정 보 보 호 학 회 지
제28권 제6호, 2018. 12

방위산업 사이버 보안을 위한 방산 정보 공유·분석센터(ISAC) 설립 방안

박 흥 순*

요 약

미래 군사력은 첨단 무기체계가 병력 위주의 군 구조를 대체할 것임은 자명하다. 이를 증명하듯 최근 국내 방위산업은 무기체계의 고도화·첨단화로 급속하게 성장하고 있으며 해외 수출도 성공적으로 진행 중이다. 그러나 컴퓨터 해킹 등 사이버 공격에 의한 방산 정보나 방위산업기술의 유출은 방위산업의 성장을 저해시킬 뿐 아니라 국가 안보까지 심대한 영향을 미친다. 국방부는 방산업체 사이버 보안을 위해 2010년부터 보안관제를 실시하고 있으나, 지능형 지속 위협(APT) 공격과 같은 최근의 공격 양상에 대응하기 위해서는 위협 정보를 다각적으로 수집·분석하는 노력이 필수적이다. 미국을 중심으로 한 선진국은 정보공유·분석센터(ISAC) 등 정보공유체계 구축을 통해 주요 기반시설의 사이버 보안을 강화하고 있으며 국내에서도 금융, 통신 분야 등을 시작으로 최근에는 의료 분야로 점차 확대되고 있는 추세이다. 본 논문에서는 정보공유·분석센터 설립 사례와 국내 방산업체 보안관제 환경 분석을 통해 방산 정보공유·분석센터 설립 방안을 제안한다.

Ⅰ. 서 론

2016년 세계 방위산업 시장 규모는 약 3,120억 달러였으며, 2019년에는 3,380억 달러로 증가할 것으로 전망된다. 국내 방위산업 또한 2019년 약 14.3조 원 규모로 증가할 것으로 전망되고, 이는 세계 방위산업 총 생산액의 약 2.5%로써 세계 10위권 내 수준이다[1]. 국내 방산시장 규모 증가에 따라 첨단 방위산업기술이 복제되거나 유출되는 등 국가 안보나 국익에 저해될 가능성 또한 증대되고 있는데, 최근 방산업체를 대상으로 여러 차례의 해킹 시도가 있는 등 사이버 위협이 지속되고 있다[2].

20세기 정보통신기술의 발달로 국가의 주요 기반시설이 정보통신망을 통해 네트워크로 연결되면서 특정 기반시설에 대한 사이버 침해사고 피해가 다른 기반시설 및 국가 전체의 위험이 될 가능성이 증대되고 있다. 이에 미국을 비롯한 세계 주요 선진국은 주요 기반시설 보호의 중요성을 인식하여 국가 주도로 정보보호전략, 주요 기반시설보호법 등을 제정하여 보호 조치를 취하고 있다. 각국의 국가정보보호전략에는 대부분 사이버 침해사고 예방을 위해 분야별 주요 기반시설 및 정부간 정보공유와 협력이 중요하다는 내용이 담겨있으며 이러한 활동을 수행하는 전문 조직으로 정보공유·분석센터(Information Sharing & Analysis Center, ISAC)가 설립되어야 함을 강조하고 있다. 국내에서도 이에 발맞추어 국가 차원의 사이버 위협 정보공유체계 구축 관련 법규 제정 및 정책 연구가 활발하게 진행 중이다[3-6].

방산업체를 대상으로 한 사이버 위협에 대응하기 위한 방안으로 국방부는 2010년부터 일부 업체를 시작으로 보안관제 시스템 구축을 지원하였다. 하지만 제한된 예산으로 전 방산업체를 지원하기에는 어려움이 있었으며 정부 개입에 대한 민간 업체의 부정적 인식으로 다수의 업체가 자체적으로 보안관제 시스템 구축을 추진하였다. 그러나 개별 방산업체의 역량만으로는 고도화된 APT(Advanced Persistent Threat) 공격이나 최신 해킹 기술이 적용된 사이버 위협에 대응하기 어렵기 때문에 민간·공공기관이 연결된 사이버 위협 정보공유 협의체 설립이 필요하다.

