토대로 시스템 고장 영향성을 판단하는 기준
	NPR7150.2	- NASA의 소프트웨어 안전에 관한 표준으로 소프트웨어 공학 요구사항을 명시한 것으로 이에 따라 소프트웨어 안전 표준인 NASA-STD-8719.13을 통해 소프트웨어 안전을 수행하기 위한 진단 단계와 방법을 제시하고 적용함 - 안전필수 소프트웨어를 식별하고 안전등급을 정의, 소프트웨어 안전에 대한 개발 범위와 활동 정의, 소프트웨어 요구사항과 설계 검토 재평가를 통한 개선활동과 같은 소프트웨어 안전 진단 단계를 수행함

자료 : 소프트웨어정책연구소(2015), 소프트웨어 안전(Safety) 산업 동향 조사 보고서, pp.13-50

2) 안전(Safety)과 보안(Security) 관점의 SW안전 범위[10)]

최근 ICT기반 패러다임이 IoT(Internet of Things, 사물인터넷)에서 IoE(Internet of Everything)로 확대되는 추세에서 각 산업도메인뿐만 아니라 실세계 전반이 소프트웨어화 되어 SW안전이 사회 안전이 되는 소프트웨어 중심사회로 진화하는 중이다. 또한 상황을 모니터링하고 위험을 감지, 분석해서 경보 또는 전파하고 최종적으로 안전문제를 해결하거나 안전을 유지하는 필수 수단으로서 소프트웨어의 역할과 활용이 증가하고 있다.

이러한 관점에서 SW안전은 안전(Safety)과 보안(Security)의 두 가지 측면 모두를 포함한 개념으로 이해할 수 있다. 즉, 안전(Safety)이란 '위험이 생기거나 사고가 날 염려가 없음 또는 그런 상태' 이며 보안(Security)은 '안전을 유지함' 으로서 위험에 대해서 방호하는 것, 또는 그와 같은 위험에 노출되지 않도록 하는 것을 의미한다. 또한, 하드웨어 오류(운영미숙), 소프트웨어 오류(설계결함), 안전관리 부실(대응지연) 등의 안전문제는 복합적으로 상호 영향을 미친다고 할 수 있다.

10) 이근상(2015), IoT산업의 키, 소프트웨어 안전, (재)전북테크노파크, Issue&Tech vol.49, pp.13-17

<표 2-2> 상호 영향을 미치는 안전 문제

No	안전 문제	설명(예시)
1	하드웨어 오류 (운영미숙)	- 최신 자동운전장치(ATO)와 구식 자동정지장치(ATS)를 내구연한이 지난 전동차에 혼용 사용
2	소프트웨어 결함 (설계결함)	- 신호기 통신 장애 등의 오류감지 시 정지 신호가 켜지도록 소프트웨어의 안전 설계가 안됨
3	안전관리 부실 (대응지연)	- 전방 열차와 후속 열차간 근접을 모니터로 확인했으나 신호제어 장치에 이상이 표시되지 않았기에 아무런 대응안함

자료 : 이근상(2015), IoT산업의 키, 소프트웨어 안전, (재)전북테크노파크, Issue&Tech vol.49

소프트웨어 결함으로 인한 피해를 최소화하고 산업 경쟁력을 높이기 위해서는 안전 소프트웨어와 이런 SW 안전을 담보하기 위한 검증이 필요하다. 여기서 SW안전이란 '소프트웨어 내적의 위험요소 제거를 통해 소프트웨어 오류로 인한 사고를 예방하는 것 또는 소프트웨어 위험요소로부터 자유로운 상태, 안전한 소프트웨어'를 말한다.

소프트웨어 안전성을 위해 미국, 유럽 등에서는 안전관리 시스템이 필수인 원자력, 항공, 철도, 의료 등의 분야에서 국제 표준을 근간으로 한 검증 요구가 증가하고 있다. 또한 국내에서는 안전과 보안문제로 구분하여 안전 측면에서는 SW안전을 위해 주요 국가기반시설 소프트웨어에 대한 안전 진단과 컨설팅을 추진하고 있으며, 보안 측면에서는 기반시설보호법, 전자정부법, 정보통신망법, 개인정보보호법 등의 법과 기술적 대응을 통해 추진하고 있다.

특히 소프트웨어 보안 문제는 시큐어 코딩(Security Coding)등의 방법을 통해 개발 반계부터 보안성을 고려한 소프트웨어를 개발하도록 정부 중심으로 의무화가 추진되고 있다.[11] 그에 앞서, '소프트웨어 개발보안'은 소프트웨어 개발과정에서 개발자의 실수, 논리적 오류 등으로 인해 소프트웨어에 내포될 수 있는 보안약점을 최소화하고 사이버 위협에 대응할 수 있는 안전한 소프트웨어를 개발하기 위한 일련의 보안활동을 말한다. 이는 광의적 개념으로 소프트웨어 개발생명주기(SDLC)의 각 단계별로 요구되는 보안활동을 모두 포함하는데 협의적 의미로는 소프트웨어 개발과정 중 소스코드 구현단계에서 약점을 배제하기 위한 '시큐어코딩(Secure Coding)'을 의미한다.

소프트웨어 개발보안의 중요성을 먼저 인식한 미국의 경우, 국토안보부(DHS)를 중심으로 시큐어코딩을 포함한 소프트웨어 개발 전과정(설계, 구현, 시험 등)에 대한 활동 연구를 활발히 추진하고 있으며 NIST를 통해 각 단계별 활동 및 절차를 표준화하고 정보시스템 구축 및 운영 시 참고하고 있다. 국내의 경우, 정부는 2015년부터 행정기관과 공공기관의

11) 2012년 전자정부 시스템에 대한 사이버 공격이 일어나면서 시큐어코딩 도입을 전 공공기관에 의무화했으며 2015년부터 모든 공공기관 전자정부 사업에 의무적용 되었다.

정보시스템 전 사업에 시큐어코딩을 의무화하고 있으며, 2016년부터는 소프트웨어 감리 필수검사 항목을 지정하고 의무화는 아니나 사업 자체적으로 감리를 추진하도록 하고 있다.

시큐어코딩은 소프트웨어 개발 단계별 결함 중 설계과정의 결함으로 인한 비용이 코딩 과정이나 통합과정의 결함으로 인한 비용보다 최대 30배까지 나타난다는 점[12]을 고려하여 개발단계에서부터 설계 결함으로부터 발생하는 보안 취약점을 이해하고 조치할 수 있도록 하는 개념으로 다음과 같은 취약점 항목을 제거하도록 하고 있다. 시큐어코딩 시 필수 제거 대상 항목은 입력데이터 검증 및 표현(15개), 보안기능(16개), 시간 및 상태(2개), 에러처리(3개), 코드오류(4개), 캡슐화(5개), API(Application Programming Interface) 오용(2개)의 총 47개 항목이다.[13] 결국, 시큐어코딩의 소프트웨어 개발 요구사항은 SW안전의 범위로 이해할 수 있다.

<표 2-3> 시큐어코딩 시 필수 제거 대상 소프트웨어 약점 유형

No	유형	내용
1	입력데이터 검증 및 표현	- 프로그램 입력값에 대한 검증 누락 또는 부적절한 검증, 데이터의 잘못된 형식 지정으로 인해 발생할 수 있는 약점
2	보안특성	- 보안기능(인증, 접근제어, 기밀성, 암호화, 권한 관리 등)을 부적절하게 구현할 때 발생할 수 있는 약점
3	시간 및 상태	- 동시 또는 거의 동시 수행을 지원하는 병렬 시스템, 하나 이상의 프로세스가 동작되는 환경에서 시간 및 상태를 부적절하게 관리하여 발생할 수 있는 약점
4	에러처리	- 에러를 처리하지 않거나, 불충분하게 처리하여 에러정보에 중요정보(시스템 등)가 포함될 때 발생할 수 있는 약점
5	코드오류	- 타입변환 오류, 자원(메모리 등)의 부적절한 반환 등과 같이 개발자가 범할 수 있는 코딩오류로 인해 유발되는 약점
6	캡슐화	- 중요한 데이터 또는 기능성을 불충분하게 캡슐화할 때 인가되지 않은 사용자 또는 시스템에게 데이터 누출이 가능해지는 약점
7	API오용	- 의도된 사용에 반하는 방법으로 API를 사용하거나 보안에 취약한 API를 사용하여 발생할 수 있는 약점

자료 : 한국인터넷진흥원(2017), 소프트웨어 개발보안 가이드

앞서 살펴본 바와 같이, SW안전의 범위 및 요구사항은 하드웨어 오류(운영미숙), 소프트웨어 오류(설계결함), 안전관리 부실(대응지연) 등의 안전문제와 소프트웨어 개발 시 보안문제 등을 모두 포함하는 것으로 이해해야 할 것이며, 특히 이러한 안전문제를 해결하기 위해 공유될 필요가 있는 SW 안전 정보는 예방뿐만 아니라 대응을 위한 안전관리 측면에서도 다루어져야 할 것이다.

12) 행정안전부(2012), 전자정부 SW개발 운영자를 위한 소프트웨어개발보안가이드, pp.5, 2012.5.
13) CWE(Common Weakness Enumeration) 분류방법론 중 하나인 '7 Pernicious Kingdoms' 분류체계를 준용하여 분류한 것으로 행정안전부 소프트웨어개발보안가이드 참고

제2절 SW안전 정보공유체계

1. 정보공유체계의 정의 및 유형

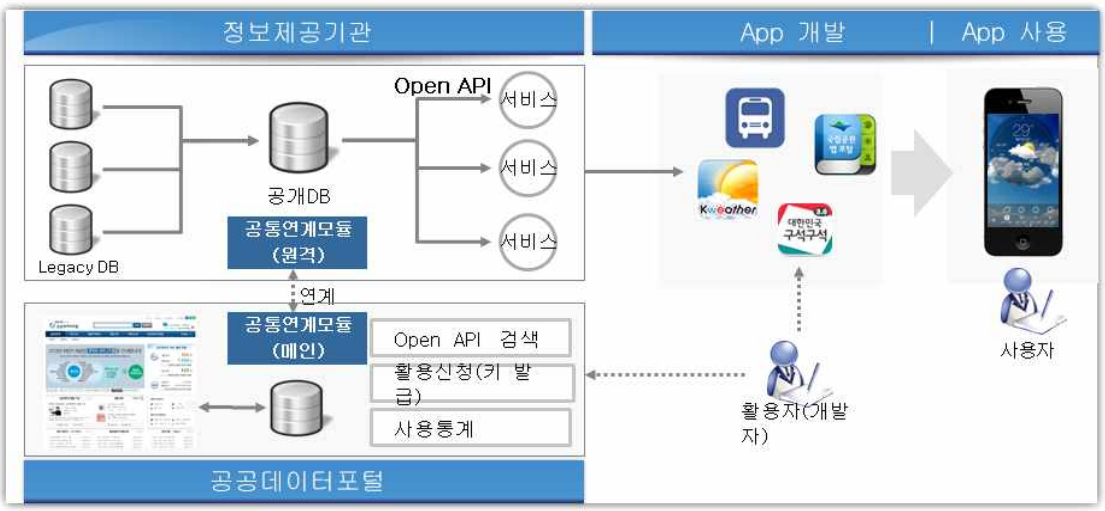
1) 정보공유체계의 정의

일반적으로 정보공유체계는 ‘하나 또는 그 이상의 구성원이 보유하고 있는 정보나 기술을 모든 이해관계자가 서로 공유하고 협력할 수 있도록 네트워크를 구축하는 방법 또는 시스템’으로 정의한다. 특정 분야의 정보를 활용하여 이익창출의 목적으로 또는 위협으로부터 발생 가능한 위험의 관리 목적으로 정보공유를 위한 체계 또는 시스템을 구축할 수 있다.

2) 다양한 분야의 정보공유체계 유형

행정 분야에서는 국가 또는 행정기관이 보유한 정보자원을 개방하여 민간에서 활용하도록 ‘국가정보자원 개방공유체계’를 구축·운용하고 있는데 이것이 행정 분야의 대표적인 정보공유체계이다. OpenAPI 표준체계를 통한 여행 및 관광, 수송 및 물류, 문화 및 예술 등의 국가가 보유한 다양한 분야의 공공정보를 단일방향으로 국가기관, 자치단체 및 민간기관에 제공하는 형태이며 정보 활용 신청과 승인을 거쳐 정보제공이 이루어진다.[14]

[그림 2-1] 국가정보자원 개방공유체계



자료 : 행정안전부(2014), 2013년 국가정보자원 개방공유체계 구축사업 완료보고

14) 행정안전부(2014), 2013년 국가정보자원 개방공유체계 구축사업 완료보고,2014.3.

환경 및 과학기술 분야에서는 '국가 생물다양성 정보공유체계(CBD-CHM)'와 같이 세계 여러 나라가 국가 간 정보관리 및 연구능력의 차이를 극복하고 생물다양성 보전을 위하여 각 국이 보유하고 있는 관련 정보와 기술을 상호 공유하고 협력할 수 있는 네트워크를 구축하고 정보공유체계를 구축한 경우도 있다. 정보에의 자유로운 접근을 제공하고 필요로 하는 요구정보를 충족시키며 각기 다른 수준의 국가 능력을 보완하기 위하여 다른 수준의 정보처리 능력을 상호 보완하는 기능을 갖추었을 뿐만 아니라 관련 정책 결정 시 과학적 정보를 지원한다는 특징을 갖추고 있다.[15)]

정보공유체계 시스템은 관련 부처나 기관이 정보를 수집하여 정보공유시스템을 통해 메타데이터DB와 분류체계DB에 정보를 보관 및 분류하고, 정부기관, 연구기관, 산업체, 국민, 해외사용자 등이 메타데이터를 검색하거나 오픈API를 통해 정보서비스를 제공받는 체계의 시스템을 구축하고 서비스를 제공한다.

[그림 2-2] 국가생물다양성 정보공유체계

자료: 국가생물다양성 정보공유체계(CBD-CHM KOREA) 홈페이지 (http://www.kbr.go.kr)

사이버보안 분야의 경우, 최근 전 세계가 우려하고 있는 사이버 위협에 대응하기 위한 정보공유체계가 구축되고 있는데 활발히 운영되고 있는 정보공유체계의 대표 유형으로 볼 수 있다. 사이버 위협에 대응하기 위한 효율적이고 안전한 정보공유 체계 구축의 필요성을 인지하고, 사이버 위협 정보에 대한 표준을 바탕으로 일관성 있는 분석이 가능하도록 사이버 위협 정보공유체계를 구축하고 있다. 특히 사이버 공격의 주요 목표가 되는 국가 주요기반시설의 보호를 배경으로 하고 있어 국가안보 차원에서 각국의 보호 정책이

15) http://www.kbr.go.kr/content/view.do?menuKey=442&contentKey=4

수립되고 그 일환으로 정보공유가 추진되고 있으며, 그 어떤 분야보다도 법체계를 기반으로 관련 시스템을 구축하고 활발하게 운영되고 있다. 따라서 다양한 각국의 구축 사례를 찾아볼 수 있다.

대표적인 사례로 최초의 민관 사이버위협 정보공유시스템으로 알려진 '사이버 위협정보시스템(C-TAS, Cyber Threat Analysis & Sharing System)' 을 들 수 있다. C-TAS는 각종 위협정보를 수집해 통합 저장관리 하고, 이들 간 연관분석 등을 통해 사이버공격 시도에 대한 위협을 신속히 탐지해 이를 유관기관과 민간업체에 실시간으로 공유하게 된다. 일종의 클라우드 스토리지 형태로 구성되어 한국인터넷진흥원(Korea Internet & Security Agency, KISA)의 침해대응센터에서 수집한 사이버 위협정보를 비롯해 보안업체들이 수집한 정보가 모두 이를 통해서 공유되는 형태로 운영된다. C-TAS는 정부주도로 '정부-민간', '민간-민간' 의 정보공유 시스템을 체계화했다는 특징이 있다.[16)]

[그림 2-3] 사이버위협정보 분석공유시스템(C-TAS)

자료: 한국인터넷진흥원(2014), 사이버침해사고 정보공유 세미나 자료집(14년 3분기)

자동차 분야의 경우, 소비자의 자동차 결함신고정보를 관련 기관이 공유하여 자동차 결함조사의 시의성과 실효성을 확보하고 이해관계 기관간에 협력적 파트너십을 발휘할 수 있도록 하는 '자동차 결함 정보공유체계' 가 최근 몇 년 전부터 추진되고 있다. 이것은

16) 디지털데일리(2017), 민관 사이버위협 정보공유시스템 'C-TAS' 본격 가동, 2017.9.7. http://www.ddaily.co.kr/news/article.html?no=121428

자동차 결함정보를 대상으로 자동차 결함조사의 시의성과 실효성을 확보하기 위한 방안으로 ‘자동차 결함정보 공유 및 조사협의회’를 구성하여 운영하고 있는 형태이다.[17]

상기와 같은 정보공유체계는 스마트카 이용과 같은 IoT 시대의 위험을 대비하기 위하여 보다 미래지향적인 형태가 되어야 할 것이다. 따라서 SW안전 분야에서의 정보공유체계의 필요성은 한층 높아질 것인데, 아직까지 SW안전 분야의 정보공유 목적이나 형태는 사고예방을 위한 관련 사고사례 정보공유에 그치는 경우가 많다. 그 형태도 관련 기업의 활동 조사를 통해 일부 기업들이 사고사례를 수집하고 일정 범위에서 한정적으로 제공하고 있으며, 사고 시 비상채널을 구축하는 것으로 짐작된다.

2. SW안전 정보공유체계의 의의

국민의 안전과 관련된 철도, 항공, 원자력, 국방, 의료, 승강기 등 우리사회의 기반 영역에 대해서는 인간의 생명에 심각한 위협을 줄 수 있는 SW안전 관련 정보를 체계적으로 공유하여 SW오류 등에 의한 사고를 미연에 방지하거나 대응해야 하며 여기에 SW안전 정보공유체계의 의의가 있다.

정보공유체계의 일반적 정의에 따라 SW안전 정보공유체계의 정의를 살펴보면 다음과 같이 정의할 수 있다. 즉, ‘SW안전 정보공유체계란, 하나 또는 그 이상의 SW안전 관련 구성원(정부기관, 유관기관 또는 민간기업 등)이 보유하고 있는 SW안전에 대한 정보나 기술을 일부 또는 전체 구성원과 서로 공유하고 협력할 수 있도록 네트워크를 구축하는 방법 또는 시스템’이라 할 수 있다.

17) 한국소비자보호원(2013), 협력적 파트너십을 통한 자동차 결함정보 공동 활용, 2013.11.

제3장 미국 사례 연구

미국은 주요 국가 인프라 보호를 위한 정보공유체계에 있어 선진적인 대처를 진행하고 있는 대표적인 국가이다. 따라서 미국 ISAC을 대상으로 그 운영체제와 정보 공유나 민관 협력 방식을 조사하는 것은 매우 유의미하다.

미국의 산업도메인별 ISAC 현황은 다음과 같다.

<표 3-1> 미국의 ISAC 현황 비교

구분	설립취지	소관 부처	회원사	사무국 운영방법	주요기능	재원조달
IT-ISAC (정보기술)	해당분야의 정보공유 (민간주체)	국토 안보부	- IT벤더 - IT서비스제공업체 - 회원수: 비공개 - 가입조건: 회원계약	- IT-ISAC :비영리 유한책임회사 - 이사회 운영	- 분야간 정보 공유 · 분석	민간 (회비 운영, 정부 미부담)
Chemical ISAC (화학)	ACC 및 CHEMTREC 활동의 일환, 지역정보 공유 (민간 주체)	국토 안보부	- 활동 현황 없음	-	-	-
Communication ISAC (통신)	NS/EP 통신 보호의 일환, 분야간 연계 (정부 주체)	국토 안보부	- NCC직원(NS/EP 통신 관련 정부기관 및 민간기업으로부터의 파견자) - 가입조건: NCC 직원선정기준	- NCS/NCC운영	- NS/EP 통신 보호 - 모니터링 및 사고 대응	정부 NCS/NCC 예산 운영)
ES-ISAC (에너지)	NERC 활동 일환, 전력분야 정보 공유 (민간 주체)	에너지부	- 전력회사 및 전력 관련회사(NERC회원) - 회원수: 695기관 (2010.3 현재) - 가입조건: NERC 회원 계약	- NERC운영	- 분야간 DHS 및 타기관과의 정보 공유 · 분석 - ·전력 분야의 정보보안에 관한 검토	민간 (NERC 자금 운용, 정부 미부담)
FS-ISAC (금융 Financial Service)	분야간 정보공유 (민간 주체)	재무부	- 은행, 증권회사, 보험회사 등 - 가입조건: 회원계약	- FS-ISAC, Inc. 이사회 운영	- 분야간 정보 공유 · 분석 - DHS, 재무성, FSSCC, FBIC에 정보 제공	민간 (회비 운영, 정부 미부담)
MS-ISAC	분야간 정	국토	- 미국 50개주, 워싱	- 뉴 욕 주	- 분야의 정보	정부

(공공)	보공유 및 보안교육·인식제고 (정부 주체)	안보부	턴 프로그램 컬럼비아 특별구, - 각 지자체 각 미국령 정부	CSCIC 및 운영위원회 운영	공유·분석 - 정보보안 교육 및 인식제고 활동	(DHS 예산 운영)

자료: http://www.isac.or.kr/intro/intro01.jsp Home > 정보통신ISAC > ISAC 현황

제1절 미국의 주요기반시설 보호 및 정보공유에 대한 법적 근거 및 배경[18)]

1) 주요정보통신기반보호를 위한 법제 및 정책 추진 배경

9.11 테러 이후 미국 사회 내 안보강화 필요성이 확산되면서 제정된 국토안보법에 근거한 국가기반보호계획 등이 중요기반 보호의 법제도적 근간을 형성하게 되었다. 2001년 애국법에서 중요기반(Critical Infrastructure)을 '무력화나 파괴로 인해 국가안보, 경제안보, 공중 보건 및 안전에 영향을 미치는 물리적 또는 가상적 시스템 및 자산'으로 정의하고 정부운영이나 기반시설이 정보혁명에 크게 의존하는 통신, 에너지, 금융, 상하수도, 교통 등을 물리적, 정보적 기반의 네트워크에 점차 의존한다는 점을 고려하여 중요기반보호법을 애국법에 포함시켰다. 이후 중요기반보호와 관련하여 주요기반보호 행정명령(PDD-63), 중요기반 지정우선순위보호 국토안보행정명령(HSPD-7, Homeland Security Presidential Directive) 등을 시행하게 되었다.

2) 관련 법제

1) 행정명령 제63호(PDD-63)

※ Presidential Decision Directive 63(PDD-63) in 1998(행정명령 제63호)에 따라 설립

1998년 5월, 클린턴 정부는「행정명령(PDD, Presidential Decision Directive) 제63호」공표를 통해 주요기반시설에 대한 범정부적 보호체계를 처음으로 마련하였다. 이때부터 국

18) (참고) 미국의 보안 정보 공유 조직 (ISAC)의 상황 및 운영 실태에 관한 조사

(출처) 일본 내각관방에서 미국의 ISAC 현황을 상세히 비교분석한 조사보고서
※ 조사 목적 및 배경
일본의 중요 인프라의 정보보안 대책에 관한 제2차 행동 계획 '계획에 포함할 정보보안 대책'(2009년 2월 3일 정보 보안 정책의 결정)을 바탕으로 국제 협력을 추진하는 입장에서 실시하는 조사로써 셉터위원회의 창설과 국제 전략 그룹에 의한 각종 국제회의에 참여하는 형태의 사업을 진행하는 내각관방 정보보안센터(NISC)가 중요 인프라 보호에 대한 정보공유방법에 대해 검토하며 실시한 것임

가 주요기반 보호를 위한 전략개발이 연방정부를 중심으로 이루어지기 시작하였는데 이 행정명령을 통해 공공 및 민간 영역에서 위협, 취약점, 사고에 관한 정보를 공유하여 미국의 핵심 인프라를 보호할 수 있도록 상호 파트너쉽을 구축할 것을 요청하였다. 2003년, PDD-63은 HSPD-7(국토안보를 위한 행정명령 제7호)으로 업데이트되었으며 파트너쉽 미션을 재확인하였다.

2) 국가 인프라 보호 계획 2013(NIPP 2013)

※ The National Infrastructure Protection Plan (NIPP 2013)(국가 기반시설 보호 계획)

주요 기반시설 보안과 복원을 위한 제휴: 주요 기반시설 커뮤니티를 통해 정부와 민간 영역이 상호 협력하여 위험을 관리하고 보안과 탄력성을 회복할 수 있는 방법을 제공하였다. 2006년 발표되고 2009년 개정된 초기버전으로부터 진화한 개념인 “물리적, 사이버상의 핵심 기반시설이 안전하고 탄력적이며 취약점이 감소되며 결과적으로 위험가능성이 최소화되고, 위협이 식별, 분석되고, 대응 및 복구가 신속하게 진행되는 국가” 라는 비전 달성을 위한 통합적이고 협업적인 접근방식의 토대를 제공하는 국가계획을 의미한다.

3) 대통령 정책지침 제21호(PPD-21)

※ Presidential Policy Directive-21 (PPD-21): Critical Infrastructure Security and Resilience (대통령 정책지침 제21호) : 주요 기반시설 보안 및 복원에 관한 정책지침

주요 기반시설 보호에 관련되는 중앙 부처들의 역할과 의무를 명확히 하는 것을 주요 내용으로 한다.

제2절 분야별 정보공유체계 현황

1. 일반 SW안전 부문

1) 일반 SW안전부문 정보공유 관련 표준 현황

미국의 SW안전 관련 산업도메인에서는 아직까지 SW안전에 관한 정보공유 표준이 존재하지는 않는다. 다만, 해당 산업의 SW개발이나 이에 관한 인증, 평가 등의 기준을 위한 표준을 마련하고 있어 필요 시 이를 적용할 것으로 예측된다. SW안전에 관한 일반 현황을 이해하기 위해 소프트웨어 안전 산업 동향 조사 보고서(2017)를 토대로 간단히 살펴보면 다음과 같이 이해할 수 있다.

항공 분야에서 항공기는 우주항공, 국방, 그리고 민간에서 사용되는 것으로 구분될 수 있으며 각각의 표준이 용도에 맞게 발전하였다. 미국 항공분야의 안전 중요 소프트웨어 개발 표준은 민간 항공기를 규제하는 FAA (Federal Aviation Administration, 미국연방항공청)에서 사용되는 RTCA (Radio Technical Commission for Aeronautics) DO-178C, NASA (National Aeronautics and Space Administration, 미국우주항공국) 표준과 국방 표준인 MIL-STD 498의 3가지 부문으로 나눌 수 있다. 3가지 표준 중 민간 항공기에 적용되는 표준인 DO-178C 표준은 항공기에서 사용되는 안전 필수 소프트웨어의 안전성을 취급하는 가이드이며, 항공전자 소프트웨어 시스템을 개발하기 위한 사실상의 표준이다. FAA(Federal Aviation Administration)가 인증을 위한 기술 표준 오더(Technical Standard Order, TSO)를 명시할 때, DO-178C를 사용하여 소프트웨어가 항공 환경에서 신뢰할 수 있게 수행할 수 있는지를 확인하는 가이드로 활용한다. 따라서 DO-178C는 하드웨어 표준, 항공기 안전관련 개발 또는 평가 절차 가이드와 함께 기능시스템 구축의 요건으로 사용된다.[19)]

의료 부분에서 의료 소프트웨어에는 진단 또는 치료목적으로 사용되는 응용프로그램, 의료기기에 내장된 임베디드 소프트웨어, 의료기기의 부속품으로 작동하여 의료 기기 사용을 돕는 소프트웨어, 의료기기의 설계・생산・검사를 위해 사용되는 소프트웨어, 또는 의료기기의 품질제어관리용 소프트웨어 등이 포함된다. 2006년 유럽과 미국의 의료제품 소프트웨어 설계 표준으로 개발된 IEC 62304는 의료기기 소프트웨어의 안전 설계, 개발에 필요한 활동에 대한 소프트웨어 생명주기를 다루는데, 사용자 및 환자 등에 대한 상

19) SPRi(2015), 소프트웨어 안전 산업 동향 조사, pp.23-35, 2015.8.

해 심각도에 따른 A, B, C의 3단계 소프트웨어 안전등급을 적용한다. 2016년 개발된 건강 소프트웨어의 안전과 보안에 관한 국제표준인 IEC 82304-1은 주로 제조사에 대한 요구사항을 다루며, 소프트웨어 개발 전 생명주기를 다룬다. 특히, IEC 62304와 다르게 독립 실행 형 소프트웨어만을 다룬다는 특징이 있다.[20]

2) 일반 SW안전 관련 기업 정보공유 현황

미국에서 SW안전과 관련된 대표적인 5개 기업으로 SGS, Bureau Veritas, Intertek, Dekra, DNV GL사가 있다. 이들 기업은 대략 100년 이상의 역사를 가지고 있는 회사인데 주로 유럽을 중심으로 기업활동을 지속하고 있다. 이들은 소프트웨어 안전과 관련된 서비스를 제공하는데, 이들 기업을 서비스 제공 분야를 기준으로 살펴보면 다음과 같이 SW안전에 관한 특징을 이해할 수 있다.

SGS, Bureau Veritas, DEKRA는 자동차 산업에 대한 기능 안전성 평가 및 검증을 수행한다. 특히, SGS는 자동차뿐만 아니라, 제조 산업, 소비재&유통산업에 대해서도 테스팅, 컨설팅, 인증 및 교육 서비스를 제공한다. Bureau Veritas는 항공분야 인증을 위한 설계 및 인증 절차 운영을 하며 철도 수송 안전성 관련 가이드를 배포한다. Intertek는 온라인 가스 분석 시스템 및 전기차의 기능안전성 검증을 한다. DNV GL은 임베디드 소프트웨어 관련 안전성 검증, 평가, 기술개선 활동을 한다.

일반 SW안전에 관한 표준 및 기업 정보공유의 상세한 현황은 소프트웨어 안전 산업 동향 조사 보고서(2017)를 통해 확인할 수 있다.

20) SPRi(2017), 소프트웨어 안전 산업 동향 조사, pp.44-49,2017.4.

2. 정보통신 부문 : INFORMATION TECHNOLOGY ISAC[21)]

<표 3-2> IT-ISAC의 정보공유 현황 및 특징 요약

No	구분	해당 유형		현황 및 특징
1	관련 분야	1) 일반 분야		
		2) 보안 분야	○	IT 분야의 보안위협 최소화가 주목적
		3) SW안전 분야		
2	법적 근거	1) 법령 근거	○	대통령 결정지침 63 (PDD-63)
		2) 그 외 방법		
3	재원 조달	1) 정부		
		2) 민간		
		3) 정부 + 민간	○	IT산업기업-정부 파트너십 미국연방법의 비영리단체임
4	조직 형태	1) 일반 정보공유체계		
		2) 산업도메인별 대표 ISAC	○	미국 IT 산업도메인 대표 ISAC
		3) 기관 또는 기업의 자체 ISAC		
5	운영 활동	1) 일반		
		2) 커뮤니티	○	• IT업계 전문가 및 임원, 보안 분석가로 구성된 기술위원회 운영 • 위험 관리 및 대응 포럼 운영
		3) 스터디 그룹	○	4개의 Special Interest Groups(SIG) 운영
		4) 표준화		
6	정보 공유 방식	1) 시스템	○	Threat Intelligence Platform 독자 개발
		2) 이메일	○	오픈 소스의 사이버 위협 보고서 공유
		3) 인쇄물		
		4) 온라인 토의		
		5) 워크숍(컨퍼런스)	○	기술위원회 주관 오프라인 워크숍 개최
7	정보 공유 기술	1) 표준 규격 또는 기술	○	STIX / TAXII 프로토콜을 사용
		2) 독자 규격 또는 기술	○	플랫폼 독자 기술 개발
8	정보 공유 범위	1) 멤버십 별	○	Membership Level 에 따른 정보 공유
		2) 정보 유형별		
		3) 운영 활동별	○	SIG 별 공유 정보 범위 상이

※ 문헌부족으로 확인이 어려운 항목은 표기하지 않았음

21) http://www.it-isac.org/

1) 조직 및 운영 체계

법적 근거 및 관련 제도는 2장에서 설명한 주요기반시설에 대한 범정부적 보호체계인 행정명령 63 (PDD-63)이다.

(1) 조직 구성

IT-ISAC은 전 세계 규모의 IT 회사로 구성된 위원회가 운영하는 501(c)(6)[22] 회원기구로서, IT 관련 업계 전문가 및 임원, 보안 분석가 등으로 구성되어, IT 분야에서의 특별 이슈(주제) 또는 산업별 특별 관심 그룹에 참여한다.

IT-ISAC은 산업-정부 파트너십을 통해 사이버 보안을 발전시키는 것을 지원하기 위하여 IT 분야 조정 협의회(IT-SCC; IT Sector Coordinating Council)의 집행위원회를 구성하고 임명하는 일을 수행한다. IT-SCC는 광범위한 인프라 보호, 사이버 보안 활동 및 보안 문제에 대하여 정부와의 조정을 위한 주체 역할을 수행하여, 안전하고 탄력적이며 보호된 글로벌 정보 인프라 구조를 촉진한다. IT-ISAC은 National Council of ISACs(NCI)[23]을 창립하였으며, National Council of ISACs를 통해 정보를 공유·수신하고 파트너 ISAC의 분석가와 협력할 수 있는 방법을 제공한다.

<표 3-3> IT-ISAC 구성

IT-ISAC Officers	President: Peder Jungck, BAE Systems
	Vice President, Mary Ann Davidson, Oracle Corporation
	Acting Treasurer: Jim O'Conner, Cargill Corporation
IT-ISAC Board of Directors	Patrick Hellman, Arrow Electronics Jeff Huegel, AT&T Dan Melcher, BAE Systems, Inc. 등
Foundation Members	Arrow Electronics ,BAE Systems, Inc., Bunge, Cargill Conagra, Hewlett Packard Enterprise, Informatica Intel Corporation, Mimecast, NSS Labs, Oracle Corporation

자료: IT-ISAC Members, (http://www.it-isac.org/members)

22) 501(c) 조직은 미국 연방법의 비영리 단체로 일부 연방 소득세가 면제되는 단체이다. 그 중 501 (c)(6) 조직은 미국 상공 회의소와 같은 비즈니스 리그, 부동산 이사회, 무역위원회, 에디슨 전기 연구소, 보안 산업과 같은 조직이 포함된다. 협회는 이익을 위해 조직되지 않는다.

23) https://www.nationalisacs.org/

(2) 역할 및 책임

IT-ISAC은 기업이 위협을 최소화하고 위험을 관리하며 실제 사이버 보안 문제에 실시간으로 대응할 수 있도록 만들어진 단체로, 기술 회사들의 주제별 전문가 네트워크를 통해 업계 간 이해를 높이기 위한 서비스를 제공한다. 회원들의 위험 관리는 사이버 보안 커뮤니티를 통해 정보 공유를 하며 개선되며, 새롭고 실시간의 사이버 위협에 대한 글로벌 가시성을 제공하여 기업과 고객을 보호 할 수 있다.[24)]

회원들의 위험 관리 능력을 향상시키기 위해 신뢰할 수 있는 파트너와 관계 네트워크를 구축하고, 다 방향 정보 공유를 통해 개별 기업 네트워크와 핵심 인프라 커뮤니티의 보안을 공동으로 향상시킨다. IT-ISAC은 정보 보안 위협, 취약점, 사건, 대책 등에 대한 정보를 수집하고 분석하여 회원에게 제공한다. 격일로 오픈소스, 회원, 보안 파트너가 공유하는 사이버 사건에 대한 주요 정보를 문서화하여 위협 보고서를 서비스한다. 사이버 공격 및 물리적 관련 공격 및 회원 회사의 IT 분야에 영향을 줄 수 있는 자연 재해 또는 사건에 대한 정보 및 대응방법을 제공한다.

(3) 운영 방식 및 활동

IT-ISAC은 IT 분야에 영향을 미치는 보안 위협을 최소화하고 위험을 관리하며 사이버 사건에 대응할 수 있는 IT 기업들이 참여하는 일종의 포럼을 만들었고, 회원들은 신뢰할 수 있는 협력을 통해 지식, 관행 및 통찰력을 공유한다.

IT-ISAC은 1개의 Technical Committee 및 4개의 SIG (Special Interest Groups)를 갖는다. Special Interest Groups에는 Security Intelligence SIG, Insider Threat SIG, Food and Agriculture SIG, Physical Security and Business Continuity Group 등이 포함된다.

기술위원회(Technical Committee)는 IT-ISAC 회원들이 주요 주제 전문가 및 외부 회원사의 최신 사이버 보안 위협 정보 및 동향에 대한 브리핑을 받을 수 있는 포럼을 제공한다. 이러한 주제에는 새로운 공격 동향 및 전술, 취약점 및 회사 별 위험 관리 프로세스에 대한 프레젠테이션이 포함된다. 기술위원회는 IT-ISAC이 사이버 사건에 대한 대응을 조정하고 사이버 위협 정보를 공유하기 위해 사용하는 기본 포럼이기도 하다.

Security Intelligence SGI는 고급 위협 탐지와 관련된 아이디어, 전략, 기술 및 정보를 교환 할 수 있도록 하는 것에 중점을 둔다. Insider Threat SGI는 IT-ISAC 구성원이 조직

24) it-isac.org, YOUR PARTNER IN THE DEFENSE AGAINST CYBER THREATS, WHO IS IT-ISAC?, pp.2, (http://docs.wixstatic.com/ugd/b8fa6c_9ab65f4ac8a34ca9bf38603012754ec5.pdf)

내에서 악성 및 비 악의적인 위협을 식별하는 방법에 대해 협력할 수 있도록 하기 위해 존재한다. 내부 위협을 식별하고 완화하기 위해 사용되는 도구, 프로세스, 기술 및 정책에 대한 정보를 공유할 수 있는 포럼을 제공한다. Food and Agriculture SGI는 식품 및 농업 부문에서 사업을 하는 IT-ISAC 회원들 간에 신뢰할 수 있는 정보 공유 및 협업 분석을 용이하게 한다. 회원들이 공통으로 가질 수 있는 공격, 사건 및 위협 요소를 보다 효과적으로 식별하고 완화 전략을 공유한다.

Physical Security and Business Continuity Group은 회원 내의 주제별 전문가가 물리적 보안 및 비즈니스 연속성 문제를 논의하고 위협을 완화하거나 대응할 수 있는 효과적인 방법을 공유할 수 있는 포럼을 제공한다. 자연 재해, 사고, 의도적 공격, 물리적 보안 및 비즈니스 연속성에 영향을 미치는 사안으로부터 물리적 보안 위협 및 사건 보고서에 대한 정보를 효율적으로 배포 할 수 있는 방법을 제공한다.

2) 정보공유 체계

(1) 정보공유 방식

IT-ISAC은 자동화된 공유 및 위협 분석을 가능하게 하는 독점적인 Threat Intelligence Platform을 활용한다. 이 플랫폼을 통해 회원은 미국 국토 안보부, IT-ISAC 회원, 전 세계 IT-ISAC 파트너 및 IT-ISAC 직원 연구원을 포함하여 매주 수천 개의 위협 표시기에 액세스 할 수 있다.[25] 정보 공유 표준으로 매주 STIX / TAXII 프레임워크[26]를 활용하여 정보를 자동 공유하고 수천 개의 지표를 저장·집계하는 IT-ISAC의 플랫폼에 대한 액세스를 할 수 있다.

