Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.30, NO.6, Dec. 2020 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2020.30.6.1189

ICT 공급망 보안기준 및 프레임워크 비교 분석*

민 성 현,[1†] 손 경 호[2‡]
[1,2]강원대학교 (대학원생, 교수)

Comparative Analysis on ICT Supply Chain Security Standards and Framework*

Seong-hyun Min,[1†] Kyung-ho Son[2‡]
[1,2]Kangwon National University (Graduate Student, Professor)

요 약

최근 ICT 기업은 제품과 서비스들을 직접 설계, 개발, 생산, 운용, 유지 보수, 폐기 등을 직접 수행하지 않고 이를 외부에 위탁하거나, 외주업체가 담당하는 경우가 많아지고 있다. 위탁과 재위탁되는 과정에서 제품 및 서비스에 대한 취약점 관리 어려움 등으로 이로 인해 발생하는 공격 또한 증가하는 추세이다. 이에 대응하기 위해 해외에서는 ICT 공급망 보안 위험관리를 위한 기준과 제도를 만들어 운영 중이며, 다양한 사례 연구를 진행하고 있다. 또한, SBOM(Software Bill of Materials)등 기술적으로 공급망 보안 문제를 해결하려는 연구도 진행하고 있다. ISO 등 국제표준화기구에서도 ICT 공급망 보안을 위한 기준과 프레임워크도 만들어졌다. 본 논문에서는 미국, EU 등 주요 국가와 국제표준으로 개발된 ICT 공급망 보안기준과 제도를 비교 분석하여 국내 실정에 적합한 ICT 공급망 보안 관리 항목을 제시하고 ICT 공급망 보안제도 수립을 위한 사이버 보안 프레임워크의 필요성을 설명한다.

ABSTRACT

Recently, ICT companies do not directly design, develop, produce, operate, maintain, and dispose of products and services, but are outsourced or outsourced companies are increasingly in charge. Attacks arising from this are also increasing due to difficulties in managing vulnerabilities for products and services in the process of consignment and re-consignment. In order to respond to this, standards and systems for security risk management of ICT supply chain are being established and operated overseas, and various case studies are being conducted. In addition, research is being conducted to solve supply chain security problems such as Software Bill of Materials (SBOM). International standardization organizations such as ISO have also established standards and frameworks for security of ICT supply chain. In this paper, we presents ICT supply chain security management items suitable for domestic situation by comparing and analyzing ICT supply chain security standards and systems developed as international standards with major countries such as the United States and EU, and explains the necessity of cyber security framework for establishing ICT supply chain security system.

Keywords: Supply Chain Security, Supply Chain Attack, Supply Chain Risk Management

Received(10. 05. 2020), Modified(11. 12. 2020), Accepted(11. 12. 2020)

* 이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2020-0-00185,공급망 장비에 대한 하드웨어 보안 및 신뢰성 검증 기술 개발)

† 주저자, tjdgus1277@gmail.com
‡ 교신저자, khson@kangwon.ac.kr(Corresponding author)

I. 서 론

최근 ICT 제품과 서비스의 설계·개발·제조·운용·보수·폐기 단계의 프로세스에서 업무를 외부에 위탁하는 일이 일반적으로 행해지고 있다. 이런 공급 프로세스를 공급망(Supply-Chain)이라 하며, 공급망 보안 관련 국제표준(ISO/IEC 27036:Information security for supplier relationships)에서는 '획득자, 공급자 또는 각각이 구매 주문, 계약 또는 공식적인 소싱 계약을 체결할 때 설정된 연속적인 관계를 형성하기 위한 연결된 자원 및 프로세스의 조직적인 집합'으로 정의하고 있다. 최근 기업과 기업에서 IT 기술 적용 확대와 글로벌화 등의 사업환경의 급격한 변화로 공급망은 더욱 다양화되고 있다. 또한, 외부에 위탁한 업무 일부분이 다른 조직으로 재위탁되는 등 위탁 관계는 더욱 복잡해질 것을 고려해 위탁업체의 정보보호 정책, 대응수준과 본사에서 요구하는 정보보호 정책 등의 공급망 위기관리(Supply Chain Risk Management)의 중요성이 높아지고 있다.

최근, 이런 공급망 구조에서 다양한 사이버 보안 문제가 발생하고 그 공격 기법은 고도화되어 ICT 공급망 위협은 모든 산업 활동에 잠재되어 있다. 특히 SW빌드나 업데이트 시 변조, 인증서 및 개발 계정 유출을 통한 변조 등 다양한 방법으로 공급망 보안 침해사고가 발생하고 있다[1]. 대부분의 공급망 공격은 대규모 사용자를 한 번에 감염시킬 수 있으며, 탐지되지 않고 장기간 스파이 활동을 벌일 수 있다. 현재까지 발견된 공급망 공격은 대부분 소프트웨어 공급망을 해킹하거나 코드사인 인증서를 탈취해 악성 프로그램이 배포되도록 하는 방식으로 진행된다.

이런 공격에 대응하기 위한 공급망에 대한 정보보호 위험관리의 문제점은 공급자와 획득자 사이에서 사전에 정보보호 요구사항에 합의된 문서가 없는 점과 사고 발생 시에 손해 책임이 불분명한 점이 있다. 업무 위탁 시 정보보호 수준은 제안서의 요구사항 정의서, 기본 설계서, 운영 절차서 등의 형태로 구체적인 요구사항을 명시하는 것이 기본이 되지만, 보통 보안과 관련된 사항은 명확한 합의가 없는 상태로 진행되거나, 한정된 예산 등의 이유로 보안 요구사항이 애매한 상태로 위탁이 이뤄지고 있다.

위탁업체가 수행해야 할 보안대책의 수준이 IT 기술과 위협의 고도화에 따라, 계약 시점에 합의한 보안 요구사항이 개발과정이나 운용단계에서 불충분한 대책이 될 수 있다. 또한, ICT 공급망에서 정보 유출 등의 보안사고가 발생했을 경우, 피해의 범위에 따라 고객에게 배상이나 원인 규명을 위한 비용 등의 금전적인 피해가 위탁 업무 자체와 비교해 매우 커지고 있다. 이를 위해, 업무 위탁할 때 본사와 위탁업체 간의 충분한 위험률 평가를 통해 필요한 정보보호 대책을 합의해 위험에 대응하는 것이 중요하다.

