Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.2, Apr. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.2.309

사이버 공급망 보안 관점의 국가 정보보안 기본지침 개선방안 연구

유 영 인,[1†] 배 선 하,[1] 김 소 정,[2] 김 동 희[1‡]
[1]국가보안기술연구소 (선임연구원), [2]국가안보전략연구원 (책임연구위원)

A Study on the Supplementation of the Korea's National Information Security Manual from the Perspective of Cyber Supply Chain Security

Young-in You,[1†] Sunha Bae,[1] So Jeong Kim,[2] Dong Hee Kim[1‡]
[1]National Security Research Institute(Senior Researcher),
[2]Institute for National Security Strategy(Principal Researcher)

요 약

주 산업 분야에서 ICT 융합화가 진행되고 공급망의 글로벌 생태조성이 가속화됨에 따라, 공급망 위험 또한 지속적으로 증가하고 있다. 특히, ICT 제품의 공급망은 관리해야 할 기술적·환경적 요인들이 매우 복잡하여, 전체 생명주기에 걸친 투명한 관리가 어렵다. 이에 미국·영국·EU 등 세계 주요국과 국제연합은 ICT 제품 공급망 대상의 사이버 공급망 보안 관련 연구와 정책을 수행·수립 중이다. 우리나라도 2019년 발표한 국가사이버안보전략의 기본계획 내에 주요 ICT 장비의 공급망 보안을 위한 관리체계를 구축하는 등 현안으로써 추진하고 있으나, 국가·공공기관을 위한 조직·기관 수준의 정책은 아직 부재한 상황이다. 본 논문에서는 미국의 사이버 공급망 보안 관리체계를 검토하여, 사이버 공급망 보안 관점의 우리나라 국가 정보보안 기본지침 보완방안을 제시한다. 이는 국내 정보보안 분야에서 도입 가능한 사이버 공급망 조치사항의 참고 자료가 될 것으로 기대한다.

ABSTRACT

As ICT convergence is progressing in all industrial fields and creating the global ecosystem of the supply chain is accelerating, supply chain risk related with cyber area are also increasing. In particular. the supply chain of ICT products is very complex in terms of technical and environmental factors to be managed, so it is vert difficult to transparently manage the entire life cycle. Accordingly, the US, UK, and EU, etc. are conducting and establishing cyber supply chain security-related research and policies for ICT product supply chains. Korea also has the plan to establish management system to secure the supply chain of major ICT equipment as a task in the basic plan of the national cybersecurity strategy announced in 2019, but there is no concrete policy yet. So, In this paper, we review the cyber supply chain security management system in the United States and present a supplementary way to the National Information Security Manual in Korea from the perspective of cyber supply chain security. It is expected that this will serve as a reference material for cyber supply chain measures that can be introduced in domestic information security field.

Keywords: Cyber supply chain security, security controls, security manual

Received(01. 25. 2022), Accepted(02. 25. 2022)

† 주저자, crenius@nsr.re.kr
‡ 교신저자, dh_kim@nsr.re.kr(Corresponding author)

I. 서 론

오늘날 全 산업 분야에서 ICT 융합화가 진행됨에 따라, 반도체, 소프트웨어 등의 안정적 수급은 국가 경제에 영향을 미치는 중요한 요인으로 작용하게 되었다. 그러나 많은 기업이 제품생산 단가 등 경제적 이익을 목적으로 공급망 해외 진출을 가속화함에 따라, 공급망에 참여하는 이해관계자의 다양화, 국가 간 정치적 갈등으로 인한 규제 등이 안정적 운용을 방해하는 변수로 작용하여 공급망 위험이 증가하고 있다. 특히 ICT 제품의 공급망은 관리해야 할 기술적·환경적 요인들이 매우 복잡하여 제품의 설계·생산·배포 모든 단계에서 위·변조 방지 및 투명한 관리가 다른 산업부문에 비해 어려운 상황이다.

미국, 영국, EU 등 세계 주요국과 국제연합은 ICT 제품 공급망 대상의 사이버 공격 대응을 위한 사이버 공급망 보안 관련 연구와 정책들을 수행·수립하고 있다. 사이버 공급망의 주요 위협 식별, 공격 시나리오 분석 및 권고사항 제시가 골자이다[1][2]. 이 중 미국은 오래전부터 사이버 공급망 보안을 위한 표준 문건과 지침을 마련해왔으며, 이미 연방기관이 수행해야 하는 세부업무까지 수립한 상태이다. 또한, 최근 국토안보부를 중심으로 민·관이 협력하여 사이버 공급망 위험평가, 관리 중요도 우선순위 도출 및 실무 활용 자료·도구 개발 등의 다양한 강화 활동을 추진 중이다[3].

우리나라도 ICT 의존도가 매우 높은 국가로, 사이버 공급망 보안위험 대응 정책 수립을 위한 적극적인 검토가 필요하다. 관련하여, 2019년 국가사이버안보전략 발표 후, 국가사이버안보기본계획 내에 주요 ICT 장비의 공급망 보안을 위한 관리체계 구축 과제가 이행 중이다. 그러나 국가·공공기관 대상의 사이버 공급망 보안관리를 위한 포괄적인 정책, 지침 등은 아직 부재한 상황이다.

우리나라는 국가정보원법, 보안업무규정, 정보통신기반 보호법 등에서 국가·공공기관이 수행해야 하는 보안·보호 업무를 규정하고 있는데, 정보보안과 관련한 기본업무는 국가 정보보안 기본지침이 규정한다.[4] 정보화 사업 발주·관리·도입 등 사이버 공급망과 관련된 업무도 기본지침을 따르도록 규정하고 있기에 기본지침에서 공급망 보안업무를 일부 제시하고 있으나, 전체 정보보안 업무 관점에서 보완이 필요하다. 최근 기본지침을 국가사이버안보센터가 공개 운영하여(2021.11.) 민·관 모두 참고하는 자료가 됨에 따라, 기본지침이 사이버 공급망 보안 개념의 반영을 우선 수행해야 하는 정책문건인 것으로 판단된다.

이에, 본 논문에서는 현재 조직·기관 수준의 사이버 공급망 보안관리를 가장 체계적으로 수립·운용 중인 미국 사례를 검토하여 국내 활용방안을 모색한다. 연방기관 대상의 사이버 공급망 보안관리체계를 분석하여, 미국의 사이버 공급망 보안에 대한 개념, 신규 고려요소 등 방향성을 살펴보고, 세부 관리를 위한 보안통제를 분석한다. 다음, 국가 정보보안 기본지침에서 고려할만한 미국의 사이버 공급망 보안통제를 식별한다. 식별 결과를 활용하여, 사이버 공급망 보안이 필요한 기본지침 각 조항에서 고려되어야 하는 보안업무를 제시한다.

II. 미국의 사이버 공급망 보안 관리체계

미국은 정보·정보시스템 도입·운영 전 과정을 대상으로 하는 공급망 공격에 대응하기 위해, 이를 사이버 공급망 위험으로 정의하고 기존 정보보안 관련 지침 및 가이드라인의 업데이트를 진행 중이다. 연방기관 정보보안 지침인 위험관리 프레임워크(Risk Management Framework), 사이버보안 프레임워크(Cybersecurity Framework)가 대표적 사례로, 기존 개념에 공급망 위험을 반영하고 있다[5][6]. 이외 정보보안을 위한 지침이 다수 존재하는데, 각 지침을 공급망 관점에서 융합·활용하는 문건이 NIST SP 800-161(이하 800-161)이다[7]. NIST는 초기 ICT 공급망 위험관리를 위해 800-161 발표 이후(2015), 공급망 위협요소 증가와 OT 부문으로 관리 범위 확장 및 관련 지침들의 업데이트 사항을 반영하기 위해 800-161의 개정을 진행하고 있다[8]. 현재 800-161 개정(안)이 공개된 상태로, 본 고에서는 해당 문건을 분석하여 미국 사이버 공급망 보안관리의 주요 특징을 파악하고 우리나라 공급망 보안체계 수립과정에서 참고할만한 사항을 식별하고자 한다.

2.1 800-161 개정(안)(이하 개정(안)) 검토배경

개정(안)에서부터 사이버 공급망에 대한 NIST의 명확한 위험인식과 관리대상 및 목적, 달성을 위한 업무 내용이 파악 가능해졌다[9]. 기존 800-161은 ICT 공급망 위험의 정의를 보편적인 정보보안 위험과 다르게 보지 않았으나, 개정(안)에서 이를 구체적

으로 정의함에 따라 수반 개념·내용이 명확해졌다. 현재 버전이 개정(안)이긴 하나, 주요 변경사항을 모두 포함하며, 최근 진행한 개정(안) 업데이트에 대한 워크샵(2021.12.01.)에서도 전반적 구성 내용, 방향성의 변동은 없기에 참고에 의의가 있다[10].

2.2 개정(안) 핵심 개념

개정(안)은 사이버 공급망 위험을 공급자, 공급자의 공급망, 공급자의 제품 및 서비스의 사이버 부문 관련 위협·취약점으로부터 기인하는 것으로 정의한다. 해당 위험을 관리하기 위한 체계화된 프로세스가 사이버 공급망 위험관리(Cyber-SupplyChainRiskManagement, 이하 C-SCRM)다. C-SCRM을 위한 연방조직 내에 프로세스와 위험 완화조치의 식별·평가·선정·구현에 대한 지침을 제공하는 것이 개정(안)의 골자이다. 개정(안)의 주요 내용은 다음과 같이, C-SCRM 체계, 역할·책임, 통제, 권고사항으로 개관할 수 있다.