IT-ISAC 파트너는 IT-ISAC과 회원들과 분석 보고서를 공유한다. 보고서에는 국토 안보부, 기타 산업별 ISAC 및 보안 공급 업체 파트너의 분석이 포함된다. 정기적인 보고 외에도 IT-ISAC은 회원들에게 향상된 상황 인식 및 완화 전략을 제공하는 사건별 보고서를 발행한다. 이 보고서는 회원들과의 협조 하에 개발되어 회원들의 합의 권고를 반영하고 회원들이 완화 활동을 조정할 수 있도록 한다.[27]

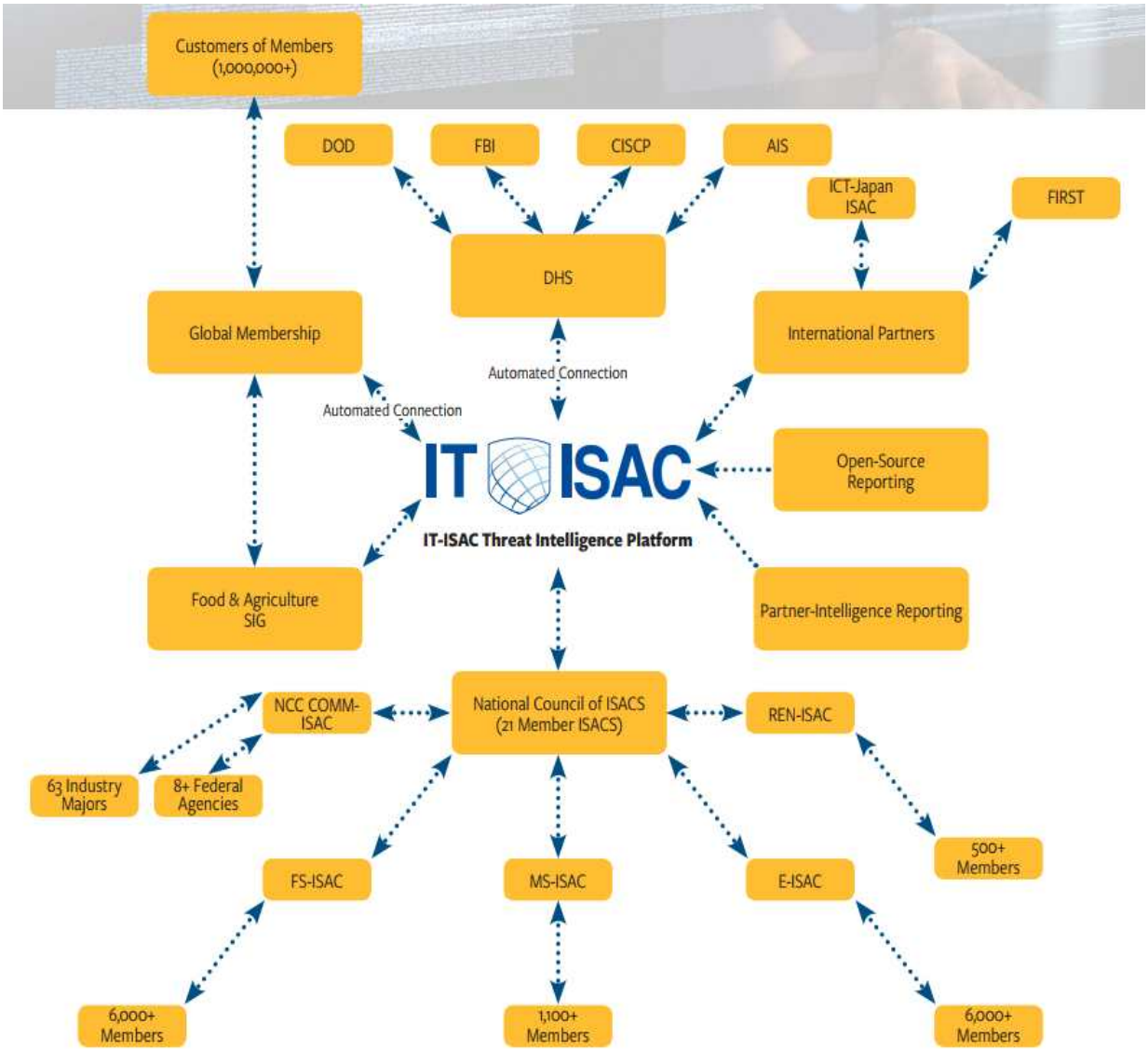
---

25) it-isac.org, YOUR PARTNER IN THE DEFENSE AGAINST CYBER THREATS, pp.3, (http://docs.wixstatic.com/ugd/b8fa6c_9ab65f4ac8a34ca9bf38603012754ec5.pdf)

26) 미국의 국토안보부는 13년 4월에 사이버 위협 정보 전송 규격인 TAXII(Trusted Automated eXchange of Indicator Information) 공식 버전 1.0을, 10월에는 사이버 위협 표현 규격인 STIX(The Structured Threat Information eXpression) 공식버전 1.0.1을 각각 발표하였다

27) IT-ISAC MEMBER PARTICIPATION GUIDE (http://docs.wixstatic.com/ugd/b8fa6c_d8e6c5df296c43b6acddc28e65b42949.pdf)

[그림 3-1] IT-ISAC 정보 공유 관계도



자료: it-isac.org, YOUR PARTNER IN THE DEFENSE AGAINST CYBER THREATS
(https://docs.wixstatic.com/ugd/b8fa6c_9ab65f4ac8a34ca9bf38603012754ec5.pdf P.4)

IT-ISAC은 CERT (Computer Emergency Response Team)와 매일 정보를 공유하며, CERT는 관련 정보를 연방 기관 및 민간 기관에 전달한다. 또한 IT-ISAC은 웹 사이트에 경고 및 경고를 게시하며 이러한 공공 부문과의 협력은 새로운 보안 위협에 대한 조기 통보를 가능하게 한다.

IT-ISAC은 지난 24 시간 동안 발견하거나 보고된 중요한 사이버 사건 및 취약점을 요약한 일일 보고서를 작성한다. 여기에는 구성원과 파트너가 공유한 공개 소스 및 우선순위 또는 플랫폼에서 사용할 수 있는 위협 정보에 대한 분석을 통해 식별되는 정보가 포함된

다. 주간 보고서는 매주 금요일 발행되며 주간 주요 공개 소스 보고를 요약한다.

IT-ISAC은 FIRST[28]의 회원사이며 매일 FIRST 회원에게 오픈 소스의 사이버 위협 보고서를 제공한다.[29]

(2) 정보공유 범위

IT-ISAC은 사이버 위협 정보를 국토 안보부와의 공유하면서 강력한 협력관계를 유지하고 국토 안보부는 회원이 지정한 정보 공유 수준에 따라 해당 정보에 접근할 수 있다.

위협 정보, 정보 공유 및 공동 작업 서비스는 지정된 세 가지 회원 등급(Membership Level)에 따라서 제공된다. 예를 들어, Foundation Gold 회원등급은 Arrow Electronics, BAE Systems, Inc., Bunge 등이 가입되어 있고, 보장되는 이사회 회원, Threat intelligence Platform 접속 가능수 등과 같은 서비스에서 다른 회원 등급보다 많은 서비스를 제공받는다.

[그림 3-2] IT-ISAC GOLD Foundation 회원

자료: it-isac.org, YOUR PARTNER IN THE DEFENSE AGAINST CYBER THREATS (https://docs.wixstatic.com/ugd/b8fa6c_9ab65f4ac8a34ca9bf38603012754ec5.pdf P.6)

28) 사고 대응에 있어 세계적인 선두 주자이며, 정부기관, 상업기관 및 교육기관의 다양한 컴퓨터 보안 사고 대응 팀으로 구성됨. (http://first.org/)
29) What relationships does IT-ISAC have with organizations outside the U.S.? (http://www.it-isac.org/faq)

[그림 3-3] IT-ISAC 회원 등급

BENEFITS OF IT-ISAC MEMBERSHIP (List of Services)	FOUNDATION Gold ($25,000)	PREMIUM Silver ($8,000)	PARTICIPANT Bronze ($3,000)
Guaranteed Board Memberships	2	0	0
Number of credentials to access the Threat Intelligence Platform	20	10	7
Number of persons receiving daily IT-ISAC Report	15	5	5
Number of persons with access to the IT-ISAC Technical Committee weekly meeting	10	5	2
Number of IT-ISAC Special Interest Groups your company can participate in	Unlimited	3	1

자료: it-isac.org, YOUR PARTNER IN THE DEFENSE AGAINST CYBER THREATS (https://docs.wixstatic.com/ugd/b8fa6c_9ab65f4ac8a34ca9bf38603012754ec5.pdf P.5)
참고: 숫자는 등급별 혜택 수를 의미함

각 회원사는 다음과 같다.

<표 3-4> IT-ISAC Member List

Member Grade	Member Name
Foundation Gold (8)	Arrow Electronics, BAE Systems, Inc., Bunge, Cargill, Hewlett Packard Enterprise, Intel Corporation, NSS Labs, Oracle Corporation
Premium Silver (11)	Afilias USA, Inc., Cisco Systems, CSC, Fire Eye, HCA Healthcare, Jabil, Juniper Networks, Monsanto, Netflix, Neustar, Trend Micro, USA
Participant Bronze (24)	Acquia, AT&T, Black Box, Box.com, BrandProtect, Inc., Cimpress USA, Inc., Commvault, Dell Technologies, DocuSign, Fastly, Inc., Foreground Security, InfoReliance, IBM, Lockheed Martin Corporation, Nuance, Optiv, Paladion Networks, Prescient Solutions, RedSeal, Syngenta, Tech Data Corporation, The DigiTrust Group, The Hershey, Company, Workday, Inc.

자료: it-isac.org, YOUR PARTNER IN THE DEFENSE AGAINST CYBER THREATS (https://docs.wixstatic.com/ugd/b8fa6c_9ab65f4ac8a34ca9bf38603012754ec5.pdf)

(3) 정보공유 기술 및 활용

IT-ISAC에서 공유하는 모든 지표는 모든 구성원이 접근할 수 있는 Anomali[30] 위협 정보 플랫폼으로 가져온다. IT-ISAC의 직원 및 회원이 업로드 한 정보 이외에도 이 플랫폼은 DHS(Department of Homeland Security, 미국국토안보부) CISCP(Cyber Information Sharing and Collaboration Program) 및 AIS(Automated Indicator Sharing)[31] 프로그램의 일

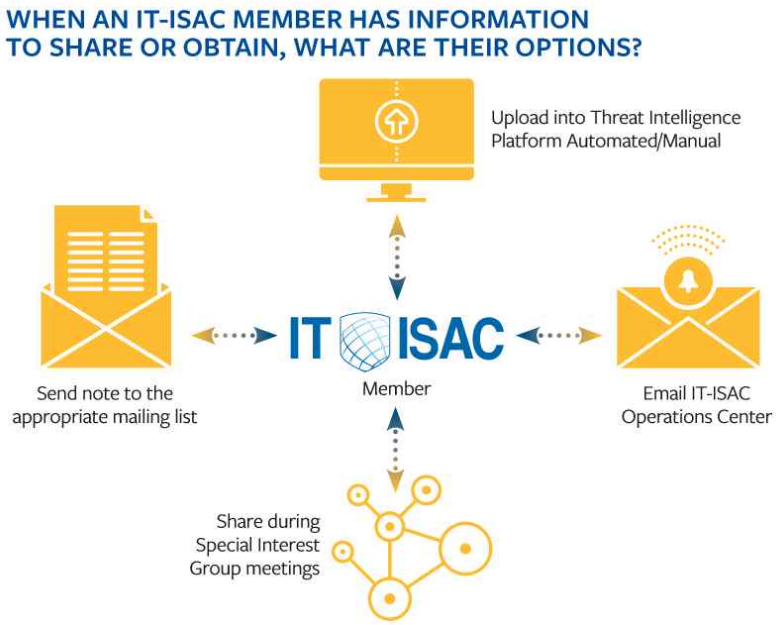
30) Anomali: Threat Intelligence Platform (http://www.anomali.com/)
31) AIS (Automated Intelligence Sharing)

부로 자동화 된 피드를 수신한다. 또한 멤버가 기존 도구와 쉽게 통합할 수 있는 STIX / TAXII 프레임워크를 활용한다.

미국 국토 안보부(DHS)의 자동화된 피드를 받고 위협 정보 플랫폼을 활용하여 구성원과 자동으로 공유한다. 플랫폼은 STIX / TAXII 프로토콜을 사용하며 API를 통한 자동화된 연결을 가능하게 한다. 이 플랫폼은 모든 STIX / TAXII 지원 제품에서 작동하도록 설계되었으며 IT-ISAC이 받는 모든 지표는 회원들의 자동 연결을 통해 이 플랫폼에 제출된다.[32]

회원, 보안 파트너 및 포럼에 푸시 알림 형식으로 알리고, 사이버 사건, 위협 및 동향을 감지하여 대응 시간을 단축시킨다. IT-ISAC에 합류함으로써 효과적인 사이버 위협 정보 공유 및 분석을 통해 정보 인프라 구조를 강화하고 신뢰할 수 있는 분석, 협업 및 조정을 통해 위험을 관리하여 해당 정보에 입각한 의사 결정을 내릴 수 있다.

[그림 3-4] IT-ISAC 기술 개념도



자료: (https://docs.wixstatic.com/ugd/b8fa6c_9ab65f4ac8a34ca9bf38603012754ec5.pdf P.3)

32) Does IT-ISAC partake in automated information sharing? (http://www.it-isac.org/faq)

3. 항공 부문 : AVIATION ISAC[33)]

<표 3-5> AVIATION ISAC의 정보공유 현황 및 특징 요약

No	구분	해당 유형		현황 및 특징
1	관련 분야	1) 일반 분야		
		2) 보안 분야	○	항공 산업에 대한 사이버 위협 정보 공유
		3) SW안전 분야		
2	법적 근거	1) 법령 근거	○	국가 인프라 보호 계획 (NIPP)
		2) 그 외 방법		
3	재원 조달	1) 정부		
		2) 민간		
		3) 정부 + 민간	○	민간 주도의 정부 파트너가 참여하는 비영리 기구
4	조직 형태	1) 일반 정보공유체계		
		2) 산업도메인별 대표 ISAC	○	항공부분 대표 ISAC
		3) 기관 또는 기업의 자체 ISAC		
5	운영 활동	1) 일반		
		2) 커뮤니티		
		3) 스터디 그룹	○	공유 데이터 분석 그룹 (Analyst Working Group)
		4) 표준화		
6	정보 공유 방식	1) 시스템	○	실시간 위협 공유를 위한 가상 플랫폼 제공
		2) 이메일	○	업계 간행물 및 인터뷰 기사 제공
		3) 인쇄물		
		4) 온라인 토의	○	• WebEx를 통한 가상 커뮤니티 회의 개최 • 격주 전화 회의 • 1:1 지원
		5) 워크숍(컨퍼런스)	○	연례 정상 회담을 가짐
7	정보 공유 기술	1) 표준 규격 또는 기술	○	TLP (Traffic Light Protocol) 사용
		2) 독자 규격 또는 기술		
8	정보 공유 범위	1) 멤버십 별	○	멤버 등급에 따라서 서비스를 제공
		2) 정보 유형별		
		3) 운영 활동별		

※ 문헌부족으로 확인이 어려운 항목은 표기하지 않았음

33) (http://www.a-isac.com/)

1) 조직 및 운영 체계

정보 공유 및 분석 센터 (ISAC)는 1998년 대통령 결정 지침 63 (PDD-63, Presidential Decision Directives)의 결과로 창안되었다. PDD-63은 2003년에 국토 안보부 행정명령 / HSPD-7(Homeland Security Presidential Directive)과 함께 업데이트되었다. 또한 국가 인프라 보호 계획(NIPP, National Infrastructure Protection Plan)를 근거로 한다. 조직은 국토안보부, 교통보안관리, 연방항공국, 연방수사국, 국방부 등으로 구성된다.

(1) 역할 및 책임

A-ISAC(AVIATION ISAC)은 항공 산업 내에서 안전한 익명의 사이버 위협 정보 공유를 위해 만들어졌으며, 세계 항공 산업 전반의 협력을 촉진하여 취약성, 사건 및 위협에 대비하는 능력을 향상시키는 것을 목표로 한다.

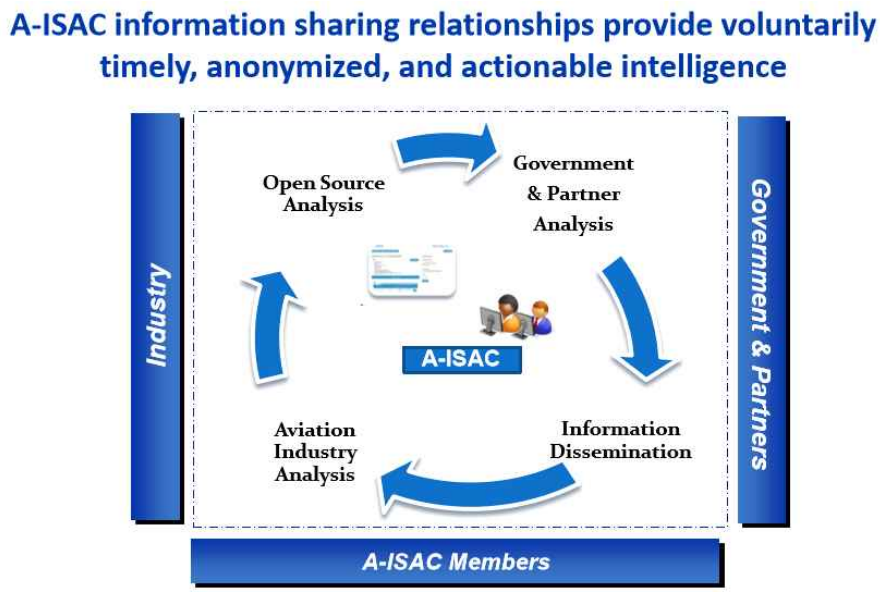
회원들에게 적절하고 실행 가능한 정보를 보급하고 위협, 취약성, 잠재적 보호 조치 및 관행에 관한 시기적절하고 실행 가능한 정보의 공유를 촉진한다. 표준을 사용하여 회원 등급에 따라 정보를 제공하고, 위협의 정확성과 심각성을 확인하기 위하여 받은 정보를 분석하고 적절한 조치를 권고한다.

(2) 운영 방식 및 활동

최고 정보 책임자, 최고 기술 책임자 (CTO), 최고 정보 보안 책임자, 분석가, 사이버 보안 전문가, 정부 파트너가 참여한다. 안전하고 신뢰할 수 있는 네트워크를 사용하여 회원 간의 협력과 통신을 촉진하며, 정보를 조사 및 분석하여 정확성과 심각성을 검증하고 완화 전략을 권고한다. 공공 및 민간 부문에서 전문적이고 신뢰할 수 있는 관계를 발전시키는 것이 가능하다.

A-ISAC의 분석가들은 데이터베이스를 사용하여 회원들에게 적절하고, 유익하며, 실천 가능한 실시간 위협 대상의 정보와 분석을 제공한다. 또한 회원들이 문제가 있거나 우려사항이 있는 경우 각 구성원과 직접 협력하고, 데이터 제출에 대해 질문이 있을 경우 각 회원들에게 답변해 준다.

[그림 3-5] A-ISAC 운영 개념도



자료: (http://trbcybersecurity.erau.edu/resources/01_14_16_Francy_TRB_Panel_AISAC_FINAL.pdf P.12)

2) 정보공유 체계

(1) 정보공유 방식

A-ISAC은 실시간 위협 공유를 위해 세계적으로 접근 가능한 가상 플랫폼을 제공하고, WebEx를 통한 가상 커뮤니티 회의를 개최한다. A-ISAC은 전 세계 항공 업계의 협력을 위해 대면 네트워킹 및 교육인 연례 정상 회담을 개최함으로써 정보 공유 효과를 극대화 한다. 2017년의 주제인 '항공 공동체의 글로벌 탄력성 (Global Resiliency)' 은 보다 탄력적인 인프라를 구축하기 위해 전 세계에 걸친 행동 네트워크를 구축하는데 필요한 사항을 주제로 한다.

A-ISAC은 사이버 위협 및 공격에 가까운 실시간 알림, 항공 산업 전반의 익명 정보 공유, 최신 사이버 활동에 대한 토론을 격주로 하는 전화 회의, 일대일 지원, 연례 정상 회의 참석 등 다양한 혜택에 대한 액세스를 제공한다. 업계 간행물의 인터뷰와 기사는 항공 사이버 전문가에게 정보 공유의 중요성을 향상시킨다.

(2) 정보공유 범위

A-ISAC은 전 세계 항공 업계가 직면한 보안 위협, 취약성 및 위험 정보를 수집한다. 정보 출처에는 회원, 정부 기관, 학술 기관, 오픈 소스 및 기타 신뢰할 수 있는 출처가 포함된다. 업계 전문가가 분석한 후, 회원 등급에 따라서 경고가 전달된다. A-ISAC은 플래티넘, 골드, 실버 멤버쉽을 제공하며 멤버쉽에 따라서 서비스를 제공한다.

[그림 3-6] A-ISAC Member Benefits

Member Benefit	Silver	Gold	Platinum
Secure Portal Access/Accounts**	1	5	20
Summit Attendance***	1 pass	3 passes	7 passes
Analyst Workshop Attendance	—	2 attendees	up to 5 attendees
Red Team Exercises	—	✓	✓
Tabletop Exercises	—	✓	✓
Regional Training	✓	✓	✓
Daily Aviation Memo/Weekly Aviation Memo	✓	✓	✓
Daily Portal Posting Report	—	✓	✓
Critical Industry Alerts	✓	✓	✓
Strategic and Analytic Products	limited	✓	✓
Bi-weekly Analyst Calls	—	✓	✓
Analyst Working Group	—	✓	✓
Phish Program	✓	✓	✓
Dark Web - Private Contracted Services	✓	✓	✓
Domain Squatting Alerting Service	✓	✓	✓
IA Collection, Strategic, Tactical Analysis	—	✓	✓
NIAB: Network Scanning Tool/IRP	SLA	SLA	✓
On-Site Incident Response Assistance	fees & expenses	expenses only	✓
IOCs	limited access	✓	✓
Social Media Monitoring	✓	✓	✓
Member Surveys	✓	✓	✓
Member Directory		✓	✓

*** Additional portal accounts are available for a fee.*
**** Additional Summit passes are available for a fee.*

자료: (http://www.a-isac.com/join)

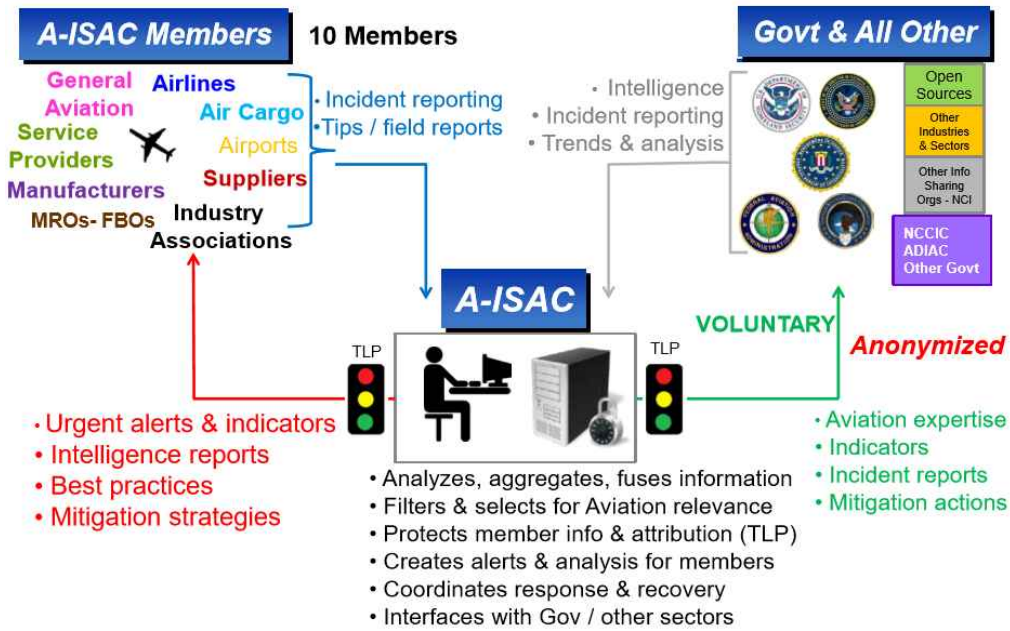
모든 국가 또는 법 집행 기관은 회원의 사전 승인 없이 회원이 제출한 데이터에 액세스 할 수 없다. A-ISAC은 데이터를 제공하는 회원이 승인한 범위에 따라 적절하게 처리하여 정부 기관에 데이터를 제공한다.

(3) 정보공유 기술 및 활용

전 세계 항공 업계의 참가자들에게 적시에 익명으로 실행 가능한 정보를 공유할 수 있는 기능을 사용한다. 신뢰할 수 있는 회원 공유는 항공 공동체의 상호 이익을 위해 협력 및 통신을 촉진하는 안전하고 사적인 방식으로 수행된다.

TLP(Traffic Light Protocol)을 사용하여 정보 공유 범위를 설정한다.[34)]

[그림 3-7] A-ISAC 기술 개념도



자료: (http://www.ecedha.org/docs/default-source/energy-and-power/faye-francy.pdf?sfvrsn=0 P.11)

* ISAC 형태가 아닌 항공 분야 정보공유 체계

GAIN(Global Aviation Safety Network)은 항공 안전 전문가가 잠재적인 안전 문제를 파악하고, 우선순위를 정하여 솔루션을 개발하고 솔루션의 작동 여부를 평가할 수 있는 유용한 정보로 전환하도록 도와주는 도구와 프로세스를 개발하고 있다.

GAIN은 많은 양의 데이터 수집을 장려하고 촉진하는 법적 및 문화적 환경을 조성하는데 도움을 준다. 자발적이고 개인 소유로 운영되는 데이터 수집 및 교환 시스템의 글로벌 네트워크를 통해 정부, 산업 및 노동계는 안전한 시스템을 보다 안전하게 만들기 위해 서로 협력하여 상호 이익을 얻고 있으며 항공 안전 전문가가 해당 데이터를 유용한 정보로 변환하는데 도움이 되는 도구와 프로세스를 개발하고 있다.

34) 제6장 국내외 정보공유 규격 및 표준에 자세히 설명

4. 의료 부문 : NATIONAL HEALTH ISAC[35)]

<표 3-6> NH-ISAC의 정보공유 현황 및 특징 요약

No	구분	해당 유형		현황 및 특징
1	관련 분야	1) 일반 분야		
		2) 보안 분야	○	보건 부문의 사이버 보안 보호 및 사이버 위협을 대비함
		3) SW안전 분야		
2	법적 근거	1) 법령 근거	○	국가 인프라 보호 계획 (NIPP)
		2) 그 외 방법		
3	재원 조달	1) 정부		
		2) 민간		
		3) 정부 + 민간	○	민간 주도의 정부 기관과의 파트너십을 갖는 비영리 조직
4	조직 형태	1) 일반 정보공유체계		
		2) 산업도메인별 대표 ISAC	○	건강 분야 대표 ISAC
		3) 기관 또는 기업의 자체 ISAC		
5	운영 활동	1) 일반		
		2) 커뮤니티	○	정보 공유를 위한 커뮤니티 및 포럼 운영 MD-VIPER 프로그램
		3) 스터디 그룹	○	CYBERFIT® 보안 서비스 그룹 운영
		4) 표준화		
6	정보 공유 방식	1) 시스템	○	포탈
		2) 이메일	○	Intelligence Reports
		3) 인쇄물		
		4) 온라인 토의		
		5) 워크숍(컨퍼런스)	○	• 교육 행사 서비스 개최 • HHS SCC Meetings 개최
7	정보 공유 기술	1) 표준 규격 또는 기술	○	TLP (Traffic Light Protocol) 사용
		2) 독자 규격 또는 기술	○	AIS (Automated Intelligence Sharing) 기술 사용
8	정보 공유 범위	1) 멤버십 별	○	Tier에 따라서 서비스를 제공
		2) 정보 유형별		
		3) 운영 활동별		

※ 문헌부족으로 확인이 어려운 항목은 표기하지 않았음

35) (http://nhisac.org/)

1) 조직 및 운영 체계

NH-ISAC도 1998년 행정명령 63 (PDD-63)과 국가 인프라 보호 계획 (National Infrastructure Protection Plan, NIPP-13)에 근거하여 구성되었다. NH-ISAC은 미국 보건 복지부 (HHS)[36], 보건 부문 조정 협의회 (SCC)[37], ISAC 전국 협의회, 정보 기관 (미국 국토 안보부, NSA[38])을 통해 미국의 보건 및 공공 보건 기반 시설에 대한 공식 ISAC으로 인정 받고 있다.[39] ISAC은 CIKR[40]을 통한 사고대응에서 체계적인 협업을 수행하기 위해 특정 기관 및 협의회와 협력한다.[41]

(1) 조직 구성

NH-ISAC은 건강관리 분야의 비영리 회원 중심의 조직이다. NH-ISAC은 HIMSS[42], MDISS[43], EHNAC[44] 및 CHIME[45]과 같은 정부, 법 집행 기관, 공급 업체 커뮤니티, 기타 ISAC 및 HPH[46] 협회와 같은 외부 파트너와 지속적으로 관련되어 상황 인식을 촉진한다. 의료 서비스 제공자, 제약회사, 약국, 보건부, 혈액은행, 의료기기 제조업체, 건강관리 및 공공 보건 분야의 이해 관계자 또는 파트너가 참여한다. NH-ISAC은 전 세계 여러 파트너 및 사이버 비상대응 팀 (CERTS)과 협력하고 있다.

[그림 3-8] NH-ISAC Board of Directors

NH-ISAC BOARD OF DIRECTORS

Aetna, Inc.	Johnson & Johnson
Allergan	Merck & Co.
Amgen	Medtronic
City of Hope	Partners Healthcare
CVS Health	Royal Phillips
Emory University	Texas Health Resources
Human Longevity, Inc.	Wellmark Blue Cross Blue Shield
Intermountain Healthcare	NH-ISAC President

자료: (http://nhisac.org/nhisac-board/)

---

36) HHS (U.S. Department of Health and Human Services)
37) SCC (Health Sector Coordinating Council)
38) NSA (National Security Agency)
39) How is the NH-ISAC recognized? (http://nhisac.org/nhisac-faq/)
40) CIKR (Critical infrastructure/Key Resources)
41) Why IS IT Called NH-ISAC And Not NH-ISAO? (http://nhisac.org/nhisac-faq/)
42) HIMSS (Healthcare Information and Management Systems Society)
43) MDISS (Medical Device Innovation, Safety and Security Consortium)
44) EHNAC (Electronic Healthcare Network Accreditation Commission)
45) CHIME (College of Healthcare Information Management Executives)
46) HPH (Health care and Public Health sector)

(2) 역할 및 책임

NH-ISAC은 보건 부문의 사이버 보안 보호와 사이버 위협 및 취약성을 대비하고 이에 대응하는 능력을 향상시킴으로써 대중의 신뢰를 얻고 유지하는 것이다.[47] 국민 건강관리 ISAC 커뮤니티로서 유사 업종의 관계자가 요구하는 개인정보 보안 문제를 관리하면서 의료 혁신을 지원하고 기술의 통합을 확대하고 있다.

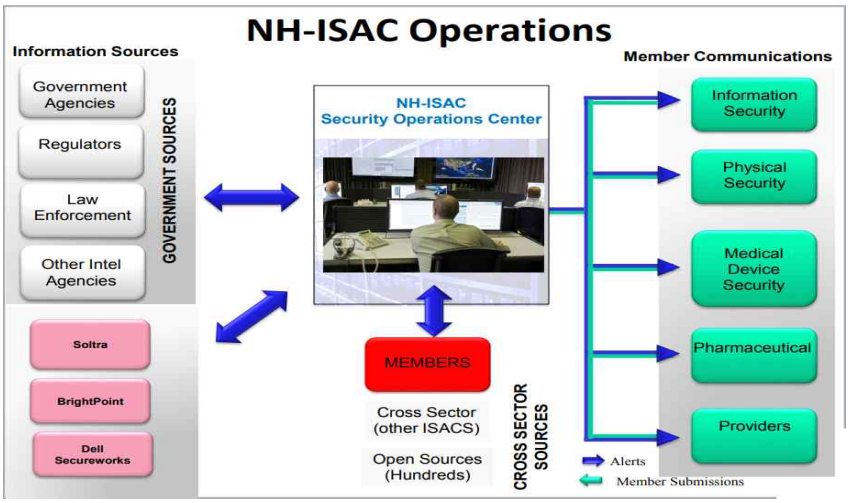
전 세계 보건 부문의 사이버 및 물리적 보안 및 보호, 사이버 및 물리적 위협과 취약점을 실시간 공유·대비를 통해 회원사의 브랜드 자산, 환자 및 소비자를 보호한다. NH-ISAC 회원사는 핵심 위협 정보뿐만 아니라 위협 완화 전략을 공유하여 잠재적인 공격 위험을 줄인다. 사이버 보안에 대한 상황 인식, 정보 공유, 분석 및 대응 도구를 제공한다.[48]

(3) 운영 방식 및 활동

NH-ISAC은 현재 유럽 전역에 빠르게 확산되고 있는 Petya 랜섬 공격을 추적하고 있다. 각 멤버들에게서 의료기기, 제약 등의 보안 관련 정보를 제출받고 NH-ISAC은 확인된 정보를 정부나 다른 ISAC에게 경고하고 알림으로서 공유한다.

NH-ISAC은 비영리 및 영리를 목적으로 하는 의료 관계자에게 사이버 및 물리적 보안 위협의 지표, 모범 사례 및 완화 전략을 공유하기 위한 커뮤니티 및 포럼을 제공한다.

[그림 3-9] NH-ISAC 운영 개념도



자료:
(http://www.first.org/resources/papers/conf2017/Medical-Device-Security-A-Sucking-Chest-Wound-That-Needs-Emergency-Medicine.pdf, P.12)

47) What Is NH-ISAC's Mission? (http://nhisac.org/nhisac-faq/)
48) Why is there a fee for being a member? (http://nhisac.org/nhisac-faq/)

2) 정보공유 체계

(1) 정보공유 방식

CYBERFIT®은 NH-ISAC에서 제공하는 보안 서비스 그룹으로, 의료계 내의 사이버 보안 위험을 줄이는 데 중점을 둔다. 회원사의 내부 및 제 3자 공급 업체의 위험을 관리하고 모니터할 수 있다.[49] 워킹 그룹과 위원회는 CYBERFIT®과 같은 서비스에 중점을 두고 NH-ISAC 커뮤니티를 활용하여 서비스를 제공한다.[50]

CYBERFIT®은 합리적인 조달 및 추천 프로세스를 통해 공유 데이터 및 보안 서비스에 대한 경제적인 액세스를 제공하므로 대량 판매 가격으로 인해 신뢰할 수 있는 공급 업체를 쉽게 찾고 멤버십 요금을 낮춘다. CYBERFIT®은 사고 대응 및 악성 코드 분석, 침투 테스트, 웹 응용프로그램 테스트, 취약점 평가·관리를 제공한다.

(2) 정보공유 범위

NH-ISAC은 공유되는 데이터에 접근 가능 범위를 지정하기 위해 TLP (Traffic Light Protocol)를 사용한다.

<표 3-7> TLP (Traffic Light Protocol)

Traffic Light Protocol	
Red	정의된 그룹 (예: 미팅참여인원) 으로 제한됨. RED로 표시된 정보는 그룹 외부의 누구와도 공유되어서는 안 된다.
Yellow	ISAC 회원들과 공유할 수 있는 정보.
Green	ISAC 회원 및 파트너 (예: 공급 업체, MSSP[51], 고객)와 정보를 공유할 수 있다. 이 카테고리의 정보는 공개 포럼에서 공유할 수 없다.
Whtie	자유롭게 공유할 수 있으며 표준 저작권 규칙의 적용을 받는 정보.

자료: NH-ISAC, Advancing the global health Sector’s Cyber and Physical Security, pp.15

49) http://nhisac.org/cyberfit/
50) http://nhisac.org/about-nhisac/
51) Managed Security Service Provider

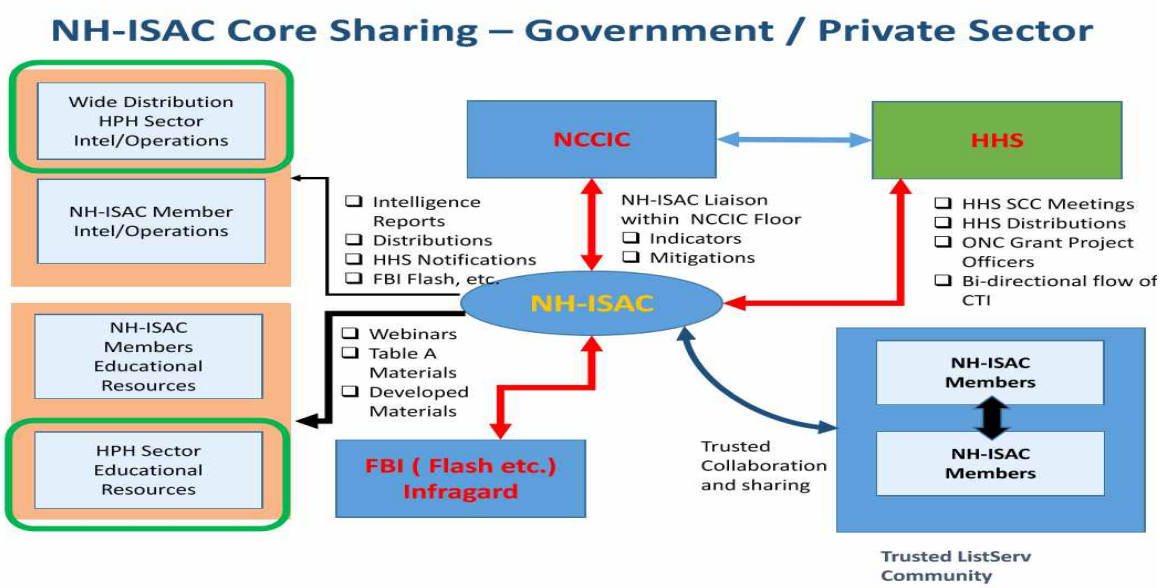
(3) 정보공유 기술 및 활용

HPH(Health Care and Public Health sector)의 취약성과 관련된 위험을 사전 예방하기 위해 AIS(Automated Intelligence Sharing)기술을 사용하여 정보를 공유한다.

NH-ISAC은 보건 및 공공 보건 부문(HPH)의 위협 요소에 대한 기술 및 절차(TTP), 조언 및 모범사례, 사건 및 취약성에 대한 기밀정보를 포함하여 시기적절하고 실행 가능한 정보를 서로 공유하는 것에 주력한다. 완화 전략 및 기타 가치 있는 자료의 공유는 기계 또는 사람 간에 발생하며 신뢰를 촉진하기 위해 다양한 교육 행사를 통해 관계 구축 및 네트워킹을 촉진한다.

NH-ISAC는 MDSISC[52] 프로그램인 MD-VIPER[53]를 제공한다. MD-VIPER 프로그램은 의료 기기 취약성 공유·평가 및 대응 서비스 제공, 의료 기기의 사이버 보안에 대한 시판 후 관리를 한다. 또한 정보 공유 접근관리 및 의료 기기 보안 관계자 (제조업자, 의료 제공기관 (HDO), 독립적 보안 연구원, 규제 기관 등)의 열린 커뮤니티를 운영한다.