따라서 본 논문에서는 방위산업기술 등 방위사업 관련 정보 보호가 요구되는 공공기관 및 업체를 회원으로 사이버 위협에 공동 대응하기 위한 방산 정보공유·분석

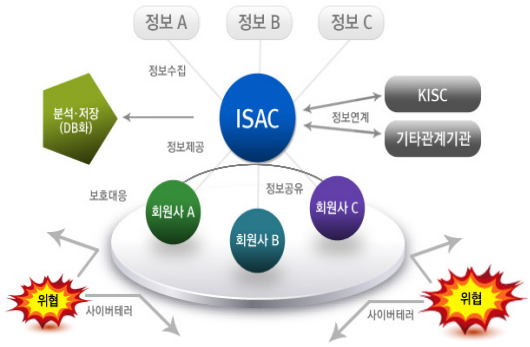
* 국방보안연구소 방산보안실 (heungsoon.park@gmail.com)

센터 설립 방안을 제시한다. 구성은 2장에서 국내외 정보공유·분석센터 설립 사례를 살펴보고, 3장에서 국내 방산업체 보안관제 환경 분석을 통해, 4장에서 방산 정보공유·분석센터 설립 방안을 살펴본다.

Ⅱ. 정보공유·분석센터(ISAC)

2.1. 정보공유·분석센터 개요

사이버 위협과 정보보호 시스템은 창과 방패로 비유되어 해킹 기술이 지능화·첨단화될수록 보안 시스템 또한 고성능이 요구되고 있다. 보안관제 시스템은 사이버 위협에 대응하기 위한 최소한의 필수 요소지만, 장비 도입뿐만 아니라 이를 운영하기 위한 전문 인력 확보 등 많은 비용이 요구된다. 따라서 단위 기관이나 업체 중 예산 확보가 어려운 곳은 보안관제 시스템을 구축·운영하기 제한되며, 설사 운영을 하더라도 고도의 전문성이 요구되는 분야기 때문에 제대로 운영하기 쉽지 않다. 정보공유·분석센터(ISAC)는 이러한 제한점을 극복하기 위해 1990년대 후반 미국에서 최초로 도입되었다. 이는 유사 산업 분야별로 해킹이나 사이버 테러 등 정보 침해 행위에 효과적으로 예방·탐지·대응하기 위한 서비스 조직으로 사이버 위협, 취약점 정보 등을 수집·분석하고 침해 사고 발생 시 대응요령을 신속하게 제공하는 업무를 수행한다[7]. 또한, 회원사 간 유대관계를 통해 운영되는 것이 일반적으로 산업 분야별 보안 전문가를 고용하여 해당 분야 정보통신기반시설을 보호한다. ISAC에서 제공되는 주요 기능은 표 1과 같이 각종 정보를 수집하여 분석한 후 그 결과를 회원사에게 제공하는데 그



〔그림 1〕 정보공유·분석센터 기능(출처: 정보통신 ISAC)〔8〕

〔표 1〕 정보공유·분석센터의 주요 기능

구 분	내 용
정보 수집	해킹·바이러스 등 사이버 위협 정보를 수집
정보 분석	수집된 정보를 분석, 최적의 대응 방안 수립
정보 제공	분석 정보를 회원사에 배포 · 공유
정보 연계	유관기관과의 정보 공유를 통해 공동 대응

외에도 산업 분야별 특성에 맞는 보안관제 서비스나 모의훈련, 취약점 진단 등의 업무도 제공한다.

ISAC의 일반적인 특징을 살펴보면 첫째, 국가 차원의 필요성에 의거하여 정부 주도로 설립한 후 민간으로 이전되는 특징이 있으며, 둘째, 주요 정보통신기반시설을 중심으로 산업 분야별로 구축되어 유사 취약점에 대한 효율적인 대응이 가능하다. 셋째, 타 기관 및 국가와 연계하여 국제적인 서비스 제공을 하기도 한다. 또한, 기존의 전통적인 보안관제센터는 개별적으로 운영됨에 따라 정보 공유가 제한되어 개별 기관의 독자적 대처에 따른 과다 비용 및 인력 소모의 단점이 있지만, ISAC은 공동 대응을 통한 신속한 대응 및 비교적 효율적인 비용으로 운영이 가능하다.