특히, ICT 공급망 보안 관리는 ICT 제품·서비스의 설계, 개발에서 공급망 생명주기 내에 다양한 이해관계자가 참여하고 있어, 기존의 조직 중심의 보안 관리체계에는 한계가 존재하므로 특정 조직을 한정하는 보안 관리체계가 아닌 이해관계를 가진 모든 조직의 보안 관리체계를 보증할 수 있는 대응 전략이 필요하다.

이런, 공급망 위험관리체계 마련을 위해 미국, EU 등은 공급망 위험관리에 대한 새로운 보안 프레임워크를 구축하고 보안 인증을 통한 안전한 제품·서비스를 도입하기 위해 다양한 정책을 추진 중이다. 미국 국립표준기술연구소(NIST)에서는 사이버 보안 프레임워크과, 공급망 보안을 기준을 책정하고 있으며, 특히, 미 국방성(DoD)은 국방분야 조달체계에서 공급망 보안체계를 갖추도록 의무화하고 있다.

EU에서는 단일시장을 목표로, 공급망 보안을 위해 사이버 보안 인증 프레임워크를 수립하고 있다.

본 논문에서는 공급망 프로세스에서의 공격 유형과 분류를 살펴보고, 미국, EU 등과 국제표준으로 제시된 공급망 보안기준과 관리체계를 비교 분석하여[2][3], 국내에 적합한 공급망 보안을 위한 사이버 보안 프레임워크 수립 방향을 제시하고자 한다.

II. 공급망 공격 분류

공급망 공격과 관련해 미국 연방 정부의 후원을 받는 비영리 연구개발 기관인 미국의 MITRE에서 공급망 생명주기에서 발생한 공격패턴을 분류하고 있다[4]. 이 문서에서는 공급망 보안사고 유형을 12개의 속성과 5가지의 장비 도입단계와 4가지 공격지점을 상정해 41개의 공급망 공격패턴을 분류하고 있다.

MITRE의 41가지 공격패턴의 5가지 예시는 아래와 같다.

- 진본 부품을 위조 펌웨어 부품으로 대체(생산 및 전개 단계, 펌웨어 타겟)
- 개발 단계에 시스템 소프트웨어에 악성코드를 삽입(공학 및 제조 개발 단계, 소프트웨어 타겟)
- 시스템 구축단계에서 데이터의 변경으로 인한 의

도적인 시스템 구성 오류를 발생(운영 및 지원 단계, 시스템 정보 또는 데이터 타겟)

- 장비 도입단계에서 부품이 악의적인 하드웨어로 대체(운영 및 지원 단계, 하드웨어 타겟)
- ICD(Initial Capabilities Document) 또는 CDD(Capability Development Document) 에서 시스템 역량 서술이 거짓이거나 변경되어, 파생 시스템 요구사항에 에러를 발생(재료 솔루션 분석 및 기술 발전 단계, 시스템 정보 또는 데이터 타겟)

Fig. 1.의 공급망 공격의 위치 관점의 분류에서는 공격 가능성이 있는 지점으로 프로그램 개발사이트, 주계약자, 위탁업체, HW/SW 통합업체, 개별 SW/HW 개발 제조가 있으며, 모든 위치에서 악의적인 SW 삽입, 위조된 HW 변조와 같은 악성 행위가 가능하다는 것을 보여준다. 공급망 위치 간 물리적, 정보 및 데이터 흐름을 '위치 간 공급망 연결'이라 정의하고 위치 간 공급망 연결에서 공급업체와 위탁업체의 물류 네트워크 또는 위탁업체와 공급업체 외부의 ICT/IDE의 물리적, 정보 및 데이터 흐름에서 공급망 공격지점을 보여주고 있다. 또한, 공급망에 속한 프로그램 개발사이트, 주 계약자, 위탁업체, HW/SW 통합업체, HW/SW 제조업체를 대상으로 치환, 변조, 멀웨어 같은 공격이 가능하고, 해당 공급망의 모든 단계에서 공급망 공격이 발생할 수 있으며, 공급망에 연결된 모든 업체에 연계되는 공격이 발생할 수 있다고 정리하고 있다[5].

Fig. 2.의 공급망 공격의 흐름 관점의 분류에서는 공급망 공격지점으로 공급업체와 위탁업체의 물류 네

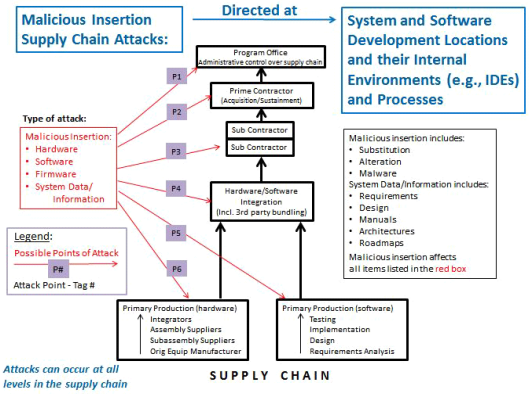

Fig. 1. Points of Attack - Supply Chain Locations

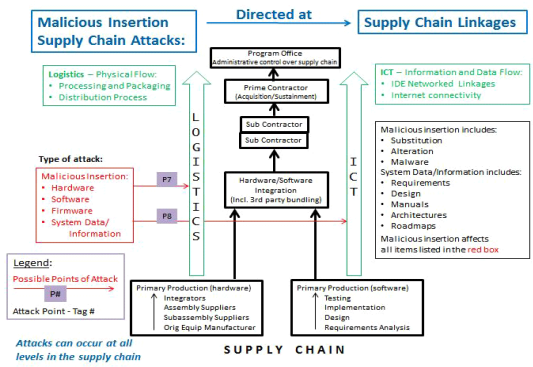

Fig. 2. Points of Attack - Supply Chain Linkages

트워크 같은 물리적 흐름, 공급업체와 위탁업체의 외부 ICT/IDE 환경 같은 정보 및 데이터 흐름으로 정하고, 위치 및 흐름을 통해 추가적인 공급망 연계 공격이 가능하다는 것을 보여주고 있다.

또한, MITRE에서는 위에 나타난 공격 목표, 지점, 단계 등 공급망 공격 속성을 활용하여 공급망 공격패턴 프레임워크를 정리하고 있으며, 분류된 공격패턴을 이용해 공급망 공격의 전반적인 프로세스의 위험 감소를 위한 대책 방안 연구 지침을 제시한다.