[그림 3-10] NH-ISAC 기술 개념도



자료: (https://secwww.jhuapl.edu/IACD/Resources/AIS/HHSWorkshop/NHiSAC%20Roles%20and%20future%20-%20JH%20Workshop.pdf pp.17) , * NCCIC (National Cybersecurity and Communications Integration Center)
* HHS (United States Department of Health and Human Services

52) MDSISC (Medical Device Security Information Sharing Council)
53) MD-VIPER (Medical Device Vulnerability Intelligence Program for Evaluation and Response)

5. 자동차 부문 : AUTOMOTIVE ISAC[54)]

<표 3-8> Auto-ISAC의 정보공유 현황 및 특징 요약

No	구분	해당 유형		현황 및 특징
1	관련 분야	1) 일반 분야		
		2) 보안 분야	○	차량 사이버 보안 위험에 대한 정보 공유
		3) SW안전 분야		
2	법적 근거	1) 법령 근거	○	대통령 결정지침 63 (PDD-63)
		2) 그 외 방법		
3	재원 조달	1) 정부		
		2) 민간		
		3) 정부 + 민간	○	정부 기관과 파트너십을 갖는 비영리 기관임
4	조직 형태	1) 일반 정보공유체계		
		2) 산업도메인별 대표 ISAC	○	자동차 분야 대표 ISAC
		3) 기관 또는 기업의 자체 ISAC		
5	운영 활동	1) 일반		
		2) 커뮤니티	○	정보 공유 커뮤니티를 제공
		3) 스터디 그룹	○	모범 사례 개발을 위한 워킹 그룹 존재
		4) 표준화		
6	정보 공유 방식	1) 시스템	○	포탈에 정기 보고서를 포함함
		2) 이메일		
		3) 인쇄물		
		4) 온라인 토의	○	월별 회의를 개최
		5) 워크숍(컨퍼런스)	○	차량 사이버 기능 향상을 위한 워크숍 개최
7	정보 공유 기술	1) 표준 규격 또는 기술		
		2) 독자 규격 또는 기술		
8	정보 공유 범위	1) 멤버십 별		
		2) 정보 유형별		
		3) 운영 활동별		

※ 문헌부족으로 확인이 어려운 항목은 표기하지 않았음

54) (http://www.automotiveisac.com/)

1) 조직 및 운영 체계

Auto-ISAC은 IT, 항공 ISAC과 동일하게 1998년 행정명령 63 (PDD-63), 국가 인프라 보호 계획(NIPP)에 근거한다.

(1) 조직 구성

Auto-ISAC 포탈을 통한 공유 형식. 전 세계 30개 이상의 경량 및 중형 차량 OEM, 공급업체, 상업용 차량 회사가 Auto-ISAC에 가입한 상태이다. Auto-ISAC에 글로벌 주요 자동차 회사, 글로벌 부품회사들이 참여하고 있으며 세계 최대 자동차 반도체 공급업체이자 자동차 사이버보안 선두기업인 NXP반도체는 2017년 2월 Auto-ISAC에 합류했다고 발표했다. 국내 자동차 업체인 현대 모비스 또한 2017년 2월 Auto-ISAC의 정규 회원으로 가입했다.

(2) 역할 및 책임

Auto-ISAC은 자동차 제조업체가 차량 사이버 보안 위험을 해결하기 위한 글로벌 정보 공유 커뮤니티이며, 고유한 글로벌 정보 공유 커뮤니티를 제공하여 차량 사이버 보안을 촉진한다.

Auto-ISAC은 전 세계의 연결된 차량이 직면한 사이버 보안 위험에 대한 정보를 모으고 보급하며 정보 출처에는 회원, 정부 기관, 학술 기관, 공급 업체, 오픈 소스 및 기타 신뢰할 수 있는 출처가 포함된다.

(3) 운영 방식 및 활동

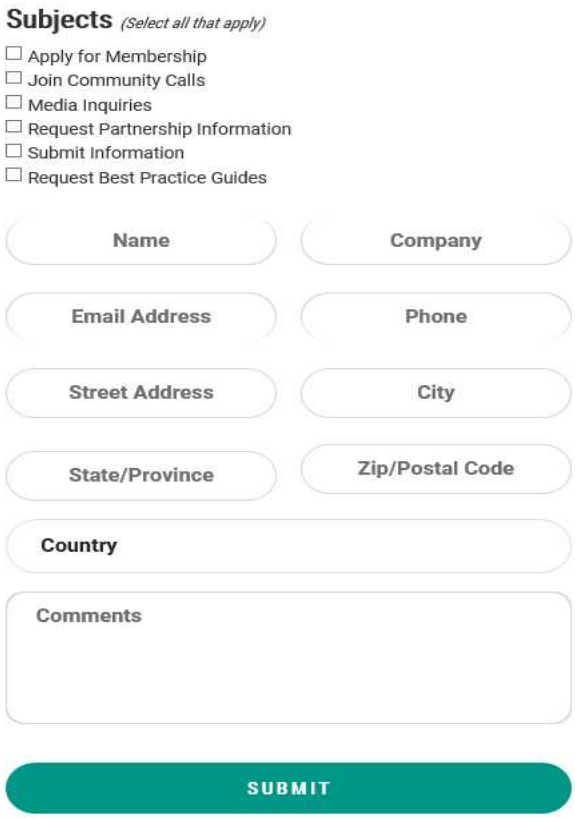
Auto-ISAC은 북미, 유럽 및 아시아에 본사를 두고 있는 글로벌 대표이며 북미 지역의 모든 경량 차량의 99%가 Auto-ISAC의 회원이다. Auto ISAC은 National ISAC 이사회 멤버로서 의료 및 항공, 통신 및 금융 서비스와 같은 분야를 다루는 24가지 중요한 인프라 ISAC에 협력한다.

Auto-ISAC는 보안 정보 공유 포탈을 운영하며, 누구나 익명으로 사이버 위협, 취약성 및 사건 사고들을 제출하여 공유하고, 현재 시스템의 취약점, 해커의 공격 패턴, 위험도 등을 추적 및 분석할 수 있게 하여 사이버 위협에 효과적으로 대처할 수 있도록 돕고 있다.

보안 정보 공유 포탈은 회원들이 익명으로 사이버 위협에 효과적으로 대응할 수 있는 정보를 제출하고 수신할 수 있으며, 정보 공유 외에도 회원들의 차량 사이버 기능을 향

상시키기 위해 워크샵, 정보 교환 행사, 정상 회의를 제공한다.

[그림 3-11] Auto-ISAC Submit Format



자료: http://www.automotiveisac.com/contact.php

Auto-ISAC은 업계 최고의 모범 사례 개발에 중점을 둔 워킹 그룹을 운영하고 있으며 사고 대응, 타사와의 협력 및 참여, 위험 관리, 설계상의 보안, 위협 탐지 및 보호, 교육 및 인식을 포함하여 차량 사이버 보안의 조직적이고 기술적인 측면을 포괄하는 모범 사례를 개발한다.[55]

Auto-ISAC은 연결된 차량과 관련된 사이버 위협, 취약성 및 사건에 대한 정보를 공유, 추적 및 분석하는 중앙 허브 운영에 활용되며 산업 리더 및 사이버 보안 전문가로 구성된 기밀 커뮤니티를 사용한다. 판매회사, 학계 및 연구원을 위한 파트너십 프로그램을 공식화하기 위해 노력하고 있으며 업계 협회 및 정부 기관을 위한 파트너십 프로그램을 운영하고 있다.

55) https://www.automotiveisac.com/assets/img/executive-summary.pdf

[그림 3-12] Auto-ISAC 운영 개념도

자료: https://www.automotiveisac.com/

2) 정보공유 체계

(1) 정보공유 방식

Auto-ISAC은 업계 전문가들의 분석을 통한 정보를 보고서에 포함하고 안전한 Auto-ISAC 포탈을 통해 공유한다. 커뮤니티 회원은 월별 회의에 참여하여 자동차 업계의 주요 주제에 대해 월별 상황을 제공한다.

(2) 정보공유 범위

정부 기관이나 법 집행 기관은 제출자의 사전 승인 없이 제출한 데이터에 접근 할 수 없다. Auto-ISAC은 정부 부서에 필요한 정보를 제공하고 회원이 승인 한 데이터를 공유한다.

(3) 정보공유 기술 및 활용

가) 위험 평가 및 관리

표준화된 프로세스를 수립하여 사이버 보안 위험의 원천을 파악, 측정 및 우선순위를 정한다. 식별 된 위험을 관리하기 위한 의사 결정 프로세스를 수립하고 적절한 이해 관계자에게 리스크를 보고하고 전달하는 프로세스를 문서화한다. 위험 평가 피드백 루프의 일부로 식별 된 위험의 변화를 모니터링하고 평가한다. 보안 요구 사항, 지침 및 교육을 검증하기 위해 중요한 공급 업체의 컴플라이언스를 확인하는 프로세스를 수립한다. 초기 차량 개발 단계에서 위험 평가를 포함하고 차량 라이프 사이클의 각 단계에서 재평가한다.

나) 사고 대응 및 복구

사고 대응 팀이 차량 사이버 사건에 대한 전사적 대응을 조정할 수 있도록 한다. 사고 대응 팀 준비를 촉진하기 위해 정기적인 테스트 및 사고 시뮬레이션을 수행하며 내부 및 외부 이해 관계자에게 차량 사이버 사건을 알린다. 차량 사이버 사건의 실제 및 잠재적 차량 영향을 파악하고 교훈을 바탕으로 시간 경과에 따른 사고 대응 계획을 개선한다.

6. 기타 부문

1) 국방 부문

DSIE(DEFENSE SECURITY INFORMATION EXCHANGE) 회원 기업의 집단 보안뿐만 아니라 주요 공급 업체의 보안을 향상시키기 위해 고안된 방식으로 공통 플랫폼 및 서비스를 개발하고 활용한다.

DSIE 회원은 주기적으로 개최되는 기술교류, WebEx 토론 교육, 위협 탐지 및 완화, 도구 개발 및 구현, 특정 기능 및 서비스 식별 작업 그룹에 참여할 수 있으며, CISO 및 CIO는 연례 CISO 정상 회의에 참석하여 경영진 차원의 전략적인 운영 문제를 토론한다.

2) 비상관리 및 대응 부문

EMR-ISAC(EMERGENCY MANAGEMENT AND RESPONSE ISAC)은 CIP (Critical Infrastructure Protection) 및 위협 정보의 수집, 연구, 협업 및 보급을 위한 주요 정보 공유 메커니즘으로 전국의 ESS (Emergency Services Sector) 부서 및 기관에 정보를 제공한다. CIP에는 조직의 핵심 인프라를 식별하고 해당 인프라에 대한 위협을 판별하고 위험한 인프라의 취약성을 분석하며 중요한 인프라가 파손되거나 손실 될 위험을 평가하고 손실이 용납 될 수없는 경우 예방 또는 탄력적 조치를 적용하는 단계가 포함된다.

EMR-ISAC은 국토 안보부 (DHS) 정보 공유 메커니즘을 통해 중요한 인프라 보호 및 위협 정보를 보급하고 ESS 리더에게 무료 기술 지원 상담 서비스를 제공한다. 또한 연방, 주, 지방, 지역 및 민간 부문 파트너로부터 ESS와 관련된 CIP 및 응급 위협 정보를 공유하기 위해 국토 안보 정보 네트워크 (Homeland Security Information Network, HSIN) 포탈에 관심 커뮤니티 (Communities of Interest, COI)를 갖는다.

EMR-ISAC은 ESS 부서 및 대행 기관과 관련성이 있는 CIP 및 CIR 정보를 수집하고 수집 된 정보를 분석하여 ESS 조직에 대한 신뢰성 및 적용 가능성을 확인한다. 비상 서비스의 지도자, 소유주 및 운영자에게 신속하게 종합 정보를 보급하고 데이터베이스 및 전자포탈을 유지하여 ESS 정보 공유를 신속하게 할 수 있다.

제3절 정보 공유 표준

이 절에서는 미국 ISAC 정보공유체계에서 공통적으로 사용되는 정보공유표준에 대해 정리한다.

1. 미국 TAXII/STIX[56]

TAXII는 상업적 또는 비상업적 인 목적에 대한 허용 라이센스 아래에 배포되며 헬퍼 스크립트 및 관련 도구는 일반적으로 Berkeley Software Distribution을 따르는 개별 라이센스를 보유한다.[57] 대통령과 의회는 사이버 보안 행정 명령 (EO), 대통령 정책 지침 21 (PDD-21), 사이버 정보 공유 및 보호법 (CISPA)에서 입증 된 위협 공유의 중요성을 강조하였다.[58]

미국 DHS(Department of Homeland Security, 국토안보부)는 TAXII, STIX 및 CybOX(Cyber Observable Expression)를 글로벌 정보 사회를 위한 개방형 표준의 개발, 통합 및 채택을 추진하는 비영리 컨소시엄인 구조화 정보 표준화기구 (OASIS, Organization for the Advancement of Structured Information Standards)가 담당하도록 했다.. 사이버 위협 인텔리전스 (CTI) 기술위원회 (TC)는 현재 이러한 표준을 지속적으로 개발하고 있으며 이러한 표준을 형성하는데 있어 정기적이고 적극적인 역할을 하고자 하는 조직 및 개인은 OASIS 및 CTI TC 가입을 고려해야 한다.[59]

STIX/TAXII 체계의 주요 사용자는 ISAC(Information Sharing Analysis Center) 및 CSIRT(Computer Security Incident Response Team), 정보보호 산업군 등이나 그 외에도 누구나 사용 가능하다.

1) 규격의 역할 및 의의

미국은 규격개발을 통해 사이버 위협 정보공유를 추진하고 있다. 미국의 국토안보부는 사이버 위협에 대응하기 위하여 효율적이고 안전한 정보공유 체계 구축의 필요성을 인지하였으나, 사이버 위협 정보가 표준화되지 않아 일관성 있는 분석의 어려움을 느끼고 이

56) Trusted Automated eXchange of Indicator Information/The Structured Threat Information eXpression (http://taxiiproject.github.io/)
57) http://taxiiproject.github.io/legal/
58) Background, (http://taxiiproject.github.io/getting-started/whitepaper/#trademark-information)
59) http://taxiiproject.github.io/community/

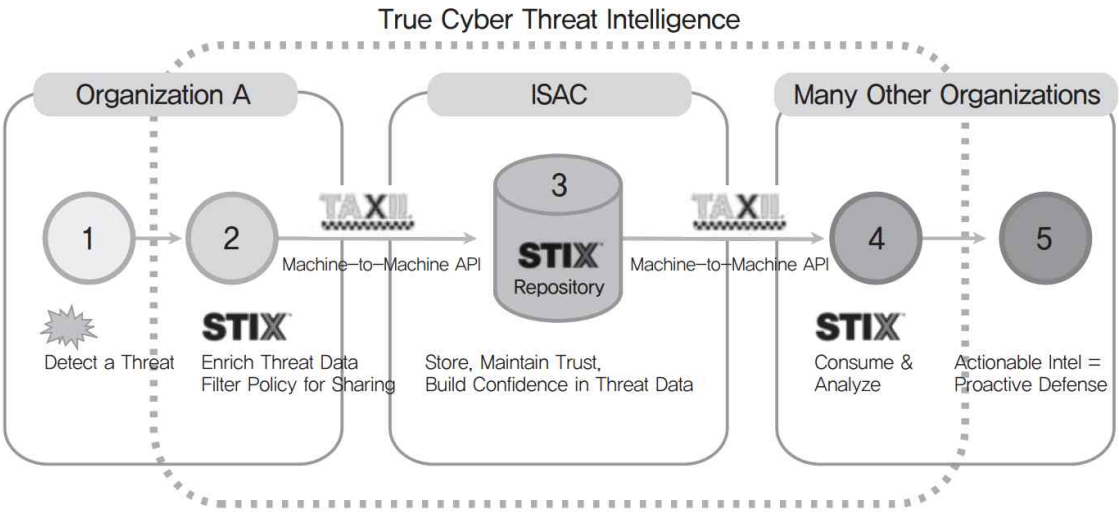
를 극복하기 위해 12년부터 규격개발에 착수하였다. 미국의 국토안보부는 13년 4월에 사이버 위협 정보 전송 규격인 TAXII(Trusted Automated eXchange of Indicator Information) 공식 버전 1.0을, 10월에는 사이버 위협 표현 규격인 STIX(The Structured Threat Information eXpression) 공식버전 1.0.1을 각각 발표하였다.

2) 구성 및 기능

TAXII는 자동화 된 방식으로 여러 공유 파트너 및 커뮤니티와 사이버 위협 정보를 광범위하게 공유 할 수 있는 기능을 제공한다. 사이버 위협의 탐지, 예방 및 완화를 위한 사이버 위협 정보를 교환하기 위한 서비스, 프로토콜 및 메시지를 정의하며 새로운 위협에 대한 상황 인식 향상을 위해 조직에 권한을 부여하고 조직은 하나의 공통된 도구 세트를 사용하면서 선택한 파트너와 원하는 파트너 정보를 쉽게 공유할 수 있다.

표준화 된 서비스, 메시지 및 메시지 교환을 통해 TAXII 구현은 자동화를 용이하게 하고 여러 가지 맞춤형 지점 간 교환 구현의 필요성을 제거하며 사이버 위협 정보 교환을 단순화하고 가속화한다.

[그림 3-13] STIX/TAXII 체계 구성 및 설명



자료: (www.kisa.or.kr/uploadfile/201402/201402141548019564.pdf P.49)

특정 조직이 사이버 위협을 탐지했을 경우, 위협 정보를 STIX로 표현하여 TAXII를 통해 중계기관으로 자동 전달함 중계기관은 수신정보를 저장하고 진위여부를 파악하여 TAXII

로 참여조직들에게 자동 전달한다. 참여조직들은 공유된 위협 정보를 적용하여 위협요소를 제거하고 차후예방을 가질 수 있다.

3) 정보공유 기술 및 활용

TAXII는 액세스 제어 제한을 포함하여 기존의 공유 계약과 통합되도록 설계되었다. 푸시 앤 풀 메시지가 지원되므로 구독 피드와 주문형 쿼리를 모두 지원할 수 있으며 HTTP 및 HTTPS를 기본적으로 지원하여 가능한 경우 기존 프로토콜을 활용한다.

TAXII는 다음과 같은 세 개의 정보공유 모델을 지원한다.

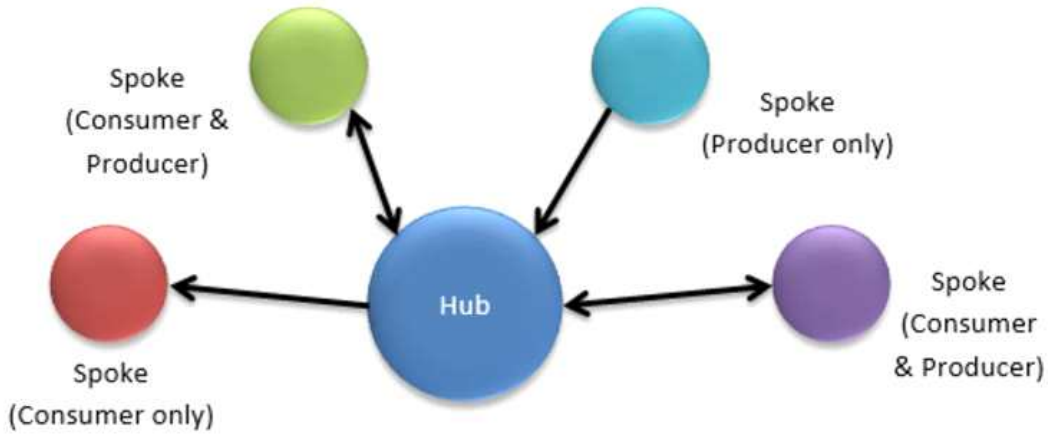
(1) Hub and Spoke

허브 앤 스포크(Hub and Spoke)는 하나의 조직이 정보를 위한 중앙정보센터 역할을 하고, 파트너 조직 또는 스포크 간의 정보 교환 조정 역할을 하는 공유 모델이다. 스포크는 허브로부터 정보를 생산 또는 소비 할 수 있고 허브와 정보를 공유하고 이 정보를 다른 모든 스포크와 다시 공유하며, 허브는 정보를 다시 공유하기 전에 분석 또는 필터링을 수행 할 수 있다.

TAXII는 구현될 때 조직 및 제품·서비스 경계에서 실행 가능한 사이버 위협 정보를 공유 할 수 있게 해주는 일련의 서비스 및 메시지 교환을 정의한다. 이 서비스와 메시지 교환은 사이버 위협의 탐지, 예방 및 완화를 위함이다. TAXII는 정보 공유 이니셔티브 또는 응용 프로그램이 아니며 사이버 위협정보 공유에 대한 신뢰 계약, 관리 또는 비 기술적 측면을 정의하지는 않지만 새로운 위협에 대한 상황 인식 향상을 위해 조직에 권한을 부여하고 조직은 하나의 공통된 도구 세트를 사용하면서 선택한 파트너와 원하는 파트너 정보를 쉽게 공유 할 수 있다.[60]

60) An Exchange Framework,
(http://taxiiproject.github.io/getting-started/whitepaper/#trademark-information)

[그림 3-14] Hub and Spoke

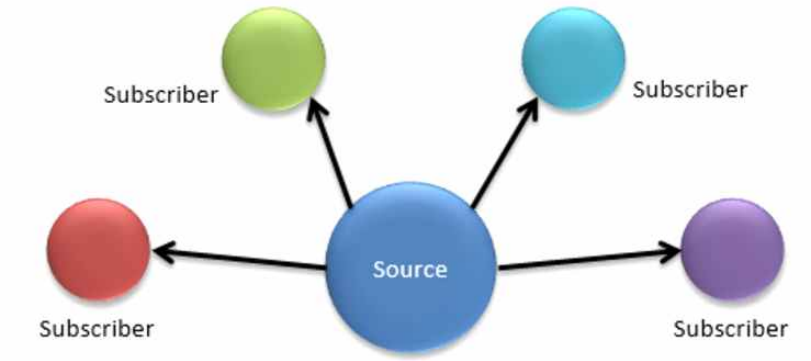


자료: (http://taxiiproject.github.io/about/#sharing-models)

(2) Source/Subscriber

한 조직이 단일 정보소스로 기능하고 해당 정보를 구독자에게 보내는 공유 모델이다.

[그림 3-15] Source/Subscriber

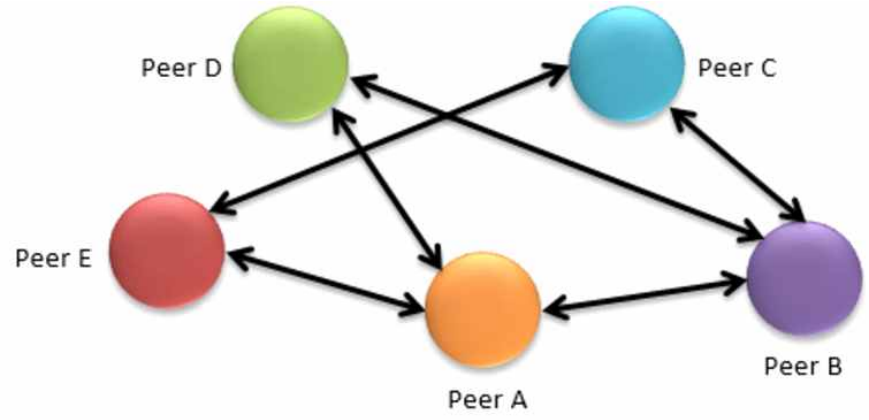


자료: (http://taxiiproject.github.io/about/#sharing-models)

(3) Peer to Peer

둘 이상의 조직이 서로 직접 정보를 공유하는 공유 모델임. 모든 수의 조직이 정보의 생산자이자 소비자가 될 수 있다.

[그림 3-16] Peer to Peer



자료: (http://taxiiproject.github.io/about/#sharing-models)

2. 미국 TLP (Traffic Light Protocol) [61]

트래픽 라이트 프로토콜 (TLP)은 정보 공유를 용이하게 이행하기 위해 만든 정보공유 범위에 관한 프로토콜이다. 즉, TLP는 민감한 정보가 적절한 대상과 공유되도록 하기 위해 사용되는 일련의 설정(set)이다. 수신자가 예상한 공유 경계를 나타내기 위해 4가지 색상만을 사용한다. 이 표준에 나열되지 않은 지정은 유효하지 않은 것으로 간주된다.

TLP는 민감한 정보를 공유 할 수 있는 시기와 방법을 나타내는 간단하고 직관적인 스키마를 제공하므로 더 자주 효과적으로 공동 작업을 수행 할 수 있다. TLP는 “통제표시” 또는 분류 체계가 아니다. TLP는 라이센싱 조건, 처리 및 암호화 규칙, 정보의 조치 또는 계측에 대한 제한을 처리하도록 설계되지 않았다.

TLP는 채택의 용이성, 사람의 가독성 및 개인 간 공유에 최적화되어 있다. 자동화된 공유 교환에 사용될 수 있지만 그 용도로 최적화되지는 않았다. 소스는 TLP 정보를 받는 사람이 TLP 공유 지침을 이해하고 준수 할 수 있도록 보장해야 한다. 수신자가 원본 TLP 지정에 명시된 것보다 더 광범위하게 정보를 공유해야하는 경우 원래 소스에서 명시적 허가를 얻어야 한다.

61) TRAFFIC LIGHT PROTOCOL (TLP) FIRST Standards Definitions and Usage Guidance . Version 1.0 https://www.first.org/tlp/ 본 문서는 국토안보부의 TLP 사용을 위해 개발된 것으로 표준TLP를 따름

1) 규격의 정의

□ TLP : 적색 TLP:RED

공개를 위한 것이 아니며 참가자들만이 이용할 수 있다. 출처는 추가 당사자가 정보를 효과적으로 처리 할 수 없으며 오용 된 경우 당사자의 개인 정보, 명성 또는 운영에 영향을 미칠 수 있는 경우 TLP : RED를 사용할 수 있다. 수신자는 TLP : RED 정보를 원래 공개 된 특정 교환, 회의 또는 대화 이외의 다른 당사자와 공유 할 수 없다. 예를 들어, 회의의 맥락에서 TLP : RED 정보는 회의에 참석 한 사람들에게만 국한된다.

□ TLP : 황색 TLP:AMBER

참가자의 조직에만 제한된 공개. 정보원은 정보를 효과적으로 지원해야 할 때 TLP : AMBER를 사용할 수는 있지만 관련 조직 외부에서 공유하는 경우 개인 정보 보호, 평판 또는 운영에 위험을 초래할 수 있다. 받는 사람은 TLP : AMBER 정보를 자신의 조직 구성원, 자신을 보호하거나 추가 위험을 방지하기 위해 정보를 알아야 하는 클라이언트 또는 고객과만 공유할 수 있다.

□ TLP : 녹색 TLP:GREEN

제한 공개, 지역 사회에 제한된다. 출처는 TLP : GREEN을 사용할 수 있다. 정보가 모든 참여 조직 및 더 넓은 커뮤니티 또는 부문 내의 동료에 대한 인식에 유용 할 때, 수신자는 자신의 섹터 또는 커뮤니티 내의 동료 및 파트너 조직과 정보를 공유 할 수 있지만 공개적으로 액세스 할 수 있는 채널을 통한 공유는 할 수 없다. 이 카테고리의 정보는 특정 커뮤니티 내에서 널리 배포 될 수 있다.

□ TLP : WHITE TLP:WHITE

공개는 제한되지 않는다. 정보 출처는 TLP : WHITE를 사용할 수 있다. 정보가 공개 될 수 있는 규칙 및 절차에 따라 예측할 수 있는 오용의 위험이 거의 없거나 전혀 없을 때, 표준 저작권 규칙에 따라 TLP : WHITE 정보가 제한 없이 배포 될 수 있다.

2) 규격의 사용방법

(1) 이메일에서 TLP를 사용하는 방법

TLP 지정 전자 메일 서신은 지정된 정보 자체에 앞서 제목 줄 및 전자 메일 본문에 있는 정보의 TLP 색상을 나타내야 한다. TLP 색상은 대문자 (TLP : RED, TLP : AMBER, TLP : GREEN 또는 TLP : WHITE) 여야 한다.

(2) 문서에서 TLP를 사용하는 방법

TLP 지정 문서는 각 페이지의 머리글과 바닥글에 있는 정보의 TLP 색상을 나타내야 한다. 기존 제어 표시 체계와 혼동되지 않도록 TLP 지정을 오른쪽 정렬하는 것이 좋다. TLP 색상은 대문자 및 12 포인트 유형 이상으로 표시되어야 한다.

제4절 요약

미국의 산업도메인 중 통신, 항공, 의료, 자동차 부문은 ISAC을 운영하고 있는 대표적인 산업으로 잘 알려져 있다. 각각의 ISAC들은 조직, 운영체계, 정보공유 방식 등에 있어 공통되거나 상이한 특징들이 나타나는데 간략하게 요약하면 다음과 같다.

우선 통신 부문에서 대표되는 IT-ISAC은 정부 기관과 파트너십을 갖는 비영리 조직이다. IT분야의 보안 위협을 최소화 하는 것을 목적으로 설립되었으며 기술위원회 또는 위험 관리 포럼을 통해 운영한다. IT-ISAC은 독자적으로 Threat Intelligence Platform을 구축하였다. 또한, 사이버위협 표준 규격인 STIX/TAXII 프로토콜 기반으로 정보 공유체계를 구축하였다. 멤버쉽 등급에 따라 공유 정보 및 참여 정보를 공유한다는 특징을 갖는다. 특히 다른 ISAC과 차별되는 다양한 Special Interest Groups을 운영하는 것이 강점이다.

항공 부문에는 A-ISAC이 운영되고 있다. A-ISAC은 정부 파트너가 참여하는 비영리 기구이며 항공 산업에 대한 사이버 위협 정보를 공유한다. A-ISAC은 공유 데이터 분석 그룹(Analyst Working Group)을 운영하는데, 정보공유를 위한 다양한 방식을 제공한다. 실시간 위협 정보 공유를 위한 가상 플랫폼, 업계 간행물 및 인터뷰 기사 제공, WebEx를 통한 가상 커뮤니티와 연례 정상회담, 격주로 진행되는 전화회의 및 회원들을 위한 1:1 지원 서비스 등이 그것이다. 특히, 정보 공유 기술로서 TLP 표준기술을 사용함으로써 멤버 등급에 따른 차별화된 서비스를 제공한다는 특징이 있다.

의료 부문의 NH-ISAC 또한 정부 기관과의 파트너십을 갖는 비영리 조직이다. NH-ISAC은 보건 부문에 대한 사이버 보안 보호 및 사이버 위협을 대비하기 위한 것이다. 정보공유를 위한 커뮤니티 및 포럼을 제공하는데 특히 CYBERFIT® 보안 서비스 그룹을 제공한다는 특징이 있다. 또한 NH-ISAC은 MD-VIPER 프로그램으로 의료 기기에 대한 취약성을 공유하고 평가 및 대응 서비스를 제공하며, Intelligence Report를 발행하거나 교육행사 서비스, HHS SCC Meeting 등을 제공한다. 다른 ISAC가 차별화되는 독자적인 기술로 AIS(Automated Intelligence Sharing)를 사용하며 Tier에 따라서 서비스를 제공한다.

마지막으로 점차 중요성이 커지는 자동차 부문의 Auto-ISAC은 정부 기관과 파트너십을 갖는 비영리 조직으로 차량 사이버 보안 위험에 대한 정보를 공유한다. Auto-ISAC은 정보 공유를 위한 커뮤니티를 제공하며 모범사례 개발을 위해 워킹 그룹을 운영하고 있다. 북미 지역의 모든 경량 차량의 99%가 Auto-ISAC의 회원일 뿐만 아니라 우리나라를 포함한 자동차 회사들이 Auto-ISAC에 회원으로 가입하고 있다는 점에서 Auto-ISAC이 의미하

는 바가 크다. 또한, Auto-ISAC은 포탈사이트를 통해 정기적으로 보고서를 제공하며, 정보 공유 이외에도 차량 사이버 기능 향상을 위한 월별회의, 워크숍을 개최한다.

<표 3-9> 미국 정보공유체계의 주요 특징

ISAC 명칭	구분	주요 특징
통신 IT-ISAC	조직 및 운영 체계	• IT분야의 보안 위협을 최소화 하는 것에 목적이 있으며, **기술위원회/위험 관리 포럼**을 통해 운영함.
	정보공유 체계	• 독자 **Threat Intelligence Platform개발, 표준 STIX/TAXII프로토콜** 기반 • 멤버쉽 등급에 따라 정보를 공유 • 다양한 Special Interest Groups 운영
항공 A-ISAC	조직 및 운영 체계	• 정부 파트너가 참여하는 비영리 기구로서, 항공 산업에 대한 사이버 위협 정보를 공유함 • **공유 데이터 분석 그룹(Analyst Working Group)**을 운영
	정보공유 체계	• 실시간 위협 정보 공유를 위한 가상 플랫폼, 업계 간행물 및 인터뷰 기사를 제공 • WebEx를 통한 가상 커뮤니티와 연례 정상회담, 격주로 진행되는 전화회의 및 회원들을 위한 1:1 지원을 제공 • 정보 공유 기술로서 **TLP 표준 기술**을 사용하여 멤버 등급에 따라서 서비스를 제공
의료 NH-ISAC	조직 및 운영 체계	• 민간주도의 정부 기관과의 파트너십을 갖는 비영리 조직으로, 보건부문의 사이버 보안 보호 및 사이버 위협을 대비 • 정보 공유를 위한 커뮤니티 및 포럼을 제공 • **CYBERFIT® 보안 서비스 그룹**을 제공
	정보공유 체계	• MD-VIPER 프로그램으로 의료 기기에 대한 취약성을 공유하고 평가 및 대응하는 서비스를 제공 • Intelligence Report를 발행하며 교육행사 서비스나 HHS SCC Meeting 등을 제공 • 독자적인 기술로 **AIS(Automated Intelligence Sharing)**를 사용하며 Tier에 따라서 서비스를 제공
자동차 Auto-ISAC	조직 및 운영 체계	• 민간주도의 정부 기관과의 파트너십을 갖는 비영리 조직으로, 차량 사이버 보안 위험에 대한 정보를 공유 • 정보 공유를 위한 커뮤니티 제공 • 모범 사례 개발의 워킹 그룹 운영
	정보공유 체계	• 포탈에 정기적인 보고서 포함 • 월별회의 및 워크숍 개최

미국 통신, 항공, 의료, 자동차의 보안 분야에서 정보 공유현황은 다음과 같다. 이 조사는 산업도메인별 대표 ISAC를 대상으로 하였다. 정보 공유를 위한 운영활동은 커뮤니티와 스터디 그룹 형태로 활성화 되어 있다. 정보 공유를 위해서는 홈페이지 등의 단순한 형태를 포함한 시스템을 유지하고 있었으며, 정보 공유 등급을 설정한 이메일 형태의 공유 방법을 활용하고 있다.

<표 3-10> 미국 산업도메인별 ISAC의 정보공유 현황 비교

No	구분	해당 유형	통신	항공	의료	자동차
			IT-ISAC	Aviation-ISAC	National Health-ISAC	Auto-ISAC
1	법적 근거	1) 법령 근거	○	○	○	○
		2) 그 외 방법				
2	재원 조달	1) 정부				
		2) 민간				
		3) 정부 + 민간	○	○	○	○
3	운영 활동	1) 일반				
		2) 커뮤니티	○		○	○
		3) 스터디 그룹	○	○	○	○
		4) 표준화				
4	정보 공유 방식	1) 시스템	○	○	○	○
		2) 이메일	○	○	○	
		3) 인쇄물				
		4) 온라인 토의		○		○
		5) 워크숍(컨퍼런스)	○	○	○	○
5	정보 공유 기술	1) 표준 규격 또는 기술	○	○	○	
		2) 독자 규격 또는 기술	○		○	
6	정보 공유 범위	1) 멤버십 별	○	○	○	
		2) 정보 유형별				
		3) 운영 활동별	○			

정보공유 표준에는 정보교환을 위한 TAXII/STIX와 정보 등급 및 범위 지정을 위한 TLP 표준이 있다.

제4장 일본 사례 연구

제1절 일본의 주요기반시설 보호 및 정보공유에 대한 법적 근거 및 배경

1) 주요 정보통신기반보호 법제 및 정책 추진의 배경[62)63)64)]

일본은 2000년 ‘e-Japan 구상’에 따라 제정된 고도 정보통신 네트워크 사회 형성법(이하 ‘IT기본법’)에 따라 정보통신기반시설에 대한 보호정책을 추진해 왔다. 이후 사이버 범죄의 증가, 국민생활 및 사회 주요기반의 정보시스템 장애, 대량 정보유출 등 사회문제가 심각해지면서 기반보호에 대항 강화정책이 필요하게 되었다. 이에 2005년 4월 내각관방 산하에 내각 사이버보안센터(National center of Incident readiness and Strategy for Cybersecurity, 이하 ‘NISC’)를 신설하고, 5월에는 정보보안 정책협의회(Information Security Policy Council, ISPC)를 설치하여 본격적인 강화 활동을 시작하였다. NISC는 주요 기반 보호대책에 대한 행동계획(사이버보안 기본계획)과 관련 안전기준 마련, ISPC는 국가 차원에서의 기본전략 수립의 역할을 담당하였다.

2006년 책정된 제1차 사이버보안 기본계획은 주요 기반의 IT장애에 대해 분야를 초월한 횡단적 보호대책이 시급함을 강조하고, 각 사업 분야와 주요기반별 사업자 특성을 고려하면서 기존의 수직형 체재뿐만 아니라 분야를 어우르는 수평적 대처를 포함하는 새로운 민관 협력체재를 재구축할 것을 강조하였다. 특히 1차 기본계획에서는 이러한 목표 하에 3년간 주요 기반 보호를 위한 ‘안전기준의 정비’와 정보공유 체제 강화 중점 정책을 추진하였는데 세부 정책으로 ‘민관의 정보제공 및 연락 환경 정비’, ‘주요기반 분야의 정보공유·분석기능(CEPTOAR, Capability for Engineering of Protection, Technical Operation, Analysis and Response) 정비’,주요기반 연락협의회(CEPTOAR-Council)’ 창설 촉진 등을 포함함으로써 정보공유분석기능 측면의 중요한 의미를 갖는다.

62) KISA(2013), 주요정보통신기반보호 강화 방안 마련 연구보고서, 2013.12.
63) KISA(2008), 일본의 최근 정보보호정책 현황 및 시사점, 2008.6.
64) KISA(2010), 주요정보통신기반시설 사이버 위협 및 대응, 2010.11.