2.2.1 C-SCRM 체계

미국 연방기관 조직 전반의 위험관리 절차를 제공하는 NIST SP 800-39[11]에 사이버 공급망 관점을 반영하여, C-SCRM을 위한 4단계의 프로세스와 각 프로세스에서 수행해야하는 과업을 정의한다. 이는 조직 사이버 공급망의 구조·범위를 식별하고 위험관리 전략을 설정하는 기반조성(Frame) 단계, 조직 고유 상황 식별 및 사이버 공급망 침해 가능성과 영향을 측정하는 평가(Assess)단계, 대응 조치를 도출하고 결정·구현하는 모니터링(Monitor) 단계로 구성된다. 각 단계를 순차적으로 수행해야하는 것은 아니며 상황에 따라 동시에 여러 단계를 수행해야 할 수 있고, 산출결과는 다른 단계에 상호영향을 준다. 본 프로세스를 통해 위험관리 전략, 프로그램 등 여러 결과물이 산출되나, 궁극적인 목표는 해당 연방조직에 적합한 공급망 보안통제 식별이다. 800-161과 개정(안)을 비교하였을 때, 프로세스별 과업의 구성은 변동이 없고 개정(안)의 사이버 공급망 위험 정의 개편에 따라 각 과업의 산출물과 참조 문건 등이 업데이트 되었다.

2.2.2 C-SCRM 역할·책임 할당

C-SCRM을 위한 역할과 책임을 조직의 모든 임직원 및 공급업체 등 내·외부 공급망 이해관계자에게 할당한다. 경영진, 중간관리자, 실무진 3개 계층으로 구분하여 공급망 위험관리 과업을 분배한다. 각 과업의 주요 내용은 상기 순서대로, 공급망 위험관리 전략 방향 수립, 구현계획 수립 및 프로그램·프로젝트 관리, 제품·서비스의 개발·구현·조달·운영이다. 기존 800-161과 개정(안)의 가장 큰 차별점은 위험전략 수립의 세분화이다. 800-161은 위험관리 전략 방향 수립에 위험허용범위(Risk Tolerance) 개념을 활용하였는데, 개정(안)에서는 위험성향(Risk Appetite) 개념을 추가 활용한다. 위험허용범위가 자산, 위협 등 특정 부분에 대한 위험 용인 수준이라면, 위험성향은 위험허용범위 도출 전에 조직이 추구·수용하는 위험 유형과 전체 위험의 양을 의미한다. 이는 C-SCRM의 거시적 방향성에 대한 책임을 경영진에게 명시적으로 부과한 것으로, 두 개념의 순차적 결정은 공급망 보안에 대한 경영진의 역할과 책임을 강화할 것으로 보인다. 또한 공급망 보안 관련 책임을 중앙에 집중하는 운영방식을 권고하여, 책임 강화와 더불어 상기 모든 계획·구현 활동에 대한 관리의 일관성과 효율성 확보를 도모하고 있다.

2.2.3 C-SCRM 통제 구성

사이버 공급망 위험 완화조치를 위한 통제집합을 NIST SP 800-53 Rev.5(이하 800-53)[12] 각 통제에 '추가 C-SCRM 지침'을 작성하는 형태로 제공한다. 800-53에서 제공하는 통제는 특정 부문에 종속되지 않는 범용적인 보안통제로, 해당 부문에서 활용 시 조정이 필요하다. 이에, 800-161도 공급망 보안에 필요한 통제를 식별하여 보완작업 후 별도의 통제집합을 구성했다. 개정(안)부터 해당 통제를, 연방조직이 공통으로 구현해야 하는 필수구현통제(C-SCRM Baseline)와 상·하위 도급업체가 필수 구현해야 하는 통제(Flow Down Control)로 지정 운영하여, 공급업체를 조직 공급망보안에 통합하고자 한다. 자세한 내용은 3장에서 기술한다.

2.2.4 C-SCRM 수행을 위한 권고사항 제시

C-SCRM은 기존 정보보호 관점의 확장적 활동임

과 동시에 새로운 개념이므로 신설에 비교적 많은 자원과 운영을 위한 추가 요소가 존재한다. 이에 개정(안)에서는 C-SCRM 활동에 대한 권고사항을 제공한다. 기존 조달·계약관리 절차에 C-SCRM 통합방안, 교육·훈련 개발·운영 및 정보공유 고려사항, 조직 공급망 보안 역량측정 방법론 및 C-SCRM 실무 구현에 대한 참조모델이 골자이다. 사이버 공급망 고유 특성에 기반한 비용 효율적 관점의 내용들로, 별도의 위험·구현·평가 지표의 수립·활용을 권고한다.

2.3 개정(안) 활용방안

개정(안)은 사이버 공급망 위험관리를 하나의 독립적 분야로 인식하고 관리체계 수립·운영을 위한 일련의 맞춤형 업무를 제공하는 것이 가장 큰 특징이다. 기존 정보보안, 조달·계약관리 체계의 활용을 적극 권장하나, 사이버 공급망 고유 위험이 반영된 관리 프로세스가 기반이 되는 방식이다. 이는 사이버 공급망 관리를 위한 현존하는 가장 체계적인 지침으로 판단되나, 미국의 위험관리체계에 기반하고 있기에 우리나라가 모든 과정을 벤치마킹하기에는 무리가 있다. 다만, 사이버 공급망 위험완화 조치를 위한 C-SCRM 통제는 유사개념의 기존 정보보안 활동에 통합되어 있어, 국내 정보보안 관련 지침들과 비교·분석이 용이할 것으로 판단된다. 또한 800-161 및 개정(안) 모두 적절한 C-SCRM 통제의 구현이 최종 목적이기에, 미국 연방조직 사이버 공급망 보안업무 전반의 포괄적 검토 및 참고로써 의의가 있다. 이에, 본 고에서는 미국 사이버 공급망 보안통제의 선제적 검토를 수행하고 활용방안을 모색한다.

III. 미국 사이버 공급망 보안통제 구성방식, 현황

본 고 2장에서 검토한 개정(안)은 미국 연방기관에서 적용 및 활용해야 하는 시이버 공급망 보안통제 전체 목록을 수록하고 있다. 조직·도급업체 등 공급망 이해관계자를 포괄하는 일련의 보안업무를 체계적으로 제공하여, C-SCRM 활동의 최종 단계인 위험완화 조치에 활용한다. 본 장에서는 개정(안)의 보안통제 구성방식을 살펴보고, 구성방식 기준의 통제 분포비율, 주요 통제 내용 등 구성현황을 개관한다.

3.1 보안통제 구성방식

개정(안)은 800-53의 보안통제 중 사이버 공급망 관점의 '필수 구현 통제', '선택 불가', '선택 지양' 등의 기준을 활용하여 사이버 공급망 맞춤형 통제집합을 생성했다. 800-53은 보안통제를 기본통제 322개와 각 통제를 보다 강화하기 위한 심화통제(Control Enhancements) 867개로 구성하고 이를 20개의 통제 도메인으로 구분한다. 개정(안)은 이 중 기본통제 190개와 심화통제 105개를 사이버 공급망 관리에 필요한 보안통제로 식별하였고(전체항목 대비 25%), 기존 20개 통제 도메인을 모두 활용했다. 통제의 내용은 공급망 관점에서 재해설 하였으나, 통제 식별자(AC-1, AT-1 등)와 통제 명(계정관리 등)은 800-53의 형식을 준용한다.

개정(안)은 각 보안통제의 활용을 위해 '계층별 수행 보안통제', '조직 필수구현 통제', '도급업체 필수 적용 통제' 3가지 개념을 활용한다. 앞서 2.2.2. C-SCRM 역할·책임 할당에서 구분한 조직 계층에 따라 보안통제를 지정하여 계층별로 수행해야 하는 보안업무를 명확히 한다. 각 조직은 사이버 공급망 보안통제로 제공된 항목 중 조직 환경에 적합한 보안통제를 선별하여 활용하게 되는데, 해당 선별·활용 작업 전 필수구현이 권고되는 통제가 조직 필수구현 통제이다. 사이버 공급망 특성상, 보안 확보를 위해 도급업체의 관리와 도급업체와의 협업이 매우 중요한데, 해당 관점에서 도급업체에 적용해야 하는 통제를 지정하고 있다. 도급업체 필수 적용 통제는 1차 도급업체의 하도급업체까지 적용할 것을 권장한다.

3.2 보안통제 구성현황

기본통제 190개와 심화통제 105개를 모두 포함한, 사이버 공급망 보안통제 295개 항목의 구성현황을 보안통제 구성방식 기준으로 살펴본다. 조직 내 전 계층이 사이버 공급망 보안통제를 수행하도록 개정(안)이 구성한 보안통제의 분포율은 〔표 1〕과 같다. 경영진 수행 항목(Level 1), 중간관리자 수행 항목(Level 2), 실무진 수행 항목(Level 3) 범주 내에 각 보안통제의 할당은 〔조직 전 계층 수행, 중간관리자/실무진 수행, 실무진이 수행 등〕과 같이 중복을 허용하여 분포되어 있다.

경영진이 수행해야 하는 사이버 공급망 보안통제는 전체 항목대비 25%로 적으나, 정보보안, 물리보

Table 1. Distribution ratio of C-SCRM control by level

Category	The Number of controls	ratio	Top 3 Domains
Level 1	76	25%	Program Management, System·Service Acquisition Risk Assessment
Level 2	235	77.3%	Configuration Management, Program Management, Access Control
Level 3	249	81.9%	Configuration Management, System·Service Acquisition, Access Control

안 등 기존 보안요소와의 조정작업을 수행하여 조직 공급망 보안 기반을 마련해야 하는 중요 업무가 많다. 관련 보안활동은 '프로그램 관리', '시스템 서비스 및 획득', '위험평가'에 가장 많이 할당되고, 주요 업무는 사이버 공급망 보안에 대한 고위 직급 책임자 지정, 전용 예산과 인력확보, 조직 위험평가에 사이버 공급망 요소 반영 및 관련 위험을 조직 전체 대응 태세에 연계 등이다. 중간 관리자가 수행해야 하는 사이버 공급망 활동은 '구성관리', '프로그램 관리', '접근통제'에 가장 많이 할당하고 있다. 주로 사이버 공급망 보안 미비점 개선, 정보시스템/네트워크 및 시스템 개발 생명주기 전반의 구성에 대한 기준값 설정·추적관리 및 공급업체 불만사항 처리 등과 관련된 계획의 수립·관리를 수행한다. 실무진의 수행업무는 전체 항목대비 81.9%로 가장 많고, 주로 영향분석·테스트·개발·구현 관련 위주의 업무를 수행한다. 전체 업무의 1/3이 '구성관리', '시스템 및 서비스 획득', '접근통제'에 해당한다.