특히, 'Supply Chain Attacks and Resiliency Mitigations'란 보고서에는 HW, SW, Firmware, 시스템 정보와 데이터의 악의적 행위에 대한 공급망 공격 초기 대책을 포함한 대책의 초점, 공격 완화방안, 설명, 목표, 단계와 시간, 비용 같은 리소스 속성을 가진 대책을 제시하고 있다[6].

또한, 해당 문서에서는 Fig. 3.와 같은 단계에 걸쳐 공격이 진행되며 공급망 공격을 통해 최종 시스템에 아래와 같은 이점을 가질 수 있다고 설명한다.

- 악성코드를 포함해 탐지되지 않는 지속 가능한 무기를 확보할 수 있음.
- SW 업데이트 서버에 신뢰할 수 있는 알고리즘을 삽입하여 의심받지 않는 공급망 공격이 가능
- 시스템 설계 초기에 악성코드를 삽입하여 시스템이 구축되기 전에 공격 지속의 가능성을 확보할 수 있고 펌웨어 같은 낮은 계층의 구성요소에 삽

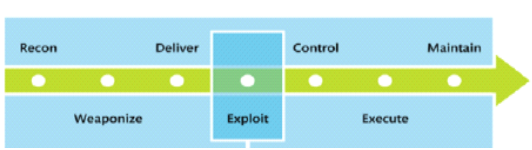

Fig. 3. Cyber Attack Life cycle

입하여 탐지가 어렵게 할 수 있음.

III. 미국 공급망 보안기준 및 정책

미국은 국가 주요 기반시설의 사이버 보안 강화를 위해 사이버 보안 프레임워크 만들어 산업별로 적용을 추진하고 있으며, 트럼프 행정부 출범 후 연방 정부 기관들의 보안 위협 점검을 위한 목적으로 확대하고, 기존 특정 기능의 방어(중요 인프라 중심)로부터 공급망 위험관리로 확대하고 있다. 이를 국방부를 비롯해 연방정부 조달분야로 확대해, 공급망에서의 신뢰성을 확보하기 위한 다양한 정책을 추진중에 있다.

본 절에서는 미국에서 시행되는 공급망의 보안기준과 정책을 소개한다.

3.1 NIST Cybersecurity Framework(CSF)

사이버 보안 프레임워크(CSF, Cyber Security Framework) v1.0은 2013년 2월 오바마 대통령이 발표한 '국가 주요기반시설의 사이버 위협 대응 강화를 위한 행정명령'에 따라 마련했다[7].

2017년 5월 트럼프 대통령이 발표한 '연방 네트워크 및 핵심 인프라의 사이버 보안 강화에 관한 행정명령'에 따라 인프라 사이버 보안 개선을 위한 프레임워크 1.1을 마련했다[8]. 사이버 보안 프레임워크는 에너지, 은행, 통신, 국방 산업 기지를 포함한 국가 주요 기반시설의 운영 주체가 사이버 위협 상황에 대한 인식 및 적절한 대응을 할 수 있도록 안내하는 일종의 보안관리 가이드라인이다. ISMS 등 대표적인 보안기준과 비교하면 CSF는 사이버 공격대책에 대해, 다양한 산업과 기업에 적용할 수 있도록 요구사항을 일반화와 위험기반 접근방식을 채택하고 있으며, 조직의 보안수준 개선에 초점이 맞춰져 있어, 끊임없는 보안수준에 대한 모니터링을 강화하기 위함이다.

공급망 보안과 관련해 CSF v1.1에서는 공급망 위기관리(Supply Chain Risk Management)와 사이버 보안 위험의 자기 평가(Self-Assessing Cyber Security Risk)의 중요성이 강조됐다[8]. 이는 조직에서 공급망은 복잡하고 전 세계적으로 퍼지고 있어 이러한 복잡한 상호작용의 관계 아래, 공급망 위험관리를 조직의 중요한 보안로 보고 있으며, 공급망에 있어 불충분한 제조나 개발, 잠재적으로 악의가 있는 기능, 가짜 혹은 취약성이 있는 제품이나 서비스를 특정하고, 평가, 경감하는 것을 목적으로 두고 있다.

3.2 NIST SP800-161

NIST에서 개발된 공급망 보안관리 기준으로 SP800-161, C-SCRM(Cyber-Supply Chain Risk Management)가 있다[9][10]. 미 정부의 공급망 보안대책으로 2015년부터 일부 미국 연방 정부 기관에서 NIST SP800-161 준수가 의무화되어 2016에는 미국 행정관리 예산국이 발행하는 통지 A-130호에서 미국 연방 정부의 공급망 보안을 위한 요구사항으로 자리매김하게 됐다.

SP800-161에서는 ICT 시스템의 구축·운용 시, 외부의 서비스, 기능이용이나 시스템을 구성하는 제품·부품의 제공을 담당하는 플레이어의 다양화에 따라 공급망이 복잡화·다양화가 진행되고, 효율성과 호환성의 향상을 위해 공급망 전체의 프로세스를 상세히 파악하는 것이 어렵게 됐다. 이에 따라, 공급의 품질 저하 문제나 악의적 개입으로 ICT 시스템에 피해가 생기는 사례가 발생함에 따라, 이런 위협에 대해 종합적인 대책을 실시하는 목적으로 수행해야 할 보안 관리대책을 담고 있다. 기본 개념으로 공급망 보안대책 수행에 있어, 공급망에서 위협과 조직의 취약점에서 보안 문제가 발생할 확률과 영향을 평가해 위험기반의 공급망 대책을 실행한다. 또한, 조직 전체를 통한 통합적인 위험 관리 수행을 위해 위험 관리 계층화하는 접근법을 채택해 조직 계층 간 위험을 전략적으로 통합 관리하는 목표를 달성하고자 한다.

SP800-161은 SP800-39에서 요구하는 조직 전체의 위험관리 프로세스에 통합되어야 함을 기술하고 있다[11]. 또한, 공급망 보안 활동은 해당 위험을 확인, 평가, 적절한 완화 조치 결정, 선택된 완화 조치를 문서화 할 공급망 보안계획 개발과 성능을 포함해야 한다. ICT 공급망은 조직마다, 조직 내에서도 달라 공급망 보안계획은 개별 조직, 프로그램 운용 상황에 맞게 조정되어야 하고 조직은 맞춤형 ICT SCRM 계획을 다음과 같이 설계해야 한다.

- 위험을 제거하는 대신 관리한다.
- 운영이 끊임없이 진화하는 위협에 적응할 수 있는지 확인한다.
- 자체 조직, 프로그램 및 지원 정보시스템 내의 변화에 대응해야 한다.
- 글로벌 ICT 공급망에서 빠르게 진화하는 관행에 맞게 조정한다.