2.2. 국내·외 ISAC 운영 사례

ISAC은 1999년 미국의 금융 ISAC을 시작으로 주요 선진국을 중심으로 운영 중인데, 각 국가별 설립 과정이나 운영 방식에 따라 각기 다른 형태의 ISAC을 운영하고 있다. 국내의 경우, 정부 주도로 설립이 시작되었으나 최근 민간 영역에서도 관심이 급증하고 있다.

2.2.1. 해외 ISAC

미국은 1990년대 후반부터 연방정부를 중심으로 사이버 보안정책이 추진되었다. 2009년 출범한 오바마 정부는 사이버 보안을 최우선 과제로 선정하고 백악관 중심의 사이버 보안 추진체계를 구축하였으며, 주요 기반시설의 사이버 위협 정보 공유체계 강화, 사이버 보안 프레임워크 개발 및 보급, 사이버 보안 강화 프로그램 등을 진행하였다[9-11]. 그로 인해 현재 타 국가 대비 다수의 ISAC을 운영 중에 있으며, 국토안보부(DHS)에서 전체 ISAC을 총괄하고 있고, ISAC 협의회를 두어

분야별 ISAC 간에도 커뮤니티가 형성되어 있는 것이 특징이다[7].

영국은 유럽 내에서도 사이버 보안과 관련된 기술과 전문 인력을 보유한 국가에 속한다. 영국의 주요 기반시설보호는 내무부(Home Office)에서 담당하며, 산하기관인 국가기반보호센터(CPNI)에서 통신, 에너지 등 약 14개 분야의 ISAC을 운영이다. 영국은 2009년 최초로 사이버 보안 전략을 발표하고 국가 사이버 보안 프로그램을 통해 전략 추진을 위한 노력을 경주하고 있다[12].

유럽연합(EU)의 경우는 소속된 국가 간에 정보 공유를 실시하고 있는데 그리스에 있는 유럽정보보호원(ENISA)에서 회원국들을 대상으로 정보보호 서비스를 제공하고 있으며, 금융·에너지·산업 제어·사법 등 4개 분야에 대한 정보 공유를 통해 사이버 위협에 공동 대응하고 있다[13].

2.2.2. 국내 ISAC

국내 ISAC은 정보통신기반보호법 제16조를 근거로 주요 정보통신기반시설 보호를 위해 설립 및 운영 중이다. 사이버 보안 관련 공공분야는 국가정보원에서, 민간분야는 과학기술정보통신부에서 총괄하고 있는데, 각 중앙행정기관의 장은 주요 정보통신기반시설을 지정하고 별도 관리기관을 두어 ISAC을 운영하고 있다. 표 2와 같이 금융 ISAC[14], 정보통신 ISAC[7], 지자체 ISAC[15] 등 3개 분야에서 운영 중이나 올해 11월에는 의료분야에서도 ISAC이 설립되어 운영되고 있다.

〔표 2〕 국내 ISAC 운영 현황

구분	금융	정보통신	지자체	의료
운영기관	금융보안원	한국정보통신진흥협회	한국지역정보개발원	사회보장정보원
대상	금융회사(은행·증권 등)	통신사업자	17개 시·도 지자체	의료기관
기반시설	금융전산망 및 시스템 등	기간통신망 및 통신시설 등	국가정보망, 교통시스템 등	전자의무기록 시스템 등

2.2.3. 미국의 방산 ISAC

미국은 방산분야를 국가기반시설의 중요 부분으로 인식하여 국가기반시설 보호계획의 세부계획으로 수립하여 관리하고 있다[16]. 미국 방산 ISAC(Defense Industrial Base ISAC)은 2014년에 설립되었으며, 방위산업의 특수성으로 인해 국방부에서 관리·감독하고 있고 국토안보부와 공조체계를 구축하고 있다[10]. 미국의 방산 ISAC의 특징은 대기업보다는 정보보호시스템 기반시설이 열악한 대다수 중소 방산업체 지원에 초점을 두고 있으며, 사이버 위협뿐만 아니라 자연재해·화재·테러 등 물리적 피해에 대한 대응도 함께 지원한다. 또한 화재 발생 시 대피훈련이나 심폐소생술 등 산업안전에 필요한 정보도 제공함으로써 방산업체의 전반적인 커뮤니티 역할을 수행한다[17].