전체 사이버 공급망 보안통제 중 92개, 약 30%의 항목을 '조직 필수구현 통제'로 지정하고 있다. 지정된 필수구현 보안통제 중 90% 이상을 중간 관리자와 실무진이 수행하도록 할당한다. 구성관리, 접근통제 등 도메인별 계획을 수립하고 이행 및 이행을 확인하는 통제 위주이다. 통제 도메인 중 '프로그램 관리'와 '개인정보보호 처리'는 조직 필수구현 통제를 포함하지 않는다. 프로그램 관리 부분은 기존 관리체계와의 통합, 효율성 제고 관련 통제로 다른 통제에 비해 우선순위가 낮아진 것으로 보인다. 개인정보보호 처리 부분은 도급업체에 어떤 정보가 공유되고 어떤 도급업체 직원이 접근 가능하며 이를 도급업체가 어떻게 처리·관리하는지에 대한 것으로, 도급업체의 필수 구현항목으로 분류되어 있다.

상·하위 도급업체에 필수 적용해야 하는 통제는 39개로 전체항목 대비 약 13%이고, 전반적인 통제 도메인에 고르게 분포한다. 공급망 위협지표, 감사정보 등 조직과 주요 도급업체 간 정보공유와 조직·도급업체 간 사고대응 협업, 비상계획 연계 등이 해당한다. '식별 및 인증', '위험평가', '시스템 및 서비스 획득'에는 별도의 항목을 지정하지 않았다. 사이버 공급망 내에 핵심 시스템, 구성요소의 추적성 확보를 위한 식별자 및 인증자(Authenticator) 관련 조치사항과 위험 식별·대응 관련 보안통제는 조직 내부 활동으로 규정했다. 또한 시스템 및 서비스 획득 활동 부분도 신뢰할 수 있는 조달 경로확보, 개발 관련 교육·훈련 등 조직이 식별·관리해야 할 요소에 대한 보안통제로 구성되어 있다.

사이버 공급망 보안통제 전체항목을 기준으로, '구성관리', '접근통제', '시스템/서비스 획득'에서 가장 많은 통제 및 필수구현 항목을 제시하고 있다. 사이버 공급망 관리 전반에 영향을 미치는 요소로써 정보시스템·네트워크와 시스템개발 생명주기 구성에 대한 추적·관리를 식별하고 도급업체와의 협업과정에서 발생 가능한 상황에 대한 보안대책을 강조하는 등 주로 무결성, 기밀성, 부인방지 목적의 통제가 많다.

IV. 국가 정보보안 기본지침 보완방안

기본지침은 우리나라 각급기관이 수행해야 하는 정보보안 관련 기본업무를 규정한 지침으로, 사이버 공급망 보안사고 증대에 대응하기 위해 관련 업무의 보완이 필요하다. 현재 기본지침 내에 '용역업체에 대한 보안 요구사항', '도입 제품 현황' 등에 사이버 공급망 보안업무가 일부 존재하나, 관련 내용을 강조 또는 보완하고 정보보안 업무 전반에 확장 적용해야 한다. 이에 기본지침의 각 조항에서 고려될만한 사이버 공급망 보안업무를 개정(안)의 사이버 공급망 보안통제에서 식별하고자 한다. 본 고에서는 기본지침의 각 업무 내용, 목적 등과 개정(안) 보안통제의 유사성을 근거로 식별하였으나, 문건 간 개발환경, 구성, 활용처 등의 차이로 식별한 내용이 완전히 부합

하지 않을 수 있다.

4.1 국가 정보보안 기본지침 - NIST SP 800-161 개정(안) 매핑 결과

기본지침의 보안업무와 개정(안)의 사이버 공급망 보안통제 간의 매핑 작업을 수행했다. 개정(안)의 사이버 공급망 보안통제를 모두 반영하고자 하였으나, 항목 중 내용이 포괄적이며 다른 보안통제와의 중복성이 강할 경우 제외하였다. 기본지침의 151개 조항 중 38개 조항에서 개정(안)의 보안통제 143개를 고려할 만한 것으로 [표 2]와 같이 판단되었다.

Table 2. National Information Security Manual-NIST SP 800-161 Rev.1(Draft) Mapping Result

Category	National Information Security Manual	NIST SP 800-161 Rev.1(Draft)
Total number of Items	151 clause	190 control
↓		
The number of mapped Items	38 clause	← 143 control

매핑 작업 시 개정(안) 각 통제의 심화통제 개수는 집계하지 않았으나, 해당 업무 내용은 반영했다.

기본지침의 보안업무 범주별 사이버 공급망 보안통제 매핑 비율은 아래 [그림 1]과 같다.

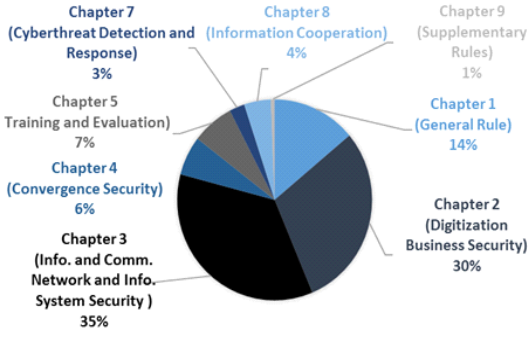

Fig. 1. National Information Security Manual Mapping Ratio

개정(안) 사이버 공급망 보안통제는 공급망 보안을 위한 업무·역할·책임을 정의하고 제품/서비스의 도입·운영·유지보수 목적의 항목을 주로 구성하고 있다. 이에 관련 내용을 다루는 기본지침의 '정보통신망 및 정보시스템 보안', '정보화 사업 보안', '총칙' 순으로 사이버 공급망 보안통제가 가장 많이 매핑되었다.

개정(안) 사이버 공급망 보안통제 중, '조직 필수 구현 통제'와 상·하위 도급업체 필수 적용 통제'는 기본지침 보안업무 중 6개 범주에 매핑되었다. 조직이 기본적으로 구현해야 하는 필수구현 통제는 전체 통제항목 매핑 비율과 유사하게 '정보통신망 및 정보시스템 보안', '정보화 사업 보안'이 가장 많은 비율을 차지한다. 반면 도급업체에 필수 적용해야 하는 통제의 경우, 도급업체의 보안 구현현황 확인과 필수 교육 항목 등으로 인해 '훈련 및 평가'가 높은 비중을 나타냈다.

Fig. 2. Mapping Ratio of C-SCRM Baseline and Flow Down Controls

4.2 국가 정보보안 기본지침 매핑 조항 및 800-161 개정(안) 통제 목록

기본지침은 보안업무를 장-절-조 범주로 구분한다. 본 고에서는 기본적으로 기본지침의 조항 수준에서 개정(안)의 사이버 공급망 보안통제 검토를 수행했다. 개정(안)에 부합하는 기본지침 조항이 없을 경우, 보다 포괄적 개념을 포함하는 상위 범주에서 고려했다. 매핑된 기본지침의 조항별 개정(안) 통제 매핑 현황은 [표 3]과 같다.

Table 3. Mapped Items of National Information Security Manual and NIST SP 800-161 Rev.1(Draft)

National Information Security Manual			NIST SP 800-161 Rev.1(Draft)
Chapter	Section	Clause	Control Identifier
Chapter 1 (General Rules)	-	Clause 4 (Duty)	PM-2, PM-29, PS-1
		Clause 5 (Operating of Information Security Officer)	AC-1, AT-1, AT-3, AU-1, CA-1, CM-9, MA-1, IR-1, MP-1, PM-3
		Clause 6 (Establishment of Annual Implementation Plan)	PM-4
		Clause 8 (Information Security Audit, etc.	AU-1, PM-6
		Clause 9 (Information Security Education)	AT-1, AT-3, AT-4, PM-13, SA-5, SR-11
Chapter 2 (Digitization Business Security)	Section 1 (Business Plan)	Clause 12 (Establish Security Measure)	CM-1, CM-2, CM-5, CM-6, CP-1, PE-1, PE-18, PL-8, PM-28, RA-1, RA-2, RA-3, RA-5, RA-7, RA-9, RA-10, SA-2, SA-9, SC-27, SR-2, SR-3, SR-5, SR-6
		Clause 13 (Details of the Request for Proposal)	AU-13, PE-17, PE-20, SA-1, SA-3, SA-4, A-10, SA-11, SA-15, SA-16, SC-8, SR-8
	Section 2 (Security Review)	- Consider on the overall clause	CM-4
	Section 3 (Product Introduction)	- Consider on the overall clause	PL-8
		Clause 24 (Submission of Introduction Status)	PM-5, SR-4, SR-13
	Section 4 (Contract and Business Execution)	Clause 26 (Contractor Security)	AC-3, AC-17, AU-16
		Clause 27 (Software Development Security)	CM-7, CM-10
		Clause 28 (Off-site Development Security)	AC-17
		Clause 30 (Actions in case of Leakage Information which prohibited leakage)	AU-13