3.3 NIST SP800-171

또 다른 공급망 보안기준으로 NIST에서는 연방정보시스템 및 기구 내에서의 비기밀통제정보(CUI,Controlled Unclassified Information)의 보호를 목적으로 SP800-171을 발표했다[12]. 연방정부와 거래 시, 비 기밀정보 보호 요구사항의 이행 혹은 이행을 위한 보안계획을 기술하고 필요한 경우, 시스템 보안계획과 조치 일정을 연방 정부나 연방 측의 계약 상대방에게 제출한다. 2018년 6월에는 사이버 보안 위험 자체 평가, 공급망 내의 사이버 보안 관리, 취약점 공개 등의 기존 내용을 보완하여 발표했다. NIST SP800-171은 연방을 대상으로 조달계약을 체결하는 모든 계약자(또는 공급자)가 준수해야 하는 것을 목표로 하고 있으며, 특히, 미 국방성(DoD)는 이 기준을 준수하도록 강제하고 있다.

CUI는 미국의 국가안보에 관한 중요한 기밀정보(Classified)로 분류되지 않은(Unclassified) 정보가 기밀 관리되는 정보를 의미한다. 미국 정부의 조달계약에 관한 정보도 CUI의 일부가 되어야 한다고 설명한다. 구매한 제품의 기술정보를 포함해 조달계약이 유출되면, 무기와 정비 등의 구매 상황이 추정될 수 있기 때문이다. 이전에는 CUI에 해당하는 정보는 정부의 각 기관에서 통일되지 않고 취급되었으나, 2010년 11월 대통령령 13556에서 CUI가 어떤 정보인지 정의됐고 구매 합병 구분은 4가지가 있다.

- 관리해야 할 기술정보(Controlled Technical Information)
- 일반구매와 인수정보(General Procurement and Acquisition)
- 중소기업의 연구개발과 기술이전 정보(Small Business Research and Technology)
- 조달처 선정에 관한 정보(Source Selection)

또한, 미국의 국가안보의 관점에서 국방 관계만을 보호 대상으로 하지 않고 악의적으로 조작되면 사회 혼란이 발생하는 사회 인프라까지 확장됐다. 조달에 관한 정보는 정부 기관에만 저장되는 것이 아니며 사본은 공급처에 보관되어 있다. 또한, 중요한 기술정보 등을 공급처가 보유할 때도 있다. 따라서 CUI 보안의 범위를 공급망 전체에 확대할 필요성이 생겼으며, 그 결과 공급처가 보유한 CUI의 사이버 보안 기준에 따른 보호가 이루어질 것을 요구하고 공급처에 직접 발주와 위탁업체도 포함됨을 기술하고 있다.

공급처(비 연방시스템과 조직)에서 CUI의 기밀성을 보호하기 위해, 연방 정부 표준인, FIPS 200(Minimum Security Requirements for Federal)의 보안 요구사항을 제시하고 있다[13]. 기본 보안 요구사항을 보완하는 파생된 보안 요구사항은 NIST SP800-53의 보안 통제항목을 추가하도록 하고 있다[14]. 미 국방성에서는 ICT 조달에서 관련 공급처(위탁업체 포함)가 사이버 보안 기준 SP800-171을 2017년 12월 말까지 따르도록 “DFARS Clause 252.204-7012”(Safeguarding Covered Defense Information and Cyber Incident Reportng)에서 명시하고 있다[23]. 이 문서에서 미국 국방부의 조달 보호 대상 정보는 CDI(Covered Defense Information)로 정의되며, 위탁업체가 보호 대상으로 하는 국방 관련 정보를 다루고 있는 경우 직접 계약하고 공급처는 위탁업체에 보호를 요청하고 사이버 사고가 발생했을 때 신속하게 보고(위탁업체에서 발생 시 발주자에게 즉시 보고)해야 함을 명시하고 있다.

연방 정부와의 계약자는 정보의 손실, 오용 또는 무단 접근, 변조 가능성과 결과에 비례하는 보호 조치로서 ‘적절한 보안(Adequate Security)’을 제공하기 위하여 14개 카테고리의 110개 보안 요구사항을 제시하고 있다. 또한, SP800-171의 준수 여부를 위해 정부 기관에 의한 제3자 인증제도는 없고, 자기 선언이라고 하는 형태로 준수하는지 판단하는 자체(Self)인증 방식을 채용하고, SP800-171 부칙A 에서는 보안 요구사항에 따라 그 실시 상황을 평가, 판정하기 위한, 평가목적(assessment objects), 예상되는 평가방법과 평가대상(potential assessment methods and assessment object)을 정의한다.[15]. 평가방법과 대상은 “Examine(구조의 정비 상황의 확인”, “Interview(실시 상황의 인터뷰 확인)”, “Test(현장 테스트)” 3가지로 구분하고 어떻게

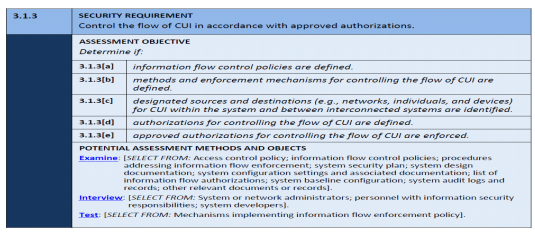

Fig. 4. Assessment Procedure for CUI Securty Requirement

해야 할지 가이드 방식으로 기술하고 있다.

3.4 미국 공급망보안 주요기준 비교

앞에서 살펴본 미국의 공급망 보안관련 주요기준인 SP800-161, SP800-171과, NIST CSF, SP800-53은 아래와 같은 관계를 갖는다. 특히, SP800-161은 위탁업체에 공급망 보안과 관련된 요구사항을 준수하게 하고, SP800-171은 공급망 보안기준을 준수하는지 증빙을 하게 하는 차이점이 있다.