2.2.4. 시사점

국내·외 ISAC 사례에서 도출된 시사점은 먼저, 관련 법적 근거를 마련한 상태에서 민·관 협력체계를 구성했다는 점이다. 조직운영에 필요한 예산 확보와 민간 업체의 정보 공유 참여 유도를 위해서는 명확한 법적 근거가 필수적이다. 둘째는 산업 분야별로 그 환경과 특성에 따라 차별화된 ISAC을 운영한다는 점이다. 금융 ISAC은 금융전산망에 대한 대응태세 유지 및 전자금융사고 예방, 핀테크 보안 등을 제공하고, 정보통신 ISAC은 각 주요 통신사업자가 정보보호 서비스를 운영하고 있어 보안관제보다는 정보보호 준비도 평가나 취약점 분석 등의 업무를 수행한다. 셋째, 미국은 방산 인프라를 국가 주요 기반 시설로 규정하여 방산 ISAC을 운영한다는 점이다. 국내에서는 방산업체의 공장이나 연구센터 등을 주요 기반 시설로 지정하여 관리하고 있지 않지만, 방산 ISAC 설립에 있어서 법적 근거 마련 및 방산업체 실정에 부합한 시스템 구축이 필요함을 알 수 있다.

Ⅲ. 방산업체 보안관제 환경

본 장에서는 방산업체 사이버 위협 정보 공유의 필요성을 살펴보기 위해 방산업체 보안관제 환경을 진단한다. 이를 위해 방산업체 현황, 관련 법규, 보안관제 추진경과 등을 살펴본다.

3.1. 방산업체 현황

방위사업에 참가하는 업체는 방산업체, 일반업체, 방위산업과 관련없는 일반업체로 구분된다. 그중 방산업

체는 정부에서 지정한 방산물자를 생산하는 업체로써, 대통령령이 정하는 시설 기준과 보안 요건 등을 갖추어야 한다[18]. 방산업체는 생산하는 물자에 따라 주요·일반 방산업체로 구분되어 관리되며, 약 95개 업체 중 중소기업이 약 70%를 차지한다[19].

3.2. 방산업체 보안관제 관련 법·규정

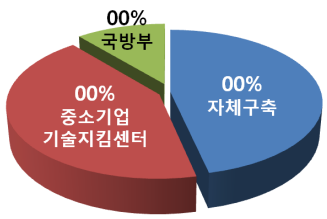
국방부 방위산업보안업무훈령 제89조 5항에는 해킹에 의한 방산 자료 유출 예방을 위해 보안관제를 위한 시스템을 설치하거나 24시간 모니터링 담당자 운영을 명시하고 있으며[20], 방위사업법 시행령 제44조의 위임규정인 방위산업물자 및 방위산업체 지정 규정 제19조는 방산업체에 필요한 보안대책을 강구하도록 제시하고 있다[21]. 하지만, 보안관제 관련 세부기준이 미흡하여 업체의 자의적인 해석이 가능하고 행정규칙에 근거하기 때문에 구속력 또한 미약하다.

3.3. 방산업체 보안관제 추진 경과

국내 방산업체 보안관제는 2000년대 후반에 들어서면서 사이버 위협에 의한 방위산업기술 유출 심각성 인식으로 시작되었다. 2010년부터 국방부는 방위산업보안업무훈령을 근거로 방산업체와 협의하에 정부 주도의 보안관제 시스템 도입을 시작하였다. 하지만, 제한된 예산으로 단기간에 전 방산업체를 대상으로 보안관제 시스템 구축을 추진하기에는 어려움이 있었다. 이에 국방부는 방산업체 보안관제 시스템 조기 정착을 위해 한국산업기술보호협회의 중소기업기술지킴센터[22]와 2012년 MOU를 체결하여 중소 방산업체를 대상으로 보안관제 서비스를 제공하였다. 중소기업기술지킴센터는 2011년부터 중소벤처기업부의 지원으로 보안관제 등의 정보보호서비스를 제공하고 있어 중소기업의 투자비용을 절감시키는 효과를 얻고 있다. 현재 대부분의 방산업체는 방화벽, UTM과 같은 정보보호 장비를 구축하였으나, 보안관제 주체가 국방부, 중소기업기술지킴센터, 업체 관제 등으로 분산 운영되고 있다.