National Information Security Manual			NIST SP 800-161 Rev.1(Draft)
Chapter	Section	Clause	Control Identifier
Chapter 3 (Information and Communications Network and Information System Security)	- Consider on the overall clause		CM-3, SC-1, SC-18, SC-30, SR-9, SR-11
	Section 1 (Information and Communications Network Security)	Clause 40 (Separation of Internal Network and Internet Network)	AC-4, IA-3, IA-4, SC-7, SC-37, SI-3
		Clause 43 (Wireless Lan Security)	AC-18
	Section 2 (Information System Security)	Clause 50 (Information System Security Responsibility)	CM-7
		Clause 51 (Information System Maintenance)	MA-3, MA-6, SA-22, SI-2, SI-7, SR-9
		Clause 52 (Online Maintenance through designated device)	MA-4, MA-5
		Clause 54 (Public Sever Security)	SC-5
		Clause 55 (Maintain Log records)	AU-2, AU-3, AU-6, AU-10, AU-12
		Clause 57 (Security for Work using Mobile Device)	AC-19
		Clause 61 (Disposal of Storage Media)	MP-5, MP-6, PE-20, SR-12
	Section 3 (Data Security)	- Consider on the overall clause	PM-25, PM-26, PM-27, PT-1, SC-28
		Clause 68 (Prevent Leakage of undisclosed Business data)	SI-20
		Clause 70 (Posting Materials Security such as website)	AC-22
		Clause 71 (Information and Communications Network Status Data Management)	CM-8, CM-10
		Clause 72 (Big Data Security)	AC-23
	Section 4 (User Security)	Clause 73 (Security for Individual User)	PS-3, PS-7, SA-21
		Clause 75 (Account Management)	AC-5, AC-6, AC-20, AC-4, IA-2, IA-8, PL-4, PM-10
		Clause 76 (Password Management)	IA-5
	Section 5 (Critical Infrastructure Protection)	Clause 81 (Establish Protection Measure)	PM-8

National Information Security Manual			NIST SP 800-161 Rev.1(Draft)
Chapter	Section	Clause	Control Identifier
Chapter 4 (Convergence Security)	Section 1 (Information and Communication Facilities·Device Protection)	Clause 87 (Information and Communication Protection Measure)	PE-2, PE-3, PE-6, PE-16
		Clause 90 (RFID Security)	AC-18
		Clause 92 (Disaster Prevention Measure)	CP-2, CP-6, CP-7, CP-8, SC-47
Chapter 5 (Training and Evaluation)	Section 1 (Training and Diagnosis)	Clause 96 (Response Training for Cyber Attack)	AT-2, AT-3, AT-4, CP-3, CP-4, IR-2, IR-3, PM-14
	Section 2 (Information Security Management Status Evaluation)	- Consider on the Overall Clause	CA-2, CA-3, CA-5, SR-10
Chapter 7 (Cyber Threat Detection and Response)	- Consider on the Overall Clause		CA-7, PM-12, SC-38, SI-4, SI-5, IR-4
Chapter 8 (Information Cooperation)	-	Clause 145 (Cooperation on Information Sharing between Institutes)	AU-16, PM-16, PM-17, PM-23
		Clause 146 (Information Sharing System Operation)	AC-21, IR-1, SC-4
Chapter 9 (Supplementary Rules)	-	Clause 149 (National Information Security Association)	PM-15

V. 국가 정보보안 기본지침 조항별 사이버 공급망 보안업무 고려사항

5장에서는 4장의 기본지침 각 조항과 개정(안) 보안통제의 매핑 결과를 기본지침 기준의 고려사항으로 정리하여 제시한다.

5.1 제1장-총칙

제1장은 기본지침의 목적·범위·책임 등을 규정한다. 사이버 공급망 보안과 관련하여, 총괄 책임자 및 필요 업무 분야의 담당자 지정과 필요 업무의 역할·책임을 정의의 보완이 주로 필요하다. 자세한 내용은 다음과 같다.

5.1.1 제4조(책무)

제4조는 보안대책 수립·시행 및 정보보안 책임을 규정하는 조항으로, 사이버 공급망 보안을 위해 다음을 추가 고려해야 한다.

고위 정보보안 책임자(CISO 등) 및 고위 인수·조달 관계자를 사이버 공급망 보안의 핵심 책임자로 지정한다. 또한, 인수, 관리, 실행 등 공급망 보안활동에 대한 직원의 역할을 정의한다. 이때, 시스템개발 생명주기 전체를 고려하고 다양한 공급망 인프라 활동에 필요한 역할과 책임을 반영해야 한다.

5.1.2 제5조(정보보안 담당관 운영)

제5조는 정보보안 정책 수립·시행/전담조직 관리, 관련 예산과 전문인력 확보 등을 다루는 조항으로 다

음을 추가 고려해야 한다.

사이버 공급망을 포함하는 인식제고 및 훈련 절차를 개발·실행하기 위한 담당자와 공급망 정보시스템·네트워크에 대한 감사 정책·절차의 개발·실행을 위한 담당자를 지정한다. 이러한 사이버 공급망 책임자는 공급망 이해관계자에 대한 접근통제 정책을 수립하고, 조직의 모든 정보시스템·네트워크에 대한 유지보수 정책·절차에 사이버 공급망이 포함되도록 해야 한다. 특히, 유지보수 단계에서 원격접근, 외부 직원의 시스템 조작 등 취약점 요소가 많은 활동이 수행되기에, 구체적으로 명시적 업무 조항을 설정해야 한다. 또한 사이버 공급망 네트워크 내에 핵심 시스템 및 구성요소의 추적성 확보를 위해, 식별자(ID)와 접근 정책·절차의 검토 및 개선 주기를 수립하고 수행해야 한다. 책임자는 소속 조직과 도급업체의 공통업무로써, 사이버 공급망 관련 위협과 사고를 처리, 보고 및 관리해야 하는 시기와 방법에 대한 사고대응 지침을 수립한다.

사이버 공급망 보안업무의 평가 및 권한 부여를 위해 조직 내 역할·책임에 대한 정의를 명확히 해야 하는데, 정보시스템·네트워크 구성관리 수행에 대한 역할 정의는 특히 강조된다. 상기 사이버 공급망 보안의 요구사항 구현을 위한 전용 예산과 인적 자원을 반드시 할당해야 한다.

5.1.3 제6조(연도 추진 계획 수립)

정보보안 업무 추진 계획의 수립·시행 관련 조항으로, 본 조항 수행 시 조직 내에 모든 미비점 식별 및 개선 활동 계획에 사이버 공급망 보안요소가 포함되도록 해야 한다.

5.1.4 제8조(정보보안 감사 등)

감사 메커니즘은 조직 공급망 정보시스템·네트워크의 활동 추적을 위한 데이터를 제공해야 한다. 또한, 사이버 공급망 활동의 영향도·효과성·효율성·구현 확인을 위한 성능 측정을 수행해야 하며, 전담조직이 본 측정 방법의 개발·활용 활동에 책임이 있도록 한다.

5.1.5 제9조(정보보안 교육)

교육·훈련 정책은 〔정보시스템 소유자, 인수, 공급망 물류 시스템 엔지니어링, 프로그램 관리, IT 품질 등〕 사이버 공급망에 영향을 미치는 개인·기능에 대해 역할 기반으로 수립한다. 이는 조직과 도급업체 모두를 대상으로 수행하며 내역을 기록해야 한다. 특히, 하드웨어, 소프트웨어 및 펌웨어 구성요소의 위조품 탐지를 위한 자원을 식별하고 이를 수행하기 위한 교육을 마련해야 한다. 조직 내부 사이버 공급망 보안업무에 대해 조직 사용자에게 교육해야 한다.

5.2 제2장-정보화사업 보안

제2장은 정보통신망·정보시스템의 개발·구축·운용·유지보수 사업과 관련한 일련의 보안업무를 규정한다. 사이버 공급망 보안관 관련하여, 시스템개발 생명주기 전반의 구성관리, 보안대책 및 관련 사항에 대한 도급업체 요구사항의 보완이 주로 요구된다. 세부 내용은 다음과 같다.

5.2.1 제1절(사업계획) - 제12조(보안대책 수립)

정보화 사업계획 수립 시 포함되어야 하는 보안대책을 정의하는 조항으로, 사이버 공급망 보안 관점에서 다음을 추가 고려해야 한다.

시스템개발 생명주기를 고려한 구성관리 정책·절차를 정의하여, 구성요소의 출처 파악 등 무결성을 확보하고 구성설정 변경작업을 관리한다. 공급망 이해관계자와 협의하여 정보시스템 및 개발환경에 대한 기준구성(Baseline Configuration)을 설정한다. 기준구성은 시스템개발 생명주기 전체에서 구성요소 및 코드에 대한 설정변경 추적을 목적으로, 공급망 이해관계자의 개발·테스트 기준을 유지해야 한다. 정보시스템·네트워크의 변경된 물리적·논리적 접근제한에 관하여 요구사항을 정의하고 구현한다. 이는 소프트웨어 구성요소 업데이트 및 패치 배포를 위한 중앙관리 프로세스 변경 등을 포함한다.

물리적 환경 보호대책에 사이버 공급망 관리 실무요소 및 요구사항을 포함한다. 물리적·환경적 요소는 조직이 활용하는 제품의 생산, 저장, 유통 모두에 영향을 미칠 수 있으므로, 대체 공급자 등 대책을 수립하고 있어야 한다. 또한, 도급업체의 업무 위치에 적절한 보호조치가 마련되어 있어야 한다.

보안 아키텍처는 시스템개발 생명주기 전반의 보안내재화를 보장할 수 있는 요소로서, 사이버 공급망 보안의 근본적 요소이다. 이에, 조직은 제로 트러스트

아키텍처 구현을 고려해야 한다.

계획상 고려하지 않았던 구성요소의 오류나 후속 조치 등 사이버 공급망 보안 관련 사항을 포함하는 비상계획을 수립한다. 이는 기능 개선, 유지관리, 업데이트 및 현대화와 관련된 교체 사안과 제품 또는 서비스 중단을 포괄해야 한다. 정보보안 및 사이버 공급망 문제 해결을 위해 공급업체 다양성 확보를 권장한다.

조직관리 구성 계층 등 수준별 위험평가를 수행 후 대응 활동을 해야 한다. 예를들어, 시스템 수준의 위험평가는 사이버 공급망 인프라(개발 및 테스트 환경, 전송 시스템 등)와 사이버 공급망 관련 정보시스템 및 구성요소를 모두 포함한다. 이러한 위험평가는 중요도, 위협, 취약점, 발생 가능성, 영향에 대한 분석을 포함하고 가능한 대응을 식별·평가 후 대응안을 결정·실행해야 한다.