※ 제1차 사이버보안 기본계획의 중점 정책 중 ‘정보공유 체제 강화’ 정책(2006)

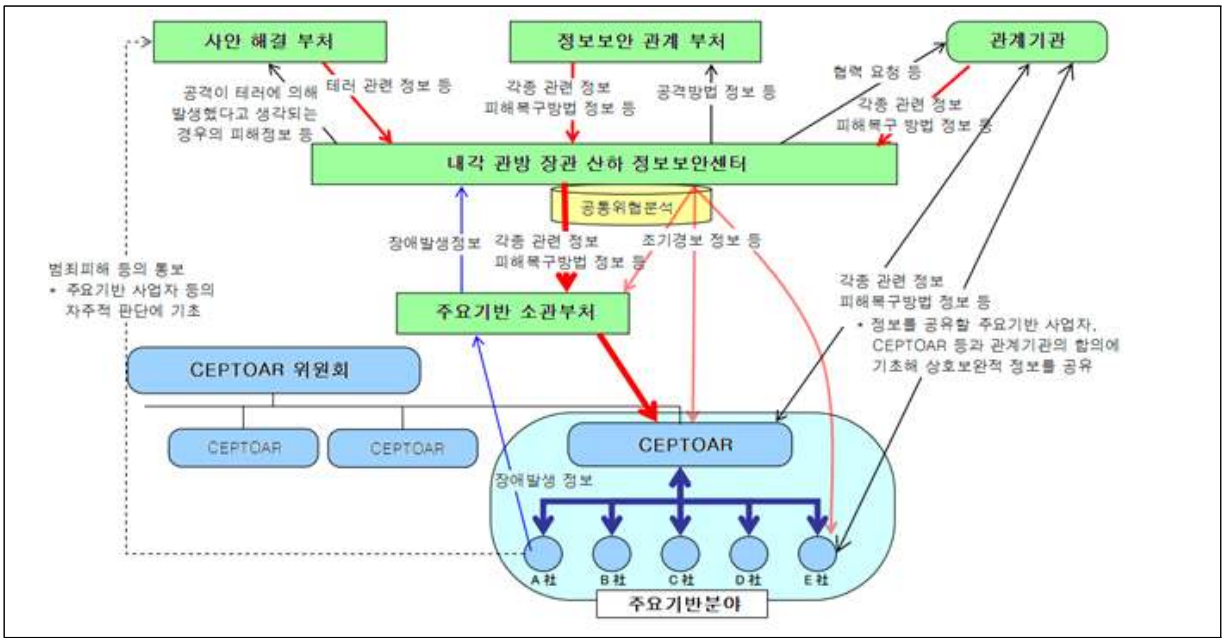
정부 등은 주요기반 사업자에게 IT장애 사전 방지, IT장애 확대방지·신속한 복구, IT장애 요인 등의 분석·검증을 통한 재발방지 등 3가지 측면에서 적절한 IT장애 관련 정보를 제공하고, 주요기반 사업자간 또는 상호의존성이 있는 주요기반 분야 간에는 이러한 정보를 공유하는 체제를 강화

1) 민관의 정보제공·연락을 위한 환경정비 : 관계기관과 협력해 주의환기 등 대책 마련을 위해 주요기반 사업자 등에게 제공하는 정보를 수집하고 CEPTOAR 등을 통해 정보를 제공. 또한 주요기반 사업자 등이 법령 등으로 보고가 의무화된 사고, 장애, 업무지연 등외에 연락이 필요하다고 판단되는 특이하고 중대한 정보를 정부에 연락하기 위한 환경 정비를 촉진
2) 주요기반 분야의 정보공유·분석기능(CEPTOAR) 정비 : IT장애의 사전방지, 발생시 피해확대 방지·신속한 복구 및 재발방지를 위해 정부 등이 제공하는 정보를 주요기반 사업자에 적절하게 제공하고 이들이 공유함으로써 주요기반 사업자 등의 서비스 유지·복구능력 향상에 기여하도록 주요기반 분야 내에 ‘정보공유·분석기능’(CEPTOAR: Capability for Engineering of Protection, Technical Operation, Analysis and Response) 정비를 촉진
3) 가칭 ‘주요기반 연락협의회(CEPTOAR-Council)’ 창설 촉진; 주요기반 사업자간 분야를 초월한 횡단적인 정보 공유를 추진하고 서비스 유지·복구에 다양한 지식을 활용하기 위해 각 CEPTOAR간 정보공유의 장으로 가칭 ‘주요기반 연락협의회’ 창설을 촉진

2009년 2월 발표된 제2차 사이버보안 기본계획의 중요 메시지 중 하나는 ‘사고전제사회’에 대한 대응력 강화이다. 그동안 분야 횡단적 관점에서 민관의 노력을 연계하는 구조였다면 2차 기본계획에서는 주요 기반 사업자가 실시하는 것이 바람직하다고 판단되는 자주적 대책과 내각관방 장관을 중심으로 정부 및 관계기관이 실시하는 것이 바람직하다고 판단되는 시책으로 구성된 체계적인 구조를 정리하고자 하였다. 즉, 정부기관과 주요기반 사업자 등의 주체적인 대처 및 연계를 확립하고 IT장애에 관한 정보공유 가치를 보편화할 것을 강조한 것이다. 또한 이 계획에 ‘안전기준의 정비 및 침투’, ‘정보공유 체제 강화’ 등을 포함함으로써 정보공유·분석기능의 토대를 확립하고자 하였다.

※ 제2차 사이버보안 기본계획의 중점 정책 중 ‘정보공유 체제 강화’ 정책(2009)

제1차 행동계획으로 구축된 CEPTOAR, CEPTOAR 위원회(주요기반 연락협의회)을 포함해 관계 주체간 공유할 정보를 정리하고 정보제공, 정보연락 등에 필요한 환경을 정비하는 동시에 각 CEPTOAR, 주요기반 연락협의회의 자주적인 활동을 충실하게 강화



이후, 2010년부터 일본 정부는 미국의 행정명령에 자극을 받아 사이버보안 전략을 발표하고 민관 사이버보안 거버넌스를 강조한 전략을 발표하였는데, 2013년 '사이버보안 2013'을 발표하고 스마트시티, ITS를 비롯한 교통통제시스템 등의 새로운 네트워크 계열 서비스, 방위산업, 에너지 관련 산업 등 그동안 주요기반으로 속하지 않은 분야의 대응방안의 필요성을 검토하도록 하면서 구체적인 대책으로 안전기준 책정 및 평가, 정보공유 체제의 심화 및 확충 등 요구하였다. 또한 중점 추진전략으로 '민관학연 등 관련 주체 각각의 능력강화 및 상호 협력'을 강조함으로써 총무성이나 경제 산업성과의 구체적인 정보공유가 추진되었다.

※ 사이버보안 전략에 따른 연차계획 '사이버보안 2013'의 '정보공유 체제의 심화·확충' 정책(2013)

- 장애정보 및 공격·위협·취약성 등에 관한 정보는 주요기반 사업자와 CEPTOAR간에 지속적으로 정보를 공유하고, 업종간 정보공유가 어려운 표적형 공격에 관한 정보는 비밀유지 계약을 기초로 하는 정보공유 체제를 심화·확충
- 주요기반 사업자 등의 사업담당 부처에 대한 신속한 보고, 자주적 판단을 통한 담당부처에 대한 통보 및 관계기관과의 정보공유는 개인정보·비밀정보를 배려한 후에 촉진
- 주요기반 사업자 등 사이버 공간관련 사업자 및 관련 CSIRT(Computer Security Incident Response Team)[65] 간에 민간 조직간의 신뢰관계를 전제로 사이버 연습 등을 실시해 사이버 공격에 대한 연계 대응 능력을 강화함

65) 기업과 행정기관 등의 정보시스템에 보안상의 문제가 발생하지 않는지 감시함과 동시에 문제 발생시 원인 분석 및 영향범위 조사 등을 실시하는 체제

※ ‘사이버보안 2013’의 ‘민관학연 등 관련 주체 각각의 능력강화 및 상호 협력’ 전략(2013)

- 정보통신 분야의 사업자와 민관 협력의 추진(총무성) : 총무성에서 정보보안 사안에 대해 ISP 사업자 단체인 ‘텔레콤ISAC 추진회의(Telecom-ISAC Japan)’과 정보공유를 추진
- 중요인프라에서 사용되는 정보시스템의 보안, 신뢰성 향상을 위한 지원체제 정비(경제산업성) : IPA를 통해 장애사례집을 정비 및 공유하고, 자발적으로 제안했던 정보의 거시적인 정량 분석, 축적된 정보를 센터에 제공

제1차 사이버보안 기본계획에서 민관 협력모델을 제시한 후, 2012 Active Japan ICT전략, 사이버보안 2014 & 2015을 거쳐 2014년 ‘사이버보안 기본법’이 제정되었다. 사이버보안 전략 2014에서 일본은 정부기관과 주요 기반시설 사업자간 정보공유를 활성화하고 정부주도 사이버보안 거버넌스를 확립하였으며 내각관방이 민관 정보공유 네트워크의 구심점 역할을 주도하였다.[66] 즉, 2015년 사이버 보안 기본법[67]이 시행되고 사이버 보안 전략본부가 발족하여 국가 안전 보장 회의와 IT 종합 전략본부와 긴밀한 협력을 도모함과 동시에 각 부처에 대한 권한이 강화되었다. 또한 사무국인 내각관방의 내각 사이버 보안 센터(NISC: National center of Incident readiness and Strategy for Cybersecurity)의 인력과 예산의 증가 등으로 정부 추진 체제가 강화되었다. 새로운 추진 체제에 대해 경단련(일본 경제 단체 연합회)은 중요 인프라 등을 사이버 공격으로부터 보호하기 위해 ’사이버 보안 강화를 위한 제언’을 공표했으며 이를 토대로 금융 ISAC을 비롯하여 여러 ISAC이 생겨났다. 따라서 일본은 2014년도 사이버 보안 기본법에 의거하여 각종 인프라 보호 및 ISAC 설립을 추진하게 되었다고 볼 수 있다.

사이버보안 기본법(2014년 법률 제104호)은 인터넷 및 고도 정보통신 네트워크의 정비 및 정보통신 기술이 진전됨에 따라 전 세계적으로 발생하는 사이버 보안 위협의 심각성 및 기타 내외 정세 변화에 따라 정보의 자유로운 유통 판로를 확보하면서 사이버 보안 확보를 도모하는 것이 매우 중요한 과제가 되고 있는 상황을 감안하여 제정된 법이다. 일본의 사이버 보안에 관한 시책에 관한 기본 이념을 정하고 국가 및 지방 공공단체의 책무 등을 밝히고 사이버 보안 전략 개발 및 기타 사이버 보안에 관한 시책의 기본이 되는 사항을 규정하고 사이버 보안 전략 본부를 설치하고 있다. 고도 정보통신 네트워크 사회 형성 기본법(2000년 법률 제144호)과 함께 사이버 보안에 관한 시책을 종합적이고 효과적으로 추진하므로 경제 사회의 활력을 불어 넣고 지속적인 발전과 국민이 안전하면

66) 전자신문 보도자료(2017)‘시작은 늦었지만 체계 갖춘 일본’[사이버보안 새틀을 짜자], 2017.5.14.
67) 일본 내 사이버보안 관련 입법 영역을 지배하는 기본 이념이며 국제 추세에 맞춰 사이버보안 분야 민관 협력 체계 구축을 구체화한 법률임

서 안심하고 살 수 있는 사회 실현을 도모함과 동시에 국제사회의 평화와 안전 확보 및 일본의 안전 보장에 기여하는 것이 그 목적이다.

※ 사이버보안 기본법(2014년 법률 제104호) 사이버보안 전략

정부는 사이버 보안에 관한 기본 계획인 '사이버 보안 전략'을 정하여야 한다(제12조). 총리대신은 사이버 보안 전략 방안 의결을 요구하고 정부는 사이버 보안 전략을 수립 공표하고 정부는 사이버 보안 전략의 재원을 확보하여야 한다(제12조).

2) 일본 센터 및 ISAC운영 배경[68)69)70)]

일본 센터(CEPTOAR)는 IT장애 등에 관한 대책개선의 정보 공유・분석 기능 'Capability for Engineering of Protection, Technical Operation, Analysis and Response' 의 머리글자를 따서 명명한 것으로 일본 ISAC의 모체와 같은 존재이다. 일본의 중요 인프라는 정보 시스템의 기능 부전에 의한 장애가 국민 생활이나 사회 경제 활동에 심각한 영향을 미치지 않도록 대책을 추진하고 있으며, 그 일환으로 중요한 인프라 분야별로 정보 공유・분석 기능(센터)이 정비되어 있다. 중요 인프라의 정보보안 대책을 더욱 강화하기 위해서는 분야의 횡단적인 정보 공유 추진을 도모하고, 다양한 지식을 서비스의 유지・복구로 살려 나가는 것이 중요하다. 2009년 2월에는 각 센터로 구성된 센터협의회를 설립하고 정부 기관으로부터 독립적인 회의체로서 중요 인프라 사업자 등의 서비스 유지・복구 능력의 향상을 촉진하기로 하였다. 센터협의회는 중요 인프라 분야의 센터를 연계하여 설치되었으며 독립적 회의체로서 각 센터의 주체적인 판단에 따라 분야의 횡단적인 정보 공유 등의 연계를 추진하고 있다. 처음에 중요 인프라는 정보통신, 금융, 항공, 철도, 전력, 가스, 정부, 행정, 의료, 수도, 물류의 10개 분야로 구분되었으며, IT 장애의 대책 마련을 위한 기능을 하고 있다. 2017년 현재는 정보통신, 금융, 항공, 철도, 전력, 가스, 정부 및 행정 서비스, 의료, 수도, 물류, 화학, 크레딧, 석유와 같이 13개 분야 17개 센터로 확대되었다. 현재는 기존 사업 영역을 뛰어넘어서 다음과 같이 연계하거나 확장하고 있다.

- 정보통신(Telecom-ISAC의 활동을 신규 설립된 ICT-ISAC으로 이행시키고 일부 방송사

68) https://www.nisc.go.jp/active/infra/pdf/cc_ceptoar.pdf#search=%27CEPTOAR%E3%81%A8%EF%BC%A9%EF%BC%B3%EF%BC%A1%EF%BC%A3%27
69) https://www.telecom-isac.jp/public/t-ceptoar.html
70) http://www.keidanren.or.jp/policy/2016/006_honbun.html

업자 및 케이블 TV사업자가 가맹)

- 전력(전력 ISAC을 설립, 4월부터 운영개시)
- 화학(석유화학공업협회와 일본화학공업협회의 정보공유 및 활동연계)
- 크레딧(네트워크 사업자로 확장)
- 제어시스템(JPCERT/CC가 제공하는 ConPaS 등) J-CSIP(IPA: 표적형 공격 등의 정보공유)
- 사이버테러 대책 협의회(중요 인프라 사업자 등과 경찰과 연계, 47도도부현에 설치)
- 조기 경계 정보 WAISE (JPCERT/CC : 보안정보전반)

<표 4-1> 중요 인프라 센터의 특성

중요 인프라 분야	사업 범위	명칭	주체	사무국	구성원	NISC로부터의 정보를 공개하는 곳(회원이외)
정보 통신	전기통신	T-CEPTOAR	사단 법인	ICT-ISAC	23사 1단체	376사 및 단체
	방송	케이블 TV CEPTOAR	사단 법인	일본 케이블TV연맹	335사 1단체	438사
		방송 CEPTOAR	사단 법인	일본민간방송연맹, 일반방송협회	195사 1단체	
금융 (금융 CEPTO-AR 협의회)	은행 등	은행CEPTOAR	사단 법인	전국은행협회 사무, 결제 시스템부	1,428사	3사 및 단체
	증권	증권 CEPTOAR	임의 단체	일본증권업협회 IT 총괄부	261사 7기관	
	생명보험	생명보험 CEPTOAR	사단 법인	생명보험협회 총무부조직법무 그룹	41사	
	손해보험	손해보험 CEPTOAR	사단 법인	일본 손해보험협회 IT추진부 품질그룹	29사(옵저버 3사 포함)	
항공	항공	항공분야 CEPTOAR	임의 단체	정기항공협회	14사 1단체	
철도	철도	철도 CEPTOAR	사단 법인	일본 철도 전기 기술협회	22사 1단체	
전력	전력	전력 CEPTOAR	임의 단체	전기사업연합회 정보통신부	12사 2기관	
가스	가스	GAS CEPTOAR	사단 법인	일본 가스 협회 기술부	10사	38사
정부 및 행정 서비스	정부 및 지방 공공단체	지자체 CEPTOAR	정부	지방공공단체 정보시스템기구 정보화지원전략부	47도도부현 1,7441시구정촌	
의료	의료	의료 CEPTOAR	정부	후생노동성의정국 연구개발진흥과 의료기술 정보추진실	1그룹 6기관	377사 및 기관

중요 인프라 분야	사업 범위	명칭	주체	사무국	구성원	NISC로부터의 정보를 공개하는 곳(회원이외)
수도	수도	수도 CEPTOAR	공사	일본수도협회 총무부총무과	8수도사업체	내용에 따라 1,351 사업체에 공개
물류	물류	물류 CEPTOAR	사단 법인	일본 물류단체 연합회	6단체 16사	
화학	화학	화학 CEPTOAR	임의 단체	석유화학공업협회	13사	
크레딧	크레딧	크레딧 CEPTOAR	사단 법인	일본 크레딧협회	28사	
석유	석유	석유 CEPTOAR	임의 단체	석유연맹	13사	

자료: 내각관방(2017), 셉터 특성 맵

* 셉터에 대한 상세 설명은 별첨 참조

제2절 분야별 정보공유체계 현황

1) 일반 SW안전부문 정보공유 기준 현황

미국과 마찬가지로 일본의 SW안전 관련 산업도메인에서도 아직까지 SW안전에 관한 정보공유 표준이 존재하지 않는다. 다만, 해당 산업의 SW개발이나 이에 관한 인증, 평가 등의 기준내지 국내표준을 미국표준이나 국제표준을 바탕으로 마련하고 필요 시 적용하는 것으로 파악된다. SW안전 표준은 아니더라도 HW를 바탕으로 SW개발 시 기능 안전을 담보하기 위한 기준이 다양하게 적용되고 있으므로 이를 살펴볼 필요가 있다. 그에 앞서 일본과 서양의 안전에 대한 인식차이를 살펴봄으로써 일본의 안전 관련 기준의 근간을 이해하고자 한다.

(1) 일본과 서양의 안전에 대한 사고 차이

일반적으로 안전에 대한 개념에 있어 일본은 '위험 제로의 상태' 즉, '해로운 것과 손해를 입는 위험이 없는 안전한 상태'로 인식한다. 반면, 서양은 안전을 '해로운 것이나 위험으로부터 보호되고 있는 것' 즉, '모든 위험을 제거하는 것은 어렵고 고비용이 들며, 안전이란 부상이나 물적 손해의 위험성을 낮추고 관리 가능한 것'이라고 인식한다.

따라서 일본의 시각에서 안전은 기본적으로 공짜이며 눈에 보이는 구체적 위험에 대해 최소한의 비용으로 대응해야 하고 일어나지 않을 재해 대책에 기술적 대책을 하지 않는다고 본다. 또한 재해가 발생하면 규제를 강화하되 일어나지 않을 재해 대책에 기술적 대책을 하지 않는다는 입장이다. 따라서 위험 검출형 기술(발견한 위험을 없애는 기술, 발생 건수 중시)을 중시한다.

이에 반해 서양의 시각에서 안전은 기본적으로 비용이 발생하며 위험 요소를 샅샅이 찾아내어 비용을 들여 대책을 마련해야 하는 것이며 사고가 발생해도 중대한 재해에 이르지 않는 기술대책이 필요하다고 본다. 또한 인간은 반드시 실수를 범하므로 기술력 향상으로 안전을 확보해야 하며 일어날 재해를 줄이기 위해 노력해야 한다는 입장이다. 따라서 안전 검출형 기술(논리적으로 안전을 입증할 기술, 중대한 재해 중시)을 중시한다. 일본의 각 산업도메인별 중요 인프라 안전기준은 이러한 시각에서 이해할 필요가 있다.

(2) 일본의 안전표준

일본의 SW안전 관련 산업도 미국과 마찬가지로 SW안전의 요구사항을 직접적으로 반영하고 있지는 않으며 기능안전 중심의 표준으로 이해할 수 있다. 각 분야별 기준 역시 미국과 상당부분 유사하며 일부에서 자체 표준을 갖추고 있는 것으로 파악된다. 도메인별 표준이 없는 경우는 IEC 61508을 적용한다.

2) 일반 안전 관련 산업 정보공유 현황

(1) 소방에 관련된 사고 사례의 정보 수집 및 제공 시스템[71)]

일반 안전 측면의 소방 부문에서는 소방 활동의 안전 관리 및 확보에 도움이 되도록 전국적 공유・축적 시스템을 구축하고 있다. 이 시스템은 전국 각지의 소방관련 직원들이 경험한 사고와 히야리 핫토(중대한 재해나 사고 등으로 이어지지는 않았지만 미연에 방지하고자 하는 사고)[72)] 사례 등의 정보를 정기적으로 수집하고, 수집된 정보의 배후 요인을 분석·실시하는 등의 필요 조사를 실시하여 전국적으로 공유・축적하고 소방 활동의 안전 관리 및 확보에 이바지하는 것을 목적으로 하고 있다.

수집 대상은 소방관련 직원과 소방관이 활동 중에 발생한 부상 사고 사례이며, 부상 사고 사례를 웹을 이용한 설문 방식을 통해 정기적으로 수집하고 있다. 다만 모두 웹으로 수집하는 것은 현실상 불가능하기 때문에 필요에 따라 웹 이외의 방법도 함께 병행하고 있다. 수집은 소방본부에 사례 등록을 의뢰하고 소방본부는 미리 규모에 따라 할당된 건수의 사례를 등록하며, 사례가 한꺼번에 등록이 집중되지 않도록 소방본부는 2~4달 기준으로 마감일을 설정한다.

수집된 부상 사고 사례를 바탕으로 여러 사고 사례의 경향을 파악하며 배후 요인을 포함한 사고 사례 분석을 실시한다. 사고 사례의 분석에 있어서는 소방 관계 직원 및 관련 전문가 등으로 구성된 검토 회의를 개최하고 공개할 정보에 대해 검증을 실시하여 이러한 정보를 받아보는 쪽에 편리한 내용인지 검토하고 공개한다.

정보 시스템 기능 및 구성은 다음과 같다.

---

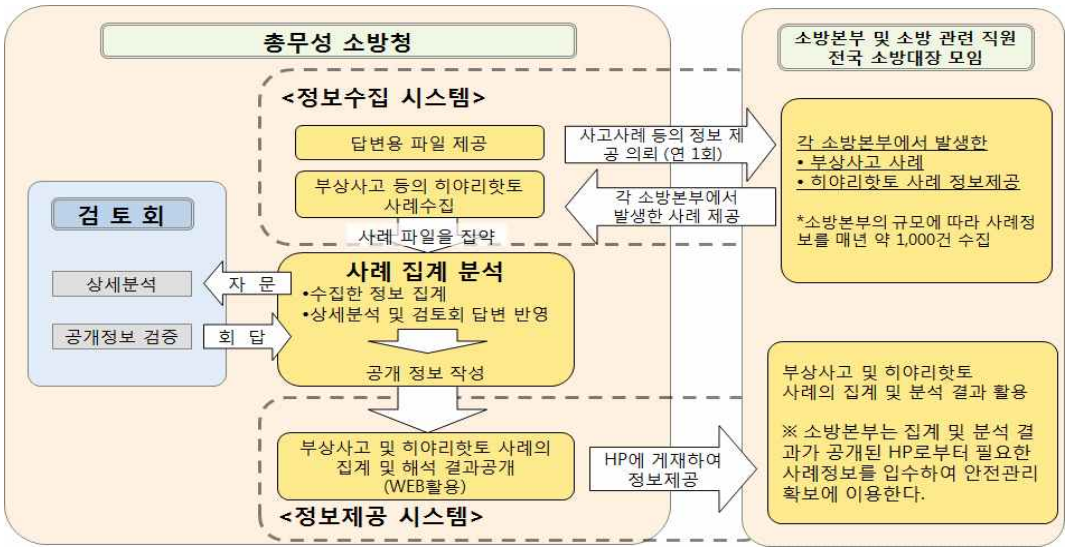
71) http://www.fdma.go.jp/html/new/pdf/161129_kentou/4-1-1.pdf#search=%27%E5%AE%89%E5%85%A8%E3%81%AE%E6%83%85%E5%A0%B1%E5%85%B1%E6%9C%89%27

72) 히야리 핫토란, 사고에는 이르지 않았으나 경우에 따라서 사고와 직결 될지도 모르는 에피소드를 말한다. 어원은 "히야리(아찔했다)" "핫토(깜짝 놀랐다)" 잘못된 행위를 할 뻔했지만 미연에 인식하고 방지할 수 있는 케이스와 어떤 행위에 실수가 있었지만 피해가 직접적으로 미치지 않은 경우 등이 여기에 포함된다.

① 정보 수집 시스템: 소방 직원의 일상 활동과 훈련 등에서 발생하는 부상 사고와 히야리 햇토 사례를 대상으로 설문 조사 방식으로 정기적으로 전국의 소방 본부에서 연간 1,000 건 정도를 목표로 수집한다.

② 정보 제공 시스템: 수집된 사례 정보를 단순 집계에 의한 경향 파악이나 관련 전문가 등으로 구성된 검토회의에서 배후 요인 분석하는 등 필요한 조사를 실시하여 전국적으로 공유·축적하고 소방 직원과 각 소방 본부 등 관계 기관은 웹상에서 필요한 정보를 얻을 수 있게 된다.

[그림 4-1] 소방관련 직원의 사고 사례 정보 수집·제공 시스템 구성



자료: http://www.fdma.go.jp

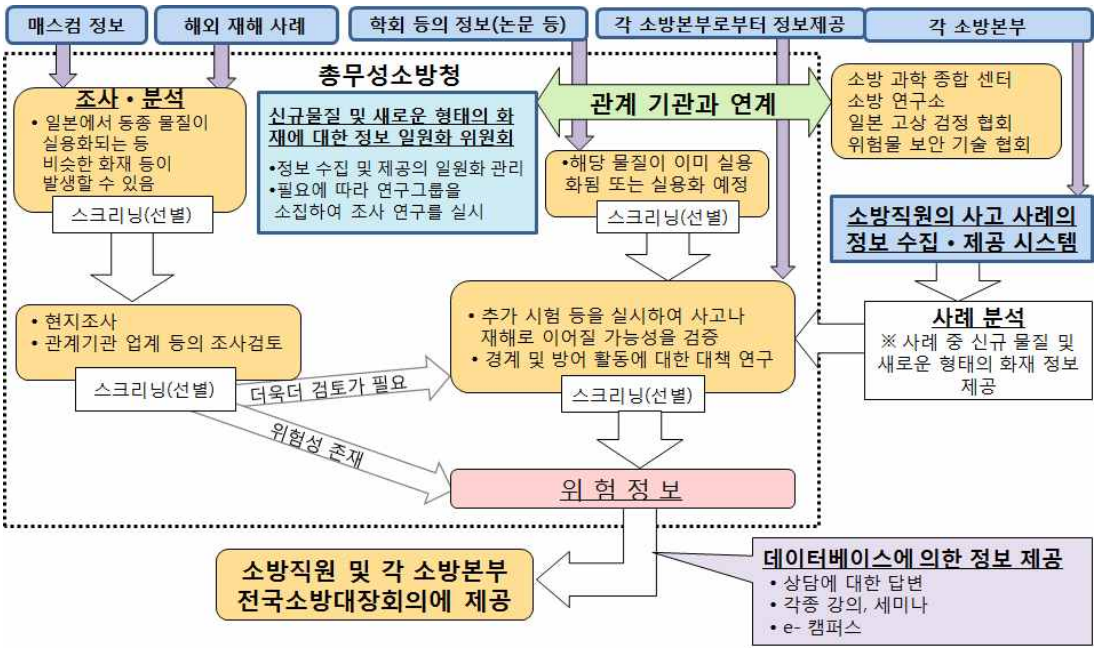
(2) 신규 물질 및 신형 화재에 관한 정보의 일원화 시스템

2003년에 일어난 미에현 RDF 시설의 소방 공무원 순직 사고처럼 일상생활 속에서 위험물이 아닌 물품이나 건축물에서 화재 시에는 위험성이 있는 것을 사전에 파악할 필요가 있다. 따라서 위험성이 있는 물품이나 건축에 대한 정보 수집, 조사 분석 후 저장하는 시스템을 구축하고 전국적으로 정보를 축적·공유하여 소방 활동에 종사하는 소방 직원의 안전 관리 및 확보에 이바지하는 것을 목적으로 하고 있다.

소방 활동에 있어서 새로운 형태로 사용되는 물품의 화재가 증가하고 있는 것에 대응하기 위해 특수 화학 성질을 띠는 물질로 화재의 위험이 있는 것 등 소방 활동에 있어서 위험물로 지정되어 있지 않지만, 지장을 초래할 수 있는 것에 관한 정보를 수집한다.

정보 수집 방법은 매스컴 정보, 해외의 재해 피해 사례, 학회 정보 등을 통해 폭넓게 정보를 수집한다. 수집 정보는 수집된 대로 모든 것을 제공하는 것이 아니라, 연구자 등으로 구성된 검토회의에서 정보의 선별 및 실증 실험 실시를 통해 정보 확인 작업을 실시한 후, 소방 직원, 각 소방본부·전국 소방대장 모임 등에 정보를 제공한다.

[그림 4-2] 신규물질 및 신형 화재에 관한 정보 일원화 시스템



자료: http://www.fdma.go.jp

2. 통신 부문 : Telecom ISAC[73)]

일본은 하나의 중요 산업도메인 인프라의 안전정보 체계를 공유하는 개념으로서 셉터(CEPTOAR) 즉, IT 장애 등에 관한 대책 및 개선 관련 정보를 공유하고 분석하는 기능과 각종 인프라 분야간 정보 공유를 위한 셉터 카운슬(이하 '셉터협의회')이 설치되어 운영되고 있다. 통신 부문에 있어 초기 텔레콤 ISAC의 활동은 이후 일부 방송사업자 및 케이블 TV사업자가 가맹하여 새로이 설립된 ICT-ISAC으로 이행시켜 오늘날에 이르렀다. 이러한 배경을 이해하며 Telecom-ISAC과 ICT-ISAC을 살펴본다.[74)]

※ CEPTOAR의 연계 및 확장

기존 사업 영역을 뛰어넘어서 현재는 다음과 같이 연계하거나 확장하고 있다.

- 정보통신 부문: Telecom-ISAC의 활동을 새로이 설립된 ICT-ISAC으로 이행시켜 일부 방송사업자 및 케이블 TV사업자가 가맹
- 전력 부문: 전력 ISAC을 설립, 4월부터 운영개시
- 화학 부문: 석유화학공업협회와 일본화학공업협회의 정보공유 및 활동연계
- 사이버테러 대책 협의회: 중요 인프라 사업자 등과 경찰과 연계, 47도도부현에 설치
- 조기 경계 정보 WAISE (JPCERT/CC : 보안정보전반)

73) (https://www.telecom-isac.jp/)

74) ※ 셉터 관련 사이트

- https://www.telecom-isac.jp/public/t-ceptoar.html
- http://www.nisc.go.jp/conference/seisaku/ciip/dai9/pdf/9siryou0202.pdf#search=%27TCEPTOAR%27

<표 4-2> Telecom-ISAC의 정보공유 현황 및 특징 요약

No	구분	해당 유형		현황 및 특징
1	관련 분야	1) 일반 분야		
		2) 보안 분야	○	정보통신 분야 네트워크 보안
		3) SW안전 분야		
2	법적 근거	1) 법령 근거	○	사이버보안 기본법
		2) 그 외 방법		
3	재원 조달	1) 정부		
		2) 민간		
		3) 정부 + 민간	○	비영리단체
4	조직 형태	1) 일반 정보공유체계		
		2) 산업도메인별 대표 ISAC	○	일본의 통신관련 대표 ISAC
		3) 기관 또는 기업의 자체 ISAC		
5	운영 활동	1) 일반		
		2) 커뮤니티		
		3) 스터디 그룹	○	11개의 워킹그룹(WG)과 1개의 스페셜 인터레스트 그룹(SIG)
		4) 표준화		
6	정보 공유 방식	1) 시스템		
		2) 이메일	○	메일링리스트 작성
		3) 인쇄물	○	회원사 간 뉴스레터 작성 공유
		4) 온라인 토의		
		5) 워크숍(컨퍼런스)	○	전문가 지식인 초청 의견교환
7	정보 공유 기술	1) 표준 규격 또는 기술		TLP
		2) 독자 규격 또는 기술		
8	정보 공유 범위	1) 멤버십 별	○	회원사 간 정보 공유
		2) 정보 유형별		
		3) 운영 활동별	○	워킹그룹별 활동

※ 문헌부족으로 확인이 어려운 항목은 표기하지 않았음

1) 조직 및 운영 체계

(1) 설립 배경

Telecom-ISAC Japan(이하 ‘텔레콤ISAC’) 추진회의는 2002년 7월 ’사고 정보 공유·분석 센터’로 출범한 비영리단체이다. 2002년 7월, 일본 국내 주요통신사업자(ISP) 7개사 등이 발기인이 되어 비영리단체인 ‘사고 정보 공유·분석 센터’로 시작하였다. 통신 서비스가 안전하면서 안심할 수 있게 운용 될 수 있도록 회원들이 관련 정보를 공유·분석하는 시스템을 구축하며 사업자 단독으로는 커버할 수 없는 사이버 위협에 대응하여 적시에 조치를 취할 것을 목적으로 한다.

출범 이후 회원 기업 수가 확대되고 있으며 계속 진화하는 새로운 정보 보안의 위협에 대해 회원사 간의 협력을 바탕으로 정보통신 분야 보안대책을 충실하게 도모하고 있다. 텔레콤ISAC은 ‘건전한 보안은 고결한 협업에서!’를 활동 목표로 내걸고 ISP·정보통신 분야의 네트워크 보안대책에 관련된 다양한 활동을 지속하고 있다.

(2) 조직 구성

회원기업은 일본전기 주식회사, NTT 커뮤니케이션즈 주식회사, KDDI 주식회사 외 총 20개 회사이며, 텔레콤ISAC의 활동에 동참하고 공헌 협력을 희망하는 신규 회원을 모집하고 있다. 가입 등은 담당자를 통해 연락하도록 하며, 현재 가입 사이트는 ICT-ISAC과 연계되어 있다.[75]

(3) 역할 및 책임

11개의 워킹 그룹(WG)과 1개의 스페셜 인터레스트 그룹(SIG)을 통해 다양한 통신 분야의 사이버 위협에 대응하는 활동을 수행함으로써 사업자가 스스로 대응할 수 없는 사이버 위협에 대해 즉각 조치할 수 있도록 하고 안전하고 안심할 수 있는 통신 서비스가 운용되도록 하는 역할과 책임을 가진다.

워킹 그룹을 통하여 경로 정보 공유, 사이버 공격 대응 훈련, DoS(Denial of Service) 공격 대응, 사이버 공격 대응 체계 검토, 사이버 공격 등에 대한 대책 검토, 취약성을 보유한 네트워크 디바이스 조사 등의 다양한 역할을 수행한다.

75) https://www.telecom-isac.jp/contact/index.html 현재 텔레콤ISAC은 ICT-ISAC으로 확대운영중임

(4) 운영 방식 및 활동

11개의 워킹 그룹(WG)과 1개의 스페셜 인터레스트 그룹(SIG)을 통해 정보수집 및 공유 등을 포함한 통신 분야의 사이버 위협에 대응하는 다양한 활동을 수행한다.

※ 경로 정보 공유 WG

- 2005년 7월 설치, 책임 회사: 인터넷 멀티 피드 역할 및 책임
- ISP 간의 경로 정보 공유, 경로 정보 이상 시 신속한 대응 (경로 봉행(奉行) 시스템의 운용)

※ ACCESS WG

- 2007년 4월 설치, 책임 회사: KDDI
- 인터넷 NW 서비스 운영 품질 향상을 위한 정보 교환, 모범 사례 공유

※ SoNAR WG

- 2007년 12월 설치, 책임 회사: IIJ
- 네트워크를 이용한 부정 불법 행위 대응(ABUSE 대응)에 대한 정보의 공유. 사고의 확대를 억제하는 프레임워크를 개발한다.

※ 사이버 공격 대응 훈련 WG

- 2009년 5월 설치, 책임 회사: 서일본 전신 전화
- 전기 통신 사업자 등이 참가하는 사이버 공격을 상정한 대응 훈련을 기획하고 실시한다.

※ DoS 공격 대응 WG

- 2011년 10월 설치, 책임 회사: IIJ
- DoS 공격에 대한 신속한 대응과 여러 사업자에 의한 공동대처 방식의 검토. 일본에서 DoS 공격발생 예측, 조기 발견, 신속하고 적절한 대응의 실현을 목표로 한다.

※ 사이버 공격 대응 체계 검토 WG (국제 사이버 WG)

- 2011년 12월 설치, 책임 회사: NTT 커뮤니케이션즈
- 악성 코드 등의 다양한 사이버 공격정보를 ISP 간 또는 보안관련 기관과 공유하며 예측・대응 가능한 사이버 공격 대응 체계를 검토한다.

※ ACTIVE 업무 추진 WG

- 2013년 7월 설치, 책임 회사: NTT 커뮤니케이션
- 총무성 실증 실험 사업 ACTIVE 운영. 악성 코드 감염 방지, 제거를 추진하여 보다 안심하고 안전한 인터넷 실현을 목표로 한다.

※ 사이버 공격 등에 대한 적절한 대책 방법 검토 WG (통신비밀 WG)

- 2013년 12월 설치, 책임 회사: NTT 커뮤니케이션
- 총무성 '전기 통신 사업의 사이버 공격에 대한 적절한 대처 자세에 관한 연구회'의 통신 사업자, 특히 ISP 시선으로 제언하는 전기 통신 사업자의 업무를 정리하고 통신 비밀로 대표되는 법적 처리를 행한다.

※ WiFi 능력 향상 WG

- 2013년 9월 설치, 간사 역할: 기획 조정부
- 전파의 유효 이용(오프로드 추진)을 목적으로 WiFi의 이용 및 설치・운영에 장벽이 되는 정보보안에 관한 과제 검토, WiFi 보급 계발 텍스트 작성・세미나 등을 실시한다.

※ 라우터 취약점 문제 WG

- 2012년 7월 설치, 책임 회사: NTT 커뮤니케이션
- 위험이 발생 가능한 취약점을 보유한 특정 라우터에 대한 구체적인 대응 검토와 조사를 실시한다.

※ 취약성을 보유한 네트워크 디바이스 조사 WG

- 2013년 5월 설치, 책임 회사: NTT 커뮤니케이션
- 일본 국내 IP로 연결된 네트워크 장치의 취약점 보유 상황에 관한 전체적 경향을 파악하며 조사를 실시한다.

※ 스페셜 인터레스트 그룹(SIG) : DNS 운영자 연락 모임

- SIG 2008년 6월 설치, 간사 역할: 소프트뱅크 주식회사
- DNS 운영자 간의 정보 공유・연락 체제의 정비

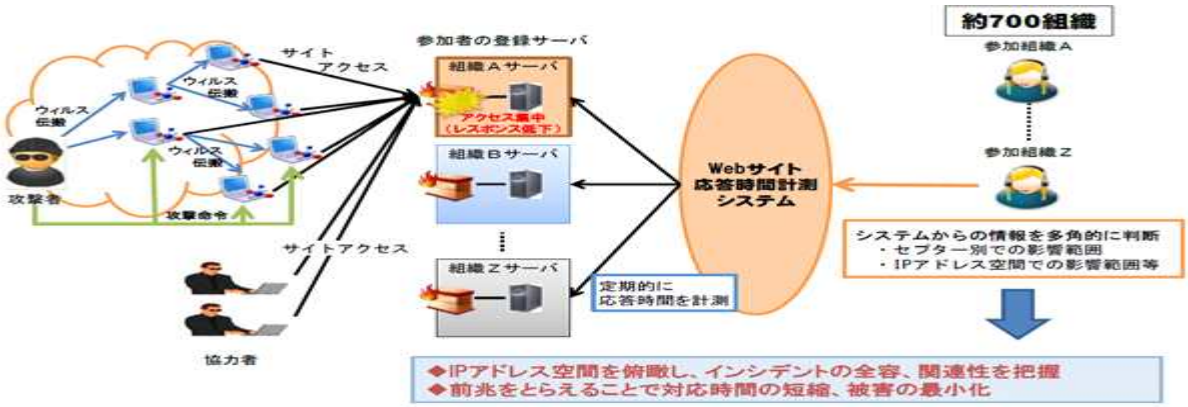
2) 정보공유 체계

(1) 정보공유 방식

회원 간의 뉴스레터 또는 메일링리스트를 통해 전달한다.