3.4. 방산업체 보안관제 운영 실태

보안관제 운영현황을 관제 주체별로 살펴보면, 그림 2와 같이 자체 보안관제 시스템을 운영하는 업체(00%)



〔그림 2〕 관제 주체별 보안관제 구축 현황

와 중소기업기술지킴센터의 보안관제 서비스를 받는 업체(00%)가 방산업체의 대부분을 차지하고 있다.

자체 보안관제를 구축하고 있는 업체는 국방부나 중소기업기술지킴센터 등 외부기관 관제 시 업체 영업비밀 누설이나 해킹사고 발생에 대한 업체 이미지 손상을 우려하여 자체적으로 운영하는 경우가 많았다. 업체 규모별로 보면, 대기업은 기업 정보보호를 위한 예산 투자 및 그룹사 차원에서의 보안관제를 실시하여 자체 구축 비율이 높았으며, 중소기업은 정보보호를 위한 예산 투자에 소극적이어서 중소기업기술지킴센터의 무료 보안관제 서비스를 이용하는 업체가 많았다. 또한 중소기업의 경우 방산업체 지정·취소가 대기업에 비해 빈번하여 보안관제 시스템 구축이 미흡한 업체도 있었다. 방산업체에 비해 보안 시스템 구축이 열악한 협력업체를 통해 방위산업기술이 해킹될 소지도 있다. 원인을 살펴보면 해당 업체의 재정 규모와 경영진의 관심에 따라 보안관제 운영에 대한 편차가 컸으며, 이를 보완하기 위해서 관제 결과 및 위협 정보를 공유할 수 있는 시스템 구축이 필요하다.

Ⅳ. 방산 ISAC 설립 방안

본 장에서는 방산업체 보안관제 실태 진단 결과 도출된 문제점을 해소하기 위해 관련 법적 근거 마련 등 단계별 방산 ISAC 설립 방안을 제시한다.

4.1. 관련 법적 근거 마련

ISAC과 같은 사이버 위협 정보 공유체계를 구축에 있어서는 기술적인 고려 사항도 중요하지만 정책적 기반 마련이 먼저 선행되어야 한다[23,24]. 국내 ISAC은 기본적으로 정보통신기반보호법을 근거로 설립되었는데, 이를 위해서 먼저 해당 보호대상을 정보통신기반시설로 지정 및 관리하여야 한다. 현재 방산업체에서 보유

하고 있는 방산시설이나 정보시스템은 정보통신기반시설로 지정되어 있지 않기 때문에, 국방부에서 방산업체의 주요 연구시설이나 체계업체의 전산센터 등을 정보통신기반시설로 지정하는 방안이 필요하다.

방산 ISAC을 설립해도 방산업체의 가입 노력이 없으면 그 효과는 미미할 것이다. 방산업체 실태 진단에서도 보았듯이 방산업체는 영업비밀 누설 및 업체 이미지 손상을 우려하여 자체 관제를 하고 정보 공유에 부정적인 시각을 가지고 있었다. 방위산업의 공공재적 특성 등을 고려하여 초기 방산 ISAC 설립 시에는 방산업체의 의무 가입 방안이 적절하다고 판단되며 차후에 협력업체 등은 자발적으로 가입되도록 유인책을 마련해야 한다. 이를 위해서는 방위산업물자 및 방위산업체 지정 규정이나 방위산업기술보호법에 ISAC 가입 조항을 포함해야 한다.

4.2. 단계별 방산 ISAC 설립 추진

방산 ISAC 설립에는 많은 시간과 비용이 투자된다. 따라서 단기적으로는 현재 운영 중인 보안관제 시스템을 보완하고 중장기적으로 정보공유 체계를 구축하는 등 전문적인 조직 설립이 필요하다.