5.2.2 제1절(사업계획) - 제13조(제안요청서 기재사항)

제13조는 누출금지정보 목록, 용역업체 작업장소 등 제안업체에 대한 요구사항을 규정하는 조항으로, 다음을 추가 고려해야 한다.

조달 계약상에 필수 보안 요구사항을 명시하고 충족 여부 확인방안에 사이버 공급망 보안평가를 평가요소 중 하나로 포함한다. 대체 근무지를 활용하여 공급망 인프라에 접근 가능한 조직 및 도급업체 직원의 관리를 위해 보안통제를 일괄적용하는 사항을 포함한다. 도급업체 평가 시 설비 위치에 대한 고려사항을 포함하고, 중요 제품일 경우 해당 위치 관련 요구사항을 구체적으로 명시한다.

조직뿐 아니라 도급업체도 사이버 공급망 보안활동이 시스템개발 생명주기 전반에 반영되도록 한다. 요구사항 정의, 설계와 같은 전통적 시스템개발 활동뿐 아니라, 재고관리, 인수·조달 및 시스템·구성요소의 물류 배송 등을 포괄해야 한다. 시스템개발 생명주기 각 단계에서 개발자에게 보안평가를 위한 일련의 활동과 개발 및 보안평가에 사용되는 표준과 도구 및 옵션값 등 세부 사항에 대한 문서화를 요구한다. 개발자에게 보안통제의 활용·적용 관련 교육을 제공하도록 한다.

인증, 암호화 등의 보안 메커니즘을 활용하여 전송 간 기밀성 및 무결성을 확보하도록 한다. 소프트웨어 코드, 데이터 및 정보 등이 검토나 활용을 위해 조직에 제공될 시 해당 요소들의 지적 재산권 관리를 위한 요구사항과 특정 ICT/OT 도급업체에 대한 활용 금지조항 등의 규제의무를 포함한다.

5.2.3 제2절(보안성 검토)

제2절은 정보통신망·정보시스템 구축·운용 시의 보안성 검토 관련 조항들을 규정하고 있다. 관련하여 조직은 변경사항에 대한 영향이 기존 보안통제에 미치는 영향도를 파악하고, 보안수준 유지를 위해 추가 또는 다른 보안통제의 적용 여부를 검토해야 한다. 이때, 공급망 이해관계자는 해당 활동에 참여하여 사이버 공급망 보안 관점의 고려사항을 제공해야 한다.

5.2.4 제3절(제품도입)

제3절은 제품도입 기준 등에 관한 보안업무를 다루고 있는데, 인수 보안평가 시 기성품 구성요소에 대해, 공급업체의 대체경로 조달 능력 등 다양성을 추가로 확인해야 한다.

5.2.5 제3절(제품도입) - 제24조(도입현황 제출)

시스템 목록 정보는 사이버 공급망 보안활동의 기본으로, 이를 항시 확보·유지해야 한다. 특히, 시스템, 시스템 구성요소 및 관련 데이터의 유효한 출처를 문서화, 모니터링 및 유지관리 해야 한다. 이는 공급망 요소 또는 구성의 변경정보를 포함하기에, 출처정보에 대한 변경사항 추적, 부인방지 등에 활용이 가능하다.

5.2.6 제4절(계약 및 사업수행) - 제26조(용역업체 보안)

공급업체 이해관계자를 대상으로, 접근이 필요하지 않거나 권한 남용 또는 위반이 발생하는 경우 즉각적 권한해제를 위한 프로세스를 갖춰야 한다. VPN, 다중 인증, 접근 시간 제한 등 도급업체의 원격접근 요구사항을 명확히 명시한다. 공급망 이해관계자의 인프라 등을 활용하여 외부 조직에 감사 정보를 전송하는 방법을 도급업체가 반드시 통제하도록 해야 한다.

5.2.7 제4절(계약 및 사업수행) - 제27조(소프트웨어 개발보안)

소프트웨어, 펌웨어, 정보시스템·네트워크의 무결

성 보장을 위해, 코드 실행 시의 코드 인증 메커니즘을 구현해야 한다. OEM·개발자 또는 기타 승인·검증된 출처로부터 직접 바이너리·기계실행 코드를 획득해야 한다.

오픈소스 사용 시, 라이선스 조건을 모두 준수하고 조직에 허용되는지 여부 등 관련 절차와 위험을 검토한다. 오픈소스 개발자가 제공하는 오픈소스 소프트웨어의 공급망(출처, 구성관리, 재사용 가능 라이브러리 등)을 확인해야 한다.

5.2.8 제4절(계약 및 사업수행) - 제28조(원격지 개발보안)

발주기관 이외 장소에서 개발 작업 시의 보안대책으로, 사이버 공급망에 대한 원격접근은 조직 또는 도급업체 직원으로 제한해야 한다. 여기에는 분산 소프트웨어 개발환경이 포함되며, 정보시스템 및 사이버 공급망 정보가 무단 사용 또는 공개되지 않았는지 확인해야 한다.

5.2.9 제4절(계약 및 사업수행) - 제30조(누출금지정보 유출 시 조치)

제30조는 정보 유출 등의 이벤트 발생 시 계약위반에 따른 조치, 즉시 보고 의무 등을 포함한다. 사이버 공급망 관점에서 정보 공개는 여러 경로를 통해 가능하다. 예를들어, 도급업체가 제공하는 오류 수정표 등은 시스템의 위험을 증가시키는 위협과 연관된 정보를 제공할 수 있다. 이에 조직은 도급업체 시스템의 데이터 무단 공개를 감지할 수 있는 모니터링을 추가 시행해야 한다.

5.3 제3장-정보통신망 및 정보시스템 보안

제3장은 정보통신망·정보시스템 구축·운영 전반의 보안업무를 규정한다. 사이버 공급망 관리를 위해, 사용자·도급업체의 권한과 모바일 코드, 공급망 메타데이터, 공유정보 및 업데이트 수반요소 조달의 관리 등이 강조된다. 각 내용을 3장 전반에서 고려해야 하는 사항과 조항별 권고사항으로 구분했다. 3장 전반에서 고려해야하는 내용은 아래와 같다.

정보통신망, 정보시스템 구축·운영 전반의 보안업무를 규정하는 제3장 전반에서 다음 내용을 고려해야 한다.

정보시스템과 상호 운용 시스템 및 네트워크 보호를 목적으로 시스템 변경사항에 대한 정책·절차가 필요하다. 이는 위조된 구성요소의 삽입 탐지와 대응을 위한 정책·절차를 포함해야 한다. 보안 및 개인정보보호 담당자는 구성설정 변경통제가 가능한 인원으로 한다. 기존 보안통제에 영향을 줄 수 있는 변경사항을 모니터링하여, 필요한 기능을 지속적으로 수행하는지 확인한다.

공급망 정보의 전자 전송, 소프트웨어 구성요소 수신 등 모바일 코드를 사용하는 다양한 응용프로그램에 모바일 코드의 획득, 개발, 사용 관련 보호 기술을 적용한다. 모바일 코드 획득 시 검증된 소스로 생성되었는지 확인·승인 기준에 대한 검증 프로세스 구축 여부 등이 해당한다.

보편적인 공급망 프로세스는 효율성과 비용 절감을 위해 예측·반복 가능한 프로세스로 구성되는데, 이는 잠재적 침해사고를 초래할 수 있다. 이를 완화하기 위해 정보시스템·네트워크에 은폐 및 무작위성 관련 기술을 도입할 수 있다. 해당 기술은 임의의 재공급 시간 설정, 정보 저장소 임의 변경, 공급자 소프트웨어 수신 일시 변경 등을 의미한다.

5.3.1 제1절(정보통신망 보안) - 제40조(내부망·인터넷망 분리)

제40조는 내부망과 기관 인터넷망 간 안전한 자료 전송 대책 등을 규정하는 조항으로, 다음 공급망 관점 업무를 추가 고려해야 한다.

사이버 공급망 내에서 시스템, 개인, 문서, 장치 및 구성요소에 식별자 등을 할당하여, 각 요소를 명확하게 식별하는 기능을 구현한다. 장치·소프트웨어의 식별자는 유형별, 장치별 등의 기준으로 분류해야 하고 운영 간에 식별자의 진위성 여부를 판단 가능해야 한다. 공급망 이해관계자들은 당사의 공급망 관리를 위한 식별자를 각각 활용하고 있는데, 조직은 반드시 해당 식별자와 조직 내 식별자를 연계시켜야 한다. 이는 시스템 및 구성요소뿐 아니라 공급망 활동에 참여하는 개인도 포함한다.

공급망 이해관계자들의 시스템 간 경계에 적절한 모니터링 메커니즘과 프로세스를 구현한다. 시스템·시스템 구성요소, 인수 세부정보 등 공급망 메타 데이터의 식별 및 공유를 위한 정보흐름 통제를 구현하고 악성코드 보호 기능을 구현해야 한다. 정보시스템 및 해당 정보시스템의 개발 환경·프로세스에 대한 정보는 특정 사용자 또는 시스템만 수신 가능하도록 한다.

5.3.2 제1절(정보통신망 보안) - 제43조(무선랜 보안)

사이버 공급망에는 공급망 물류를 지원하는 RFID와 같은 무선인프라가 포함될 수 있다. 이에 무선 접근통제 메커니즘 구현 여부를 확인해야 한다.

5.3.3 제2절(정보시스템 보안) - 제50조(정보시스템 보안책임)

정보시스템 관리대장의 작성·관리 등을 규정하는 조항으로, 미승인된 하드웨어, 소프트웨어를 감지하고 사용을 제한하도록 하는 사항을 포함해야 한다.

