4차 산업혁명 시대의 통합 사이버 보안 프레임워크 구축에 대한 연구

이진용*, 양선주**, 장형진*
*한국정보통신기술협회 정보보호단
**한국인터넷진흥원 보안인증단
topjin55@tta.or.kr, sjyang@kisa.or.kr, chj760@tta.or.kr

A study on the Establishment of an Integrated Cyber Security Framework in the Era of the 4th Industrial Revolution

Jin Yong Lee*, Sun Joo Yang**, Hyoung Jin Jang*
*Infomation Security Department, Telecommunications Technology Association
**Security Certification Team, Korea Internet & Security Agency

요 약

국가 4차 산업혁명의 성장 동력으로 데이터 경제가 주목받고 있으며, 現산업계는 초연결, 초지능, 초융합 사회로 진보하고 있다. 이와 같은 환경에서는 산업군 간의 경계가 사라지고 전방위적인 상호 유기적인 복합 생태계를 구성하게 된다. 따라서 사이버 보안사고 발생 시 단순 데이터 탈취 정도에 국한되지 않고 안보, 생명, 국가 경제 등에 돌이킬 수 없는 손실을 끼칠 것으로 예상된다.

그러나 현재 사이버 보안의 각종 제도 및 법령 등은 중복·혼재되어 있거나 특정 산업군에 적용하기에는 일부 미흡한 요소도 존재한다. 본 논문에서는 이와 같은 문제점을 개선하고 전방위적인 보안 거버넌스를 달성하기 위한 통합 사이버 보안 프레임워크 구축 방안을 제언한다.

1. 서론

4차 산업혁명시대로 진보하고 있는 現사회는 초지능, 초연결, 초융합의 특성에 따라 각 산업군은 그 경계를 넘어 환경, 자원 및 행위 결과물을 상호 연결·융합하여 이용자에게 기대 이상의 가치를 창출하고 있다.

이와 같은 환경은 빅데이터 기반의 고도의 인공지능 기술을 중심으로 구현되고 있기 때문에 데이터 무결성과 정보의 안전성은 목적 달성을 위한 필수불가결한 요소이자 핵심이 된다.

또 다른 한편으로는 데이터 및 정보의 주도권을 획득하려는 경쟁이 국가, 회사 및 개인 간에 치열하게 발생하고 있다.

이중 국가별로 조직화된 APT(Advanced Persistence Threat : 지능형지속위협공격) 그룹은 충분한 활동 범위와 시간을 바탕으로 정보의 모든 연결고리를 장악한다는 점에서 전방위적인 보안 대응체계가 필요함을 시사해준다.

따라서 사이버 보안 프레임워크는 다양한 측면에서 통합·유기적으로 대응할 수 있어야 하나 現국내 사이버 보안 프레임워크 및 법령 등은 분할되어 및 단절되어 중복·상충·누락 등이 발생하고 있다.

따라서 본 연구에서는 現사이버 보안 프레임워크의 현황 및 한계를 분석하고 4차 산업혁명 시대에 적합한 통합 사이버 보안 사이버 보안 프레임워크의 구축방안을 제시하고자 한다.

2. 사이버 보안 프레임워크 현황 분석

사이버 보안 프레임워크는 절차(Process)측면과 제품(Product)로 나누어지고 있으며 산업군, 서비스, 규모 등에 따라 적용받는 제도와 법률 등이 상이하게 관리되고 있다. 또한 관련 법률 들은 직·간접적 보호대상을 바탕으로 넓은 스펙트럼으로 구성되어 있다.

2.1. 국내 사이버 보안 프레임워크 운영 현황

<표 1>과 같이 프로세스, 제품측면의 사이버 보안 프레임워크는 과학기술정보통신부(이하 과기부)가 상당 부분 주도하고 있는 실정이며, 개인정보보호위원회(이하 개보위)와 국정원이 일부 참여하고 있다. 따라서 우리나라 주요 사이버 보안 프레임워

크는 정보통신 서비스 제공자의 관점으로 발달하고 있다.

<표 1> 국내 사이버 보안 주요 인증제도

구분	인증 제도	대상군	주관 부처	법률
프로세스	개인정보보호 및 정보보호 관리체계인증	정보통신 서비스 제공자 및 개인정보 취급자	과기부, 개보위	정통망법, 개인정보 보호법
	정보보호 준비도 평가	全산업군 (영세기업)	과기부	정보보호 산업법
	클라우드 인증	공공기관을 위한 클라우드 서비스 제공자	과기부	클라우드 발전법
	데이터보안 인증	全산업군	과기부	N/A
	산업보안 인증	全산업군	N/A	N/A
제품	정보보호 시스템 보안성 평가 (CC)	공공·민간 (정보보호제품)	과기부	국가정보화 기본법
	암호모듈 검증제도 시험·평가	공공 (암호제품)	국정원	전자정부법
	IoT보안인증	全산업군 (IoT 제품)	과기부	N/A

<표 2>와 같이 일반 산업직군은 산자부, 국방부, 특허청 등의 주관하에 직·간접적인 보안 통제를 위한 법률이 존재하나 해당 통제를 위한 체계적인 사이버 보안 프레임워크는 보편화되지 않았다.