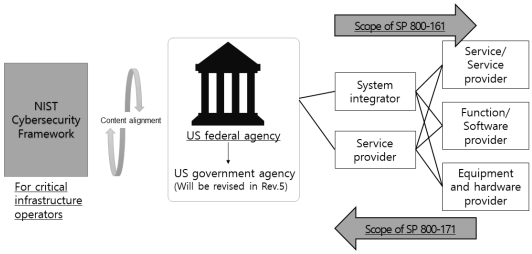

Fig. 5. NIST CSF vs SP800-53 vs SP161,171

IV. EU의 공급망 보안기준 및 정책

4.1 유럽, ENISA의 공급망 보안기준

유럽에서는 공급망 보안정책과 관련 EU 차원에서 단일시장 구현과 중요 인프라에 최신의 사이버 보안 대응(NIS Directive)을 구현하고, 네트워크에 접속하는 기기의 보안성을 인증·확인하기 위한 사이버 보안 인증 프레임워크(Cybersecurity Certification Framework)를 수립하고 있다[16]. 단일 사이버 보안 시장을 목표로 하고, 네트워크에 연결되는 기기의 인증 프레임 도입을 검토하고 있으며 규제가 아닌 자발적이고 산업계는 국제표준에 근거하는 자기 적합 선언을 하도록 할 방침이다. NIS Directive에서는 EU 각국의 중요 인프라 사업자(에너지, 교통, 은행, 금융 등)에겐 보안 대책을 의무화하고 보안 관련 국제표준을 따르도록 지시했다. 독일의 경우 NIS Directive에 앞서 2015년 IT 보안법을 제정해 중요 인프라 사업자에 대해서는 ① 사이버 보안과 관련된 최저한의 기준을 만족시키고 있는 것에 대해 정보보안청의 증명을 받아야 하고, ② 2년마다 보안감사 등을 받아야 하며, ③ 사이버 공격이라고 판단되는 사건이 발생했을 때 정보보안청에 보고하도록 하며, 'small office and homes'의 라우터 기술 가이드라인을 만들어 공표했다.

EU는 회원국에 따라 ICT 제품·서비스의 보안 인증 제도를 달리하고 있고, 제조사는 납품하는 국가에 따라 개별인증을 받아 비용·관리부담·상호운용성 등의 문제가 발생하고, EU 위원회는 디지털 기술이 광범위하게 확산에 따라 ICT 제품·서비스의 신뢰와 보안을 향상하고, 디지털 단일시장을 성취하기 위해 사이버 보안 인증 프레임워크를 제안했다. Cybersecurity Act에 따르면 ENISA와 유럽 사이버 보안 인증그룹이 협력해 EU 전체 인증체계를 개발하고 EU 회원국은 인증 감독기관과 적합성 평가기관을 운영할 예정이다.

인증제도 설계를 위해 제품이 준수할 필요가 있는 기술 요구사항 및 평가절차는 CC(Common Criteria) 등 기존의 기준을 사용하고, 기술 표준 자체를 개발하지 않는다.(예를 들면, 현재, SOG-IS MRA 스킴으로 국제 CC 규격에 맞춰 시험하고 있는 스마트카드 등의 기기에 관한 EU 전체의 인정스킴을 준수한다는 의미이다.)

또한, 인증방법에 대해서는 각국, 산업별 협의를 통해, 인증 및 범위는 기존의 인증 메커니즘에 근거해 구축하는 것을 제안하고 있다.

4.2 영국의 ICT 공급망 보안정책

영국의 NCSC(National Cyber Security Centre)에서 공급망 보안 원칙과 평가/인증체계를 연구하고 있다. 공급망 보안 원칙은 4단계에 걸쳐 12개의 원칙을 포함하고 있다[27].

- 위험 이해
  - 보호 대상 및 보호 이유 정당화
  - 공급업체 파악 및 보안상태 확인
  - 공급망 보안위험 식별
- 통제권 확립
  - 공급업체에 보안 필요성 전달
  - 공급업체에 최소 보안 요구사항 설정
  - 계약 프로세스의 보안 요구사항 구축
  - 보안 책임 완수
  - 공급망 내 보안 인식 제고
  - 보안사고 대응 지원
- 준비사항 확인
  - 공급망 관리에 보증 활동 구축
- 지속적인 개선
  - 공급망 내 지속적인 보안 개선 활동
  - 공급업체와 신뢰 구축

2012년 6월 영국 내각부는 ISWG(Industrial Security Working Group)에서 개발한 SAF(Supplier Assurance Framework)를 발표하였다[28]. SAF는 공급망에서 발생하는 위험에 대한 기업 가시성과 효과적으로 식별과 관리가 되는지를 제공한다. 8가지의 주요 항목으로 구성되며, 요구사항을 충족하기 위해 조직과 공급업체의 자체 위험평가 결과를 분석해 사업자 선정과 계약 보안대책 수립에 활용한다. 아래는 8가지의 주요 항목에 대한 설명이다.

- 공급업체와 계약 식별: 계약현황 파악과 목록작성
- 위험평가가 필요한 계약식별: 개인정보, 기밀정보 취급 계약 등 분석
- CC 위험평가 주체 식별: 정보자산과 시스템 소유자, 계약 주관부서, 보안 부서 등 참여
- 위험관리 전략 확보: 기밀성, 무결성, 가용성 관점에서 비즈니스 영향 평가와 위험 완화 전략은 조직의 위험 성향과 일치
- CC 위험평가 대응 조정: 공급자의 CCfAR 검토하여 위험 허용 수준과 위험 성향을 매핑
- 결과 정리: 계약과 관련된 위험평가의 우선순위 지정하여 우선적인 대책 수립
- 보증 구현 프로그램: SoA(Statement of Assurance)를 기반으로 상, 중, 하 계약을 분류하여 공급업체 보증 프로세스의 비례적인 접근방식 채택

V. 국제 표준의 공급망 보안 기준

공급망 보안과 관련 주요 국제표준으로는 ISO/IEC: 27036(Information Security for Supplier Relationships)과 ISO/IEC:20243(Open Trusted Technology Provider TM Standard)가 있다. 이번 절에는 이 기준들을 살펴보도록 한다.

5.1 ISO/IEC 27036

ISO/IEC 27036은 취득자와 공급자에게 공급자 관계에서 정보 및 정보시스템을 보호하기 위해 공급자와의 관계의 맥락에서 정의한 국제표준이다[17][18][19][20]. 주요 내용으로, ICT 공급망 보안을 위한 비즈니스 케이스(정당성 보고서)를 간략히 기술하고 있으며, 공급망 유형에 따른 위험, 이에 대한 조직적 역량개선 방안, 보안대책과 절차를 통해 위험을 관리할 수 있는 생명주기 접근방법을 제시하고 있다.