5.3.4 제2절(정보시스템 보안) - 제51조(정보시스템 유지보수)

용역업체 유지보수 활동 시의 보안조치 등을 포함하는 유지보수 정책 조항으로 다음을 추가 고려해야 한다.

유지보수 도구는 공급망의 일부로 간주되고 각 도구에 해당하는 고유의 공급망이 존재하기에, 이를 지속적으로 검토 및 승인한다. 구체적으로 공급망 인프라 내에 유지보수 도구가 당초 예상한 상태인지 확인하기 위한 수용 테스트를 수행한다. 또한 진단 및 테스트를 위한 매체가 당초 예상한 대로 작동하며 필요한 기능만 제공하는지 확인해야 한다. 정보시스템·네트워크 유지보수 도구를 제거하기 전에 발생 가능한 영향도 파악 및 조치 등을 위한 검사를 수행한다. 유지보수 도구에는 통합개발환경(IDE) 등이 포함된다.

정보시스템·네트워크 내에 자동 업데이트가 요구되는 소프트웨어 자산을 지정해야 한다. 배포 전 업데이트를 평가 및 관리하기 위하여 중앙 집중식 패치 관리 프로세스를 활용할 수 있다. 공급업체로부터 직접 업데이트가 필요한 경우 OEM에서 직접 생성한 업데이트만 허용한다. 예비·교체 가능한 OEM, 공인 유통업체, 공인 대리점을 통한 구매 순으로 조달 경로를 유지하고, 적절한 리드타임을 보장해야 한다. 만약 상기 조달 경로가 불가할 경우, 거래 업체의 위조기록·범죄기록 등 출처에 대한 신뢰성 검증을 수행한다.

5.3.5 제2절(정보시스템 보안) - 제52조(지정 단말기를 통한 온라인 유지보수)

인터넷을 통한 온라인 유지보수 허용 관련 규정으로, 동급업체 직원이 원격 유지보수를 수행할 경우 조직 내부 유지보수 담당자에게 적용하는 통제를 해당 직원에게 동일 적용해야 한다.

5.3.6 제2절(정보시스템 보안) - 제54조(공개서버 보안)

서비스 거부 공격 보호를 위해 공급망 이해관계자와의 계약에 초과 대역폭, 용량 및 이중화에 대한 요구사항을 반드시 포함한다.

5.3.7 제2절(정보시스템 보안) - 제55조(로그기록 유지)

제55조는 로그기록 유지·관리 의무 및 포함하는 요소를 정의하는 조항으로 다음을 추가 고려해야 한다.

공급망 네트워크에서 관찰 가능한 사건은 조직 시스템개발 생명주기 관점과 요구사항에 기반하여 공급망 감사 이벤트로 식별한다. 감사 이벤트에는 소프트웨어·하드웨어 변경, 공급망 정보시스템에 대한 접근 시도 실패, 소스코드 이동 등이 해당한다. 포착된 정보는 이벤트 유형, 날짜·시간, 발생 빈도 등을 포함하며, 공급업체와의 계약 갱신 시 로그를 통합 검토해야 한다. 새로운 위협의 부상 등과 관련한 특정 공급업체의 위험 변화에 기반하여 감사 기록의 검토 수준을 조정한다. 해당 감사 기록은 무결성 유지, 정보 및 출처의 기밀성 유지 등 보존 요구사항을 준수한다. 또한, 공급망의 구성요소를 설명하는 공급망 메타데이터, 공급망 통신, 배송 수락 등과 관련한 정보에 부인방지 기술을 적용한다.

5.3.8 제2절(정보시스템 보안) - 제57조(모바일 업무 보안)

스마트폰, 스마트워치, 테블릿 등 모바일 장치는 SI(Service Integrator)의 공급망 경유 시 조직 운영 지원 또는 공급망 물류 데이터 추적 등에 활용된다. 조직은 이에 대한 접근통제 메커니즘을 정의해야 하고, 해당 장치와 연결된 모든 관련 데이터 및 메타데이터에도 구현해야 한다.

5.3.9 제2절(정보시스템 보안) - 제61조(저장매체 불용처리)

조직 내·외 직원 등 매체의 이관 작업을 수행하는 인원의 소속과 관계없이 사이버 공급망 보안활동의

통제를 받아야 한다. 이관·보관 간 매체 보호 방법에는 암호화 기술 및 공인된 관리 서비스 등이 있고, RFID와 같은 위치식별 기술을 이용하여 시스템 구성요소를 추적관리 해야 한다. 매체는 시스템개발 생명주기 전반에 활용되고 사이버 공급망 내에서는 재사용·재가공 될 수 있기에, 매체 삭제 정책을 수립하고 도급업체와의 계약에 포함한다.

5.3.10 제3절(자료보안)

제3절은 비밀·공개·비공개 등 정보 유형별 관리 규정을 다루고 있다. 3절 조항 전반에서 다음 내용을 추가 고려해야 한다.

공급망 이해관계자 조직에 저장된 소스코드, 테스트 데이터, 지적 재산권 정보 등의 데이터에 대한 적절한 보호를 제공한다. 정보 가공·활용 시 개인정보 활용을 최소화해야 하며 투명성을 확보해야 한다. 개인정보에 접근 가능한 도급업체 직원, 보관 계약 기간, 계약 종료 시 처리 내용 등을 규정한다. 개인정보 관련 불만 사항, 우려 사항 등의 이슈 처리 절차 또는 메커니즘을 구현한다.

5.3.11 제3절(자료보안) - 제68조(비공개 업무자료 유출방지)

공급망 이해관계자는 조직 내 민감한 정보에 접근 가능하므로, 해당 데이터의 유출 또는 무단삭제 여부를 식별할 수 있는 역량을 갖춰야 한다.

5.3.12 제3절(자료보안) - 제70조(홈페이지 등 게시자료 보안)

사이버 공급망 보안활동 내에서 공개적으로 접근 가능한 콘텐츠는 자료요청서(RFI), 제안요청서(RFP)와 시스템 및 구성요소 조달 관련 정보로 한정한다.

5.3.13 제3절(자료보안) - 제71조(정보통신망 현황자료 관리)

정보통신망 구성, 정보시스템 운용현황 등의 관리 관련 조항으로 다음을 추가 고려해야 한다.

정보시스템·네트워크 내의 다음과 같은 중요 구성요소를 자산 목록에 포함한다. 목록은 구성요소에 대한 책임 정보를 포함하고 소프트웨어 정보, 소프트웨어 버전, 구성요소 소유자, 네트워크 구성요소·장치, 시스템 이름 및 네트워크 주소를 포함한다.

정보시스템·네트워크 구성요소를 설치, 업데이트 또는 제거 시 중요 구성요소의 최신화를 수행한다. 가능한 경우 자동화된 목록관리 메커니즘을 구현해야 하며, 중앙 집중식 저장소 방식을 권고한다. 중앙 집중식 목록관리는 조직 내에 손상·위반·완화 조치가 필요한 구성요소의 위치 및 책임자 식별에 용이하다.

5.3.14 제3절(자료보안) - 72조(빅데이터 보안)

제72조는 데이터 수집 출처 확인, 데이터 오·남용 방지 등의 보안체계 수립 관련 조항으로, 주요 계약자가 내부자 위협 활동의 일환으로 수행할 수 있는 데이터마이닝 활동에 대해 통제를 구현해야 한다.

5.3.15 제4절(사용자 보안) - 제73조(개별사용자 보안)

제73조는 비밀 취급 인가 자격 심사 등과 관련한 조항으로, 정보시스템 구성요소 또는 서비스에 접근 권한이 있는 도급업체 직원에게 인력 검증·관리 정책·절차를 적용해야 한다. 이 중 모니터링 활동의 경우 접근 정보의 민감성 등 도급업체 보안수준에 상응하도록 한다.

5.3.16 제4절(사용자 보안) - 제75조(계정관리)

시스템 접근자는 정보·정보시스템 활용, 보안에 대한 책임 규칙이 존재하는데, 도급업체 직원은 이에 대한 준수를 입증해야 한다. 도급업체 직원의 계정 권한 부여 시 적합한 심사를 수행하고 계약기간 만료 시 해당 직원의 권한 만료를 적용해야 한다.

5.3.17 제4절(사용자 보안) - 제76조(비밀번호 관리)

제76조는 비밀번호 정책 또는 대체 인증수단 활용 등을 규정하고 있다. 사이버 공급망과 관련하여, 추적성 및 부인방지를 위해 인증자(Authenticator)를 선정·관리해야 한다. 여기에는 개발자 또는 설치 인원이 고유 인증자를 설치하거나 설치 전 인증자를 변경하는 행위 등이 포함된다.

5.3.18 제5절(주요정보통신기반시설 보호) - 제81조(보호대책 수립)

제81조는 주요기반시설별 시스템 현황 및 기능 등을 포함하는 평가·개선의 보호대책을 규정하는 조항이다. 관련하여, 주요 인프라 및 자원을 정의하고 계획 개발 시, 초기 단계부터 사이버 공급망 보안 고려사항을 포함해야 한다.

5.4 제4장-융합보안

제4장은 출입관리, 재난대책 등 기관 내 시설관리에 대한 보안업무를 규정한다. 사이버 공급망 관점에서 사용자·도급업체의 물리적 접근통제, 비상계획 연계 강화가 주로 요구된다, 자세한 내용은 다음과 같다.

5.4.1 제1절(정보통신시설 및 기기보호) - 제87조(정보통신시설 보호대책)

물리적 접근이 인가된 개인에 한하여 정보 및 정보시스템에 접근 가능하도록 해야 한다. 권한 부여 시, 개인의 물리적 접근허용 범위·작업(변경, 구성, 삽입, 연결, 제거 등)을 지정해야 한다. 물리적 시설 접근이 요구되는 관계자의 권한은 계약에 작성된 활동에 따라 관리되어야 하며, 불필요할 경우 즉각적인 통제 및 권한해제가 중요하다.