그림과 같이 바이러스 전파에 대응하는 경우의 예시로, 약 700개 조직으로부터 관련 정보를 시스템으로부터 받아 다각적으로 판단하게 되며 IP주소 대역 등 센터별 영향범위를 판단한다. IP주소 대역을 예측하고 사건의 전모와 관련성 등 징조를 파악함으로써 회원들의 위협에 대한 대응 시간을 단축하고 피해를 최소화할 수 있다.

[그림 4-3] (예시)정보수집 및 공유를 통한 위협 대응



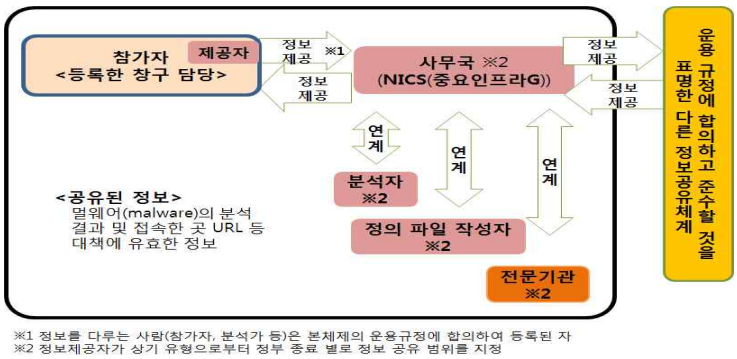
자료: https://www.ict-isac.jp/news/news20160622.html

(2) 정보공유 체제 및 범위 유형

다음과 같은 정보공유 체제를 통해 회원사 간에 정보를 공유한다.

참가자(정보를 등록한 창구 담당자)(제공자)가 사무국에 정보를 제공한다. 이때 정보를 다루는 사람(참가자, 분석자 등)은 본체제의 운용규정에 합의하여 등록된 자이다. 사무국(NISC 중요인프라G)은 정보를 제공받아 분석자, 정의파일 작성자, 전문기관 등과 연계하면서 회원사들에게 정보를 공유한다.[76] 이때 정보제공자가 상기 유형의 정보 종류별로 정보공유 범위를 지정한다. 해당 정보공유 체제를 통해 멀웨어(malware)[77]의 분석결과 및 접속한 곳 URL(uniform resource locator, 홈페이지 주소) 등 대책에 유효한 정보들을 공유하게 된다.

[그림 4-4] 정보공유 체제



자료: NISC Japan, “중요인프라의 정보보안대책에 관한 행동계획의 정보연락정보제공에 관한 실시 세목 개요에 대하여”

76) 운용 규정에 합의하고 준수할 것을 표명한 다른 정보공유체제
77) 멀웨어(malware)란, 바이러스, 웜 및 트로이 목마를 포함한 악성 코드의 범주

내각관방 정보보안 센터와 중요 인프라 소관부처 등이 상호 연락하고 정보를 제공하기 위한 규정을 마련하였는데, 다음과 같이 단계적 절차를 통해 연락 및 정보제공이 이루어진다. 또한, 정보공유 수준을 설정을 위한 교통신호 프로토콜(TLP, Traffic Light Protocol)을 개발하여 적용하도록 하고 있다.

① 정보공유 수준 설정(TLP 적용)

② 정보연락 순서 설정

③ 정보연락의 IT장애에 관한 공통의 분류 및 카테고리 설정

④ 통계적인 발생 상황 파악

⑤ 정보제공 순서 결정

(3) 정보공유 기술 및 활용

정보공유를 위한 실질적인 기술은 문헌부족으로 확인하기가 어려웠으나 회원들에게 제공하는 정보공유 수준을 설정을 위한 프로토콜은 교통신호 프로토콜(TLP)를 사용한다는 것을 확인할 수 있었다.

교통신호 프로토콜(이하 ‘TLP)이란, 정보제공자(제공 소관부처)가 중요 인프라 분야 전체 또는 일부에 정보를 공유하는데 있어 정보공유의 범위와 수준을 유형화한 일본 내각관방이 마련한 정보공유 규격이다. 이것은 미국이 사이버기반보호를 위해 개발한 TLP 규격을 일본 자국 내 체제로 개발한 것으로 일본의 교통신호 프로토콜은 매년 사이버전략을 발표하면서 점차 구체화되고 개선되고 있다.

TLP는 다음과 같이 5개 레벨의 유형으로 구성하고 이 규칙에 따라 정보를 공유한다. 단, 정보공유 레벨이 명시되지 않은 경우에는 원칙적으로 정보는 황색(AMBER)로서 취급하며, 정보원(정보제공자명)은 적색(RED)로 취급한다.

① RED: 정보제공원[78]에 한정 즉, NISC[79](해당 정보제공처와 관련된 분야를 직접 담당하는 심의관, 참사관, 사무관 리에종)

② AMBER: 정보를 알 필요가 있는 사람에게만 한정 즉, 직접 관계되는 중요 인프라 분야(중요 인프라 소관부처, CEPTOAR, CEPTOAR를 구성하는 사업자 등에 속한

78) 중요 인프라 소관부처로부터 'RED' 정보의 정보연락을 받을 경우에는 정보제공원은 해당 중요 인프라 소관부처가 된다.

79) 내각 사이버보안센터(National center of Incident readiness and Strategy for Cybersecurity)

자, NISC(직접관계 있는 분야를 담당하는 심의관, 참사관, 사무관 리에종)

③ YELLOW : 규정에 합의하고 준수할 것에 동의한 사람까지 제공

④ GREEN: 각 계층 관계자와 공유 가능한 정보 즉, 다른 중요 인프라 분야(중요 인프라 소관부처 등, CEPTOAR, CEPTOR를 구성하는 사업자 등, 정보보안에 종사하는 개인/단체 등, NISC(관계있는 분야를 담당하는 심의관, 참사관, 사무관 리에종)

⑤ WHITE: 공공의 정보(인터넷 상에서 공개, 방송에 의한 공개를 포함)로 공개

[그림 4-5] TLP(교통신호 프로토콜)

자료: NISC Japan, “중요인프라의 정보보안대책에 관한 행동계획의 정보연락정보제공에 관한 실시 세목 개요에 대하여”

3. 통신부문 확장 : COMMUNICATIONS ISAC[80)]

<표 4-3> ICT-ISAC의 정보공유 현황 및 특징 요약

No	구분	해당 유형		현황 및 특징
1	관련 분야	1) 일반 분야		
		2) 보안 분야	○	정보보안에 대하여 종합적으로 대응
		3) SW안전 분야		
2	법적 근거	1) 법령 근거	○	사이버보안법
		2) 그 외 방법		
3	재원 조달	1) 정부		
		2) 민간		
		3) 정부 + 민간	○	텔레콤ISAC + SI 벤더 계열 + 방송 계열
4	조직 형태	1) 일반 정보공유체계		
		2) 산업도메인별 대표 ISAC	○	텔레콤 ISAC의 활동을 새로이 전개
		3) 기관 또는 기업의 자체 ISAC		
5	운영 활동	1) 일반		
		2) 커뮤니티	○	ISP를 포함한 통신 사업자뿐만 아니라 방송 사업자, SW 벤더, 정보 제공 서비스(ISP) 사업자, 정보 관련 기기 제조 사업자 등 다양한 분야 전문가들이 함께 활동
		3) 스터디 그룹		
		4) 표준화		
6	정보 공유 방식	1) 시스템		
		2) 이메일		
		3) 인쇄물		
		4) 온라인 토의		
		5) 워크숍(컨퍼런스)		
7	정보 공유 기술	1) 표준 규격 또는 기술		
		2) 독자 규격 또는 기술		
8	정보 공유 범위	1) 멤버십 별	○	회원사 간의 정보 공유
		2) 정보 유형별		
		3) 운영 활동별		

※ 문헌부족으로 확인이 어려운 항목은 표기하지 않았음

80) (https://www.ict-isac.jp/news/news20160622.html)

1) 조직 및 운영 체계

(1) 설립 배경

더욱 엄격해지는 사이버 보안 환경에 대응하기 위하여 통신사업자의 시점을 중심으로 한 텔레콤ISAC 활동으로는 충분하지 않았다. 그렇기 때문에 ICT-ISAC을 통해 IoT 기기의 제조 사업과 방송 사업 등에 관한 ICT 이해관계자를 끌어 들여 고도화된 정보 공유 및 분석 대응의 조직을 구축하여 정보보안에 관한 종합적으로 대응할 수 있는 틀을 실현하고자 하였다. 따라서 기존의 텔레콤ISAC으로부터 SI벤더와 방송 계열 사업자, 보안 벤더까지 포함한 형태로 확대 운영되는 현재의 ICT-ISAC이 되었다.

(2) 조직 구성

텔레콤ISAC, SI・벤더 계열, 방송 계열 및 보안 벤더로 조직이 구성되어 있다.

- 텔레콤 ISAC (ISP, 통신 캐리어, 휴대전화 캐리어)

・ KDDI 주식회사, NTT 커뮤니케이션 주식회사, 주식회사 인터넷 이니셔티브, 주식회사 NTT 도코모, 소네트 주식회사, 소프트뱅크 주식회사, 서일본 전신 전화 주식회사, 동일본 전신 전화 주식회사, 주식회사 KDDI 연구소 외 다수

- SI·벤더 계열(루터 벤더, FW/NAT 벤더, 통신기기 메이커, SIer, IoT 벤더, 가전 메이커)

・ 주식회사 히타치 제작소, 일본전기 주식회사, 후지쯔, NTT 컴퓨터 보안 주식회사

- 방송 계열(방송 사업자, CATV 사업자) 및 보안 벤더(안티 바이러스 계열, 보안 콘솔)

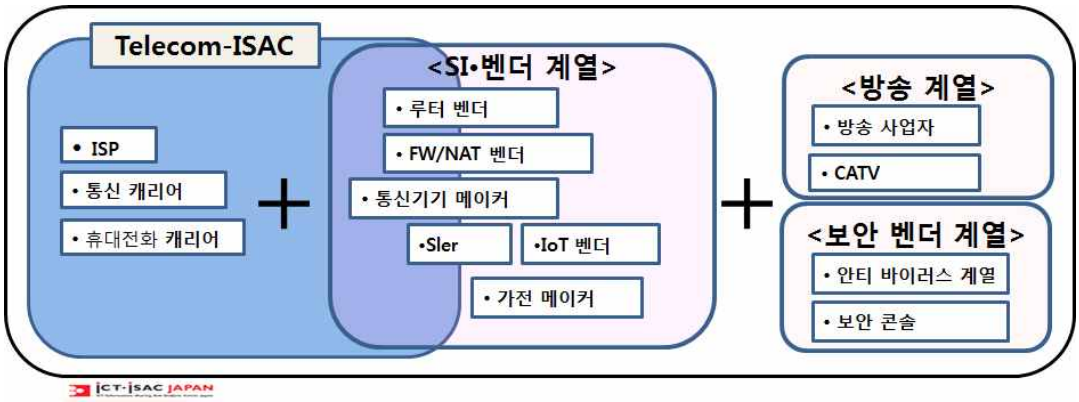
・ 주식회사 TBS 텔레비전, 주식회사 텔레비전 아사히, 주식회사 텔레비전 도쿄, 주식회사 후지 텔레비전, 일본 텔레비젼 방송망 주식회사

- 보안 업체 계 NRI 시큐어 테크놀로지스 주식회사

・ 주식회사 FFRI 외

감독기구에는 총무성, 국립 연구 개발 법인 정보 통신 연구기구 (NICT), 일반 사단법인 일본 인터넷 프로바이더 협회 (JAIPA), 일반 사단법인 텔레콤 서비스 협회, 일반 사단법인 전기 통신 사업자 협회 (TCA), 일반 재단법인 일본 데이터 통신 협회, 일반 사단 법인 일본 민간 방송 연맹 등이 있다.

[그림 4-6] ICT-ISAC의 회원 구성의 미래 이미지



자료: ICT-ISAC 홈페이지 (https://www.ict-isac.jp/news/news20160622.html)

(3) 역할 및 책임

ICT-ISAC은 다양한 사업자가 사이버 공격 등의 정보수집・분석 및 대응에 대한 정보공유, 업계의 테두리를 넘어 제휴・협력하고 위협에 대처하는 조직이다.

(4) 운영 방식 및 활동

ICT-ISAC은 ICT 분야의 종합적인 보안 확보에 기여하기 위해 ISP를 포함한 통신 사업자뿐만 아니라 방송 사업자, 소프트웨어 벤더, 정보 제공 서비스 사업자, 정보 관련 기기 제조 사업자 등 다양한 분야의 구성원들이 함께 활동한다. 다양한 사업자가 정보 수집・분석 및 대응에 대한 정보 공유, 업계의 테두리를 넘어 제휴・협력하는 조직으로 위협에 대처하기 위함이다. ICT-ISAC은 매일 변모하는 정보 보안의 위협에 직면한 분야에 안전한 ICT 환경을 충실히 기여할 수 있도록 한다.

최근 정보통신기술(ICT)의 보급・발전을 통해 우리의 일상생활이나 사회・경제 활동 등의 모든 활동이 ICT에 의존하게 되는 한편, 정보보안 위협이 더욱 교묘화・복잡화되는 경향이 발생한다. 또한 향후 IoT (Internet of Things)의 진전에 따라 그것을 활용하여 산업 경쟁력을 높이려는 국제 경쟁도 진행될 것으로 예상된다.

따라서 ICT에 관련된 다양한 기업・단체와 협력 연계함으로써 안전한 ICT 사회 형성에 기여할 수 있는 조직 'ICT-ISAC'을 설립함으로써 해결하고자 하였다.

4. 금융 부문 : 금융 ISAC[81)]

<표 4-4> F-ISAC의 정보공유 현황 및 특징 요약

No	구분	해당 유형		현황 및 특징
1	관련 분야	1) 일반 분야		
		2) 보안 분야	○	금융시스템의 안전성 확보
		3) SW안전 분야		
2	법적 근거	1) 법령 근거	○	사이버 보안법
		2) 그 외 방법		
3	재원 조달	1) 정부		
		2) 민간		
		3) 정부 + 민간	○	금융, 보험, 증권 등 다양한 회원사
4	조직 형태	1) 일반 정보공유체계		
		2) 산업도메인별 대표 ISAC	○	일본의 금융 ISAC
		3) 기관 또는 기업의 자체 ISAC		
5	운영 활동	1) 일반		
		2) 커뮤니티		
		3) 스터디 그룹	○	워킹그룹
		4) 표준화		
6	정보 공유 방식	1) 시스템		
		2) 이메일	○	TLP를 사용하여 정보공유범위 제한
		3) 인쇄물	○	리포트 발신
		4) 온라인 토의		
		5) 워크숍(컨퍼런스)	○	연례 컨퍼런스 및 워크숍 개최
7	정보 공유 기술	1) 표준 규격 또는 기술		
		2) 독자 규격 또는 기술		
8	정보 공유 범위	1) 멤버십 별	○	정회원, 준회원, 찬조회원, 제휴회원
		2) 정보 유형별		
		3) 운영 활동별		
9	정보 공유 내용	1) 일반 정보		
		2) 보안(위협) 정보		
		3) SW안전 정보		

※ 문헌부족으로 확인이 어려운 항목은 표기하지 않았음

81) (http://www.f-isac.jp/press_release/20140807.html)

1) 조직 및 운영 체계

(1) 설립 배경

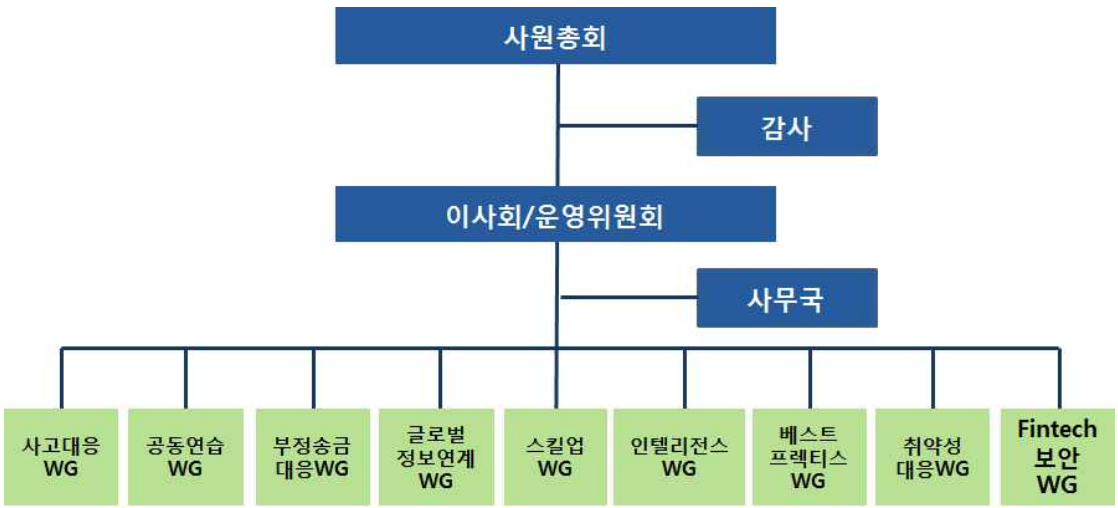
일본은 최근 다양한 형태로 사이버 공격의 위협이 고조되고 있으며, 2012년 후반부터 악성 코드 감염에 의한 부정 송금을 비롯하여 심각한 사태에 직면해 있다. 단기간에 고도화되는 공격에 대하여 별도 조직으로 대응해 나가는 것은 매우 어려운 상황이며, '나라에서 나라로 확산', '동종의 큰 조직에서 작은 조직으로 확산'의 공격이 확산되고 있다. 따라서 정보 공유 등을 촉진하여 이러한 위협에 대처해 나가는 움직임이 활발해지고 있다.

미국에서는 FS-ISAC(Financial Services ISAC)이 1999년에 설립되었는데 5,000명이 넘는 회원 조직이 활발한 정보를 공유하고 있다. 이에 일본 금융 ISAC은 미국의 FS-ISAC을 모델로 일본 금융 기관의 정보 공유 활동을 발전시키고 금융 시스템 기반 전체에서 안전 향상에 기여하는 다양한 활동을 추진하게 되었다.

(2) 조직 구성

금융 ISAC은 다음과 같이 사원총회 아래 감사, 이사회/운영위원회와 사무국을 두고 다수의 워킹그룹을 구성하고 정보공유 및 분석 업무를 담당하고 있다.

[그림 4-7] 금융ISAC의 조직도



자료: F-ISAC Japan 홈페이지, (http://www.f-isac.jp/institute/outline.html)

가입 대상 및 구성 회원은 다음과 같다.

- 정회원: 아이오이 닛세이 동화 손해보험 주식회사 등 323사

- 준회원: 아이치신용금고 등 12사
- 찬조회원: 일반사단법인 JPCERT 코디네이션센터
- 제휴회원: 골드(12사), 실버(10사), 브론즈(1사)로 구성

(3) 역할 및 책임

일본 금융 기관의 사이버 보안에 대한 정보 공유 및 분석을 실시하여 금융 시스템의 안전성 향상을 추진함으로써 이용자의 안심을 지속적으로 확보하는 것을 목적으로 하고 있다.[82]

(4) 운영 방식 및 활동

금융ISAC은 한 회사에서 일어난 사안을 여러 조직 간에 확장하여 그 대책을 공유하는 '컬렉티브 인텔리전스' 기능과 공통의 과제에 대한 리소스를 공유하고 협력하면서 대책을 검토해 가는 '리소스 쉐어링' 기능을 갖춘 활동 기반을 구축하고, 동종의 조직과 사람들이 공통의 문제인식 하에 스스로 운영하는 것을 목표로 활동을 수행하고자 한다.

[그림 4-8] 금융 ISAC 활동 개요

사고 및 취약 정보 등에 대하여 메일링 리스트를 통하여 정보를 공유한다. 메일링 리스트는 TLP(Traffic Light Protocol)[83]을 사용하여 정보 공유 범위를 제한함으로써 제보자의 불이익을 피할 수 있으며 익명의 정보 제공도 가능한 구조가 준비되어 있다. 정회원은 메일링 리스트에 포함되며, 준회원은 특정 정보만 사무국으로부터 전달받는다.

워킹그룹(WG)은 특정 중요 과제 분석, 대책 검토 등을 실시하며 성과는 워크숍과 연례 컨퍼런스 등에서 발표한다. 준회원의 경우는 워킹그룹 좌장이 지명한 경우만 참가 가능하다. 워크숍은 2개월에 1회 정도 회원 간의 연구회를 개최하며, 연계기관과 제휴회원 등

82) http://www.f-isac.jp/institute/activities.html
83) 텔레콤ISAC 참고

의 주제발표도 있다. 회원끼리의 대면의 장소이기도 하다. 연례 컨퍼런스는 매년 사원 총회. 워킹 그룹・제휴 기관・제휴 회원 등의 주제 발표를 실시한다.

메일링 리스트에서 공유되는 정보의 경향, FS-ISAC 등의 연계 기관의 정보를 금융기관에 맞게 수정하여 리포트로 발신된다.

2) 정보공유 체계

(1) 정보공유 방식

금융 ISAC에서는 현재 회원 간 메일링 리스트를 통해 일상의 사건이나 취약점 정보 등을 실시간으로 공유한다. 또한 특정 중요 과제에 대해 주제별 워킹그룹(WG)을 설치하고, 회원 공동으로 대책 검토 등을 실시하면서 지식과 대응력을 높여 가고 있다. 이러한 성과는 워크숍 및 연례 컨퍼런스 등에서 공유하고 있다.

운영활동에서 기술한 바와 같이 향후 금융ISAC은 시스템 기반의 ‘컬렉티브 인텔리전스’ 기능과 ‘리소스 쉐어링’ 기능을 갖추고 본격적인 정보공유 활동을 수행할 것으로 기대된다.

(2) 정보공유 범위

회원 등급에 따라 정보 공유 내용이 다르다. 정회원의 경우 대부분의 활동과 정보를 제공받을 수 있으며, 준회원의 경우 사무국에서 허락된 정보 공유와 같이 일부 정보 및 워킹그룹의 활동 등에 제약이 따른다. 메일링 리스트는 TLP(Traffic Light Protocol)[84]을 사용하여 정보 공유 범위를 제한한다.

84) 텔레콤ISAC 참고

5. 전력 부문 : 전력 ISAC[85)]

<표 4-5> JE-ISAC의 정보공유 현황 및 특징 요약

No	구분	해당 유형		현황 및 특징
1	관련 분야	1) 일반 분야		
		2) 보안 분야	○	전기사업자 간의 사이버 보안 정보
		3) SW안전 분야		
2	법적 근거	1) 법령 근거	○	사이버 보안법
		2) 그 외 방법		
3	재원 조달	1) 정부		
		2) 민간		
		3) 정부 + 민간	○	
4	조직 형태	1) 일반 정보공유체계		
		2) 산업도메인별 대표 ISAC	○	일본 전기사업 대표 ISAC
		3) 기관 또는 기업의 자체 ISAC		
5	운영 활동	1) 일반		
		2) 커뮤니티		
		3) 스터디 그룹		
		4) 표준화		
6	정보 공유 방식	1) 시스템		
		2) 이메일		
		3) 인쇄물		
		4) 온라인 토의		
		5) 워크숍(컨퍼런스)		
7	정보 공유 기술	1) 표준 규격 또는 기술		
		2) 독자 규격 또는 기술		
8	정보 공유 범위	1) 멤버십 별	○	정회원과 특별회원으로 구성하여 회원 간 정보 공유
		2) 정보 유형별		
		3) 운영 활동별		
9	정보 공유 내용	1) 일반 정보		
		2) 보안(위협) 정보		
		3) SW안전 정보		

※ 문헌부족으로 확인이 어려운 항목은 표기하지 않았음

85) (https://www.je-isac.jp/news/2017/0328_01.html)

1) 조직 및 운영 체계

(1) 배경

전력 ISAC은 2017년 3월 28일자로 전기사업자 간의 사이버 보안 정보 공유 및 분석을 하는 조직으로 설립되었다. 최근 모든 분야에서의 사이버 공격 위협이 고조되는 가운데 전력 분야는 어느 때보다도 그 중요성이 높아지고 있다. 특히 자유화의 진전에 따라 비용 절감을 위한 범용 기술의 채용이나 시스템에 연결하는 사업자가 증가하고 다양화될 전망인 가운데 그 위험이 증가할 가능성이 높기 때문에 전력분야 전체에 대한 사이버 보안 강화 노력이 요구되고 있다.

따라서 2016년 이후, 일본의 전력분야에서는 특히 스마트 미터 시스템에 대한 감사와 보안지침 강화 노력이 요구되고 있으며 금융이나 통신 등 다른 중요 인프라 분야를 참조하여 사이버 공격 등에 관한 정보공유와 해외 연계 등을 위한 새로운 채제를 정비하는데 대한 논의가 본격화되고 있다. 또한 기밀 유지가 중요한 분야인 만큼, 기밀 유지에 충분한 조치를 강구한 후에 전력 안정 공급의 핵심을 담당하는 사업자를 중심으로 외부 전문가와 함께 각 사업자의 활동 상황을 검토하는 자리를 마련하는 등의 노력을 기울이고 있다.[86)]

(2) 조직구성

정회원과 특별회원으로 구성되어 있으나, 내부의 조직에 대해서는 정보가 없다.

정회원은 오사카가스 주식회사, 오키나와전력 주식회사. 간사이전력 주식회사, 주식회사 고베 제강소, JFE 엔지니어링 주식회사, 시코쿠전력 주식회사 외 다수가 있으며, 특별회원은 전력 광역적 운영 추진기관, KDDI 주식회사가 있다.

(3) 역할 및 책임

전력 ISAC은 안정적인 전기 공급에 중요한 역할을 담당하는 사업자 간에 신뢰와 상호 조력의 정신에 따라 사이버 보안에 대한 정보 등을 교환, 분석함으로써 미연에 사고방지, 발생한 사고에 대한 신속한 대응 등을 제공하는 역할을 담당한다. 즉, 사업자 간에 신뢰와 상호 부조의 정신에 따라 사이버 보안에 대한 정보 등을 교환, 분석함으로써 사고의

86) 전력 분야의 사이버 보안책에 대하여(電力分野における サイバーセキュリティ-策について)
http://www.meti.go.jp/committee/sougouenergy/denryoku_gas/kihonseisaku/pdf/007_06_00.pdf#search=%272015%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC%E4%BF%9D%E5%AE%89%E5%AF%BE%E7%AD%96%27

미연 방지, 발생한 사고에 대한 신속한 대응 등을 제공하는 것을 목적으로 설립되었다.

(4) 운영 방식 및 활동

사이버 보안에 대한 정보 수집, 수집한 정보 내용에 입각한 정보 분석, 수집·분석 결과의 회원 간 공유, 회원 간의 정보 공유에 따른 규칙의 책정 및 상호 협력 활동의 촉진 등의 활동을 한다.

> ※ 전력분야의 최근 활동[87]
>
> 전력 분야의 사이버 보안 강화 정책에 따라 2016년 3월 스마트미터 시스템 보안지침, 2017년 5월 전력 제어시스템 보안지침이 일본 전기기술 표준위원회(JESC)에 의해 제정되었다. 이러한 지침은 향후 전기사업법의 기술기준 및 보안규정에 포함시켜 실효성을 담보할 예정이다. 따라서 향후에는 SW안전 측면에서의 적용 유무도 파악할 필요가 있다.

6. 자동차 부문 : Auto ISAC

현재 준비 중인 ISAC이다. 2017년 4월 24일 후지이 정무관은 '산업 사이버 보안 센터' 출범 기념식에 참석하여 "사이버 공격은 큰 위협이 되고 있으며, 국토교통성 소관 분야의 사이버 보안 정보 공유 등을 실시하는 횡단적 조직" 교통 ISAC의 창설을 위한 검토를 시작하는 등 사이버 보안 강화를 위한 노력을 진행하고 있다고 말했으며 이를 바탕으로 현재 교통 ISAC을 준비하고 있다.

87) https://www.nisc.go.jp/active/kihon/pdf/csway2017.pdf#search=%27%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E5%AF%BE%E5%87%A6%E8%AA%BF%E6%95%B4%E3%82%BB%E3%83%B3%E3%82%BF%E3%83%BC%27

제3절 요약

일본은 산업도메인 전반에 CEPTOAR 기능을 갖추고 있는데 이들 중 특히 통신, 금융, 전력 부문은 ISAC 형태의 정보공유체계를 갖춘 대표적인 산업으로 알려져 있다. 이들 각각의 ISAC은 조직, 운영체계, 정보공유 방식 등에 있어 다음과 같은 특징들이 나타난다.

우선 통신 부문의 텔레콤 ISAC (Telecom-ISAC)은 회원 간의 협업을 최고의 목표로 삼고 있다. 따라서 11개의 워킹그룹과 1개의 스페셜 인터레스트 그룹을 통하여 통신 분야의 사이버 위협에 대응하는 정보를 교환하며 피해를 최소화하는데 그 역할과 책임을 다하고 있다. 또한, 기업 간 정보공유 체계 역시 이들 워킹그룹을 통하여 이루어지고 있음을 알 수 있다. 따라서 워킹그룹을 세분화하고, 기업과 기관간의 협업을 통해 정보공유를 활성화시키고 있다는 점에서 의미가 있다.

통신 부문의 또 다른 대표 ISAC으로 ICT-ISAC이 있다. ICT-ISAC은 ICT 분야 전반의 총체적 보안 확보에 기여하기 위해 ISP 사업자뿐만 아니라 방송 사업자, 소프트웨어 벤더, 정보 관련 기기 제조 사업자 등 다양한 분야로 확대하여 포괄되는 사업자들과 함께 활동하고 있다. 즉, 텔레콤ISAC만으로는 부족했던 정보 공유 체계를 극복하고자 하는 의지를 담아서 새로운 ICT-ISAC을 발족시킨 것이다. 이를 통하여 시시각각 변모하는 정보 보안의 위협에 직면한 분야의 안전한 ICT 환경을 만들고자 했다는데 큰 의미가 있다. 이와 같이 ICT-ISAC은 다양한 기업 및 단체와 협력하여 조직된 ISAC으로 정보공유 범위를 넓혔다는데 그 의의가 있다.

금융 부문의 금융ISAC (F-ISAC)은 미국의 금융 ISAC을 모델로 하였기 때문에 조직 및 운영체계 면에서 매우 흡사하며 어느 정도 체계가 갖추어져 있다. 따라서 일본의 여러 ISAC 중에서 가장 완성도가 높은 조직이다. 이를 종합하여 볼 때, 그 외의 기타 ISAC에서 금융ISAC 시스템을 원용할 가능성이 높다. 또한 금융ISAC은 정보공유체계 측면도 매우 체계화되어 있다. 특히 정회원과 준회원, 찬조회원 및 제휴회원 간의 정보 제공 범위에서 확연한 차이를 보인다. 이는 등급에 따라 양질의 정보를 제공하기 때문에 안전에 관한 정보를 제공함에 있어 신뢰를 기반으로 한다는데 의미가 있다.

마지막으로 전력 부문에는 전력 ISAC (JE-ISAC)이 있다. 전력 ISAC은 조직 및 운영체계 측면에서 아직 미흡하다. 2017년 발족하였기 때문에 향후 다른 ISAC을 참조하여 운영될 가능성이 크다. 또한 전력 ISAC은 회원 간에 정보가 공유된다고 명시하고 있으나 그 범위와 제공 내용에 대한 정보가 매우 부족한 상황이다.

<표 4-6> 일본 정보공유체계의 주요 특징

ISAC 명칭	구분	주요 특징
통신 Telecom-ISAC	조직 및 운영 체계	• 회원사 간의 협업을 최우선 목표로 하고 있음
	정보공유 체계	• 워킹그룹의 세분화를 통해 전문적 정보를 공유
통신 IT-ISAC	조직 및 운영 체계	• 텔레콤ISAC의 부족한 정보공유 체계를 극복하고자 새로이 발족
	정보공유 체계	• 정보공유체계를 다양한 기업과 단체로 범위를 확산시켰다는데 의의
금융 F-ISAC	조직 및 운영 체계	• 미국의 금융ISAC을 모델로 하였기 때문에 조직 및 운영체계는 체계를 잘 갖추고 있음
	정보공유 체계	• 회원사 간의 등급을 확실하게 구분 지었기 때문에 안전에 관한 양질의 정보를 안심하고 제공 가능
전력 JE-ISAC	조직 및 운영 체계	• 2017년에 발족한 전력ISAC은 운영체계가 제대로 갖추어지지 않은 상태이므로 향후 다른 ISAC을 참조
	정보공유 체계	• 구체적 범위와 내용 공유에 대한 정보 없이 회원 간의 정보공유

일본의 산업도메인별 보안 ISAC 정보공유 현황은 다음과 같다. 이 조사는 산업도메인별 대표 ISAC를 대상으로 하였다. 정보 공유를 위한 운영활동은 커뮤니티와 스터디 그룹 형태로 활성화 되어 있다. 정보 공유를 위해서는 미국과는 달리 시스템에 대한 정보를 찾기 어려웠으며, 이메일이나 인쇄물 형태의 공유 방법을 활용하고 있다.

<표 4-7> 일본 산업도메인별 ISAC의 정보공유 현황 비교

No	구분	해당 유형	통신		금융	전력
			Telecom-ISAC	ICT-ISAC	F-ISAC	JE-ISAC
1	법적 근거	1) 법령 근거	○	○	○	○
		2) 그 외 방법				
2	재원 조달	1) 정부				
		2) 민간				
		3) 정부 + 민간	○	○	○	○
5	운영 활동	1) 일반				
		2) 커뮤니티		○		
		3) 스터디 그룹	○		○	
		4) 표준화				
6	정보 공유 방식	1) 시스템				
		2) 이메일	○		○	
		3) 인쇄물	○		○	
		4) 온라인 토의				
		5) 워크숍(컨퍼런스)	○		○	
7	정보 공유 기술	1) 표준 규격 또는 기술	○		○	
		2) 독자 규격 또는 기술				
8	정보 공유 범위	1) 멤버십 별	○	○	○	○
		2) 정보 유형별				
		3) 운영 활동별	○			

제5장 국내 정보공유체계 현황 및 문제점

제1절 정보공유 체계 개요 및 법적 근거

1) 국내 정보공유체계 개요

우리나라의 정보공유체계는 정부 중심 또는 주도로 공공정보를 관련 기관 또는 민간 기업에 제공할 목적으로 운영하는 경우가 많으며, 특정 산업도메인 내에서 기업 간에 목적에 따른 정보공유 협의체를 구성하는 경우도 존재한다.

정부 중심의 대표적인 사례로 행정안전부에서 운영하는 '국가정보자원 개방공유체계'를 들 수 있는데 국가가 보유한 다양한 분야의 공공정보를 민간에서 다양한 목적으로 자유롭게 활용할 수 있도록 일방향으로 오픈API와 같은 방법을 통해 제공하는 형태를 띠고 있다. 환경 및 과학기술 분야의 사례인 '국가생물다양성 정보공유체계'도 유사한 형태이나 정보공유의 범위에 있어 국가 간 이루어지는 범국가적 정보공유의 형태라는 점에서 차이가 있다.

민간의 대표적인 사례로 자동차 분야의 '자동차 결함 정보공유체계'가 있다.[88] 자동차 결함 정보공유체계는 특히 대표적인 안전 산업분야의 사례로 볼 수 있는데, 자동차 관련 기업들이 자동차 결함에 의한 사고사례를 수집하고 상호 정보를 교류하는데 목적이 있어 다른 분야에 비해 활발히 운영되는 것으로 생각할 수 있다. 그러나 정보공유를 위한 기술을 적용하거나 시스템을 구축한 형태라기보다는 단순히 결함정보 중심의 수동적 수집 및 공유의 형태로 운영될 뿐만 아니라 기업의 민감한 사고사례에 대한 공유라는 부담이 크므로 내부적으로는 끊임없이 소극적 정보공유 행태를 비판하면서 정보공유 활성화에 대한 고민이 큰 것으로 보인다.

최근에는 산업도메인 전반에 걸쳐 사이버위협에 의한 위험이 극대화되고 있으며 특히 IoT(Internet of Things, 사물인터넷) 시대의 도래에 따른 영향은 매우 심각할 것으로 예상되고 있는 바, 사이버위협으로부터의 위험에 대비하기 위한 정보공유 사례를 가장 많이 찾아볼 수 있고 체계화된 경우가 많다. 대표적 사례로 과학기술정보통신부가 운영하는 C-TAS, 행정안전부가 운영하는 사이버위협 정보공유센터, 국가기반시설 보호를 위해 금융, 통신,

88) 한국 소비자원 소비자위해감시시스템 자동차결함 신고 안내, 한국소비자원과 교통안전공단에 자동차 결함 및 하자 신고 (https://www.ciss.go.kr/www/contents.do?key=65)

행정 등 분야별 기반시설의 관리기관이 운영하는 정보공유분석센터(ISAC) 등을 들 수 있다.

C-TAS는 정부주도로 한국인터넷진흥원이 정보공유시스템을 구축하고 운영하면서 정부기관, 유관기관 및 기업의 정보를 수집하고 이들에게 정보를 공유하는 양방향 체계를 갖추고 있다. 다만, 기업들 특히 보안업체들은 최신 위협정보들을 제공하는 만큼 필요한 정보를 제공받지 못한다는 부담을 토로하는 것으로 보아 정보공유 시 정보제공의 불균형 문제가 현실적 문제인 것으로 보인다. 행정안전부가 운영하는 정부기관이나 지자체를 대상으로 하는 정보공유의 형태로 운영이 되고 있다. 특히, 국가의 인프라 보호를 위하여 운영하는 분야별 ISAC은 금융, 정보통신 등 분야별 주요 기반시설을 지정하고 다양한 보호임무를 달성하도록 정보통신기반보보법 등의 법적근거를 토대로 운영되므로 가장 체계적이고 시스템화 된 경우가 많다.

따라서 국내 정보공유체계를 살펴보는데 있어 가장 체계화된 사례 즉, 기반보호 차원의 정보통신ISAC의 사례를 주요 조사·분석 대상으로 하였으며 기술측면의 정보공유체계를 파악하고자 C-TAS도 함께 분석 대상으로 하였다. 또한, 통신뿐만 아니라 금융, 의료 등 분야 ISAC운영의 공통 토대가 되는 법적 근거를 미리 살펴봄으로써 ISAC체계의 이해를 돕고자 하였다.