- 27036-1(Part1) : 본 표준은 공급 관계에 대한 체계로 보안 시스템과 정보를 안전하게 지원하기 위한 보안 지침을 정의한다.
- 27036-2(Part2) : 본 표준은 공급 관계의 제품과 서비스를 통해 지원해야 할 항목들을 만족하기 위한 요구사항을 정의한다.
- 27036-3(Part3) : 본 표준은 제품과 서비스 제공자와 획득자에게 공급망 보안 지침을 제공한다.
- 27036-4(Part4) : 본 표준은 공급 관계에 있어 클라우드 서비스 관점에서 고려돼야 할 보안 지침을 정의한다.

ISO/IEC 27036-2(Information Security for Supplier Relationships Requirements)는 공급업체와의 관계에서 정보보안 요구사항과 기대치를 설정하기 위한 상위 수준의 프레임워크를 제공한다[18]. 해당 문서에서는 거버넌스, 생명주기 프로세스와 관련 고급 요구사항 설명을 포함한다.

27036-2 문서는 취득자가 공급업체 계약을 정의하고 관리와 모니터링을 하기 위해 취득자는 공급업체가 ISO/IEC 27001에 따라 인증을 받고 요구되는 제품과 서비스에 관련해서 ISO/IEC 27036에 따라 추가 요구사항과 적용 가능한 컨트롤을 포함하도록 요구할 수 있다. 취득자는 국제표준 전체를 사용하거나 요구사항 설명으로 사용할 개별 부분을 추출할 수 있다.

ISO/IEC 27036-3(Guidelines for ICT supply chain security)은 공급업체와의 관계에서 취득자가 조달한 ICT 제품이나 서비스가 반드시 공급업체만 제조하거나 운영하지 않기 때문에 공급업체가 인수자와 직접 관계로 구현한 정보보안 관리 및 제어는 항상 제품이나 서비스의 정보보안 위험을 관리하는 것이 충분하지 않음을 언급하고 있으며[19], 이를 해결하기 위해 공급을 위해 간접 공급업체(공급업체

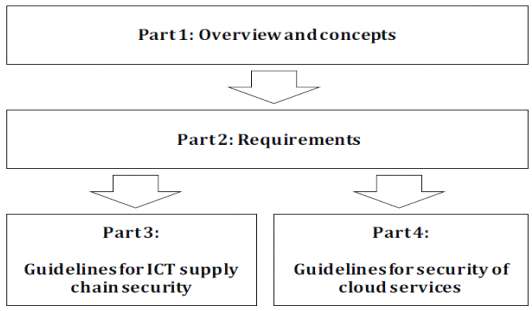

Fig. 6. ISO/IEC 27036 Architecture

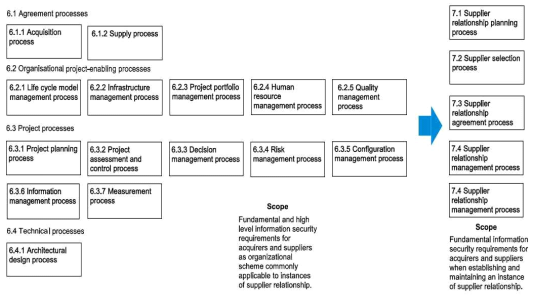

Fig. 7. Security requirements for suppliers and acquirer along the supply chain life cycle process

의 공급업체)의 제품, 서비스를 인수할 때 공급망의 가시성 확보가 필요함을 기술하고 있다.

이에 따라, ISO/IEC 27036-3에서는 ICT 제품과 서비스 공급망에 관련된 정보보안 위험 관리를 위한 취득자와 공급업체가 해야 할 활동들에 대한 지침을 제공한다. 이를 위해, Part 2의 요구사항을 기반으로 고급 요구사항을 보완하는 추가 사례를 제공하며, ICT 조달 프로세스에 공급망을 위한 프로세스 요구사항을 기술한다. ISO/IEC 27002에 기술된 정보보안 통제를 지원하면서 ISO/IEC 15288과 ISO/IEC 12207에 기술된 정보보안 프로세스와 절차를 시스템과 소프트웨어 생명주기 프로세스에 통합한다.

ISO/IEC 27036-4(Information Security for Supplier Relationships_guidelines for Cloud Services Security)에서는 ICT 외주와 Public과 Private cloud에서의 공급망 보안을 위한 가이드라인을 제시한다[20]. ICT 공급망 정보보안 위험과 마찬가지로 클라우드 컴퓨팅 서비스(예:IaaS, PaaS, SaaS)를 이용할 때, 정보보안 관리와 제어 구현의 역할, 책임의 명확성을 담아, 인수자와 공급업체 시스

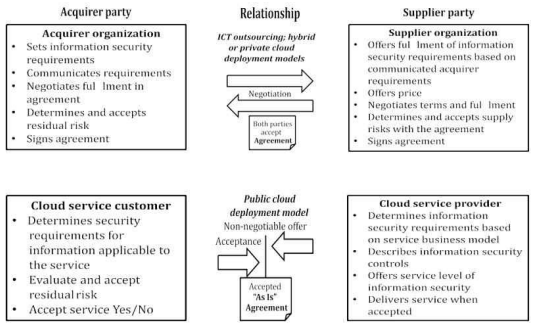

Fig. 8. Similarities and Differences between ICT Outsourcing/Private Cloud and Public Cloud

템보다 복잡한 상호 연결과 관련된 정보보안 위험을 감소시킨다.

5.2 ISO/IEC 20243(O-TTPS)

ISO/IEC 20243(Open Trusted Technology Provider™ Standard (O-TTPS) – Mitigating maliciously tainted and counterfeit products)은 악의적으로 감염된 제품과 위조된 제품의 위험을 완화하기 위한 제품 무결성과 공급망 보안을 위한 국제 표준으로 Open Group(IT 제품과 서비스 관련 표준, 정책 등을 개발하는 글로벌 컨소시엄 조직)을 주도로 개발되었다[21][22].

ISO/IEC 20243은 ISO/IEC 20243-1(Part 1: Requirements and recommendations)과 ISO/IEC 20243-2(Part 2: Assessment procedures for the O-TTPS and ISO/IEC 20243-1) 등 두 개의 파트로 구성된다. ISO/IEC 20243-1에서는 상용 ICT 제품의 전체적인 제품 생명주기에 걸쳐 악성 조작 및 위조 위험에 노출된 제품을 보증하기 위한 요구사항이 포함된다. ISO/IEC 20243-2에서는 ISO/IEC 20243-1에 포함된 요구사항에 대한 적합성을 입증하는 데 사용할 수 있는 평가절차가 제공된다.