시설에 반출입되는 모든 정보시스템 구성요소를 승인, 모니터링 및 통제하고 해당 기록을 유지한다. 사이버 공급망 위험 감소를 위해 물리적 접근에 대한 개인 활동 모니터링을 수행할 수 있다.

5.4.2 제1절(정보통신시설 및 기기보호) - 제90조(RFID 보안)

사이버 공급망에는 공급망 물류 지원 목적의 무선 인프라가 포함될 수 있는데, 이에 대한 무선 접근통제 메커니즘 구현을 확인해야 한다.

5.4.3 제1절(정보통신시설 및 기기보호) - 제92조(재난방지대책)

제92조는 인위적 또는 자연적 원인으로 발생 가능한 정보통신망의 장애 방지대책을 규정하는 조항으로, 공급망 관점에서 다음을 추가 고려해야 한다.

외부 서비스 제공업체의 비상계획을 검토하고, 조직 내 비상계획과 효율적 연계가 가능하도록 SLA 등을 활용하여 조정과정을 수행한다. 공급망 이해관계자가 대체 저장·처리 사이트를 관리하는 경우, 조직은 해당 사이트를 사이버 공급망 네트워크 범위로 고려하고, 적절한 통제를 적용한다.

1차 통신 경로 침해에 대비하여 대체 통신 경로를 확보하는데, 공급망 이해관계자가 대체 통신 경로에 포함될 수 있다.

5.5 제5장-훈련 및 평가

제5장은 사이버공격 대응훈련, 정보통신망 보안진단, 관리실태 평가 업무를 규정한다. 사이버 공급망 관리를 위해, 사이버 공급망 보안평가, 내부자 위협 인식·보고 및 비상상황 대처 교육의 개발 또는 강화가 필요하다. 자세한 내용은 다음과 같다.

5.5.1 제1절(훈련 및 진단) - 제96조(사이버공격 대응훈련)

다음 내용을 포함하는, 사이버 공급망 위협 인식제고 목적의 실습을 제공해야 한다. 사이버 공급망 내부자 위협을 인식·보고하는데 필요한 지식과 사회공학 및 소셜 마이닝과 관련된 사이버 공급망 내 잠재적 요소 또는 실제 사안을 인지할 수 있는 지식을 포함한다. 또한 공급망 시스템 내에 비정상적 행동 및 커뮤니케이션을 인지할 수 있는 역량을 함양해야 한다. 조직 고유의 공급망 환경을 표적으로 하는 사이버위협을 인지하도록 해야 한다.

인수 과정의 사이버 공급망 보안 요구사항 및 평가요소에 대한 교육을 수행한다. 사이버 공급망 보안은 제조, 배송, 시설에 대한 물리적 접근, 재고관리 등의 공급망 관련 물리적 보안 메커니즘의 영향을 받는다. 따라서 조직의 개발 및 운영 담당자(SI 업체 등 외부조직 포함)는 상기 물리적 보안 메커니즘 및 이를 통제하는 훈련을 받아야 한다.

공공부문 조직은 사이버 공급망 내에 국외 '적' 신호 감지를 위한 다양한 데이터 소스를 수집, 해석 및 조치할 수 있는 전문화된 방첩교육을 수행해야 한다. 방첩교육은 최소한, 알려진 위협 신호, 핵심 정보공유 개념 및 보고 요구사항을 다루어야 한다.

비상상황에 대비하는 실습교육 대상에 주요 도급업

체가 반드시 포함되도록 한다. 이는 공급업체의 연속성·복원력 역량 테스트를 포함해야 한다.

5.5.2 제2절(정보보안 관리실태 평가)

제2절은 정보보안 관련 평가 실시, 자체 평가, 현장 실사, 평가결과 통보 등의 조항을 규정하고 있다. 해당 절 전반의 조항에서 다음 사항을 고려해야 한다.

기존 통제 평가 계획 내에 사이버 공급망 보안통제·기능을 포함하도록 하고, 사이버 공급망 보안활동의 각 요소를 분석하고 개선하기 위한 계획을 확인해야 한다. 중요 시스템 및 구성요소 검사를 통해 변조 방지 통제가 구현되었는지 확인하고 변조의 증거가 있는지 조사한다.

사이버 공급망 보안통제 평가를 위해, 공급망 이해관계자에 대하여 외부 보안평가를 활용한다. 외부 평가는 인증, 제3자평가, 정부의 타 부서 및 기관에서 수행한 사전 평가를 포함한다. ISO, CC 인증을 충족할 경우 비정부 기관의 평가결과도 활용 가능하다.

공급자-조직의 시스템 정보 상호연동 등 데이터 교환 시 공급망 관점에서 확인이 필요하다. 상호연결에는 조직과 시스템 통합 간 공유된 개발·운영 환경, 공급업체의 기성 제품 업데이트 및 패치 관리 연계, 외부 서비스 공급자의 정보공유 환경 시스템 내의 데이터 요청 및 검색 업무 등이 포함된다.

5.6 제7장-사이버위협 탐지 및 대응

제7장은 위협탐지, 조치, 보고, 대응 및 사이버 공격·규정위반 등으로 인한 사고 재발방지대책 등을 규정한다. 사이버 공급망 관련하여 7장 전반에서 다음 내용을 추가 고려한다.

내부자 위협 관련 사건·사고 처리 수행팀과 프로그램 구성 시 사이버 공급망 보안 사항을 반영하여, 기관 시스템·네트워크에 접근할 수 있는 모든 인원에게 적용 가능하도록 한다. 공급망 이해관계자와 관련된 잠재적 위협 처리 및 포렌직 역량을 갖추고, 이벤트 발생 시 유관 조직과 사고 처리 활동을 조정해야 한다.

관제 활동을 통해 수집된 정보를 조직 자산, 정보 등의 중요 분석과 취약점·위협 정보분석에 활용하여 공급망 관리 의사결정에 반영한다. 소프트웨어 개발 중 삽입되어, 배포 후 활성화되는 악성코드 등 기존 침해 사건과 관련해 발생 가능한 취약점을 모니터링한다. 공급망 취약점·위협 정보는 관련 보안 프로세스에서 획득하고, 이를 해당 프로세스에 다시 제공하는 선순환 구조를 수립한다. 협의한 공급망 이해관계자와 발견된 사안(보안경고 등)을 공유할 수 있다.

5.7 제8장-정보협력

제8장은 공유정보의 유형, 방안 등 정보공유 관련 업무를 규정한다. 사이버 공급망 사고·위험지표 등 이해관계자 간 정보공유 절차·정책 마련이 추가로 필요하다. 자세한 내용은 다음과 같다.

5.7.1 제145조(기관 간 정보공유 협력)

제145조는 사이버위협정보의 기관 간 상호 공유를 권장하고 공유정보 유형을 정의하고 있는 조항으로, 다음 사항을 공급망 관점에서 추가 고려한다.

공급망 이해관계자와 감사 정보공유 절차에 대한 일련의 요구사항을 설정한다. SI 업체, 외부 서비스 제공자 및 조직 간 감사 정보공유 시, 감사 데이터 유형과 제공 가능항목에 대한 SLA에 사전 동의를 해야 한다.

사이버 공급망에서의 사고 및 기타 주요 위협지표에 대한 정보공유 지침을 조직 사고대응 정책·절차에 마련한다. 이는 조직 외부 시스템에 잔존 하는 기관 정보(CUI, Controlled Unclassified Information)에 대한 보호 정책을 포함한다.

사이버 공급망 보안 정보공유 및 기관 간 협업 활동·이니셔티브에 데이터 거버넌스 기구를 포함한다.

5.7.2 제146조(정보공유 시스템 운영)

제146조는 정보공유 시스템의 개별사용자 관리 등을 규정하는 조항으로, 사이버 공급망 관련 정보공유 또한 승인된 사용자만 접근 가능하도록 해야 한다. 또한 시간·정보·계약·보안·시스템 관련 사항 등을 반영하여 정보공유의 경계를 명확히 해야 한다. 개발자와의 협의하에, 공유 데이터, 공유 방법, 제공 대상을 포함한 정보공유의 구조 및 프로세스를 정의한다.

5.8 제9장-보칙

5.8.1 제149조(국가정보보호연합회)

제149조는 정보보안업무 증진 등을 위한 협의기구 구성·운영 조항이다. 관련하여, 보안 및 개인정보보호 전문가그룹, 포럼 등 교류를 활성화하고 제도화 시 사이버 공급망 보안 실무자들을 포함해야 한다.

VI. 결 론

본 논문에서는 미국 연방기관 대상의 사이버 공급망 보안 관리체계·통제를 검토하고, 우리나라 국가 정보보안 기본지침에서 참고 가능한 통제항목을 식별했다. 이를 기본지침의 각 조항에 추가 고려사항으로 제시하여, 국내 정보보안 분야에서 도입 가능한 사이버 공급망 조치사항 목록을 제공했다. 제공목록을 살펴보면, 사이버 공급망 보안요소 중 도급업체 관리를 위한 보안업무가 가장 강조되고 있다. 도급업체가 직접 수행해야 하는 업무와 도급업체 관리를 위해 사용자 조직이 수행해야 하는 업무의 두 가지 관점 모두를 의미하며, 기존 정보보안 업무 전반에 편재되어 있다. 이에 초점을 두고 제안 내용을 활용하여 우리나라 각급기관의 사이버 공급망 보안업무가 보완·강화되기를 기대한다.

6.1 논의

본 논문의 검토 결과, 사이버 공급망 보안은 도급업체와 계약, 도급업체의 규정준수 보장, 별도의 교육·훈련, 지속적 역량측정·관리 등 기존 정보보안 개념에서 확장된 업무의 범위가 상당하다. 이에, 미국은 사이버 공급망 담당자·담당조직·전용예산을 기반으로, 공급망과 관련된 정보보안 개념을 강조·강화해 사이버 공급망 요소 또는 프로세스에 확장 적용하는 방안을 활용하고 있다. 즉, 사이버 공급망 보안은 기존 정보보안 대비 완전히 새로운 개념은 아니나, 정보보안의 파생적 요소 수준은 아닌 별도의 담당자·담당조직이 필요한 독립적 분야로 간주하는 것으로 판단된다. 우리나라도 이와 같은 인식을 기저로써 사이버 공급망의 중요성을 인지하고 보안 관리체계 수립을 추진해야 할 것이다.