4.2.1. 보안관제 시스템 구축 및 운영 기준 마련

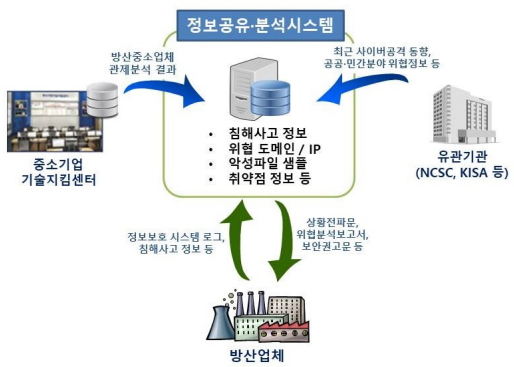
방위산업보안업무 훈령 등 방산보안 관련 규정에는 보안관제에 대한 내용이 세부적으로 명시되어 있지 않다. 따라서 방산업체 환경을 고려한 보안관제 시스템 구축 및 운영 기준에 대한 내용 보완이 필요하다. 대기업의 경우 상대적으로 다양한 정보보호 시스템을 보유하고 있지만, 중소기업의 경우 방화벽이나 바이러스 백신 체계와 같은 기본적인 시스템도 제대로 구비하고 있지 않은 업체도 있다. 다른 분야의 ISAC 관제 사례나 방위산업기술 유출 방지 등 방산업체의 특수성을 고려했을 때, 방산업체 보안관제는 기본적으로 외부 위협 탐지(방화벽, IPS, UTM 등), 자료 유출 방지(DLP), 악성코드 탐지(바이러스 백신)에 대한 보안 시스템 구축이 요구된다.

보안관제 시스템 도입 이후에도 전문 인력에 의한 관리가 되지 않으면 제대로 된 보안관제 기능을 발휘한다고 볼 수 없다. 24시간 전담 전문 인력에 의한 보안관제가 필요하며 방산업체 자체 전문 인력 확보가 제한되면 과학기술정보통신부에서 지정·고시하고 있는 보안관제 전문 업체[25]나 중소기업기술지킴센터(중소기업의 경우)에 의한 보안관제가 요망된다.

4.2.2. 정보공유·분석 기능 구축

미국 NIST 사이버 위협 정보 가이드[26]에서 제안하듯 초기 정보 공유·분석 시스템은 효율적인 운용과 통제가 용이하도록 국방부(또는 방위사업청) 주도로 기존 보안관제 조직을 활용하여 구축한 후 안정화 단계에서 별도 협의체로 이관하는 것이 바람직하다. 그림 3은 사이버 위협 정보 수집 및 업체 제공 방안에 대한 개념도를 보여준다. 먼저, 중소기업기술지킴센터와는 연동체계 구축을 통해 방산 중소기업 보안관제 분석 결과를 수집한다. 국가사이버안전센터(NCSC)나 한국인터넷진흥원(KISA)의 C-TAS 등 유관기관으로부터 최신 사이버 공격 동향이나 공공·민간분야의 사이버 위협 정보를 수집하며, 자체 구축한 방산업체로부터는 필수 보안관제 대상 시스템에 대해서 위협 정보를 수집한다. 수집된 정보는 침해사고 정보, 위협 IP, 악성코드 정보 등으로 분석 및 DB화 되며, 주기적으로 방산업체에 제공된다. 제공 시에는 상황 전파문, 분석 보고서, 보안 권고문 형태로 통보되어 업체 보안 실무자가 쉽게 이해하고 조치할 수 있도록 구성되어야 한다.

정보 공유 정책은 각 유관기관 및 방산업체와 정보공유 MOU를 체결하여 공유 방법과 범위를 설정한다. 업체의 자발적 참여를 유도하기 위해 위협 정보를 제공하는 업체에게만 정보를 공유하며, 정보를 제공한 업체



〔그림 3〕 방산 사이버 위협 정보 공유 개념도

의 동의 없이 다른 업체나 기관에 임의로 공개하는 것을 금지해야 한다. 공유 방법은 보안 시스템 구축이 비교적 양호하고 업체의 참여도가 높은 경우에는 에이전트 등을 활용하여 실시간 수집 및 공유하고, 시스템 구축이 어렵거나 참여도가 낮을 경우 홈페이지 등의 게시판을 활용하여 다운로드 받는 방식을 사용한다. 공유 범위는 위협 정보의 내용에 따라 공통적인 부분은 전체 회원사에 배포하고, 특정 분야에 한정된 위협은 해당 관련 업체만 전파하는 등 범위를 제한하여 관리하여야 한다.