<표 2> 일반 산업군의 보안통제 현황

구분	보호대상	주관 부처	법률
직접	국가핵심기술(산자부), 첨단기술(산자부), 신기술(환경부, 산자부), 건설기술(국토부), 보건기술(보건복지부) 등의 기술 보호	산자부	산업기술의 유출방지 및 보호에 관한 법률
	영업비밀 보호 (기업, 개인, 공공)	특허청	부정경쟁방지 및 영업비밀보호에 관한 법률
	중소기업 기술 보호	중소 벤처 기업부	중소기술 보호지원에 관한 법률
	국방 분야의 방위기술 보호	국방부	방위산업기술 보호법
간접	전략 물자에 수출통제	산자부	대외무역법
	국가안보 위해와 관련된 외국인 투자 제한	산자부	외국인투자 촉진법
	특허, 실용신안, 디자인, 상표, 저작권 등 보호	과기부	지식재산 기본법
	절도, 배임·횡령 등에 대한 통제	법무부	형법

2.2. 국외 사이버 보안 프레임워크 운영 현황

<표 3>과 같이 미국, EU 등 주요 국가에서는 사이버 보안 컨트롤타워를 구축하기 위한 법률을 수립하고 통합 사이버 보안 프레임워크를 구축하고있는 추세이다.

<표 3> 국외 주요 사이버 보안 프레임워크

구분	보안 프레임워크	주요 내용
미국	사이버보안 및 기반구조보안 기관법	사이버보안과 기반구조보안에 대한 관리 주체를 일원화
EU	사이버보안법	유럽연합집행위원회(EC)의 일원화된 사이버 보안의 적합성 평가 수행 ※ 인증 및 표준관리 : ENSIA
중국	네트워크 안전보장법 (사이버 보안법)	네트워크·핵심정보 인프라에 대한 정보보호
일본	사이버보안 기본법	사이버보안전략 본부 주관의 정보보안 추진 법적 근거 확립

2.3. 관련 연구

사이버 보안 프레임워크 구축에 대한 연구로는 환경과 상황적 특성에 따라 전문화되는 분야와 관리·기술·물리의 보안관리체계 관점에서의 세부 요소에 대한 측정관리 및 효과적인 연계 구성 분야로 나누어 볼 수 있다.

환경 및 상황적 특성 분야에서의 사이버 보안 프레임워크 모델은 사회공학기법, 지능형지속공격 및 제어시설 공격 등 목표 대상에 직접적인 피해를 유발시키는 침해행위에 대응하기 위한 방법[1,2,3,4] 등이 제시되고 있다.

반면 보안관리체계 영역에서는 자산, 솔루션, 탐지, 사고 처리 등 일련의 통제분야에 대한 오케스트레이션 구축을 위한 모델[5], 사이버 보안 직무 역량 강화 및 인력 양성을 위한 모델[6], 사이버 보안을 위한 핵심 요소에 대한 정량·정성적 측정을 통한 보안 거버넌스를 구축하는 모델[7,8,9] 등이 존재한다.

3. 통합 사이버 보안 프레임워크 구축

본 논문에서는 특정 환경 및 보안관리체계 분야의 일부 관점 등에 국한된 기존 보안 프레임워크의 한계성을 개선하고, 보안통제 범위를 전방위로 유기적·지속적 확장할 수 있는 통합 사이버 보안 프레임워크를 구성하는 것에 목표를 두고 있다.

이와 같은 프레임워크는 (그림 1)과 같이 제도, 협의체, 측정, 연구의 4가지 구축 방향성을 기반으로 구현할 수 있다.

(그림 1) 통합 사이버 보안 프레임워크 구축 방향성

첫째, 통합 사이버 보안법 및 컨트롤타워 구축의 제도적 기반마련이 필요하다. 현재 국내에서 800여 개 이상의 인증서를 발급한 정보보호 및 개인정보보호 관리체계(ISMS-P) 제도의 경우 법적 의무화가 적용된 2013년 이후 인증서 발급이 가파르게 상승[10]하였다. 이와 같은 사례에서 볼 수 있듯이 통합 사이버 보안 프레임워크의 활성화를 위해서는 강력한 추진체계 및 법률적 뒷받침이 필요하다.