O-TTPS(Standards)는 글로벌 공급망 보안과 COTS ICT 제품의 무결성을 향상하기 위해 적절히 준수했을 때 나타난 일련의 지침을 포함하는 개방형 표준이다. 설계, 외주, 구축, 이행, 유통, 지속 및 폐기 단계를 포함하는 COTS ICT 제품 생명주기 전반에 걸쳐 악의적으로 감염된 제품과 위조 제품을 보증하는 데 도움이 되는 지침, 요건과 권고사항을 제공한다[21].

현재 COTS 제품의 ICT 조달에서 본 표준에서 다루는 두 가지 주요 위협은 악의적으로 오염된 제품, 위조 제품으로 정의되며 다음과 같다.

- 악의적으로 오염(taint)된 제품 : 이 제품은 공급자가 생산하고 공급자의 공인 채널을 통해 획득되지만, 악의적으로 조작된다.
- 위조(counterfeit)된 제품 : 제품은 공급자가 아닌 다른 곳에서 생산되거나, 공급자의 공인 채널이 아닌 다른 곳에서 공급자에게 공급되며, 그렇지 않더라도 합법적으로 처리된다.
-

본 표준에서는 신뢰할 수 있는 기술 공급자가 정의되며 공급망을 포함하는 제품의 생명주기에서의 안전하게

활용되기 위한 검증된 모범 사례를 적용한다. 공급자와 공급 제품이 본 표준에서 명시한 요구사항과 권장 사항을 준수할 경우 제품의 무결성이 강화된다. O-TTPF에 반영된 업계의 합의는 제품 개발/엔지니어링, 안전한 개발/엔지니어링과 공급망 보안 같은 제품 무결성에 필수적인 영역에서 도출한다.

Fig. 9.에서는 COTS ICT 제품 공급망의 다양한 구성요소가 이상적으로 상호작용하는 방법의 한 예를 보여준다.

본 표준의 최적화에 중요한 것은 공급망 공격 목표와 관련된 공급망 위험에만 초점을 맞추는 것이다. 공급업체 위험의 다양성(예: 공급업체가 폐업하거나, 불량 제품을 판매)과 타겟 공급망 공격(예: 판매 중인 제품 내의 구성요소를 악의적으로 손상)과 관련 위험 사이에는 분명한 차이가 있다.

소프트웨어와 하드웨어의 경우 제품 결함에는 코딩에서 의도하지 않은 실수나 설계에서 의도하지 않은 실수를 포함한다. 소프트웨어 결함을 해결을 위해 여러 패치를 적용하는 비용은 '숨겨진 비용'이며 때에 따라 시스템 전체 비용과 효과에 영향을 미칠 수 있다. 공급업체 역시 패치를 만들고 테스트하며, 운영비용이 증가하는 의도하지 않은 결함을 줄이는데 큰 관심이 있다. O-TTPF는 모범 사례를 다음과 같은 4가지 범주로 구성하고 있다.

- 제품 개발·엔지니어링 방법
- 안전한 개발·엔지니어링 방법
- 공급망 보안방법
- 제품 평가방법

ISO/IEC 20243-1에서는 공급망 관점에서 오염된 제품과 위조 제품의 위험을 이해하는 것 이외에 위험이 어디에서 발생하는지 파악해야 한다. 공급업체 관점에서는 기술개발·공급망 활동에는 '업스트림'과 '다운스트림' 요소가 있다고 할 수 있다[21]. '업스트림'은 드라이버 개발자나 칩 제조업체 같은 구성요소(소프트웨어, 하드웨어)의 공급업체이다. '다운스트림'은 통합업체, 유통채널이며 여기서 취득자는 제품을 공급받는다. 이 연속성에서 특정 위험의 관련성을 이해하면 위험 완화를 위한 공급자가 취할 수 있는 조치를 알 수 있다. 아래 그림은 오염된 제품과 위조 제품에 대한 관련성을 보여준다.

- Malware: 시스템이나 데이터의 기밀성, 무결성, 가용성을 의도적으로 훼손하는 기능
- Unauthorized Parts: 인증되지 않은 잠재적으로 위험한 구성요소의 제품과 구성요소
- Unauthorized Configuration: 제어설정, 공격 영역 등에 잠재적으로 위험한 변경사항의 도입
- Scrap/sub-standard parts: 품질 기준을 충족하지 못하거나 수명이 다해 공급망의 초기 단계에서 폐기된 부품을 공급망에 도입
- Unauthorized production: 제조, 판매허가를 받지 않은 제품

ISO/IEC 20243-1에서는 상용 ICT 제품의 전체적인 제품 생명주기에 걸쳐 악성 조작 및 위조 위험에 노출된 제품을 보증하기 위한 요구사항이 포함된다. O-TTPS 보안 요구사항은 제공업체의 제품 생명주기 관점에서 기술 개발 요구사항과 공급망 보안 요구사항으로 구분된다.

- 기술개발 요구사항: 제공업체의 상용 ICT 제품에 대한 기술개발 활동은 주로 '제공업체의 자체감독' 하에 실행된다. 기술개발 요구사항은 제품 개발/엔지니어링 방안과 안전한 개발/엔지니어링 방안을 기반으로 요구사항이 구성된다.
- 공급망 보안 요구사항: 제품 생명주기에 걸친 제

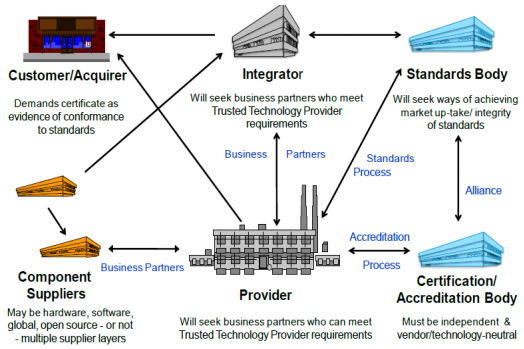

Fig. 9. Ideal interaction of supply chain

	Tainted			Counterfeit		
	Upstream	Provider	Downstream	Upstream	Provider	Downstream
Malware	Relevant	Relevant	Relevant			
Unauthorized "Parts"	Relevant	Relevant	Relevant	Relevant		
Unauthorized Configuration			Relevant			
Scrap/Sub-standard Parts				Relevant		
Unauthorized Production				Relevant		Relevant

Fig. 10. Threat Mapping

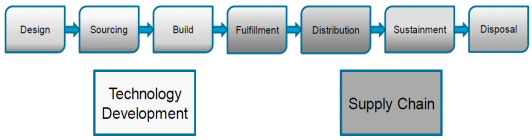

Fig. 11. Product Life Cycle - Categories and Activities

공업체의 공급망 보안 활동은'제공업체가 합의된 기여만 하는 제3의 업체와 교류'해야 한다는 모범 사례에 집중된다. 여기서 모범 사례는 제공업체와 제3 업체 간의 점검, 검증, 계약 등과 같은 교차점을 통제 혹은 관리해야 한다는 것이다.