4.2.3. 통합보안관제센터 설립

지금까지의 방산보안에서의 보안관제는 국방부 방위산업보안업무 훈령이나 방위산업물자 및 방위산업체 지정 규정 등에서 요구하는 방산업체 대상의 시스템 구축이었다. 하지만, 2016년 방위산업기술 보호법 시행으로 방위산업기술을 보유하고 있는 일반업체에서도 보안관제 기능을 구비해야한다. 일반업체는 방산업체보다 많은 000여 개의 업체로 대다수의 일반업체도 중소기업으로 구성되어 있어 정보보호 전문 인력이 부족한 실정이다. 또한 보호 대상이 되는 업체 수가 증가함에 따라 각 업체별 분산 관제되었던 위협 정보를 수집하고 공유하는 데 있어 자칫 수집·공유가 제한될 경우 침해 사고에 기민하게 대응할 수 없다.

따라서 궁극적으로는 금융 ISAC 사례와 같이 전담 조직을 구성하여 통합보안관제 서비스를 제공해야 할 것으로 판단되며 이를 위해서는 표 3과 같이 전문 인력으로 구성된 보안관제 팀과 침해대응 팀, 그리고 보안 교육 및 컨설팅을 담당하는 보안지원 팀 등이 필요하다.

〔표 3〕 방산 통합보안관제센터 조직(안)

구 분	기 능
보안관제	· 방산부문 24시간 365일 관제 · 침해사고 예·경보 전파 · 사이버 위협정보 공유
침해대응	· 침해사고 분석 · 위협정보 분석 · 대응방안 제공
보안지원	· 대상기관 취약점 진단 · 해킹 메일 등 모의훈련 · 방위산업기술보호 등 보안교육 지원 · 기타 보안컨설팅

4.3. 추가 연구

통합보안관제 기능이 포함된 방산 ISAC 설립에는 중장기적으로 통합관제기능 및 운영 기관에 대한 법적 근거 강화, 예산 및 인력 확보 방안 등이 마련되어야 한다. 법적 근거는 방위산업기술 보호법 시행에 따른 보호대상기관의 확대 등 방산보안 개념의 확장으로[27], 방위산업기술 보호법 개정을 통해 방산업체뿐만 아니라 방위산업기술을 보유하고 있는 일반업체를 포함하여 통합보안관제 근거를 마련해야 한다. 이를 통해 일반업체에 대한 정부 지원 등의 정책을 추진할 수 있을 것이다. 예산 측면은 초기 정착을 위해 정부 예산으로 보안관제센터를 설립하고, 차후 운영 유지는 취약점 점검이나 교육지원, 보안 컨설팅 등을 통한 회원사 회비로 재원을 마련한다.

그 외에도 김하영 등의 연구[28]에서와 같이 차후 방산 ISAC의 효과를 극대화하기 위해 방산업체의 공감대를 얻어 정부의 개입을 최소화한 자발적인 운영, 최고경영자들의 정보보호에 대한 관심, 정보공유에 대한 긍정적 인식이 필요하다. 또한 방산업체의 자발적인 ISAC 가입 유인을 위한 다양한 인센티브 정책도 발굴해야 할 것이다.

Ⅴ. 결 론

4차 산업혁명을 주도할 국방 핵심 분야로 방위산업이 주목받고 있다. 최근에는 방위산업기술이 국가 안보뿐만 아니라 국익 차원에서도 크게 인식되면서 방위산업기술 보호에 대한 중요성도 증대되고 있다.

본 논문은 근래에 방산업체에 대한 사이버 위협이 지속적으로 발생함에 따라 방산업체 보안관제 환경을 진단하고 방산 ISAC을 설립함으로써 방위산업 사이버 보안을 강화하는데 그 목적이 있다. 본문에서 방산업체 보안관제 환경 분석과 국내·외 사례를 통해 ISAC 설립을 위한 시사점을 살펴보았으며, 이를 통해 법적 근거 마련 및 단계별 ISAC 설립 방안을 제시하였다.