<표 5-1> 국내 ISAC 구축 및 운영 현황

구분	설립	운영주체	회원사	주요기능	재원조달[89]
정보통신 ISAC	'02.03	한국정보통신 진흥협회	기간통신사업자 (9개)	- 취약점 분석평가 지원 - 보호대책 수립 및 이행점검 기술지원 - 정보보호 교육·훈련 지원 - 기반보호 제도 연구 등	민간 + 정부 (회원사 회비, 사업수익 등)
금융 ISAC	'15.04	금융보안원	국내 금융부문 (18개 은행 및 22개 증권기관)	- 회원사(은행·증권) 관제 - DDoS 모니터링[90] - 보호대책 수립지원 등	민간 + 정부 (회원사 회비, 사업수익등)
행정 ISAC	'13.01	한국지역정보 개발원	시/도/지자체 (16개)	- 16개 시도 보안관제 - DDoS 모니터링 - 보호대책 수립지원 등	정부 (행안부)

자료: 정보통신ISAC 홈페이지 (http://www.isac.or.kr), 2015년 9월 현황

89) 서상기위원 외(2015), 민간 분야 사이버보안 역량 강화를 위한 인센티브 현황, 정보통신기반 보호법 일부개정법률안 검토보고서, 서상기의원 대표발의(2015.9.8./1916775)

90) DDos(Distributed Denial of Service attack), 여러 대의 공격자를 분산적으로 배치해 동시에 서비스 거부 공격을 하는 방법

2) 우리나라의 주요기반시설 보호 및 ISAC 구축·운용에 대한 법적 근거 및 배경

(1) 주요 정보통신기반시설 보호를 위한 법제 및 정책 추진 배경[91)]

주요사회기반시설의 정보통신시스템에 대한 의존도가 심화되면서 해킹・컴퓨터바이러스 등을 이용한 전자적 침해 행위가 21세기 지식기반국가의 건설을 저해하고 국가안보를 위협하는 새로운 요소로 대두됨에 따라 전자적 침해행위에 대비하여 주요정보통신기반시설을 보호하기 위한 체계적이고 종합적인 대응체계를 구축함을 목적으로 2001년 정보통신기반보호법이 제정되었다. 또한, 국가기반시설의 보호를 위해 재난 및 안전관리기본법에 근거를 두고 행정안전부를 중심으로 국가기반시설 보호정책이 시행되고 있다. 동법의 재난은 자연재해와 사고뿐만 아니라 에너지, 통신, 교통, 금융, 의료, 수도 등 국가기반체계 및 시설의 마비를 포함하고 계속적으로 관리할 필요가 있다고 인정되는 시설로 동법 제26조에서 정하는 지정관리 기준에 근거한다.

※ 정보통신기반시설의 정의(정보통신기반보호법 제2조(정의))
- “정보통신기반시설“이라 함은 국가안전보장・행정・국방・치안・금융・통신・운송・에너지 등의 업무와 관련된 전자적 제어・관리시스템 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호의 규정에 의한 정보통신망을 말함

(2) 정보공유・분석센터(ISAC)의 설립 배경

국내 정보통신기반보호를 위하여 기술 및 정보보호 정보의 지원을 담당하고 있는 공공 및 민간 지원기관은 한국인터넷진흥원(KISA), 국가보안기술연구소(NSRI), 정보공유・분석센터(ISAC), 한국침해사고대응팀협의회(CONCERT)를 대표적으로 꼽을 수 있다. 정보통신기반시설의 보호 및 관리를 위해서는 민간-민간, 공공-민간의 정보공유가 필수불가결한 요소이며, 이 같은 정보공유를 유도하기 위하여 정보통신기반보호법(제16조)에 근거를 두고, 정보공유・분석센터(ISAC: Information Sharing and Analysis Center)의 구축 및 운영이 장려되었다. 초창기 정부공유・분석센터는 통신ISAC, 금융ISAC, 코스콤ISAC, 전력ISAC의 4개의 ISAC이 설치되었다.

2004년부터 KISA내에서 정보공유분석업무를 수행해 왔던 통신ISAC은 2006년 독립 법인단체로 공식 출범하면서 통신정보공유분석협회(TISAA, Telecommunications Information

91) KISA(2013), 주요정보통신기반보호 강화 방안 마련 연구보고서, pp.7, 20, 27-29, 2013.12.

Sharing Analysis Association, 현재 한국정보통신진흥협회(KIAT, Korea Institute for Advancement of Technology)로 개명하였으며 출범과 더불어 침해사고 대응과 정보보안 체계를 강화하였다. 현재 취약점 및 침해요인과 대응방안에 관한 정보 제공, 주요정보통신기반시설에 대한 회원사 보호대책 업무 지원, 정보보호에 관한 회원사 의견수렴 및 정부 정책 제안, 국내·정보보호관련 회의 및 학술행사를 개최하는 등 회원사의 정보보호 역량 강화와 정보공유를 통한 회원사간 협력체계 유지 등과 같은 업무를 수행해 오고 있다.

(3) 정보통신기반시설 보호를 위한 분야별 근거 법률 체계

정보통신기반 보호법을 기반으로 하위 시행령, 시행규칙 및 행정규칙을 제정하여 기반시설 보호 업무를 수행하고 있으며, 세부 규정으로 동법 제16조(정보공유·분석센터)에 기반으로 ISAC을 구축·운영하고 있다.

[그림 5-1] 정보통신기반시설 보호 법률체계

자료: 국가법령정보센터 (http://www.law.go.kr/)

정보통신기반보호법 제16조(정보공유·분석센터) 는 금융·통신 등 분야별 정보통신기반시설 보호를 위한 정보공유·분석센터 구축 운영에 관한 조항이며, 정보공유·분석센터는 취약점 및 침해요인과 그 대응방안에 관한 정보 제공하고, 침해사고가 발생하는 경우 실시간 경보분석체계 운영하는 업무를 하도록 규정한다.

제2절 분야별 정보공유체계

1. 정보통신 ISAC(Information Sharing and Analysis Centers)[92]

<표 5-2> 정보통신 ISAC의 정보공유 현황 및 특징 요약

No	구분	해당 유형		현황 및 특징
1	관련 분야	1) 일반 분야		
		2) 보안 분야	O	통신분야 사이버테러 및 침해사고 시 공동대응, 정보공유 통한 예방활동 통한 민간분야 공동 대응체계 확립 규정
		3) SW안전 분야		
2	법적 근거	1) 법령 근거	O	정보통신기반보호법 제16조(정보공유·분석센터)
		2) 그 외 방법		
3	재원 조달	1) 정부		
		2) 민간		
		3) 정부 + 민간	O	정보통신ISAC(정부중심), 정보통신ISAC협의회(과학기술정보통신부과학부 소관 사업자 등 민간)
4	조직 형태	1) 일반 정보공유체계		
		2) 산업도메인별 대표 ISAC	O	정보통신기반시설 중 통신분야 대표ISAC
		3) 기관 또는 기업의 자체 ISAC		
5	운영 활동	1) 일반	O	보안기술 자문, 교육 및 컨설팅, 캠페인
		2) 커뮤니티	O	협력체계, 예·경보활동, 해외ISAC 기관 교류
		3) 스터디 그룹		
		4) 표준화		
6	정보 공유 방식	1) 시스템	O	최신이슈 및 긴급경보 대응방안 공유
		2) 이메일	O	최신이슈 및 긴급경보 대응방안 공유
		3) 인쇄물	O	최신 보안이슈 및 국내외 동향 뉴스레터
		4) 온라인 토의		
		5) 워크숍(컨퍼런스)	O	회원사 워크샵
7	정보 공유 기술	1) 표준 규격 또는 기술	O	
		2) 독자 규격 또는 기술		
8	정보 공유	1) 멤버십 별		
		2) 정보 유형별		

92) (http://www.isac.or.kr)

No	구분	해당 유형		현황 및 특징
	범위	3) 운영 활동별	O	8개 정보통신ISAC 협의회 기존 회원사 기타 협의회 통한 회원가입 후 회원 간 공유

국내 정보공유체계 중 최초로 구성되어 체계적으로 운영되는 정보통신 ISAC에 대해 조사한다.

1) 조직 및 운영 체계

(1) 법적 근거 및 관련 제도

가) 정보통신기반보호법 제16조(정보공유・분석센터)

※ 금융・통신 등 분야별 정보통신기반시설을 보호하기 위하여 정보공유・분석센터 구축 운영

나) 정보통신ISAC 설립 구축통지서(미래부 통지: 2013.1.30.)

통신 분야 사이버테러 및 침해사고 시 공동대응, 정보공유를 통한 예방 활동을 통해 민간분야 공동 대응체계를 확립하도록 규정하고 2002년 1월부터 정보통신ISAC 구축・운영

(2) 조직 구성

정보통신 ISAC은 과학기술정보통신부를 중앙행정기관으로 하여 하위의 정보통신인증센터에 속한 조직의 형태로 구성되며, 기반시설 정보보호, 취약점 분석평가, ISMS 인증, 연구 및 사업, 협의회 운영 등의 역할을 담당하고 있다.

또한 과학기술정보통신부 소관 사업자에 대한 자율적인 사이터테러 예방활동 강화 방안으로 정보통신ISAC협의회를 운영함으로써 민간차원의 회원 가입 권고 및 지속적인 회원 확대를 지원하고 있다.

[그림 5-2] 정보통신 ISAC 조직도

자료: http://www.isac.or.kr/ Home > 정보통신 ISAC > 조직구성

(3) 역할 및 책임

가) 기반시설 정보보호

통신, 금융, 전력 등 국가의 안전에 중대한 영향을 미치는 핵심 정보통신 시설을 정보통신기반보호법에 의해 지정하고 특별 관리하고 있다. 각 중앙행정기관은 매년 소관시설에 대한 취약점 분석평가 및 보호대책 수립 · 추진을 담당하고, 과학기술정보통신부와 국가정보원은 이행점검 등 총괄기능을 수행한다.

나) 취약점 분석평가

주요정보통신기반시설에 대한 경제적이고 실효성 있는 보호대책을 수립하는데 필요한 정보를 제공하며, 동 대책에 기초한 효과적인 분야별 주요 정보통신기반시설 보호계획 수립의 근거를 제공한다. 주요정보통신기반시설의 관리기관이 직접 수행할 경우 자체 전담반을 구성하여 운영하며, 관리기관이 외부기관에게 위탁할 경우, ISAC 및 지식정보보안 컨설팅전문업체 등 전문기관에 위탁 수행한다.

※ 「정보통신기반보호법」제8조에 의하여 지정된 주요정보통신기반시설 관리기관의 장은 동법 제9조와 동법시행령 제17조 내지 제19조에 따라 소관시설에 대한 취약점을 분석 · 평가

※ 전문기관 : 정보공유·분석센터(ISAC), 한국인터넷진흥원, 한국전자통신연구원, 지식정보보안컨설팅전문업체 등(정보통신기반 보호법 제9조)

다) ISMS인증

정보보호 관리체계(ISMS) 인증제도란, 어떤 조직이 정보보호 관리체계를 구축·운영하고 있을 때, 그 관리체계가 법에서 정한 인증기준에 적합한지를 인증기관이 객관적이고 독립적으로 평가하여 적합성 여부를 판단해 주는 제도이다.

※ 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 및 시행령」 제47조

- 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 정보보호 관리체계를 수립·운영하고 있는 자에 대하여 제3항에 따른 기준에 적합한지에 관하여 인증업무를 수행한다.

※ 정보보호관리체계 인증 등에 관한 고시(미래창조과학부고시 제2013-36호, 제2016-59호)

라) 정보보호 준비도 평가

정보보호 준비도 평가제도란, 기업의 통합적인 정보보호 수준을 향상시키기 위하여 정보보호 준비도 수준을 자율적으로 진단 및 평가받을 수 있는 제도이다. 정보보호 준비도 평가 등급을 해당 기업 전체 등급으로 부여하여 이용자에게는 기업 선택의 기준을 제공하고, 정보보호 활성화 및 투자확대를 유도한다. 대기업뿐만 아니라 영세·중소기업 및 비 IT분야 등 모든 기업이정보보호 준비도 평가를 받도록 유도하여 정보보호 인식 강화 및 저변 확대, 보안 사각 지대를 해소하고자 한다. 또한, 정보보호 수준의 향상, 정보보호 분야 투자 확대, 최선의 보안 정책 등 정보보호 준비도 평가 모델 및 체계를 제시한다.

마) 정보통신ISAC협의회 운영

과학기술정보통신부는 관련법 및 3.20 사이버 침해사고 등 급격히 증가하고 있는 각종 사이버공격에 대비하여 과학기술정보통신부 소관 사업자에 대한 사이버테러 예방활동 강화 방안으로 정보통신 ISAC 협의회를 통한 회원가입 권고 및 지속적인 회원 확대를 지원하고 있다.

(4) 운영 방식 및 활동

정보통신 ISAC은 과학기술정보통신부 소관 사업자에 대한 사이버테러 예방활동 강화 차원에서 정보통신ISAC 협의회를 운영하고 있으며 8개의 기존 회원사[93] 외에도 협의회를 통한 회원가입을 권고하면서 지속적인 회원 확대를 지원하고 있다. 정보통신ISAC 협의회의 가입대상은 과학기술정보통신부 소관 기간통신, IDC, VoIP, SO, MVNO 사업자 등과 정보보호 관련 학계, 연구계(출연연 포함), 정부 등 관련 기관이다.

정보통신ISAC 협의회의 운영활동은 협력체계, 예·경보 활동, 보안기술 자문, 교육 및 컨설팅, 캠페인 전개, 해외ISAC 기관과의 국제교류 등의 활동을 주로 수행한다. 협력체계 내의 주요활동은 사이버위협 공동 대응을 위한 민·관 협력 체계 구축을 위해 핫라인 구축, 보안관련 사고발생 경험 및 대응사례 정보공유를 통한 회원 간 협력체계 마련 등이다. 분야별 정보보호담당자의 실질적 의견수렴을 통해 현장 애로사항 파악하며, 보안문화 형성을 위한 홍보 및 캠페인 전개한다. 해외 ISAC 기관과 정기적인 교류를 통해 정보보호 협력을 강화하고 ISAC 활성화를 도모하며, 최신 정보보호관련 기술동향을 파악한다.

93) KT, SK브로드밴드, LG유플러스, SK텔레콤, SK텔링크, 드림라인, 세종텔레콤, 롯데정보통신

2. C-TAS(Cyber Threats Analysis & Sharing System)[94][95]

정보공유 및 활용 활동을 활발하게 하고 있는 C-TAS 에 대해 조사한다.

1) 조직 및 운영 체계

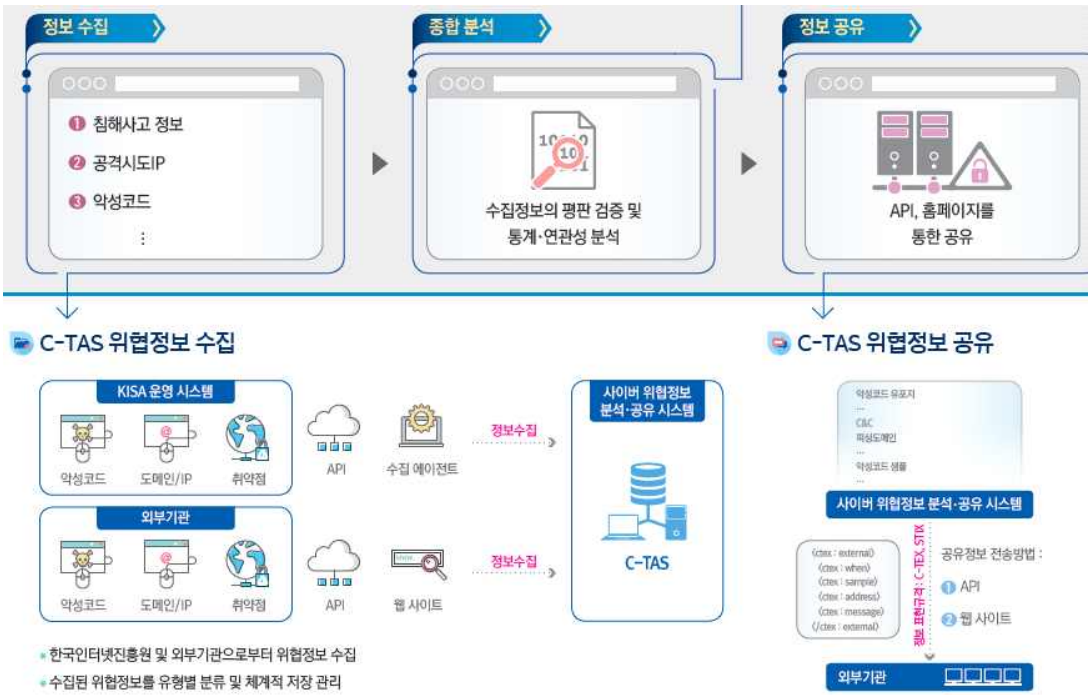
(1) 설립 배경 및 목적

C-TAS는 사이버위협 정보(악성코드, 명령과 제어(Command& Control, C&C) 서버, 악성코드 유포지, 취약점 및 침해사고 분석정보 등)를 체계적으로 수집해 관계기관 간 자동화한 정보공유를 목적으로 하는 예방·대응 시스템이다. 이는 여러 산업분야에 걸쳐 광범위하게 발생하고 있는 침해 사고에 대응하기 위하여 사이버 위협정보에 대한 실질적인 공유체계 필요에 의해 2014년 8월부터 본격적으로 가동 되었다.

(2) 구성 및 운영방식

C-TAS 시스템은 다음과 같이 정보수집, 종합분석, 정보공유의 3단계로 구성된다.

[그림 5-3] 구성 및 운영방식



자료 : 한국인터넷진흥원, 사이버위협정보 분석·공유시스템 리플렛

94) (https://cshare.krcert.or.kr:8443)
95) KISA(2015), "C-TAS System & CTEX", 사이버 침해사고 정보공유 세미나

정보 수집 및 종합분석을 통하여 각 위협 정보를 실시간으로 공유하기 위해, 실시간 자동 공유(양방향 정보공유)가 가능한 오픈 API 방식 및 홈페이지에 접속하여 정보를 다운로드 받는 방식을 제공하며, 권한 관리·접근통제를 기반으로 기관별 정보 공유 대상 및 범위를 차등 제공한다.

위협 정보는 12개 KISA 내부 운영 시스템 및 외부기관으로부터 수집하여, ‘C-TEX’라는 XML형식의 사이버 위협 정보로 저장한다. ‘C-TEX’는 사이버 위협 정보를 W3C XML 기반의 개방형 언어를 사용하여 6가지 침해사고 정보, 침해사고(IML), 도메인/IP(HML), 악성코드(SML), 취약점(VML), 공격자(AML) 정보, 수집정보(CML)를 저장한다.[96]

[그림 5-4] C-TAS 위협정보 수집 및 저장

자료 : 한인혜(2014), 사이버 위협정보 분석·공유시스템 공유체계, 사이버 침해사고 정보공유 세미나

2) 정보공유 체계

(1) 정보공유 정책 및 절차

기여기반 정보 공유를 통해 수집 정보를 확대하는 정책으로, 원칙적으로 위협정보를 제공하는 기관에게 정보를 공유한다. 정보 제공 업체가 정보 제공 항목 및 공유 범위를 결정하고, 권한관리 및 접근통제를 통해 회원별 정보 공유 대상 및 범위를 차등한다.

정보 공유는 다음과 같은 절차로 수행된다.

① CTAS 정보공유시스템 가입안내(cshare.krcert.or.kr) 및 공유정보 요청

96) 김종현(2017), 인공지능 기반 금융권 보안관제 동향 및 향후과제, 전자금융과 금융보안 (제8호, 2017-04)
자세한 사항은 ‘제6장 국내외 정보공유 규격 및 표준‘ 참조

② 공유 규격 및 방법 협의하여 C-TEX 형식 결정

③ 공유 정보 자동 수집을 위한 API(Application Programming Interface) 구현

④ 위협정보 공유시작

[그림 5-5] C-TAS 위협정보 공유절차

자료 : 한인혜(2014), 사이버 위협정보 분석·공유시스템 공유체계, 사이버 침해사고 정보공유 세미나

(2) 정보공유 목록 및 범위

공유대상으로 위협 도메인, 사이버사기 도메인, 악성파일, 취약점, 보고서 등 5개 그룹에 속하는 36종 정보를 외부기관에 공유하며, 이메일 악성코드 등 사이버 위협정보 수집·공유 항목으로 확대 추진 중이다. 상호 정보제공을 위하여 공공, 백신, 쇼핑, 포털 관제 업체로부터 악성 코드 유포지, C&C 도메인, 악성코드 샘플 등의 위협정보를 수집하고 이를 공유한다. 수집된 정보는 사고 요인간 연관성 분석 후 C-TAS를 통해 실시간으로 공유된다. 보안 사고의 특성상 실시간성이 중요시 된다.

[그림 5-6] 수집된 위협정보의 실시간 공유

자료 : 한인혜, 사이버 위협정보 분석·공유시스템 공유체계, 사이버 침해사고 정보공유 세미나

(3) 정보공유 활용[97]

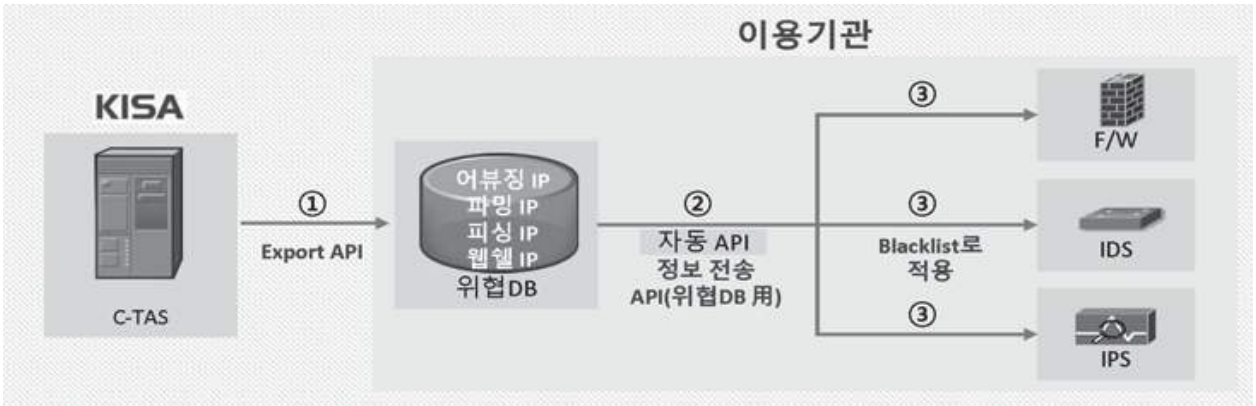
공유한 정보를 활용하는 첫 번째 사례는 보안서비스 기업이 C-TAS를 활용하여 악성코드에 대응하고 차단(Vaccine)하는 것이다. 보안서비스 기업은 C-TAS에서 사내 위협DB로 악성코드 정보를 수신하고 이를 통해 내부 백신데이터로 활용함으로써 악성코드 탐지를 강화할 수 있다.

[그림 5-7] 공유 정보를 백신으로 활용한 사례

자료 : 김태형(2016), 사이버 위협정보 분석공유 시스템 활용방안,
사이버침해사고 정보공유 세미나 자료집(2016.4분기)

두 번째 사례로는 전 산업군에 C-TAS를 활용해서 위협IP 차단 Blacklist를 적용한 것을 들 수 있다. 기업들은 C-TAS에서 전송되는 위협정보를 사내 위협DB로 수신하여 자동 등록함으로써 사내 보안장비의 위협 차단정보로 활용할 수 있다.

[그림 5-8] C-TAS to Security Solution 사례



자료 : 김태형(2016), 사이버 위협정보 분석공유 시스템 활용방안,
사이버침해사고 정보공유 세미나 자료집(2016.4분기)

97) KISA(2016), 사이버침해사고 정보공유 세미나 자료집(2016.4분기), PP.81-83,2016.12.

3) 정보공유 규격 : C-TEX(Cyber Threat EXpression)

2015년 5월, 사이버 위협을 신속히 차단하여 피해를 최소화하는 등 효과적으로 대처할 수 있도록 공공·민간이 함께 사이버위협정보를 공유·분석하는 등 협력을 활성화하여 위협을 조기 탐지·전파할 수 있는 체계를 구축할 목적으로 '사이버위협정보공유에 관한 법률안'이 발의되었다. 이에 따라 한국인터넷진흥원(KISA)은 2014년 8월 C-TAS(Cyber Threat Analysis & Sharing)을 구축하였다.

C-TAS는 정보공유 참여기관들이 수집한 악성코드와 각종 사이버 위협 정보를 분석·공유하는 시스템으로 美의 사이버정보위협 정보공유 규격인 STIX(Structured Threat Information eXpression)를 참조하여 C-TEX라는 정보표현 방식과 전송 규격을 정의하게 되었다. 현재 포털, 쇼핑몰, 게임사, 보안 기업 등 약 100여개의 민간기업이 사이버위협정보를 실시간으로 공유 활용 중이다.[98]

[그림 5-9] 사이버위협정보 분석공유시스템(C-TAX) 3단계 구조

자료: KISA(2015), C-TAS System & CTEX, 사이버 침해사고 정보공유 세미나 자료집, pp.14

C-TEX는 W3C XML 기반의 개방형 마크업 언어로서 사이버 위협(Cyber Threat) 정보를 표현하기 위한 규격으로 사이버 위협 및 침해사고 정보를 체계적으로 관리 및 분석할 수 있는 데이터 아키텍처의 필요성에 따라 개발되었다.

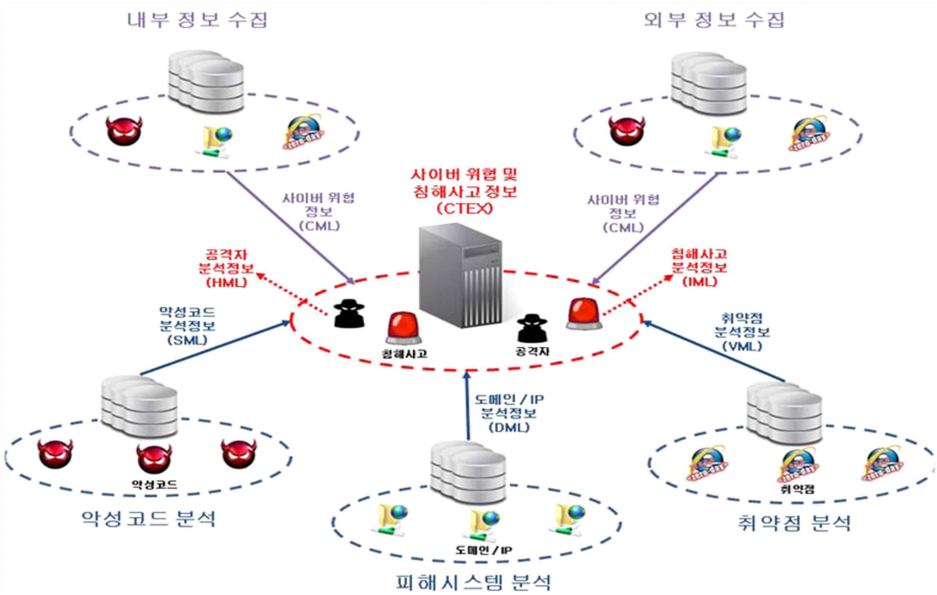
98) KISA(2015), C-TAS System & CTEX, 사이버 침해사고 정보공유 세미나 자료집, pp.13-21, 2015.3.

4) C-TEX의 구조 및 기능

C-TEX는 정보공유를 위한 사이버 위협 및 침해사고 정보를 6가지로 분류하여 구성한다.

- 사이버 위협 정보: 도메인/IP(Address), 악성코드(Sample), 취약점(Vulnerability), 수집정보(CML)
- 침해사고 정보: 침해사고(IML), 도메인/IP(HML), 악성코드(SML), 취약점(VML), 공격자(AML) 정보

[그림 5-10] C-TEX 구조



자료: KISA(2015), C-TAS System & CTEX, 사이버 침해사고 정보공유 세미나 자료집, pp.16

분류한 6가지 정보 유형들 간의 링크(IoX, Internet of eXpressions)를 설계하고 의미를 규정함으로써 상호 정보간의 관계 내에서 정보가 공유되고 분석되도록 한다.

공격자는 침해사고에 대한 링크 관리, 참해사고는 도메인/IP, 악성코드, 취약점에 대한 링크 관리를 위한 정보이며, 또한 도메인/IP, 악성코드, 취약점, 공격자는 상호 간의 행위(Action)을 관리하기 위한 것으로 정의한다.

[그림 5-11] C-TEX 정보 간의 관계

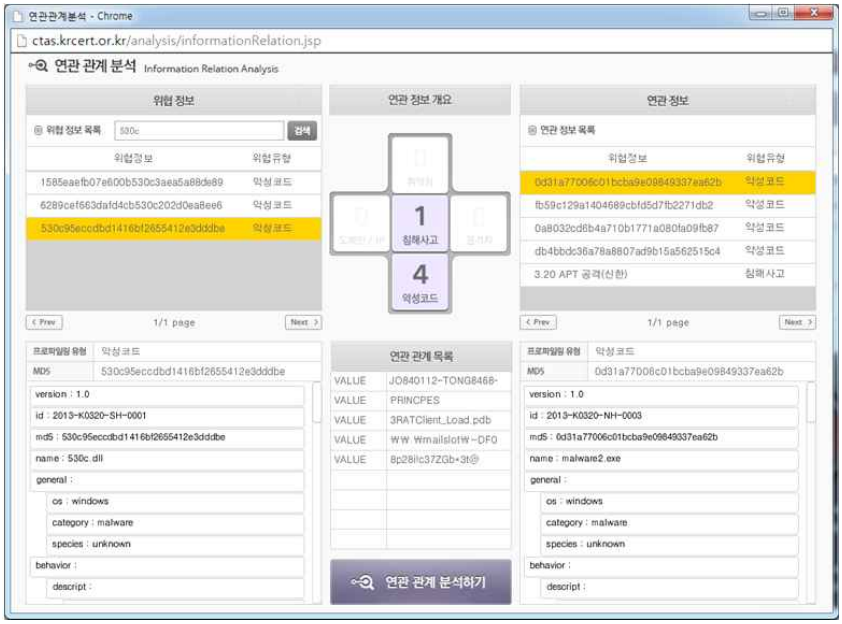
자료: KISA(2015), C-TAS System & CTEX, 사이버 침해사고 정보공유 세미나 자료집, pp.17

C-TEX의 기능은 정보를 생성하고, 정보 연관 관계를 검색하는 것이다.

사이버 위협 및 침해사고 정보를 저장하고 관리하는 기능을 수행한다. 즉, 사이버 위협 및 침해사고 정보를 수집분석 시스템들로부터 도메인/IP, 악성코드, 취약점 정보를 수집하고, 침해사고 분석시스템들로부터 침해사고, 도메인IP, 취약점, 공격자 분석정보를 수집한다.

사이버 위협 및 침해사고 정보의 연관관계를 검색하는 기능을 수행한다. 즉, 신규 유입된 사이버 위협정보에 대해서 기존 사이버 위협 및 침해사고 정보와의 연관관계 검색을 수행하고, 침해사고, 도메인, 악성코드, 취약점, 공격자 간의 연관관계를 파악한다.

[그림 5-12] C-TEX 연관관계 분석 기능



자료: KISA(2015), C-TAS System & CTEX, 사이버 침해사고 정보공유 세미나 자료집, pp.18

제3절 문제점

제4차 산업혁명으로 인해 각 산업분야에 소프트웨어 활용이 늘어나고 있으며, 소프트웨어 오류로 인한 사고의 위험성이 커지고 있다. 사고의 원인 중의 하나로 SW오류를 고려하지 않을 수 없으며, SW 오류는 어느 도메인에서나 동일한 원인으로 일어나게 된다. 사고를 일으키는 전체 매카니즘은 도메인에 귀속되어 있으나 SW 자체의 속성은 동일하여, 소프트웨어 안전 보장을 위한 한 방안으로 SW안전정보 공유와 활용을 검토하였다.

SW 안전 정보공유에 대한 다음과 같은 세 가지 문제점을 도출하였다.

첫째, 국내는 정보공유의 대한 필요성보다는 부작용에 대한 인식이 강하다. 기업들이 정보공유를 해서 얻는 기술적, 재정적 이익보다는 정보 유출에 대한 우려가 강하다.[99] 사이버보안의 경우 역설적으로 정보 유출을 막기 위해 위험정보에 대한 정보 공유를 하는 현상이 있으나, SW 안전 측면에서는 그에 대한 필요성이 인식되고 있지는 않다. SW 안전 측면에서는 사이버보안 측면보다는 사고 발생 빈도나 범위 측면에서 아직은 미약하다고 보는 견해가 지배적이나, 제4차 산업혁명으로 인해 SW에 위한 사고 우려가 커지고 있는 상황에 대한 인식을 높아지고 있다.

둘째, 국내 SW안전 분야의 정보공유는 SW안전 표준이나 사고예방을 위한 관련 사고사례 정보공유 등 부분적인 정보공유에 그치는 경우가 많다. 그 형태도 관련 기업의 활동 조사를 통해 일부 기업들이 사고사례를 수집하고 일정 범위에서 한정적으로 제공하고 있다. 그 사례로 2장에서 자동차 분야의 ‘자동차 결함 정보공유체계’를 소개하였다. 또한 각 산업 분야의 생산자 관점에서 SW안전을 설계나 기능문제로 다루고 있긴 하지만 HW안전에 비해 SW안전이 차지하는 비중이 작아 HW안전에 포함시켜 다룰 뿐 SW안전 자체를 독립적인 영역으로 취급하지 않는다. 즉 각 도메인에 포함된 정보공유체계에 SW안전 관련 정보가 포함되어 자료로 찾아보기 어려운 현상으로 나타날 수 있다. 법적으로 보장되고 체계적으로 구축된 ISAC의 대부분은 SW안전보다는 사이버 위협이나 보안 문제, 또는 이를 해결하기 위한 대응책 등에 공유의 초점이 맞추어져 있다. SW안전과 직접적으로 관련된 ISAC은 거의 찾아볼 수 없으며, 대부분의 ISAC에서 공유정보의 하나인 보안 취약점과 관련하여 취약점 발생 원인을 SW안전과 연관 지어 도출하고 있다고 짐작할 뿐이다.

셋째 국내의 경우 미국이나 일본에 비해 분야별 정보공유체계(ISAC)가 다소 미약하다. 미국의 경우는 통신, 항공, 의료, 자동차, 국방 , 소매 등 거의 모든 분야의 국가기반시설

99) KISA(2013), 주요정보통신기반보호 강화 방안 마련, pp.31-32, 2013.12.

보호를 위한 법률이나 행정명령을 통해 정보공유체계를 구성하고 있으며, 일본의 경우도 센터로 시작하여 정보공유 활동이 활성화되어 있으며, 최근 강력한 사이버안보관련 법을 제정하고 정보공유체계의 구축과 활성화 의지를 보이고 있다. 우리나라의 경우는 정보보안 측면에서는 정보공유에 대한 법적 근거를 마련하고, 정보공유체계를 마련하고 있으나, 총제적인 안전 측면의 정보공유 활동은 아직 부족하다. ISAC의 구축도 통신, 금융, 행정의 3개 분야로 그치고 있다. 물론 정부도 ISAC 확대에 대한 의지는 표명하고 점차 ISAC을 늘려가는 계획을 세우고 있다.[100]

100) 보안뉴스 (2015), 의료분야 보안위협 위험수위…ISAC 추진 탄력 받나?, 2015.8.25. http://www.boannews.com/media/view.asp?idx=47534

제6장 정보공유체계 활성화 정책 및 시사점

지금까지 국내외 정보공유체계에 대해 조사, 분석하고, SW안전 정보공유 현황에 대해 검토하였다. 조사결과 국가기반 시설 등 안전이 중요한 시설의 정보보안 측면의 정보공유는 비교적 체계적으로 시행되고 있으나, SW 안전에 대한 정보는 SW 안전 표준, 사고 정보 등 부분적으로만 공유되어 있음을 확인하였다.

그간의 정보공유 활성화 정책에 대해 검토하고, SW 안전 정보공유체계를 구축하고 활성화 하는 정책 마련을 위한 시사점을 도출하고자 한다.

제1절 정보공유 활성화 정책

1. 국외 정보공유체계 활성화 정책 및 사례

미국과 유럽은 주로 사이버보안 강화 차원에서 활성화 정책이 조사된 바 있다. 특히 미국(2013.8월)과 유럽(2010.6월) 등 선진국들은 정보공유 프로그램 참여 기업에 대한 보조금 지원 등 기업들의 자발적 참여를 유도 할 수 있는 다양한 인센티브 정책을 추진하고 있다.

1) 미국

(1) 인센티브 관련 정책

국토안보부, 상무부, 재무부는 행정명령(E13636)에 명시된 바에 따라 인센티브 방안에 대한 보고서를 제출하였고 이를 토대로 미국 국립기술표준원(NIST, National Institute of Standards and Technology)은 예비 사이버보안 프레임워크를 개발하였다. 2013년 8월 대통령 및 사이버보안 조정관 특별보좌관인 마이클 다니엘(Michael Daniel)은 백악관 블로그에서 3개 부처의 보고서를 바탕으로 인센티브 영역을 다음과 같이 압축했다.[101)102)]

101) 서상기 외(2015), “민간분야 사이버보안 역량 강화를 위한 인센티브 현황”, 정보통신기반 보호법 일부개정법률안 검토보고서 - 서상기의원 대표발의(2015.09.08.)
102) KISA(2013), 주요정보통신기반보호 강화 방안 마련, 2013.12., pp.49-61, 133-134

8개 인센티브는 ①사이버보안 보험, ②보조금(grant), ③정책 대상으로서 선호(Process Preference), ④책임 한정, ⑤규제 합리화, ⑥대중의 인정, ⑦가격규제산업에 대한 요율회복제, ⑧사이버보안 연구 등이며 세부 내용은 다음과 같다.

① 사이버보안 보험에 대해서는 상무부의 국립표준기술원은 프레임워크와 관련해 보험업계를 포함하는 조치를 취하고 있다. ③ 정책 대상으로서 선호(Process Preference)는 자발적 프로그램 참여에 대한 내용이다. ④ 프로그램 참여자들에 대한 책임을 경감하는 법의 제정은 위법행위 관련 책임 경감, 한정배상보장, 입증 부담 경감, 공시 요건을 사전에 취득할 수 있는 법적 특권 등의 영역에서 필요하다. ⑤ 프레임워크와 자발적 프로그램이 기존의 규제 구조와 효과적인 방법으로 상호작용할 수 있도록 규제를 합리화해야 한다. 프레임워크와 자발적 프로그램이 개발되면 각 부처들은 기존 법·규제의 중복 제거, 감사부담 완화 등 프레임워크 준수를 보다 용이하게 할 수 있는 영역들을 지적해야 한다.

가) 국토안보부[103]

2013년 6월 제출된 국토안보부 인센티브 연구분석 보고서에서는 총 10개의 인센티브 수단을 검토하고 효과성(effectiveness), 효율성(efficiency), 경제적 부담(equity)으로 나누어 평가하였다. 10개 인센티브 항목은 ①보조금(Grants), ②가격 규제 산업에 대한 요율회복제(Rate-Recovery for Price-Regulated Industries), ③결합보험요건(Bundled Insurance Requirements), 책임 경감(Liability Protections), 법적 베네핏(Legal Benefits), ④우선적 기술지원(Prioritized Technical Assistance), ⑤정부구매 고려(Procurement Consideration), ⑥대중의 인정(Public Recognition), ⑦보안 공시(Security Disclosure), ⑧정보 보안 규정의 합리화(Steamline Information Security Regulations), ⑨보조금(Subsidies) 사이버보안 제품 및 서비스의 직접 구매를 위한 자금 제공이나 저리 대출을 의미, ⑩세금혜택(Tax Incetives)이다.