둘째, 산업군 간의 유기적 보안 연계를 위한 사이버 보안 협의체를 구성하여야 한다. 이를 통해 중복·누락 등을 제거하고 상호 유기적 연계를 위한 협의체 구성하여 4차 산업혁명의 초연결 패러다임에 부합할 수 있어야 한다.

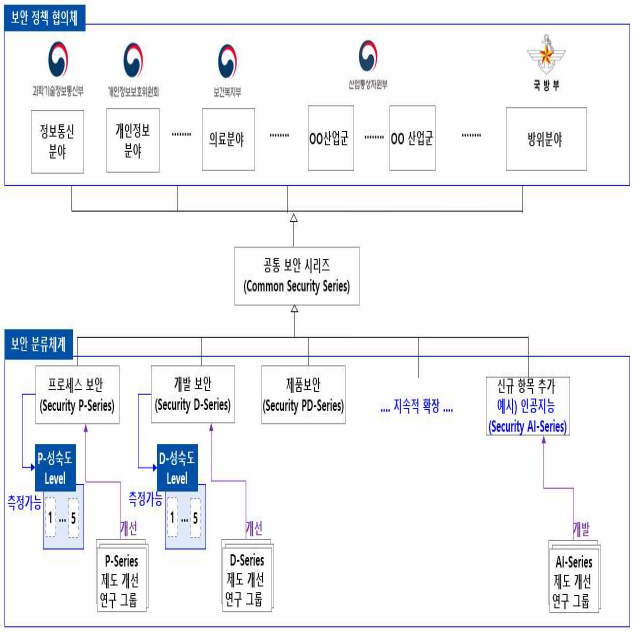
셋째, 보안 수준 측정을 통하여 동기 부여를 통한 지속적 개선 환경을 구성해야 한다. 목표 수준을 정량화하지 않을 경우 개선에 대한 동기 부여를 저하할 수 있다. 이때 측정은 프로세스 및 제품 관점을 모두 포괄하는 다차원적 관점이 필요하다.

넷째, 보안 프레임워크의 지속 개선 및 신규 영역 개발 환경을 조성할 수 있는 조직이 필요하다.

이와 같은 방향성을 바탕으로 통합 사이버 보안 프레임워크에 대한 구축방안을 도출한다.

3.1. 통합 사이버 보안프레임워크 체계

(그림 2)는 통합 사이버 보안 프레임워크를 도식화한 것이다.



(그림 2) 통합 사이버 보안 프레임워크(예시)

먼저 최상단에는 각 산업분야의 제도 및 법률을 만들 수 있는 정책기관 간의 보안정책 협의체를 구성하여 의장을 선출하고 통합 사이버 보안법을 제정하여 보안 컨트롤타워를 구축한다.

다음으로 모든 보안영역에서 준수하여야 하는 공통 기본단위로 최상단 공통 보안 시리즈(Common Security Series)를 제정한다.

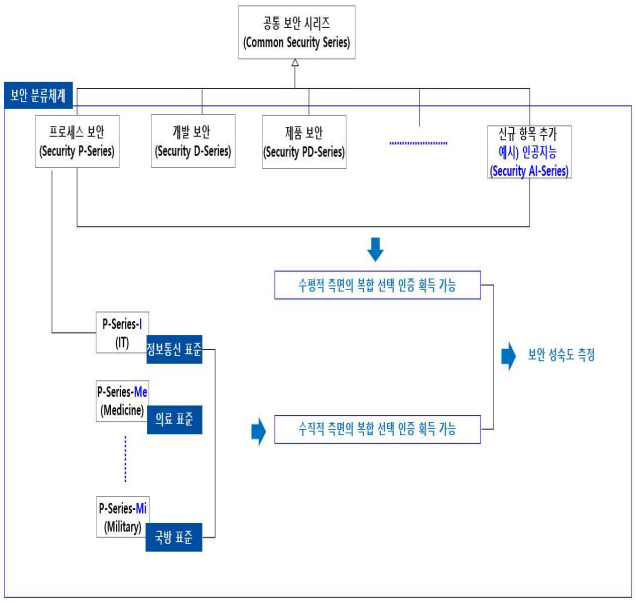
공통 보안 시리즈를 중심으로 수평적으로는 프로세스, 개발, 제품 및 신규 분야 등 보안특성 분야별 확장가능 체계로 구성하고, 수직적으로는 각 분야에서 산업군별로 세분화·전문화될 수 있도록 구성한다. 예를 들어 (그림 3)에서 수평적 측면의 방향으로는 프로세스 보안 분야는 수직적 측면의 방향으로는 정보통신, 의료, 국방 등으로 시리즈가 확장될 수 있다.