방산 ISAC은 여러 기관 및 업체에서 수집한 사이버 침해 위협을 분석하고 전파함으로써 효율적인 공동대응 체계를 구축할 수 있으며, 다양한 보안 서비스를 제공함으로써 방산업체의 보안 시스템 구축에 대한 부담을 줄이고 방위산업 사이버 보안 강화에 기여할 것으로 기대

된다.

참 고 문 헌

[1] 손서연, 권구복, 장병호, “방위산업 동향 분석과 시사점,” *Weekly KDB Report*, Aug. 2016.

[2] 안랩 시큐리티대응센터 분석팀, “국내 방위산업체 공격 동향 보고서,” July 2017.

[3] 윤오준 등, “주요국의 사이버위협정보 공유체계 분석을 통한 국내 적용모델 연구”, *융합보안논문지*, 16(7), pp. 101-111, Dec. 2016.

[4] 김동희 등, “사이버 위협정보 공유체계 구축방안에 관한 연구 - 미국 사례를 중심으로 -”, *융합보안논문지*, 17(2), pp. 53-68, Jun. 2017.

[5] 김재광, “사이버안보 위협에 대한 법제적 대응방안”, *법학논고*, pp. 145-177, May 2017.

[6] 김도승, “국가 사이버 안보의 법적 과제”, *미국헌법연구*, 28(2), pp. 99-130, Aug. 2017.

[7] National Council of ISACs, http://www.nationalisacs.org

[8] 정보통신 ISAC, www.isac.or.kr

[9] 김소선, “미국 사이버 위협 정보 공유 동향 및 시사점,” *KISA Cyber Security Issue*, 한국인터넷진흥원, pp. 24-41, May 2015.

[10] U.S. Homeland Security, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, 2003.

[11] U.S. Homeland Security, *National Infrastructure Protection Plan (NIPP) 2013 : Partnering for Critical Infrastructure Security and Resilience*, 2013.

[12] 배병환 등, “영국의 사이버 보안 추진체계 및 전략 분석,” *Internet & Security Focus*, 한국인터넷진흥원, pp. 4-21, Aug. 2014.

[13] European Union Agency for Network and Information Security, https://www.enisa.europa.eu

[14] 금융보안원, www.fsec.or.kr

[15] 한국지역정보개발원, www.klid.or.kr

[16] U.S. Homeland Security, *Defense Industrial Base Sector-Specific Plan*, 2010.

[17] Defense Industrial Base Information Sharing and Analysis Center, www.dibisac.net

[18] 국방부, 방위사업법, 2018

[19] 한국방위산업진흥회, www.kdia.or.kr

[20] 국방부, 방위산업보안업무훈령, 2018

[21] 산업통상자원부, 방위산업물자 및 방위산업체 지정 규정, 2014

[22] 한국산업기술보호협회, www.kaits.or.kr

[23] 김애찬 등, “효과적인 사이버위협 정보공유체계 수립을 위한 요구사항의 우선순위 도출에 관한 연구”, *정보보호학회지*, 26(1), pp. 61-67, Feb. 2016.

[24] 명지대학교 방산보안연구소, “방산관련업체 기술보호역량 진단 연구”, 방위사업청 연구용역 보고서, Jan. 2016.

[25] 과학기술정보통신부, 보안관제 전문업체 지정 현황, www.msit.go.kr, 2018.

[26] NIST Special Publication 800-150, *Guide to Cyber Threat Information Sharing*, 2016.

[27] H. Park, et al., “Conceptualization of Defense Industrial Security in Relation to Protecting Defense Technologies,” *in Proc. Computational Science and Its Applications - ICCSA 2018*, pp. 158-169, July 2018.

[28] 김하영 등, “국내 사이버위협 정보 공유에 영향을 미치는 요인”, *정보보호학회논문지*, 27(5), pp. 1167-1188, Oct. 2017.

〈저 자 소 개〉

박 홍 순 (Heungsoon Park)
종신회원

2002년 3월 : 육군사관학교 전산학과 졸업
2007년 3월 : 미국 Air Force Institute of Technology 컴퓨터공학 석사
2016년 1월 : 국방대학교 컴퓨터공학 박사
2016년 8월～현재 : 국방보안연구소 방산보안실 선임연구원
관심분야 : 방위산업보안, 방위산업기술보호, 사이버전, 네트워크 보안