※ (참고) 국토안보부의 프레임워크 채택을 위한 인센티브 수단 평가

o 효과성 항목에서는 비용분담(Cost Sharing)을 통해 사이버보안 비용의 한계증가를 최소화시키는 인센티브 수단으로 보조금(Grants), 가격 규제 산업에 대한 요율회복제, 보조금(Subsidies), 세금혜택 등이 효과를 가지는 것으로 평가

o 경제적 부담 항목에서는 정부나 납세자가 요율회복제, 우선적 기술지원, 정부구매 우선적 고려, 정보 보안 규정 합리화 등에서 비용이 전혀 발생하지 않거나 최소한만 발생하기 때문에 인센티브가 부여될 것으로 판단되며, 이와 마찬가지로 산업계에서는 보조금(Grants), 요율회복제, 보조금(Subsidies), 세금혜택에서, 소비자는 보조금(Grants), 우선적 기술지원, 대중의 인정, 정보 보안 규정의 합리화, 보조금(Subsidies), 세금혜택에서 인센티브가 부여될 것으로 판단

103) Department of Homeland Security Integrated Task Force, Incentives Study Analytic Report(2013.6)

o 효과성 및 효율성, 프라임워크 채택시 정부의 부담을 기준으로 놓고 시행한 통합적 분석에서는 보조금이 효과성과 효율성은 크나 정부의 부담이 크고, 가격규제산업을 위한 요율회복제는 효과성과 효율성이 크고 정부의 부담도 적은 수단으로 평가

국토안보부는 인센티브관련 워크샵을 개최하고 다음과 같이 규제대상 업계로부터 전문가를 참여시켜 정보공유 인센티브 등에 대한 질의응답을 실시하였다. “정보공유에 대한 인센티브는 무엇인가?” 라는 질문에 대한 다음과 같은 의미 있는 답변이 도출되었다.[104)]

“많은 업체들은 규제당국이 업체 자발적으로 제공한 정보를 오용하지 않을까 하는 우려를 갖고 있음. 따라서 정보공유와 관련된 법적 책임 면제를 시행할 경우 정보공유가 활성화될 것으로 판단됨”, Karl Schimmeck (Financial Services)

“경영자들을 대상으로 한 사이버 보안 교육, 근로자 교육, 시스템적 접근방법 등을 통해 유틸리티 업체의 문화 자체를 바꿔야 함.”, Miles Keogh (National Association of Regulatory Utility Commissioners, NARUC)

“프레임워크에 정보공유자들을 위한 안전피난처(safe-harbor) 조항이 있는지 궁금함.”, Anna Cochran (Federal Energy Regulatory Commission, FERC)

나) 재무부[105)106)]

재무부는 ①정보 공유를 위한 정보 활용 역량을 강화, ②책임 위험을 명확히 제시, ③사이버보안 기초연구 장려를 위해 정부자금 제공, ④기술 지원 제공, ⑤보안심사 프로세스 가속화, ⑥세금혜택, ⑦사이버보험 등 7개 사항을 검토하고, 이들 중 세금혜택과 사이버보험은 권고하지 않는 것으로 결론을 내렸다.

※ (참고) 재무부가 검토한 인센티브 사항

① 정보 공유를 위한 정보 활용 역량을 강화: 정부와 민간 부문간 실시간 정보 흐름을 개선하고 증대하기 위해서는 중요기반 관련 기관 및 민간기업으로 하여금 사이버보안 관행을 강화할 수 있는 방안을 마련하고 활성화

② 책임 위험 경감 : 사이버보안 준수와 자발적 프로그램 참여가 책임을 경감

⑥ 세금혜택 : 세금공제 또는 가속상각공제 등의 세금혜택이 추가적인 사이버보안 연구와 중요기반 투자를 장려. 세금혜택을 시행하기 위해서는 정부의 이전 세수를 사용하거나 기존의 재정을 재할당 필요.

104) KISA(2013), 주요정보통신기반보호 강화 방안 마련, 2013.12. , pp.129-134

105) Department of Treasury(2013), Treasury Department Summary Report the President on Cybersecurity Incentives Pursuant Executive Order 13636

106) Department of Treasury(2013), Treasury Department Report the President on Cybersecurity Incentives Pursuant Executive Order 13636

⑦ 사이버보험: 사이버보험은 보험사들의 보안 최소 기준 설립, 사이버 위협 모니터링, 정보수집 품질 개선 등에 강력한 재정적 인센티브를 제공하기 때문에, 주요기반 보험계약자들의 사이버보안을 강화할 수 있는 방안. 그러나 사이버보험은 아직 성장하고 있는 초기단계의 산업으로 정부가 직접 참여할 필요가 없으며, 정부의 참여로 민간시장의 발전을 저해.

다) 상무부[107][108]

상무부는 ①보험회사들을 프레임워크 수립에 참여시키는 방안, ②불법행위 책임에 대한 연구, ③국가사이버인증전략 시범 보조금 사업 및 상무부 보조금 사업 시행에 대한 하나의 기준으로서 자발적 중요기반 사이버보안 프로그램에 참여시키는 방안, ④프레임워크 준수 및 연방 보조금 프로그램 참여와 관련해 연방기관들에 안내서를 제공, ⑤실제적으로 부딪힐 과제들을 극복하기 위해 자발적 중요기반 사이버보안 프로그램을 연구개발 노력과 연계, ⑥규제합리화 대상을 규명, ⑦사이버보안을 위한 신속 특허(Fast-Track Patent) 시범사업을 모색, ⑧정부구매 고려(government procurement considerations)에 대한 연구, ⑨세금혜택, ⑩선택적 대중의 인정 프로그램 개발을 연구, ⑪특정형태의 기술지원 제공 모색, ⑫신속보안심사(expedited security clearance) 등 총 12개의 사항에 대해 검토하고, 이들 중 세금혜택과 신속보안심사는 권고하지 않는 것으로 결론을 내렸다.

※ (참고) 국토안보부의 프레임워크 채택을 위한 인센티브 수단 평가

① 보험회사들을 프레임워크 수립에 참여시키는 방안: 국립표준기술원은 프레임워크의 기초를 이룰 기준, 절차 등의 유용성과 효과성을 개발하는데 보험업계를 포함한 이해관계자들을 참여

② 불법행위 책임에 대한 연구: 일단 자발적 프로그램이 개발된 후 법적, 재정적 위험과, 이러한 위험들이 사업자들의 자발적 프로그램 참여를 촉진할 것인지 아니면 저해할 것인지에 대해 연구할 필요

③ 자발적 중요기반 사이버보안 프로그램의 참여를 국가사이버인증전략 보조금 시범사업 및 상무부 보조금 사업 시행에 있어 하나의 기준으로 적용하는 방안 : 국립표준기술원은 국토안보부와 협력해 보조금 지급 평가기준을 일관성 있게 적용할 수 있도록 해야 함. 또한 상무부는 중요인프라 개발 보조금과 관련해 프레임워크 채택 및 자발적 프로그램 참여 여부를 기준으로 적용할지 검토

④ 규제합리화 대상을 규명: 국립표준기술원과 국토안보부는 프레임워크와 자발적 프로그램이 기존의 규제 구조와 효과적인 방법으로 상호작용할 수 있도록 해야 함

⑤ 선택적(optional) 대중의 인정 프로그램 개발을 연구: 상무부는 많은 중요기반 사업자/기업/기관들이 자발적 프로그램이 가지고 있는 '대중의 인정' 요소에 관심을 보일 것이라고 생각

107) Department of Commerce(2013), RECOMMENDATIONS THE PRESIDENT ON INCENTIVES FOR CRITICAL INFRASTRUCTURE OWNERS AND OPERATORS JOIN A VOLUNTARY CYBERSECURITY PROGRAM

108) Department of Commerce(2013), Discussion of Recommendations the President on Incentives for Critical Infrastructure Owners and Operators Join a Voluntary Cybersecurity Program

라) 요약

각 부처에서 제시한 인센티브 항목과 최종 결정된 인센티브 항목은 다음과 같다.

<표 6-1> 국토안보부, 상무부, 재무부, 최종 인센티브 항목

No	최종	국토안보부	재무부	상무부
1	보조금(grant)	보조금	사이버보안 기초연구 장려를 위해 정부자금 제공	국가사이버인증전략 시범 보조금 사업 및 상무부 보조금 사업 시행에 대한 하나의 기준으로서 자발적 중요기반 사이버보안 프로그램에 참여시키는 방안
2	가격규제산업에 대한 요율회복제	가격 규제 산업에 대한 요율회복제		
3	사이버보안 보험	결합보험요건, 책임 경감, 법적 베네핏	사이버보험	보험회사들을 프레임워크 수립에 참여시키는 방안
4	대중의 인정	대중의 인정		선택적 대중의 인정 프로그램 개발을 연구
5	규제 합리화	정보 보안 규정의 합리화		규제합리화 대상을 규명
6	사이버보안 연구		정보 공유를 위한 정보 활용 역량을 강화	실제적으로 부딪힐 과제들을 극복하기 위해 자발적 중요기반 사이버보안 프로그램을 연구개발 노력과 연계
7	책임 한정		책임 위험을 명확히 제시	불법행위 책임에 대한 연구
8	정책 대상으로서 선호			
9		우선적 기술지원	기술 지원 제공	특정형태의 기술지원 제공 모색
10		정부구매 고려		정부구매 고려
11		세금 혜택	세금혜택	세금혜택
12			보안 심사 프로세스 가속화	신속보안심사
13		보안 공시 / 보조금(Subsidies) 사이버보안 제품 및 서비스의 직접 구매를 위한 자금 제공이나 저리 대출을 의미		
14				프레임워크 준수 및 연방 보조금 프로그램 참여와 관련해 연방기관들에 안내서를 제공/ 사이버보안을 위한 신속 특허 시범사업을 모색

출처 : KISA(2013), 주요정보통신기반보호 강화 방안 마련, 2013.12, pp.49-58 에서 편집

*보안 공시는 사이버 공격사실의 대외 공개 의미

인센티브의 일환으로 미국 보험회사는 2014년부터 사이버보안 프레임워크를 위험평가 지표로 활용하여 해당기관 보험료 일부를 경감하고 있으며 이에, 헬스케어, 기술, 정보통신 분야에서 75~80%의 기관이 사이버보험 가입한 것으로 조사되었다.

국토안보부, 재무부, 상무부는 2015년 9월부터 민간 부분에서의 사이버보안 프레임워크 전체도입을 위해 구체적인 인센티브 추진에 대해 검토하기 시작하였다.

(2) 사례

가) 미국 대형로펌과 금융업계의 보안정보 공유 사례[109)]

미국 은행업계와 로펌업계는 2014년부터 1년간 금융정보분석센터(FS-ISAC) 내부에 법률그룹(Legarl Group)을 만드는데 대해 논의하고 2015년 말까지 정보공유 컨트롤센터를 구축하는데 합의한 민간 분야의 정보공유 사례가 있다. 금융권과 로펌업계는 합의를 통해 금융권에 대한 사이버테러 정보를 공유함으로써 사이버테러에 대한 보안성을 높이는데 취지를 두고 이로써 은행들이 각각의 법률회사들과 자신의 보안정보를 별도로 논의함에 따른 불편함을 해소할 것을 기대한다.

구체적인 정보공유 방안으로써 ISAC을 통해 로펌들에 해킹이나 온라인상의 위협정보를 익명으로 나눌 수 있게 허가하는 방안 즉, 일종의 '느슨한 제휴' 형태를 통해 로펌업체가 갖는 정보 접근성을 확대하는 방안을 검토한 사례가 있다. 최근 로펌을 겨냥한 해킹 위협도 커지고 있으므로 로펌업체 입장에서는 사업 자체뿐만 아니라 부가적으로 로펌 자체의 보안성 향상을 위해서도 정보공유의 필요성을 인식한 것으로 파악된다.

나) 보험회사의 사이버보안 프레임워크를 활용한 보험료 경감 사례[110)]

보험회사에서 사이버보안 프레임워크를 위험평가 지표로 활용하여 해당기관 보험료 일부를 경감하고 있으며(2014년~) 헬스케어, 기술, 정보통신 분야에서 75~80%의 기관이 사이버보험에 가입한 것으로 조사된다.

---

109) 전자신문(2015), "미국 대형 로펌들, 금융업계와 보안정보 나눈다... FS ISAC에 참여", 2015.2.26. http://www.etnews.com/20150226000105

110) 서상기 외(2015), "민간분야 사이버보안 역량 강화를 위한 인센티브 현황", 정보통신기반 보호법 일부개정법률안 검토보고서 - 서상기의원 대표발의(2015.09.08.)

2) 유럽

2010년 6월, 유럽정보보호 전문기관(ENISA)은 정보공유 프로그램 참여 시 비용절감, 정보제공, 보조금 지원, 전문가 기술지원 등 12건의 인센티브 제공(안)을 제시한 바 있다. 또한 2014년 7월부터 '사이버보안 혁신 바우처'를 통해 사이버보안 관련 외부 전문인력 및 기술 도입에 필요한 자금을 보조하고 있는 것으로 알려져 있다. [111]

최근 ENISA(2010) 정부-민간 공공참여를 유도를 위한 연구를 발표하였는데, 각 국가의 정부공유 프로그램 참여에 따른 네트워크 구축으로 인한 인센티브에 대한 가이드라인을 아래와 같이 제시하였다. [112]

<표 6-2> 공공-민간 네트워크 구축 인센티브에 대한 ENISA의 연구

High importance	Medium importance	Low importance
1. 비용절감에 따른 경제적 인센티브 2. 정보의 제공에 따른 인센티브	3. 참가자간의 신뢰 구축 4. 정부나 보안서비스의 정보수신 권한에 따른 인센티브 5. 정보공유에 따른 네트워크 형성에 의한 인센티브 6. 정보공유참가자의 자율성 허용	7. 보조금 지급에 의한 경제적 인센티브 8. 영향력 확보에 따른 경제적 인센티브 9. 사이버 보험의 사용에 따른 경제적 인센티브 10. 평판으로 인한 인센티브 11. 전문가 분석, 조언, 지식 혜택으로 인한 인센티브 12. 참가자의 기호, 가치, 태도에서 기인한 인센티브

자료: ENISA(2010), Incentives and Challenges for Information Sharing in the Context of Network and Information Security

3) 일본

일본은 금융 ISAC 차원에서 미국의 관련 조직과의 협력을 통한 활성화를 도모하고 있는데[113] 이에, 미국의 금융 ISAC과 일본의 조직이 적극적으로 협력할 예정이다.

111) 서상기 외(2015), "민간분야 사이버보안 역량 강화를 위한 인센티브 현황", 정보통신기반 보호법 일부개정법률안 검토보고서 - 서상기의원 대표발의(2015.09.08.)
112) KISA(2013), 주요정보통신기반보호 강화 방안 마련(2013.12.), pp.68-70
113) http://www.f-isac.jp/press_release/20140807.html

2. 국내 정보공유체계 활성화 정책 및 사례

1) 정보공유체계 활성화 정책

2015년 9월, 서상기 의원은 사이버위협 정보공유분석센터(ISAC)에 정부가 재정을 지원할 수 있도록 '정보통신기반보호법' 개정안을 발의하였다.[114][115] 이 분야는 최근 국가안보의 핵심영역으로 인식됨에 따라 개별주체의 자발적·능동적 참여를 위한 정부의 제도 설계 및 지원이 매우 중요하다는 인식하에 추진되었음을 밝히고 있다.

즉, 기존에는 ISAC에 대한 기술적 지원 근거규정만을 두고 있어 기업의 참여 유인을 제공하는데 한계가 있었으며, ISAC 구축 운영에 소용되는 재정을 회원사의 회비로 충당하여 개별 기업에게 큰 부담으로 여겨지면서 ISAC이 타 분야로 확산되거나 활성화되지 못하는 현실적인 제약요인이 되었다.

(1) 정보통신기술(ICT) 분야

정부는 K-ICT 시큐리티 발전 전략(Security SPARK)을 통한 산업 활성화 정책 추진[116]했다. 우선, 정보보호 사각지대 없는 민간 주도의 사이버보안 강화 차원에서 산업제어시스템 등 주요 기반시설 지정 확대(2017년까지 400개) 및 정보공유분석센터(ISAC) 확대(4개에서 7개) 구축 지원을 전략으로 수립하고 추진하였다.(2015~2017년)[117]

정보보호 사각지대 해소를 위하여 중소·영세기업에 대해 사이버 침해사고 발생 시 정보보호 서비스지원(긴급대응 및 시스템 복구 등의 신속한 기술·현장지원)을 위한 '전국 118 정보보호 지원체계'의 구축을 추진(2015년~)하며, 기업 간 정보보호 격차해소를 위하여 보안취약점 점검 및 조치 비용을 지원하는 '정보보호 바우처 프로그램'을 추진하였다.(2016년~)

또한, 자발적이고 적극적인 정보보호투자 촉진 환경 조성 차원에서 중소기업의 정보보

---

114) 디지털데일리(2015), "정보통신기반보호법 개정안 발의... ISAC에 재정지원", 2015.9.8. http://www.ddaily.co.kr/news/article.html?no=134473

115) 기존 기반보호법 제16조(정보공유분석센터) 제4항(정부는 제1항 각호의 업무를 수행하는 정보공유분석센터의 구축을 장려하고 그에 대한 기술적 지원을 할 수 있다.)의 기술적 지원을 재정적·기술적 지원으로 개정

116) 미래창조과학부(2015), K-ICT 시큐리티 발전 전략(안), 2015.4. http://www.msip.go.kr/cms/www/open/go30/info/info_1/info_11/__icsFiles/afieldfile/2015/08/12/K-ICT%EC%8B%9C%ED%81%90%EB%A6%AC%ED%8B%B0%EB%B0%9C%EC%A0%84%EC%A0%84%EB%9E%B5(%EC%B5%9C%EC%A2%85).pdf

117) 현재 통신, 금융, 증권, 지자체 4개 ISAC을 에너지, 의료, 교육 분야의 7개로 확대 구축

호 제품 투자 시 조세감면(10%), 취약점 분석 등 보안컨설팅 지원 추진, 정보보호 우수업체의 공공·조달 및 연구개발 참여시 가점(0.5~1점) 부여 등의 다양한 '정보보호 투자 인센티브'를 마련하였다.(2015년~)

(2) 의료 분야

의료분야에 대한 사이버보안 위협은 생체정보와 같은 민감한 정보 취급에 따라 갈수록 고조되고 있으며 고위험 보안취약점 등을 악용한 지능적인 악성코드가 증가하는 등 의료기기와 원격진료에 대한 보안위협은 빠르게 확산되고 있다. 반면, 이에 대한 대응체계는 부족한 실정이므로 보건의료 분야 전반의 정보보호 수준 제고의 필요성이 지적되어 관련 부처는 사이버보안 강화에 나서고 있다.[118]

과학기술정보통신부의 경우 인증 취득 확대를 지원한다는 방침을 세우고 중소 병의원 및 약국에 대하여 ISMS 인증 도입, 정보보호준비도 평가, 지역정보보호지원센터 활용 등 다양한 제도 및 인프라 지원을 추진하고 있다.

행정안전부는 의료기관의 개인정보 유출 사건관련 규제 강화를 하고 있는데, 개인정보보호법 위반 업체의 실명을 공개하고 행정처분 결과 공표제도를 적극 활용하고 있다.[119]

보건복지부는 규제 강화만으로 사이버보안 수준을 향상시키기 어렵다고 보고 의료분야 ISAC의 단계별 추진을 계획인데, ISAC은 부처 간 협의는 물론 예산, 인력 확보, 의교기관의 적극적인 협조 등이 선행되어야 한다. 2018년으로 설립 예정된 의료 ISAC은 사회보장정보원에서 운영 예정이며, 보안관제, 정보공유, 취약점 분석 및 평가 업무를 맡는다.[120]

의료기관은 ISMS 인증 등 정보보호 체계 개선으로 보안사고 피해비용을 절감하고, 특히 상시 보안관제 활동으로 사이버 위협에 대한 대비가 가능하고, 최신 정보보안 기술 및 정보공유가 가능해 질 것으로 기대하고 있다.

---

118) 보안뉴스(2015), "의료분야 보안위협 위험수위... ISAC 추진 탄력 받나?", 2015.8.25. http://www.boannews.com/media/view.asp?idx=47534

119) '1회 과태료 부과 총액이 1000만원 이상' 요건에 해당되는 곳은 행정처분 사실이 공표됨

120) 政, 의료 ISAC(Information Sharing & Analysis Center) 설립 http://www.dailymedi.com/detail.php?number=824723&thread=22r02

[그림 6-1] 보건복지 분야 사이버보안 대응체계

자료: 보안뉴스(2016.9.11.), “보안위협 정보공유 ISAC, 의료 분야가 가장 시급한 이유”
(http://www.boannews.com/media/view.asp?idx=51752)

또한 미국에서 자동차 분야의 ‘Auto-ISAC’이 발간한 ‘사이버보안 실천사항’ 사례처럼 의료분야 ISAC을 통해 민간 의료기관에게 개인정보보호나 의료정보보호 가이드라인을 배포하고 사이버 위협에 효과적으로 대응 할 수 있게 취약점 및 침해요인, 대응방안 정보를 제공함으로써 침해사고 발생 시 효과적인 대응을 지원할 수 있을 것으로 기대하고 있다.

(3) 행정 분야

2017년 12월 ‘데이터기반행정 활성화에 관한 법률’이 통과됨에 따라 안전·질병 등 사전에 위험 예측 및 제거방법 제시, 경제·사회 등 분야에서 미래 수요 충족을 위한 선제적 대응책 마련, 비교·분석을 통한 최적화된 대책 마련 및 맞춤형 서비스 제공 등의 행정업무를 데이터 기반으로 처리하게 되었다. 이 법에 따라 데이터를 ‘데이터통합관리 플랫폼’에 등록하고 범부처 데이터 공유를 실시한다.[121]

공공기관의 장인 공동 활동 필요가 있는 데이터를 등록하고, 등록된 데이터는 데이터 이용목적, 분석방법 등을 제시하면 사용가능하다.

121) http://www.mois.go.kr/frt/bbs/type010/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000008&nttId=61232

2) 관련 사례

(1) 금융보안 ISAC의 운영 활성화 사례[122)]

운영 활성화를 위하여 커뮤니티 활성화를 위한 세부 방안을 마련하고 ISAC 협의회 활동에 대한 참여도 증진을 위한 해외 연수 개최, 해외ISAC 기관과의 국제교류 등을 통하여 ISAC의 활성화를 도모하고 있다.

- 커뮤니티 활성화: 정보공유 활성화를 위한 간담회/세미나/워크숍 등을 통해 정보교류 및 상호 협력의 장 마련, 유관 부처 및 정책입안담당자와의 간담회를 통해 정부정책 홍보의 장 마련 등
- 해외연수 : 회원사 보안담당을 대상으로 해외연수 실시, 회원사 담당자간 친목도모 및 유대관계 강화, 협회 사업 및 정보통신ISAC 협의회 활동에 대한 참여도 증진
- 해외ISAC 기관과의 국제교류: 해외 ISAC기관간 정보교류를 통해 ISAC 활성화 도모

(2) 정보통신기반보호 제도시행의 저해요인 및 방안 연구 사례[123)]

가) 저해요인 및 해결방향

한국인터넷진흥원은 주요정보통신기반보호 강화 방안을 연구하는 보고서에서 정보공유 분석기능을 수행하는데 따른 정보유출 우려를 중대한 저해 요인으로 조사하였다. 정보가 공유되는 상황에서 각 기관 또는 기업의 행정관리를 포함한 영업비밀 등의 정보가 어떤 형태로든 공개되는 것을 우려하는 것이다.

특히 민간의 경우, 정보통신기반시설과 관련된 기업이 대부분 동종업계의 상위그룹에 해당하는 기업들이며 정보공유의 과정에서 자회사의 정보가 상대방에게 노출되는 것에 우려가 가장 심한 것으로 나타난다. 또한 기반시설의 지정공시가 소비자 입장에서는 개인의 정보가 누출되는 것이 아닌지에 대한 의구심을 야기 시켜 부정적인 이미지를 낳을 수 있다는 입장이 있다.

이와 같은 저해요인을 해소하기 위한 방안으로 법제를 통한 규제측면의 방안 강구보다는 관계주체의 자발적인 정책참여를 유도하기 위한 방안 강구가 그 무엇보다 중요하다는 결론에 이르고 있다.

---

122) http://www.isac.or.kr/ Home > 정보통신ISAC > 정보통신ISAC협의회
123) KISA(2013), 주요정보통신기반보호 강화 방안 마련, pp.31-32, 35-36, 115-116, 2013.12.

나) 인센티브 방안

본 사례에서 주요정보통신기반보호 강화를 위해 제안한 인센티브 방안은 해당 상황의 법제적 실효성을 증대하고 참여주체간의 네트워크 구축으로 제도의 효율적 운영을 가능하게 하는 방안으로서 자발적 참여 촉진을 위한 인센티브 방안을 설정한 것이다. 그리고 이러한 방향이 가장 우리나라 실정에 적합한 것으로 판단하였다.

해당 연구방법으로 해외사례를 기반으로 중복된 방안은 제거하고 통합 구성함으로써 21개 인센티브 수단을 제안한 것으로 파악된다. 또한 제안된 인센티브 수단에 대한 도입의 즉시성, 추가 입법 여부 등을 고려할 것을 전제로 하고 있다. 또한 제안된 인센티브 수단에 대한 전문가 검토의견도 제시되므로 SW안전 ISAC 추진 시 참고할 필요가 있다.

<표 6-3> 미, 국토안보부(2013)의 분류기준에 따른 인센티브 수단 분류

효율성과 효과성				
최상위	보조금(grant)		가격규제산업을 위한 요율회복제
차상위	보조금(Subsidies), 세금혜택, 사이버보안보험 지원	책임경감, 법적 베네핏, 사이버공격(사고)발생 시 정부지원	정부구매 고려, 정부사업 가중치 제공
	연구 장려를 위한 정부자금 도입	대중의 인정, 보안 공시, 홍보 및 공청 활동, 신속보안심사 도입, 신속특허심사 도입, 인재육성 촉진, 보험회사의 프레임워크 수립참여	기술지원 제공, 연구개발 연계, 정보보안규정의 합리화
	채택시 정부에 큰 부담	⟷	채택시 정부에 적은 부담

자료: KISA(2013.12), 주요정보통신기반보호 강화 방안 마련 연구보고서, pp.115

인센티브 수단에 대한 국내도입 적정성 검증을 위해 정보통신전문가, 정보보안전문가 및 법률전문가의 인터뷰, 서면 자문, 종합적인 회의를 통하여 다음과 같은 결과를 도출하였다.

<표 6-4> 제안된 인센티브에 대한 전문가의 분석 결과

인센티브(안)	국내 도입 적절성	정부 부담감	즉시성	추가 입법 고려
책임경감 및 책임한정, 법적베네핏	●	◎	○	√
정부사업 가중치 제공	●	○	◎	
정부구매 고려	●	○	◎	
사이버공격(사고) 발생 시 정부지원	●	◎	○	√
기술지원 제공	◎	○	●	
홍보 및 공청활동(안내서제공포함)	◎	◎	●	
보안 공시	◎	◎	◎	√
인재육성 촉진	◎	◎	●	√
보조금(subsidy)	○	●	○	√
연구 장려를 위한 정부자금 도입	○	●	●	
사이버보안 연구	○	○	●	
불법행위 책임에 대한 연구	○	○	●	
연구개발 연계	○	○	●	
보조금(grant)		●	○	√
세금혜택		●	○	√
가격규제산업을 위한 요율회복제		○	◎	√
보험회사의 프레임워크 수립참여		◎	◎	
사이버보안보험 지원		●	◎	
대중의 인정		◎	○	
신속보안심사 도입		◎	◎	√
신속특허심사 도입		◎	◎	√

※ 각주

1. 국내도입적절성 항목에서 ●은 높은 수준, ◎은 중간 수준, ○은 낮은 수준, 공란은 국내도입이 부정적임을 의미함
2. 정부부담감 항목은 제안된 인센티브의 도입시 정부의 부담정도를 나타나는 항목으로 ●는 높은 수준, ◎은 중간수준, ○은 낮은 수준의 부담감을 의미함
3. 즉시성항목은 제안된 인센티브가 즉시도입 가능한 방안인지를 나타내며 ●는 높은 수준, ◎은 중간수준, ○은 낮은 수준을 의미함
4. 추가입법고려 항목은 제안된 인센티브 중 추가입법이 고려되는 인센티브 방안을 표시하였음

자료: KISA(2013.12), 주요정보통신기반보호 강화 방안 마련 연구보고서, pp.118

※ (참고) 제안된 인센티브 수단에 대한 전문가 검토의견

o 국내도입의 적절성이 가장 높은 인센티브는 '책임경감 및 책임한정, 법적 베네핏'으로 나타남

o 책임경감 및 책임한정에 대한 인센티브 다음으로 전문가들의 긍정정인 의견이 모아진 인센티브 방안은 '정부사업 가중치 제공', '정부구매 고려', '사이버공격(사고) 발생 시 정부지원' 방안임

o 모든 전문가가 국내도입에 부정적이라 판단한 인센티브 방안은 '보조금(grant)', '세금혜택', '가격규제산업을 위한 요율회복제', '보험회사의 프레임워크 수립참여', ' 사이버보안 보험지원', '신속심사 도입', ' 신속특허심사도입 '이었음

o 부정적이라 판단한 인센티브 방안 중 '보조금(grant)', '세금혜택', '가격규제산업을 위한 요율회복제'의 세가지 인센티브 방안은 민간기업에 대해서는 직접적인 차원의 인센티브이므로, 인센티브 방안 차원에서의 효과성은 높게 평가할 수 있겠으나, 궁극적인 면에서 정보통신기반시설보호 강화활동은 인센티브가 주어져야 행해지는 활동이 아니라 국가기반시설관련 기관 및 사업자가 필수적으로 행하여야 하는 활동이므로 이 같은 기본개념에서의 이해를 생각할 때 정부와 지자체의 부담을 감수하고 논의된 세 방안을 시행하는 것에는 부정적이라는 의견이었음

본 사례에서는 최종 연구결과로 인센티브 수단의 효율성과 효과성 분석, 정부 부담에 대한 분석, 인센티브 수단이 즉시 적용가능한지에 대한 즉시성 및 인센티브 수단 도입 시 추가입법 필요 여부 등을 고려하여 다음과 같은 인센티브 방안을 최종 도출하였다.

<표 6-5> 최종 결과로 도출된 인센티브 방안

	인센티브(안)	국내 도입 적절성	효율성과 효과성	정부 부담감	즉시성	추가 입법 고려
1	책임경감 및 책임한정, 법적베네핏	●	◎	◎	○	√
2	정부사업 가중치 제공	●	◎	○	◎	
3	정부구매 고려	●	◎	○	◎	
4	사이버공격(사고) 발생 시 정부지원	●	◎	◎	○	√
5	기술지원 제공	◎		○	●	
6	홍보 및 공청활동(안내서제공포함)	◎		◎	●	
7	보안 공시	◎		◎	◎	
8	인재육성 촉진	◎		◎	●	

자료: KISA(2013.12), 주요정보통신기반보호 강화 방안 마련 연구보고서, pp.123

제2절 시사점

1) 재정지원을 통한 기업의 부담 해소와 자발적 참여에 대한 검토 필요

정책의 활성화를 위한 인센티브 정책은 채택시 정부에 부담이 직접적인 재정지원과 간접적인 기술지원이나 규제해소 등의 정책이 있다. 직접적인 재정지원은 그 효과가 즉시 나타나지만, 인식 개선과 자발성 측면이 약해 지속적인 효과를 나나태기 어렵다.

우리나라는 2015년 9월 정보통신기반보호법 개정을 통한 ISAC 재정지원을 추진하면서 기존과 같이 ISAC에 대한 기술적 지원 근거규정만으로는 기업의 참여를 유인하는데 한계가 있다고 판단한 바 있다. ISAC을 추진하는 경우에는 어떤 분야든지 개별 기업에 부담으로 작용하는 자체 회원사 회비로의 재정적 충당이 아닌 정부의 기술적재정적 동시 지원을 핵심 요인으로 한다고 할 것이다.

그러나 정부의 재정지원은 정부의 부담을 높이고, 관련 기업의 자발성을 높이는 측면에서는 부정적인 영향이 있어 경제·사회적 측면에서 면밀한 검토가 필요하다.

2) 정부의 의지와 자발적 참여사이의 균형 유지

미국 국입기술표준원(NIST)의 사이버보안 프로그램이나 한국의 정보통신기반보호법 개정을 통한 ISAC 재정 지원, K-ICT 시큐리티 발전 전략, 의료 분야 ISAC 추진 등은 정부의 정보공유에 대한 의지를 표명하고 있다. 정부는 보조금, 보험, 가격규제산업에 대한 요율화, 규제 합리화 등의 혜택으로 정보공유 프로그램에 참여하도록 하며, 동시에 책임한정, 대중의 인정 등의 유인으로 기업이나 개인의 자발적 참여를 유도한다.

국가적으로 필요한 정책은 정부 의지에 의한 참여자들에 대한 혜택과 동시에 참여자들의 자발적 참여를 위한 인식의 전환이 필요하다.

3) 책임의 경감 및 책임 한정, 법적 베네핏 정책을 통한 정보공유 활성화 추진

주요정보통신기반보호 강화를 위한 인센티브 방안 중 효율성과 효과성이 높으면서 국내 도입의 적절성이 가장 높은 인센티브는 '책임의 경감 및 책임 한정, 법적 베네핏'으로 나타났다. 이는 또한 정부의 부담도 크지 않다. 국외 연구에서와는 다른 결과인데 이는 국내 규제의 정도와도 영향이 있는 것으로 판단되며, 정책 마련 시 고려해야 할 요소이다.

제7장 정책방향 제안 및 결론

이 연구에서는 미국과 일본을 대상으로 구축·운영 중인 정보공유체계의 현황 및 사례들을 살펴보았다. 그 결과, 공통적으로 ISAC을 비롯한 다양한 방식의 정보공유가 이루어지고 있음을 알 수 있었다. 통신, 금융, 의료, 자동차 등 대부분의 산업 분야에서는 정보공유체계 운영을 위하여 독자 시스템을 개발하거나 이메일, 인쇄물, 온라인 회의나 오프라인 워크숍 등의 방법으로 정보를 공유한다. 또한 효율적이고 일관된 정보공유체계 운영을 위하여 표준 규격을 적용하거나 독자적인 정보공유기술을 개발하여 이용하고 있다.

정보보안이 관심영역인 사이버 공격의의 경우 짧은 시간에 넓은 영역으로 확대되어, 정보 공유의 필요성이 확대되고 있으며 정보 공유의 실시간성도 중요하다. SW 안전의 경우는 사이버공격보다는 확대성과 실시간성 특징이 비교적 적어 정보공유의 필요성이 감소될 수 있다. 하지만 안전 기술과 매커니즘은 동일하여, 타 산업 도메인의 안전 표준 및 가이드를 연구하고 적용하는 융복합화가 진행되고 있다.[124] 도메인이 달라도 정보의 공유는 시간과 비용을 절약할 수 있는 장점이 있어, 같은 도메인은 물론이고 다른 도메인 간도 SW 안전 측면에서도 정보 공유는 필요하다.

이와 같은 국내외 현황을 통해 파악한 ISAC 운영이나 정보공유기술의 특징 그리고 정보공유체계 활성화를 위한 국내외 정책과 각종 사례들을 통해 SW안전 ISAC을 국내에 도입하고 구축하는데 있어 다음과 같은 점을 정책 방향을 도출했다.

제1절 정책 방향

1) SW 안전 정보공유에 대한 인식개선

문제점에서도 지적했듯이 ‘국내 주요정보통신기반보호 제도시행의 저해요인에 대한 연구’에 따르면 정보공유 분석기능을 수행하는데 있어 정보유출 우려가 가장 중대한 저해요인으로 조사된 바 있다. 즉, 정보공유의 관련 주체들은 정보가 공유되는 상황에서 각 기관이나 기업의 행정관리를 포함한 영업비밀 등 정보가 어떤 형태로든 공개되는 것을 우려한다는 것이다. 특히 민간의 경우 대부분 동종업계의 상위그룹에 속하는 기업들이 정보공유의 주체가 되므로 정보를 공유하는 과정에서 자회사의 정보가 상대방에게 노출

124) SPRi(2017), 소프트웨어 안전 산업 조사,2017.4.

되는 것에 대한 우려가 크다. 또한 소비자 입장에서도 개인의 정보가 기업을 통해 노출되는 것은 아닌지 의구심을 야기하게 되므로 부정적인 이미지를 갖게 된다. 따라서 SW 안전 정보공유에 있어서도 이와 같은 부담을 해소할 수 있는 기반 환경이 먼저 선행되어야 성공적 추진이 가능할 것이다.

한 방안으로 정보공유 기술 측면에 정보공유 범위 프로토콜의 적용하는 것이 될 수 있다. 트래픽 라이트 프로토콜(TLP)은 정보공유를 용이하게 해주는 정보공유 범위에 관한 프로토콜이다. 미국 국토안보부와 같이 TLP표준을 그대로 적용하는 정보공유체계도 있고 일본의 경우 같이 자국의 산업분야에 맞춰 수정 적용하는 곳도 있다. TLP는 민감한 정보를 공유하는데 대한 부담을 해소해주는 방편으로 공유 시기와 방법, 나아가 공유의 범위를 간단하고도 직관적으로 표현해주는 스키마를 제공하므로 효과적인 공유방법으로 활용되고 있다. 안전 정보는 안전 구현 기술력 보호 측면이나 기밀정보로써 가치 측면에서 정보 노출에 민감한 정보이다. 민감 정보에 대한 정보공유 범위 한정은 SW 안전 정보공유체계의 활성화를 위한 의미 있는 방안으로 적용 가능하다.

그러나 정보 유출에 대한 위험은 기술만으로는 해소하기 어려우며, 법적, 사회적, 교육적인 다방면의 위험 제거 노력이 필요하다.

2) SW 안전 관련 정보수집 추진 및 시스템 구축

(1) 정보공유 서비스 그룹 또는 프로그램 운영을 통해 정보 수집 확대

국내의 경우, SW 안전 관련 수집이 표준 및 절차, 사고사례 등 부분적으로 이루어지고 있다. SW 안전 정보가 체계적으로 수집되고, 실질적으로 활용되기 위해서는 정보 수집 확대 방안 마련이 필요하다.

미국 의료 분야의 경우 ISAC의 커뮤니티를 활용한 서비스 그룹 CYBERFIT®을 운영함으로써 효율적으로 회원사 내부와 제3자 공급업체의 위험을 관리하고 모니터한다. 자체 커뮤니티를 활용하기 때문에 보다 합리적이고 경제적인 형태의 서비스가 가능해지고 따라서 보다 신뢰 가능할 뿐만 아니라 안전하고 탄력적인 정보 수용이 가능해진다. 필요한 경우 ISAC운영의 경제적 재원 측면에서도 도움이 될 수 있다는데 의미가 있다.

국내의 경우 ‘자동차 결함 정보공유체계’처럼 필요성에 의해 만들어진 형태가 지속적으로 운영되고 있다. 이상적인 방안은 여러 도메인간의 SW안전 관련 정보 공유로 확대되어 기술 향상과 비용 절감이 목표가 되겠지만, 동일한 집단 간 정보 공유를 통한 이

익 창출이 정보 수집을 위한 방안이 된다.

(2) 정보공유 표준규격을 통한 상업적, 비상업적 목적의 광범위한 정보공유 실현

미국의 국토안보부가 개발한 글로벌 정보사회를 위한 개방형 정보공유 규격으로 TAXII, STIX가 있다. STIX/TAXII 체계는 이미 ISAC이나 정보보호 산업분야를 비롯하여 누구나 사용 가능하도록 공개된 규격이라는 점에서 활용의 범위가 광범위하고 자유롭다. 애당초 STIX/TAXII 개발의 목적은 사이버 위협 정보공유에 있다. 그러나 자동화 방식으로 광범위하게 정보를 공유할 수 있는 기능을 갖추고 있고 이미 국내를 비롯하여 수많은 ISAC에서 활용되고 있으므로 사례를 토대로 문제점을 분석하여 다른 내용의 정보공유에 적용한다면 새로운 프로토콜을 개발 없이도 효율적으로 성공적인 활용이 가능할 것이다. 특히 TAXII는 정보공유의 조직 형태에 따라 3개 정보공유 모델을 지원하고 있어 다양한 형태로 정보공유 조직이 구성되고 공유범위를 달리하는 경우 차용하기 용이하고, 다양한 조직에로의 적용을 고려할 경우 모델을 개선하여 활용할 수 있을 것이다.