3.2. 통합 사이버 보안 프레임워크의 연계성 가시화

통합 사이버 보안 프레임워크의 유기적 연계성 가시성을 확보하기 위해 최상위 공통 보안 시리즈(Common Security Series)를 기반으로 확장되는 특성에 따라 네이밍 규칙을 마련한다.

예를 들어 (그림 3)의 수평 방향으로 확장되는 프로세스 보안은 “Security P-Series”, 개발 보안은

“Security D-Series” 등으로 네이밍할 수 있다. 반면 수직 방향의 경우 프로세스 보안 시리즈(Security P-Series)를 예시로들 경우 “Security P-”의 접두사를 기반으로 하여 IT분야는 “Securty P-I”, 의료분야는 “Security P-Me” 등으로 네이밍을 하여 관리되고 있는 범위에 대한 직관적 가시성을 확보할 수 있도록 한다.



(그림 3) 통합 사이버 보안 프레임워크의 네이밍 규칙(예시)

3.3. 보안 수준·성숙도 측정 환경 구축

(그림 2)와 같이 수평영역의 프로세스 보안, 개발 보안 등의 각 영영군마다 P(프로세스), D(개발), PD(제품) 등의 보안 성숙도를 측정할 수 있도록 하여 지속 개선할 수 있는 동기를 부여할 수 있도록 한다. 또한 수평·수직 방향으로 복합 인증이 가능하도록 하고 이에 대한 결합을 통해 최종 보안 성숙도를 도출할 수 있다.

3.4. 제도 개선 연구 그룹

(그림 2)와 같이 수평 영역군마다 제도 개선 연구 그룹을 구성하여 제도의 실효성을 확보하고 신규 영역을 지속적으로 확대할 수 있는 기반을 마련한다. 연구 그룹으로는 실제 업무를 수행하고 있는 실무자 및 외부 전문가 등으로 구성할 수 있으며, 타 영역군에 대해서도 겸직이 가능하게 하여 전문성 및 보안의 관점을 넓힐 수 있도록 한다. 또한 신규 보안 영역군의 개발 및 통합 등을 위한 각 연구그룹간의 TF 조직을 구성하여 상호 시너지를 낼 수 있도록 관리한다.

4. 결론

본 논문은 4차 산업혁명으로 인한 초연결 시대의 혼재된 사이버 보안 프레임워크에 대한 통합 거버넌스를 증진하고 다양한 산업군의 특성에 보다 실효적으로 대응할 수 있는 유기적 연계 및 확장성 모델 수립을 위한 방안을 제시하였다.

이는 제도, 협의체, 수준측정, 연구·개발 측면의 통합적 측면의 방향성이 뒷받침되어야 한다.

향후 제안된 모델을 검증할 수 있는 관련 연구와 국제 정보보호 표준과의 상호 인정을 위한 체계를 갖출 경우 효과 및 보편성을 증진할 수 있을 것으로 기대된다.

참고문헌

[1] 김승준, 이석원, “지능형 지속 위협을 막기 위한 사회공학 기반 보안요구사항 추천 프레임워크”, 정보과학회논문지, 45(10), 1015-1028, 2018.

[2] 이상도, 신용태, “제어시설 사이버공격 대응을 위한 사이버보안 프레임워크(Framework)연구”, 예술인문사회 융합 멀티미디어 논문지, 8(4), 285-296, 2018.

[3] Homeland Security Advisory Council, “Top Ten Challenges Facing the Next Secretary”, A. Homeland Security, 2008.

[4] Lee, C., Park, W., “Enhancing industrial security management system for multimedia environment”, Springer, 2015.

[5] 이세호, 조인준, “사이버보안 프레임워크 기반의 보안 오케스트레이션 서비스 모델 제안”, 한국콘텐츠학회논문지, 20(7), 618-628, 2020.

[6] 미국ATE정책 기반의 신규 사이버보안 인력양성 정책 비교 프레임워크 연구, 한국정보보호학회논문지, 28(1), 249-267, 2018.

[7] 방기천, “정보보안체계 운영경험 진단을 통한 국가 사이버보안 거버넌스모델 연구 방법”, 디지털복합연구, 16(6), 205-212, 2018.

[8] Public Law, “Cybersecurity Workforce Assessment Act”, 113-246, 2014.

[9] Public Law, “Cybersecurity and Infrastructure Security Agency Act of 2018”, 115-278, 2018.

[10] KISA, https://isms.kisa.or.kr/main/isms/issue/.