6.1.1 사이버 공급망 보안 업무

기본지침과 매핑결과에 따르면, 기본지침 내 제2장(정보통신망 및 정보시스템 보안)과 제3장(정보화사업 보안)을 중심으로 사이버 공급망 보안업무가 구성되어야 할 것으로 보인다. NIST는 공급망 보안활동 중 구성관리, 접근통제, 시스템·서비스 획득에 가장 많은 기본통제와 필수구현 항목을 제시하고 있으며, 이는 주로 무결성·기밀성·부인방지가 목적이다. 일례로, 사이버 공급망 관리 전반의 영향을 미치는 요소로써 정보시스템·네트워크와 시스템개발 생명주기 전반의 구성에 대한 추적관리를 식별하고 있다. 또한, 내부 시스템 접근허용, 정보공유 등 도급업체와의 협업과정에서 발생 가능한 상황에 대한 보안대책 등을 강조하고 있다. 해당 사항은 주로 기본지침 제2장, 제3장과 관련된 내용으로, 정보화 사업 추진 시의 보안대책과 도급업체에 대한 요구사항을 추가 고려하고 정보통신망·시스템에 대한 관리 강화가 우선 수행되어야 할 것이다.

참고한 NIST의 사이버 공급망 보안에 대한 경향성이 우리나라의 환경과 완전히 부합하지 않을 수 있다. 그러나 글로벌 생태계가 배경인 사이버 공급망의 특성상, 미국 연방법에 종속되는 보안통제 등을 제외한, 보편적 개념의 보안통제는 우리나라 사이버 공급망 보안 초석 마련의 기반자료로서 의의가 있다. 다만 NIST의 보안통제는 가능한 모든 경우의 통제를 포괄·제시하여 항목 간 중복성 등이 존재하므로, 실무에서 활용 또는 참고 시 상황과 환경에 맞는 선별 작업이 필요할 것이다. 같은 맥락에서, 기본지침은 각급기관이 수행해야 할 보안업무를 상위 수준에서 기술하므로, 개정(안)에서 제공하는 보안통제와 유사한 수준을 구현하기 위해서는 별도의 시행규칙 등이 필요할 것으로 사료 된다.

6.1.2 사이버 공급망 보안 운영

사이버 공급망 보안은 기존 정보보안 개념에 기반하나, 별도의 관리·운영이 필요한 새로운 분야로 판단된다. 본 고 2장의 검토 결과, 미국은 사이버 공급망 보안관리를 위해 각 조직이 조직 전반의 구조·수행범위를 검토하고 고유 전략을 수립하도록 규정한다. 이후 조직의 사이버 공급망 관리체계 구현 추진 시, 순차적으로 구현해야하는 업무·정책에 대한 공급망 전용 로드맵을 제시한다. 또한 사이버 공급망 보안 수

행현황 점검 및 개선을 위한 별도의 지표를 권고하는 등 공급망 특성을 반영한 고유의 관리체계 마련을 추진 중이다. 즉, 사이버보안프레임워크(CSF)의 계층을 평가 기준으로 도입하는 등 기존 정보보안 체계를 활용·연계할 것으로 보이나, 사이버 공급망 보안을 위한 별도의 프레임워크 운영이 궁극적 목표인 것으로 판단된다. 우리나라도, 본 고 제안 내용에 기반한 사이버 공급망 보안업무 규정 및 수행 시, 각급기관의 조직 내 공급망 생태계 파악 정도 및 정규화된 관리체계 여부 등을 고려한 별도의 평가·관리 기준이 필요할 것이다.

조직과 도급업체를 함께 고려하여 사이버 공급망 보안에 대한 역할과 책임을 배분해야 한다. 본 고 3장 검토 결과에 따르면, 미국은 조직 각 계층이 수행해야 하는 사이버 공급망 보안통제를 구분하여 책임성을 확보했다. 또한, 제공하는 전체 사이버 공급망 보안통제 중, 각 연방조직이 필수 구현해야 하는 기준선을 제공함으로 추가 통제는 조직 상황·환경에 적합하게 활용하도록 하여 효율성을 확보했다. 사이버 공급망 보안 특성상 도급업체와 협업 또는 강제가 필요한 보안업무는 도급업체 필수 통제로 명확히 지정하여, 조직과의 연계성을 강화했다. 이에, 기본지침 내에 사이버 공급망 보안업무 규정 후 운영과정에서 책임성·효율성·연계성 확보를 위해, 가능한 경우 핵심 보안업무와 조직과 외부업체의 공동수행이 필요한 사항 등을 식별·지정할 필요가 있다. 핵심 보안업무에는, 미국 사례와 같이, 구성관리 및 접근통제를 우선 고려하여 추적성 확보를 통한 투명한 관리 방안이 선제적으로 마련되어야 할 것이다.

6.2 향후 연구

본 고에서 제기한 사이버 공급망 관점의 기본지침 개선방안은 각급기관 대상의 보안업무를 상위 수준에서 기술한 것으로, 실무도구, 가이드 자료 마련 등의 구체화를 위한 연구가 필요하다. 구체적으로, 사이버 공급망 보안업무 구현·운영의 대상과 목적이 되는 실제 공급망 위협과 위협이 야기하는 이벤트에 대한 분석을 수행해야 한다. 이러한 상황·환경별 분석결과를 통해 각급기관을 위한 필수·필요·권고 등 수준별 보안업무의 식별과 구현이 가능할 것이다. 또한, 사이버 공급망 보안업무에 대한 조직의 역량을 측정하는 평가 관점과 구체적 기준 도출 연구를 수행해야 한다. 사이버 공급망 보안은 정보보안과 유사하게 단기적·일회성 업무가 아닌 지속적 관리 대상으로, 마일스톤의 수립과 이행이 반드시 필요하다.

References

[1] NCSC(UK). "Supply Chain Security Guidance." Accessed Dec. 31, 2021. https://www.ncsc.gov.uk/collection/supply-chain-security

[2] ENISA. "Threat Landscape for Supply Chain Attacks," pp. 13-30, July. 2021.

[3] CISA. "ICT Supply Chain Risk Management(SCRM) Task Force." Accessed Dec. 31, 2021. https://www.cisa.gov/ict-scrm-task-force

[4] NCSC(KOR). "National Information Security Manual," pp. 1-118, Nov. 2021.

[5] NIST. "NIST SP 800-37 Rev.2., Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," pp. 20-76, Dec. 2018

[6] NIST. "Cybersecurity Framework." Accessed Dec. 31, 2021. https://www.nist.gov/cyberframework

[7] NIST. "NIST SP 800-161. Supply Chain Risk Management Practices for Federal Information Systems and Organization," pp. 13-49, Apr. 2015.

[8] NIST CSRC, "NIST SP 800-161 Revision Page," Accessed Dec. 31, 2021. https://csrc.nist.oov/publications/detail/sp/800-161/rev-1/draft

[9] NIST. "NIST SP 800-161 Rev.1(Draft) Cyber Supply Chain Risk Management Practices for Systems and Organizations," pp. 1-205, Apr. 2021.

[10] NIST CSRC. "2nd Public Draft SP 800-161 Revision 1 Workshop - Dec. 01. 2021." Accessed Dec. 31, 2021. http://csrc.nist.gov/events/2021/2nd-public-sp800-161-revision-1-workshop.

[11] NIST. "NIST SP 800-39, Managing Information Security Risk-Organization, Mission, and Information System View," pp. 32-45, Mar. 2011
[12] NIST. "NIST SP 800-53 Rev.5, Security and Privacy Controls for Information Systems and Organizations," pp. 428-465, Sep. 2020.

〈저자소개〉

유 영 인 (Young-in You) 정회원
2013년 8월: 서울시립대학교 수학과 (학사)
2015년 8월: 고려대학교 정보보호대학원 (석사)
2019년 2월: 고려대학교 정보보호대학원 (박사)
2018년 12월~현재: 국가보안기술연구소 선임연구원
〈관심분야〉 정보보호, 위험관리, 안보정책

배 선 하 (Sunha Bae) 정회원
2007년 2월: 한양대학교 미디어통신공학과 (학사)
2009년 1월: 한국과학기술원 전기 및 전자공학과 (석사)
2009년 1월~2013년 2월: LIG 넥스원 주임연구원
2013년 4월~2014년 1월: 두산중공업 기술연구원 주임연구원
2015년 2월~현재: 국가보안기술연구소 선임연구원
〈관심분야〉 정보보호, 전자공학, 제어시스템

김 소 정 (So Jeong Kim) 종신회원
1998년 2월: 부산대학교 사학과 (학사)
2001년 2월: 경희대학교 평화복지대학원 동북아학과 (석사)
2005년 2월: 고려대학교 정보보호대학원 정보보호정책학과 (박사)
2001년~2002년: 한국전파진흥협회 ITU-WRC 담당 연구원
2004년~2022년 2월: 국가보안기술연구소 책임연구원
2022년 3월 ~ 현재: 국가안보전략연구원 책임연구위원
〈관심분야〉 사이버안보 전략, 정보보호정책, 기반보호정책

김 동 희 (Dong Hee Kim) 정회원
2007년 2월: 단국대학교 경영정보학과 (학사)
2009년 2월: 고려대학교 정보보호대학원 (석사)
2017년 2월: 고려대학교 정보보호대학원 (박사)
2008년 1월~2015년 4월: 한국인터넷진흥원 선임연구원
2015년 5월~2016년 3월: 한국정보통신기술협회 선임연구원
2016년 3월~현재: 국가보안기술연구소 정책연구실장, 선임연구원
〈관심분야〉 사이버안보 전략, 정보보호정책