3) 정보공유 확대 및 정보공유체계 활성화 방안

(1) 일본의 센터와 같은 기능 형태의 초기 운영에서 ISAC과 같은 체계적 형태로 발전시키는 전략

우리나라와 미국은 중요 산업분야에서 ISAC을 구축하고 상하로 정보공유체계를 운영하는 경우가 많으나 일본의 경우는 ISAC 없이 협의회를 운영하면서 단순히 이메일이나 인력을 통해 정보를 공유하는 경우도 많다. 특이하게도 일본은 초기에는 조직 내에 센터라는 정보공유 기능을 두도록 하면서 중요성에 따라 단계적으로 ISAC을 구축하는 점진적 형태를 두고 있다.

국내의 경우 정보공유체계를 ISAC 형태로 구성하는 정책을 추진하고 있으나, 아직은 3개 조직으로 정보공유가 빠르게 확산되고 있지는 않다. 국내의 경우 SW안전 분야의 ISAC이 기존 보안 위협정보 공유나 일반 산업별 ISAC과 어떻게 차별화되어야 할 것인지 명확하지 않은 상태이므로 센터와 같은 기능 차원의 개념을 정의하고 조직의 형편이나 목적에 맞게 점진적으로 구성하는 것도 하나의 방안이 될 수 있을 것이다. SW 안전의 경우는 보안에 비해 그 피해빈도나 피해 규모에서 아직은 미약한 것으로 보여, 체계적 형태의 정보공유를 구축할 경우 필요성에 대한 문제가 도출될 수 도 있다. 그의 대비책

으로 높음 SW 안전 인식을 가진 SW 안전 전문가를 중심으로 협의체를 운영하면서, SW 안전 정보 공유에 대한 필요성과 중요성을 높이는 것이 필요하다.

SW 안전 협의체 운영 시에는 산업의 융복합화에 대한 대응이 필요하다. 일본의 ICT-ISAC은 같이 총체적 보안 확보를 위해 ISP 사업자뿐만 아니라 방송 사업자, 소프트웨어 벤더, 정보 관련 기기 제조 사업자 등 다양한 분야로 확대하여 활동을 하고 있다. 모든 산업에서 융복합화가 이루어짐에 따라 SW 안전 구현을 위해서는 여러 도메인 전문가 및 관련자가 정보공유에 참여하여야 한다. 각 분야의 도메인에 소프트웨어 벤더 및 정보 관련 기기 제조 사업자 등 HW, SW 관련자가 포함되는 것을 고려해야 한다.

(2) 정보공유 참여주체의 자발적 참여 촉진을 위한 인센티브 방안 연구 및 정책마련

미국은 주요정보통신기반보호 강화를 위한 자발적 프로그램 참여를 유도하기 위해 2013년 NIST를 통해 인센티브 방안을 연구하도록 하고 그 결과로 8가지 인센티브 방안을 공개한 바 있다. 행정명령에 따라 각 부처는 8개 방안을 기초로 자체 인센티브 방안에 대한 보고서를 제출하도록 의무화하였는데, 이는 강력한 의지를 표명한 것이다. 특히 국토안보부의 경우, 총 21개의 검토 가능한 인센티브 유형을 대상으로 효율성과 효과성, 채택시 정부의 부담유무의 정도에 따라 인센티브 수단을 분류하였다. 이와 더불어 세부적인 평가요소로써 즉시성, 추가입법, 도입의 적절성 등을 기준으로 하였는데 관련 분석기준과 결과는 국내 SW안전 정보공유체계 도입 시 활성화를 위한 인센티브 연구에 중요한 기초자료가 될 것이다. 특히 연구 및 정책 적용의 사례를 벤치마킹하여 유사한 인센티브 제도들이 실패하는 원인을 분석하고 정책 추진의 방향을 모색해야 할 것이다.

(3) 관련 업계의 정보공유 사례 발굴 및 적용

미국의 보험회사들은 2014년부터 인센티브 정책의 일환으로 사이버보안 프레임워크를 위험평가 지표로 활용하여 해당기관 보험료 일부를 경감하고 있으며, 이에 헬스케어, 기술, 정보통신 분야에서 75~80%의 기관이 사이버보험에 가입하고 있는 것으로 조사되었다. 또한 은행업계와 로펌업계는 금융정보분석센터(FS-ISAC) 내부에 법률그룹을 만들어 정보공유 컨트롤센터를 구축하는데 합의한 사례도 있다. 이와 같이 서로 다르지만 공통으로 필요 정보를 공유하기 위한 본격적인 논의가 다양한 영역에서 시작되고 있다. 특별히 정보공유로 인한 위험을 방지하기 위하여 ‘느슨한 제휴’ 형태 즉, 공유정보를 익명으로 나눌 수 있게 허가하는 방안을 검토하는 등 안전장치 고안에도 힘쓰고 있다. 국내 SW안전 정보공유 역시 IoT 관련 산업의 기관이나 기업들이 적용할 수 있는 사례를 다양하게 발굴하고 특히 정

보공유에 따른 안전장치 고안의 사례들의 적용 가능성을 모색할 필요가 있다.

제2절 결론

최근 산업 전반에서는 정보화의 시대를 넘어 IoT시대로의 도약이 빨라지고 이와 함께 크고 작은 SW안전사고가 빈번해지고 있는 바, SW안전사고와 관련한 문제를 해결하기 위한 연구는 매우 시기적절하다고 할 것이다. 본 연구에서는 SW안전 확보와 신속한 사고 대응을 위한 SW안전 정보공유 플랫폼의 구축 요구에 따라 이를 체계적으로 정착시킬 수 있는 정책적 연구를 수행하였다.

그 결과, 아직까지 SW안전 산업도메인 전반에서 SW안전에 기능안전 측면의 기준은 표준화되어 적용되고 있으나 SW오류 등으로 인한 안전 대응 측면의 요구사항 내용은 간접적으로만 유추해볼 수 있었다. 또한 정보공유분석센터(ISAC)를 체계적으로 구축하고 관련 정보를 수집 및 공유하는 경우는 주로 국가의 주요 기반시설보호를 목적으로 하는 경우가 많았다.

이러한 유사분야의 현황과 사례를 통하여 SW안전 분야의 정보공유 플랫폼 구축 및 활성화를 위한 정책 방향을 제시하였다. SW안전은 사람의 생명, 사회기반 시설 등과 밀접한 관련이 있고 그 만큼 중요한 역할을 담당한다. 이번 연구 결과가 향후 SW안전 ISAC 및 정보공유체계를 구축・운영하고 활성화하기 위한 기반이 되기를 기대한다.

참 고 문 헌

국내 문헌

[1] 소프트웨어정책연구소(2015.8), 『소프트웨어 안전 산업 동향 조사』, pp.10,93,131
[2] 소프트웨어정책연구소(2016.12), 『소프트웨어 안전 산업 동향 조사』, pp.10-14,47-50
[3] 한국인터넷진흥원(2013.12), 『주요정보통신기반보호 강화 방안 마련 연구보고서』, pp.7,20,27-29, 31-32,35-36,.49-61,68-70,115-116,129-134
[4] 한국인터넷진흥원(2010.11), 『주요정보통신기반시설 사이버 위협 및 대응』
[5] 이근상(2015), 『IoT산업의 키, 소프트웨어 안전』, (재)전북테크노파크, Issue&Tech vol.49, pp.13-17
[6] 행정안전부(2012.5), 『전자정부 SW개발 운영자를 위한 소프트웨어개발보안가이드』, pp.5
[7] 행정안전부(2014.3), 『2013년 국가정보자원 개방공유체계 구축사업 완료보고』
[8] 한국소비자보호원(2013.11), 『협력적 파트너십을 통한 자동차 결함정보 공동 활용』
[9] 한국인터넷진흥원(2008.6), 『일본의 최근 정보보호정책 현황 및 시사점』
[10] 전자신문(2017.05.14.), 『시작은 늦었지만 체계 갖춘 일본' [사이버보안 새틀을 짜자]』
[11] 한국인터넷진흥원(2015), 『사이버 침해사고 정보공유 세미나』-"C-TAS System & CTEX", pp.13~21
[12] 한국인터넷진흥원(2016), 『사이버침해사고 정보공유 세미나 자료집(2016.4분기)』, PP.81-83
[13] 서상기의원 대표(2015.9), 『민간분야 사이버보안 역량 강화를 위한 인센티브 현황(2015), 정보통신기반 보호법 일부개정법률안 검토보고서』, 서상기의원 대표발의(2015.9.8./1916775)

해외 문헌

[1] 미쓰비시 종합연구소(2010.3). “미국 보안 정보공유 조직(ISAC) 상황과 운용실태에 관한 보고서” 2009년도 내각관방정보보안 위탁조사, pp.119-130.
https://www.nisc.go.jp/inquiry/pdf/fy21-isac.pdf#search=%27isac%E3%81%A8%E3%81%AF%27

[2] 내각관방 정보보안센터(2008.7). “중요 인프라의 정보 보안 대책에 관한 행동계획’의 정보연락/정보제공에 관한 실시 세목 개요에 대하여”(정보 보안 정책회의 제5차 회의자료), pp.98.
https://www.nisc.go.jp/conference/seisaku/kihon/dai9/pdf/9siryou_ref04.pdf#search=%27NIPC+%E4%BA%A4%E9%80%9A%E4%BF%A1%E5%8F%B7+traffic+light+protocol%27

[3] 일본 문부과학성, “각국 보안 관련 예산 및 정책 관련 자료집”
http://www.meti.go.jp/policy/netsecurity/downloadfiles/Strategy_refer.pdf#search=%27%E6%97%A5%E6%9C%ACISAC%E8%A8%AD%E7%AB%8B%E6%A0%B9%E6%8B%A0%27

[4] 하야시 게이사쿠(2015.8). “계속되는 자동차 안전과 보안”, 덴소 도카이 세미나 자료. pp.115.
http://www.chubu.meti.go.jp/b34jyoho/shiryo/20150806securityseminar/20150806denso.pdf#search=%27%E8%BB%8A+isac%27

[5] 소방청(2013.10). “소방청의 재해정보 수집 제공에 관하여”, 제1회 방재 및 감재 분과회의 제출자료, pp.87-90.
http://www.kantei.go.jp/jp/singi/it2/senmon_bunka/bousai/dai1/siryou8.pdf#search=%27%E6%B6%88%E9%98%B2%E6%83%85%E5%A0%B1%E5%85%B1%E6%9C%89%27

[6] 총무성(2015.5). “사이버보안 정책 추진에 관한 제언”, 총무성 정보보안 어드바이저 리보더, pp.1-25.
http://www.soumu.go.jp/main_content/000359287.pdf#search=%27%E5%8E%9F%E5%AD%90%E5%8A%9BiSAC%27

[7] 경제산업성(2016.7). “전력분야의 사이버 보안대책에 대하여”, 자원에너지청, pp.111-114.
http://www.meti.go.jp/committee/sougouenergy/denryoku_gas/kihonseisaku/pdf/007_06_00.pdf#search=%272015%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC%E4%BF%9D%E5%AE%89%E5%AF%BE%E7%AD%96%27

[8] 이이쓰카 히사오(2014.7). “통신 비밀과 사이버 보안 대책”, 텔레콤 ISAC JAPAN, pp.100-104.
https://www.jaipa.or.jp/event/oki_ict2014/140703_iizuka.pdf#search=%27%E6%97%A5%E6%9C%AC%E3%81%AE%EF%BC%A9%EF%BC%B3%EF%BC%A1%EF%BC%A3+%E6%B3%95%E7%9A%84%E6%A0%B9%E6%8B%A0%27

[9] OTSL(2012). “ISO 26262의 소프트웨어 안전 분석 검토” 주식회사 OTSL, pp.1-17.
https://www.ipa.go.jp/files/000004108.pdf#search=%27%E3%82%BD%E3%83%95%E3%83%88%E3%82%A6%E3%82%A7%E3%82%A2%E5%AE%89%E5%85%A8%27

[10] 요미야 히사시 외(2010). “소프트웨어를 중심으로 한 안전설계 기술” 도시바 리뷰 vol No.7, pp.87-90.
https://www.toshiba.co.jp/tech/review/2010/07/65_07pdf/f03.pdf#search=%27%E3%82%BD%E3%83%95%E3%83%88%E3%82%A6%E3%82%A7%E3%82%A2%E5%AE%89%E5%85%A8%27

[11] 내각 관방(1957) “내각 관방 조직 시행령 제219호 https://www.nisc.go.jp/law/pdf/soshikirei.pdf

[12] 사이버보안전략본부(2017.7). “2020년 및 그 이후를 대비한 사이버 보안에 대한 본연의 자세에 대하여” 사이버보안 전략 중간 리뷰, pp.1-14.
https://www.nisc.go.jp/active/kihon/pdf/csway2017.pdf#search=%27%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E5%AF%BE%E5%87%A6%E8%AA%BF%E6%95%B4%E3%82%BB%E3%83%B3%E3%82%BF%E3%83%BC%27

[13] IT-ISAC Organization(2017). “YOUR PARTNER IN THE DEFENSE AGAINST CYBER THREATS”, IT-ISAC Membership Brochure
https://docs.wixstatic.com/ugd/b8fa6c_9ab65f4ac8a34ca9bf38603012754ec5.pdf
[14] IT-ISAC(2017). IT-ISAC Member Participation Guide, pp.54.
https://docs.wixstatic.com/ugd/b8fa6c_d8e6c5df296c43b6acddc28e65b42949.pdf
[15] Faye Francy.(2016.1). “Aviation ISAC - The Value of Information Sharing.” 2016 Transportation Research Board (TRB) Panel 2: Cyber Security and Resilience Strategies
http://trbcybersecurity.erau.edu/resources/01_14_16_Francy_TRB_Panel_AISAC_FINAL.pdf
[16] Faye Francy.(2015.3). “The Aviation Information Sharing and Analysis Center (A-ISAC).”, Aviation ISAC
http://www.ecedha.org/docs/default-source/energy-and-power/faye-francy.pdf?sfvrsn=0
[17] Denise Anderson.(2017). “Medical Device Security: The Next Frontier.”, NH-ISAC
https://www.first.org/resources/papers/conf2017/Medical-Device-Security-A-Sucking-Chest-Wound-That-Needs-Emergency-Medicine.pdf
[18] NH-ISAC(2016), “NHISAC Roles and future - Advancing the global health Sector’s cyber and Physical Security (force multiplication through sharing)”, NH-ISAC
https://secwww.jhuapl.edu/IACD/Resources/AIS/HHSWorkshop/NHiSAC%20Roles%20and%20future%20-%20JH%20Workshop.pdf
[19] Auto-ISAC(2016.7). “Automotive Cybersecurity Best Practices Executive Summary”, Auto-ISAC
https://www.automotiveisac.com/assets/img/executive-summary.pdf
[20] FEMA, “Emergency Management and Response - ISAC”
http://www.usfa.fema.gov/downloads/pdf/publications/emr-isac.pdf
[21] Department of Homeland Security Integrated Task Force(2013.6). “Incentives Study Analytic Report”, pp.140
[22] Department of Treasury(2013). “the President on Cybersecurity Incentives Pursuant Executive Order13636” Treasury Department Summary Report , pp.141.
[23] Department of Commerce(2013). “RECOMMENDATIONS THE PRESIDENT ON INCENTIVES FOR CRITICAL INFRASTRUCTURE OWNERS AND OPERATORS JOIN A VOLUNTARY CYBERSECURITY PROGRAM”, pp.142-144.
[24] Department of Commerce(2013). “Discussion of Recommendations the President on Incentives for Critical Infrastructure Owners and Operators Join a Voluntary Cybersecurity Program”, pp.142-144.

웹 사이트

[1] http://www.ddaily.co.kr/news/article.html?no=121428

[2] http://www.ddaily.co.kr/news/article.html?no=134473

[4] http://www.boannews.com/media/view.asp?idx=47534

[5] http://www.boannews.com/media/view.asp?idx=51752

[6] http://www.etnews.com/20150226000105

[7] http://www.msip.go.kr/

[8] http://www.isac.or.kr

[9] http://www.isac.or.kr/intro/intro01.jsp

[10] http://www.isac.or.kr/

[11] http://www.kbr.1go.kr/content/view.do?menuKey=442&contentKey=4

[12] https://cshare.krcert.or.kr:8443

[13]

http://www.msip.go.kr/cms/www/open/go30/info/info_1/info_11/__icsFiles/afieldfile/2015/08/12/K-ICT%EC%8B%9C%ED%81%90%EB%A6%AC%ED%8B%B0%EB%B0%9C%EC%A0%84%EC%A0%84%EB%9E%B5(%EC%B5%9C%EC%A2%85).pdf

[14] https://www.nisc.go.jp

[15] http://www.fdma.go.jp/

[16] http://www.fdma.go.jp/html/new/161129kentou.html,

[17] http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/structure/index.html

[18] http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/risk/11.html

[19] https://www.cadence.co.jp/soconline/vol20/tech/tech_2.html

[20] http://techon.nikkeibp.co.jp/escar/

[21]

http://tokyoexpress.info/2015/06/19/a400m%E5%A2%9C%E8%90%BD%E4%BA%8B%E6%95%85%E3%81%AF%E3%82%BD%E3%83%95%E3%83%88%E7%B5%84%E8%BE%BC%E3%81%BF%E9%81%8E%E5%A4%B1%E3%81%AB%E3%82%88%E3%82%8B%E3%83%87%E3%83%BC%E3%82%BF%E6%B6%88%E5%A4%B1/

[22] http://news.heraldcorp.com/view.php?ud=20150521000688&md=20150522143533_BL

[23] https://www.je-isac.jp/news/2017/0328_01.html

[24] http://www.f-isac.jp/press_release/20140807.html

[25] http://www.f-isac.jp/institute/activities.html

[26] https://www.telecom-isac.jp/

[27] https://www.ict-isac.jp/news/news20160622.html

[28] http://www.mlit.go.jp/page/kanbo01_hy_005499.html

[29] http://www.tkc.co.jp/kaze/backnum2006/0605/trend.html

[30] http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/legal/09.html

[31] http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/legal/05.html
[32] http://law.e-gov.go.jp/htmldata/H12/H12HO144.html
[33] http://law.e-gov.go.jp/htmldata/H26/H26HO104.html
[34] http://law.e-gov.go.jp/htmldata/H26/H26SE400.html
[35] http://www.news24.jp/articles/2017/07/13/04366948.html
[36] https://www.ntt-tx.co.jp/column/trend/cs20160613
[37] http://www.keidanren.or.jp/policy/2016/006_honbun.html
[38] https://www.telecom-isac.jp/public/t-ceptoar.html
[39] http://www.keidanren.or.jp/policy/2016/006_honbun.html
[40] https://www.telecom-isac.jp/contact/index.html
[41] https://www.ict-isac.jp/news/news20160622.html
[42] http://www.f-isac.jp/press_release/20140807.html
[43] http://www.f-isac.jp/institute/activities.html
[44] https://www.je-isac.jp/news/2017/0328_01.html
[45] http://www.dhs.gov/national-coordinating-center-communications
[46] http://www.it-isac.org/faq
[47]http://www.it-isac.org/members
[48] http://www.ecedha.org/docs/default-source/energy-and-power/faye-francy.pdf?sfvrsn=0
[49] http://www.anomali.com/
[50] http://www.healthcareready.org/members-and-supporters
[51] http://nhisac.org/
[52] http://nhisac.org/nhisac-faq/
[53] http://nhisac.org/membership-account/membership-levels/
[54] http://nhisac.org/about-nhisac/
[55] http://nhisac.org/nh-isac-membership/
[56] http://nhisac.org/cyberfit/
[57] http://www.automotiveisac.com/
[58] http://www.hsdl.org/?view&did=732831
[59] http://r-cisc.org/about-membership/
[60] http://r-cisc.org/our-associate-members/
[61] http://r-cisc.org/about-r-cisc/
[62] http://r-cisc.org/resources/
[63] http://r-cisc.org/education-training/
[64] http://r-cisc.org/isac/
[65] http://taxiiproject.github.io/

[66] http://taxiiproject.github.io/legal/

[67] http://taxiiproject.github.io/community/

[68] https://www.first.org/tlp/

[69] http://taxiiproject.github.io/getting-started/whitepaper/#trademark-information

[70] http://www.fdma.go.jp/html/new/pdf/161129_kentou/4-1-1.pdf#search=%27%E5%AE%89%E5%85%A8%E3%81%AE%E6%83%85%E5%A0%B1%E5%85%B1%E6%9C%89%27

[71] https://www.nisc.go.jp/active/kihon/pdf/csway2017.pdf#search=%27%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E5%AF%BE%E5%87%A6%E8%AA%BF%E6%95%B4%E3%82%BB%E3%83%B3%E3%82%BF%E3%83%BC%27

부록1. 일본 내각관방 정보보안센터(NISC) (2007.4) - 중요 인프라에 대한 셉터(CEPTOAR) 개요

<1> 셉터(CEPTOAR) 기능 명칭: (전기통신) T-CEPTOAR

사무국: (재) 멀티미디어 진흥 센터

1. 개요
IT 장애를 미연에 방지, IT 장애의 확산 방지・ 신속한 복구, IT 장애 요인 등의 분석・검증을 통한 재발 방지를 도모하고, 전기통신 사업자의 서비스 유지・복구 능력의 향상에 이바지하기 위해 정부 등으로부터 제공받은 정보를 적절하게 전기 통신 사업자 간에 공유・분석하는 것을 목적으로 전기 통신 분야의 '정보 공유 ・ 분석 기능(CEPTOAR)'으로서 'T-CEPTOAR'를 설치

2. 구성・기능
[구성]
(1) T-CEPTOAR 운영위원회 설치
(2) 이하 SG를 설치
(ㄱ) 고정 계열의 네트워크 인프라를 설치하는 전기 통신 사업자 등으로부터 구성된 SG (SG1)
(ㄴ) 액세스 계열의 전기 통신 사업자 등으로 구성된 SG (SG2)
(ㄷ) ISP 사업자 등으로 구성된 SG (SG3)
(ㄹ) 이동 통신 사업자 등으로 구성된 SG (SG4)

[기능]
(1) 전기 통신 사업의 IT 장애에 대하여 미연에 방지, IT 장애의 확대 방지 ・ 신속한 복구, IT 장애 요인 등의 분석・검증을 통한 재발 방지를 위한 구성원 간의 정보 공유 및 연계
(2) 정부와 다른 CEPTOAR 등으로부터 제공되는 정보의 구성원에 연락
(3) 정부와 다른 CEPTOAR 등으로부터 제공되는 정보와 관련된 사항의 구성원 간의 정보 공유

3. 특색・특징
・ 4 개의 SG을 설치하고 깊고 중요한 정보 공유의 실현을 목표
・ 지금까지의 활동 ・ 현행 조직을 기반으로 한 실효성 있는 체제

<2> 셉터(CEPTOAR) 기능 명칭: (방송) 방송에 관한 정보 공유 체제

사무국: 총무성 정보통신정책국 지상방송과

1. 개요
IT 장애에 관하여 내각 관방 정보 보안 센터(NISC)로부터 제공되는 정보와 이를 보완하는 정보를 적절하게 방송 사업자에게 제공하여 방송 사업자 간에 공유를 도모하기 위하여 '방송에 관한 정보 공유 체제'를 구축

2. 구성・기능
[기능]
IT 장애에 관하여 내각 관방 정보 보안 센터 (NISC)로부터 제공되는 정보와 이를 보완하는 정보를 적절하게 방송 사업자에게 제공하여 방송 사업자 간에 공유를 도모한다.

[구성원]
일반 방송 사업자

[정보 전달 경로】
총무성 정보 통신 정책국 지상파 방송과
→ 종합 통신국 등 방송 담당과
→ 일반 방송 사업자

[대상 IT 장애]
(1) 사이버 공격으로 인한 IT 장애
(2) 비의도적 요인으로 인한 IT 장애
(3) 재해로 인한 IT 장애

3. 특색・특징
[정보 취급]
내각 관방이 결정하는 정보 공유 레벨에 따라 정보 공유의 범위 또는 정보 취급 담당자의 범위가 한정되어 있는 정보는 해당 범위를 준수하는 등 주의가 필요하다.
[연락 체제]
이미 구축되어 있는 재해 대응 시 연락 체제를 참고하여 '방송의 정보 공유 체제' 를 구축

<3> 센터(CEPTOAR) 기능 명칭: 금융 CEPTOAR 연락협의회

사무국:-

1. 개요
금융 분야의 CEPTOAR(은행 등의 CEPTOAR, 생명보험 CEPTOAR, 손해보험 CEPTOAR, 증권 CEPTOAR)의 운영 방법에 대해 정보 교환을 실시한다.

2. 구성・기능
금융 CEPTOAR 연락협의회는 은행 등의 CEPTOAR 생명보험 CEPTOAR 손해보험 CEPTOAR, 증권 CEPTOA로 구성된다. 또한 필요에 따라 관계기관이 옵서버 자격으로 참가한다.

3. 특색・특징
각 금융 분야 CEPTOAR의 대처 정보 및 성공 사례 등에 대해 정보 교환을 실시한다.

<4> 센터(CEPTOAR) 기능 명칭: (은행 등) 은행 등의 CEPTOAR

사무국: 전국은행협회 사무시스템부

1. 개요
은행 등의 CEPTOAR는 예금 취급 금융기관의 각 업계 전체를 구성원으로 한 것 이외에 결제 시스템의 운영자인 사단법인 도쿄은행협회도 구성원 포함된 조직이다.
예금취급 금융기관은 결제시스템 등을 통해 상호 관련되어 있으며, 제1 금융기관에서 발생한 IT 장애로 인하여 결제 부전이 다른 금융기관에 시스테믹하게 확대될 가능성이 있다. 이것 때문에 IT 장애 정보의 공유를 추진함과 동시에 분석하고 대응책을 검토하는 기능을 은행 등 CEPTOAR에 마련했다.

2. 구성・기능
공유하는 정보에는 각 금융기관이 금융청에 보고하는 IT 장애에 대한 정보뿐만 아니라 IT를 이용한 금융 범죄에 관한 정보를 포함하고 있다. 이 밖에 취약점 정보, 바이러스 정보, 기타 IT 장애를 미연에 방지, 발생시 피해 확산 방지・신속한 복구 및 재발 방지에 도움이 되는 정보를 공유 대상으로 하고 있다.
분석에 대해서는 구성원의 각 업계를 대표하는 IT 전문가로 구성된 정보보안 대책위원회에서 실시한다. 동위원회는 금융업계 안전기준인 “금융기관 등 컴퓨터 시스템의 안전 대책 기준“의 설정 주체인 재단법인 금융정보 시스템센터(FISC)도 참여시키고 동일 센터의 협력을 얻어 IT 장애 정보를 분석하고 대응책을 검토한다.

3. 특색・특징
독자의 훈련・연습에 관해서는 금융업계의 각 결제 시스템(전은 센터, 어음 교환소 등)과 시장(단기 금융시장 등)에 대하여 지금까지 실시해오고 있으며 앞으로도 계속 실시할 예정이다. 이러한 노력과 은행 CEPTOAR와의 관계에 대해서는 향후 검토하겠다.

<5> 셉터(CEPTOAR) 기능 명칭: (증권) 증권 CEPTOAR

사무국: 일본 증권업협회 IT관리실

1. 개요

증권회사, 증권거래소, 청산・결제기관 등 증권 관계기관을 구성원으로 하여 증권시장 전체에 관련된 시스템 장애에 대하여 정부로부터 제공받는 정보 보안 정보를 구성원들에게 전달함과 동시에 필요에 따라 관계자 간의 정보 공유를 도모한다.

2. 구성・기능

정부로부터 제공받은 정보 보안 정보를 일본 증권업협회가 가지고 있는 회원전용 WEB에서 제공한다. 또한 광역 재해 등 발생시 정보제공 및 공유에 관해서는 상기 수단에 더하여 새롭게 구축하는 증권시장 BCPWEB에서 정보를 수집・제공한다.

3. 특색・특징

본 활동 실시 전에 결제기관에서는 공동훈련 등이 실시되고 있으며 또 향후 BCP 관점에서 증권시장 전체를 염두에 둔 연습 등이 필요하다는 인식이다. (구체적인 실시시기는 미정)

<6> 셉터(CEPTOAR) 기능 명칭: (생명보험) 생명보험 CEPTOAR

사무국: 사단법인 생명보험협회 총무부 조직인사 그룹

1. 개요

중요한 장애를 미연에 방지, 발생시 피해 확산 방지, 재발 방지 등을 목적으로 다음의 정보를 공유한다.

(1) IT 장애에 대한 정보
(2) IT를 이용한 금융범죄에 관한 정보
(3) 소프트웨어와 하드웨어의 취약점 정보
(4) 컴퓨터 바이러스에 관한 정보
(5) 기타 IT 장애를 미연에 방지, 발생시 피해 확산 방지, 신속한 복구 및 재발 방지에 도움이 되는 정보

2. 구성 ・ 기능

공유정보의 취급은 “중요 인프라의 정보 보안 대책에 관한 행동 계획의 정보 연락・정보 제공에 관한 실시 목록“에 준한다.

분석에 대해서는 금융업계 안전기준 등인 “금융기관 등의 컴퓨터 시스템의 안전대책 기준“의 설정 주체인 재단법인 금융 정보시스템 센터(FISC)의 협력을 얻어 IT 장애 정보의 분석 및 필요한 대응책 검토를 실시한다.

3. 특색・특징

기존의 정보연계 조직(생명보험협회 정보시스템위원회)을 이용하고 적시에 정보 공유가 가능하다. 구성원을 대상으로 연1회 이용시스템 조사를 실시하고 있다. 또한 IT 전반에 관한 의제를 전체 구성원이 심의할 기회(회의)를 분기별로 설정하고 필요에 따라 훈련・연습 등의 논의에 활용해 간다.

<7> 셉터(CEPTOAR) 기능 명칭: (손해보험) 손해보험 CEPTOAR

사무국: 사단법인 일본 손해보험협회 업무기획부 기획・안전기술 그룹

1. 개요
중요한 장애를 미연에 방지, 발생시 피해 확산 방지, 재발 방지 등을 목적으로 다음의 정보를 공유한다.

(1) IT 장애에 대한 정보
(2) IT를 이용한 금융 범죄에 관한 정보
(3) 소프트웨어와 하드웨어의 취약성 정보
(4) 컴퓨터 바이러스에 대한 정보
(5) 기타 IT 장애를 미연에 방지, 발생시 피해 확산 방지, 신속한 복구 및 재발 방지에 도움이 되는 정보

2. 구성・기능
내각관방 등으로부터 제공받은 정보의 취급은 “중요 인프라의 정보 보안 대책에 관한 행동계획“의 정보연락・정보제공에 관한 실시 목록에 정해진 정보공유 레벨에 따른다.

3. 특색・특징
기존의 정보연계조직(손해보험협회 정보시스템 위원회 및 정보시스템 부회)을 활용하고 적절한 때에 정보공유가 가능하다. IT 전반에 관한 의제를 전체 구성원이 심의할 기회(회의)를 분기별로 한 번씩 설정하고 필요에 따라 활용해 나간다. 구성원을 대상으로 1년에 한번, 임의 참여로 이용시스템 등에 관한 조사를 실시하고 있다.

<8> 셉터(CEPTOAR) 기능 명칭: 항공분야 CEPTOAR

사무국: 국토교통성 항공국 항공보안 대책실

1. 개요
중요 인프라를 담당하는 항공운송 사업자 및 관청(항공・기상청)이 소유하는 중요 시스템의 사이버 테러・장애 정보 중에서 공통 과제가 있는 정보 등을 CEPTOAR에서 수집・분석하여 분야별 관계자 간에 공유함으로써 IT 장애를 미연에 방지하고 장애 발생시에도 신속한 복구를 가능하게 한다.

2. 구성・기능
・ 항공 분야 내에서 공통적인 대책이 필요한 정보 공유를 정한다.
・ 정보 취급은 구성원만 한다.
・ 수집된 정보를 바탕으로 필요에 따라 분석을 실시하고 그 결과를 구성원에게 제공하는 것으로 IT 장애를 미연에 방지하는데 도움이 된다.

3. 특색・특징
항공 분야의 CEPTOAR 구성원은 항공운송 사업자(항공사) 및 관청(항공관제 등)으로 구성된다.

<9>셉터(CEPTOAR) 기능 명칭: 철도 CEPTOAR

사무국: 국토교통성 철도국 위기 관리실

1. 개요
IT 장애를 미연에 방지하고 발생시 적절한 대응에 이바지하기 위해 정부 등으로부터 제공받는 IT 장애 정보 및 철도 CEPTOAR 구성원이 보유하는 중요 인프라의 IT 장애 정보의 공유 등을 다룬다.

2. 구성・기능
행동 계획이 대상이 되는 철도 사업자 (JR, 대기업 민간 전철) 22개사 및 국토교통성 철도국 일본 민영철도협회에서 정보 공유・분석 기능을 구성하고 있다. 중요 인프라 소관 부처보다 철도 분야 이외의 중요 인프라에 관한 IT 장애 정보를 취득한 경우, 해당 정보가 철도 분야에서도 유익하다고 인정될 때에는 구성원에게 해당 정보를 제공하고 있다.
또한 구성원의 철도사업자로부터 보고된 IT 장애 정보도 필요에 따라 다른 구성원들에게 정보 제공과 함께 중요 인프라 소관 부처에 보고하도록 하고 있다.

3. 특색・특징
국토교통성 철도국 위기 관리실이 철도 CEPTOAR의 창구가 되어 현재 운용되고 있는 철도사고 등의 신고 규정 등에 의거 보고를 활용하여 정보 공유를 도모하고 있다.

<10> 셉터(CEPTOAR) 기능 명칭: 전력에 관한 IT 장애에 관한 정보 공유・분석기능

사무국: 전기사업 연합회 정보통신부

1. 개요

IT 장애를 미연에 방지하고 IT 장애 발생시 적절한 대응 등에 이바지하는 것을 목적으로 하며 IT 장애에 관한 소관 부처에 대한 원활한 정보 연락 및 전력 내에서 정보 공유 등을 다룬다.

2. 구성・기능

행동계획이 대상이 되는 전력 12개사 외에 전기사업 연합회, 전력중앙 연구소를 포함한 12개 회사 2기관에서 전력의 정보 공유・분석 기능을 구성하고 있다.

IT 장애에 관련된 소관부처에 대한 원활한 정보 연락 및 전력 내에서 정보 공유 등을 기능으로 하고 있으며 전화, FAX, E-MAIL, 전자 게시판, 경우에 따라서는 Face to Face로 정보 공유 등을 실시하고 있다.

3. 특색・특징

전력에서는 정보 공유・분석 기능을 정비하는데 있어 각 주체(12개사 2기관)의 역할, 정보의 취급 등을 명확히 하기 위해 “전력의 IT 장애에 관한 정보 연락・공유 지침“을 정했다.

각 주체는 이 지침을 참고로 이미 마련되어 있는 구조를 효율적으로 활용하면서 정보 공유・ 분석 기능을 구현했다.

행동 계획의 대상이 되는 12개사에 머물지 않고 분석 기능을 지원하기 위해 전력 중앙 연구소도 체제에 참가하고 있다.

<11> 셉터(CEPTOAR) 기능 명칭: GAS CEPTOAR
사무국: 사단법인 일본가스협회 보안기술 그룹
1. 개요
가스 사업자가 제조 · 공급에 관한 제어 계열 시스템의 IT 장애를 미연에 방지하고 확산 방지를 포함한 조기 복구, 재발 방지에 적절히 대응할 것을 목적으로 IT 장애에 관련된 소관부처에 원활한 정보 연락을 지원하는 등 가스 분야에서 정보 공유의 허브 역할을 하도록 노력한다.

2. 구성・기능
[구성원]
행동계획의 대상이 되는 주요 가스 사업자로서 정령지정도시의 최대 가스사업자 및 이러한 사업자와 동등한 수요 수가 있다. 가스 사업자를 가스 CEPTOAR의 구성원으로 한다.

[기능]
가스 분야에서 IT 장애를 미연에 방지, 확산 방지를 포함한 조기 복구, 재발 방지를 위하여 구성원 간의 정보 공유를 실시한다. 또한 한 가스 사업자 안에서 발생한 IT 장애가 가스 분야에서 다른 사업자에 영향이 있을 수 있는지 또는 사업자의 요청에 따라 대응하여 중앙에서 분석한다. 더욱이 IT 장애의 영향이 다른 분야에도 파급될 가능성이 있는지, 내각관방으로부터 얻은 다른 분야의 IT 장애가 가스 분야에 영향이 있을 수 있는지 여부를 검토한다.

3. 특색・특징
가스 분야는 사업자마다 사업 규모・형태가 달라 적용되는 제조・공급의 제어 계열 시스템도 다양하기 때문에 각 사업자의 자주적 판단을 존중하면서 업계에서 IT 장애의 판단 기준이 되는 생각들을 공유할 수 있도록 '장애 사례'의 정보 공유에 힘쓰며 노력하고 있다. 정보 공유 방법은 기존의 연락체제 등을 활용하여 실무자에게 상설 WG이 미연 방지책과 재발 방지책 등의 구체적인 대처 과제를 제대로 지원하는 것이다.

<12> 셉터(CEPTOAR) 기능 명칭: 지자체 CEPTOAR
사무국: 재단법인 지방자치정보센터 지자체 보안지원실
1. 개요
지방공공단체가 참여하는 행정 전용 네트워크(LGWAN)를 활용하여 지방공공단체의 정보 보안 대책 실시에 필요한 정보와 도구 등을 지방자치단체에 공유하여 적절한 예방 및 복구에 도움이 된다.

2. 구성・기능
・사무국을 (재)지방자치 정보센터 내에 설치
・내각관방 정보보안센터로부터 제공되는 정보를 LGWAN 메일로 지방공공단체에 제공

3. 특색・특징
・내각관방 정보보안센터에서 제공되는 정보 이외에 지방공공단체가 점검, 연습, 훈련 등의 실시로 유용한 도구・자료 등이나 지자체의 보안사고 대응사례 지자체의 정보보안 대책 추진사례, 조기 경계정보 등 지방공공단체의 정보보안 대책 강화에 도움이 되는 정보를 이메일 및 포털 사이트에서 제공
・지방공공단체가 참여하는 행정 전용 네트워크(LGWAN) 활용

<13> 셉터(CEPTOAR) 기능 명칭: 의료, 수도, 물류 분야R

셉터(CEPTOAR) 기능 명칭: 2007년에 검토

사무국: 2007년 검토

의료
셉터(CEPTOAR) 정비에 대하여 정보공유에 대해서는 기존 루트를 활용
분석기능에 대해서는 보건의료복지정보시스템 공업회를 활용하는 것으로 2007년 3월 기본적 합의에 이르렀다.

수도
셉터(CEPTOAR) 정비에 대하여 사단법인 일본수도협회와 기본적 합의에 이르렀다.

물류
셉터(CEPTOAR)의 모체조직인 사단법인 일본물류단체연합회로서 셉터(CEPTOAR)구성원은 물류관련 사업자 단체와 대기업 물류 사업자로 하는 방침으로 기본적 합의에 이르렀다.

주 의

1) 이 보고서는 소프트웨어정책연구소에서 수행한 연구보고서입니다.
2) 이 보고서의 내용을 발표할 때에는 반드시 소프트웨어정책연구소에서 수행한 연구결과임을 밝혀야 합니다.

93000
9 788961 084062
ISBN 978-89-6108-406-2