하지만 이러한 두 가지 경우의 요구사항에 따라 전체적인 제품 생명주기 활동이 완전히 구분되는 것은 아니다. 특정 제품은 제공업체의 자체적인 제품 생명주기 내에서 취급되기도 하며 제공업체가 관리하는 다양한 제3의 업체가 포함된 제품 생명주기 내에서 취급되기도 한다. 또한, 운영 측면에서도 두 가지 요구사항은 활동 경계가 겹칠 수 있다. Fig. 11은 본 표준에서 제시하고 있는 제품 생명주기와 두 가지 요구사항의 관계를 보여주는 그림이다. 그림에서 음영이 표시된 곳은 두 갈래 요구사항의 활동 경계가 겹칠 수 있는 부분이다.

VI. 공급망 보안기준 비교분석 및 선택지침

앞에서 미국, EU, 국제표준의 ICT 공급망 보안기준과 보안정책에 관해 살펴보았다. 해외의 다양한 공급망 보안 관련 기준들은 보안 요구사항 준수 여부를 제삼자 인증, 양자 간 인증, 자기평가 등 기준마다 이용목적이 다양하며, 기준을 준수해야 하는 이용자(정부, 민간, 산업 등)도 다양하다. 국내에 공급망 보안 기준(가이드라인)이 마련된다면, 정부 조달 등 다양한 이용목적을 고려해 볼 수 있을 것이다.

구체적으로 정부 조달과 관련해서는 미국과 EU의 방식이 상이하며, 미국의 경우, 자기평가와 양자가 평가로 이뤄지고 있으며, EU의 경우, 강제사항은 아니지만, 제3자 평가·인정을 목적으로 함을 볼 수 있다.

미국의 경우, 정부 기관에서는 NIST SP800-161 준수 여부를 외주업체가 자기평가를 통해 본사에게 제출하고 되어있으며, 미 국방성(DoD)의 경우, NIST SP800-171을 조달 의무화를 통해 국방성에서 이를 확인하는 단계를 거치게 된다.

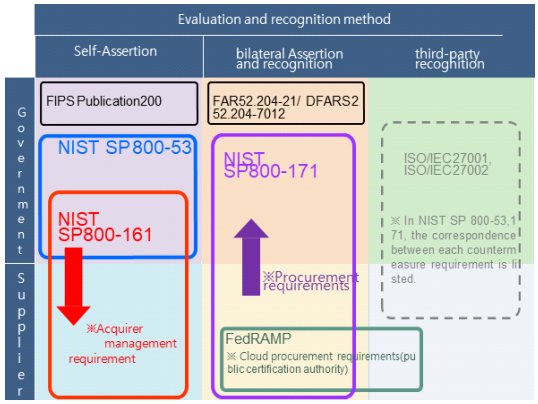

Fig. 12. U.S. supply chain security related procurement system

EU의 경우, 적용 대상을 한정한 모범 사례를 통해, 자기평가를 하도록 하고 있으나, 향후, EU의 사이버 보안 인증 프레임워크를 통해 EU 각국의 인증기관의 재량에 따라 인증 기준을 마련해 제3자 인정을 할 예정일 것으로 보인다.

또한, 정부 기관뿐만 아니라, 민간과 산업별로 공급망 보안과 관련해 다양한 기준, 정책들이 존재하므로 조직에 맞는 기준을 선택해 따를 필요가 있다.

획득자와 구매자 각각의 조직에 맞는 기준을 선택하려면 공급망 보안에 대한 전반적인 위험 관리의 프레임워크를 설정하고, 공급망을 이해하고 우선순위를 파악해야 할 것이다.

이를 위해, NIST에서는 다양한 사이버 공급망 표준들을 분류하고 선택을 위한 로드맵을 제시하고 있다[25]. 'Cyber Supply Chain Standards Mapping and Roadmap' 문서에서는 각 조직에

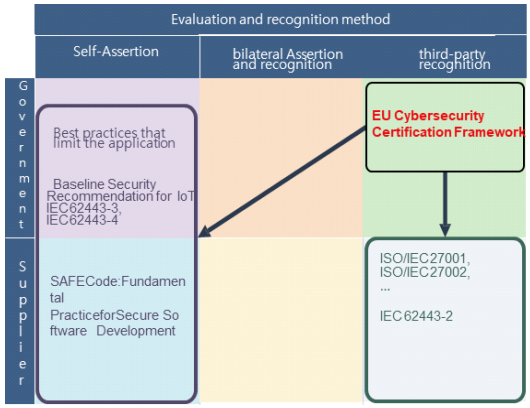

Fig. 13. EU supply chain security related procurement system

맞는 공급망 표준을 세 가지의 질문으로 조직에 맞게 대응시켜준다.

①. 현재 사용하고 있는 사이버 보안 표준, 프레임워크는 무엇인가?

②. 조직의 산업분야는 무엇인가?

③. 공급망 위험 관리를 어느 초점에 맞추고 싶은가?

Fig. 14.에서는 위의 세 가지 질문으로 조직이 선택해야 할 로드맵의 예시를 보여주며 각 숫자로 대응한다.

또한, NIST에서는 2008년부터 사이버 공급망 위험 관리를 연구했으며, 2019년에 전문가 의견과 사례 연구를 통해 공급망 보안을 위한 핵심 실행지침인 NIST IR 8276(Draft): Key Practices in Cyber Supply Chain Risk Management: Observations from Industry를 제시하고 있다[26]. 이 문서에서는 기존의 기준, 실행지침과 새로운 기준, 실행지침들을 식별하며, 사이버 공급망 위험 대응에 가장 적합한 지침을 정의한다.

- 조직 전체의 C-SCRM 통합
- 공식 C-SCRM 프레임워크 수립
- 주요 공급업체의 이해와 관리
- 조직의 공급망 체계 이해
- 주요 공급업체와 긴밀한 협업
- 조직의 복원과 개선 활동에 주요 공급업체를 포함
- 공급업체와의 관계 전반의 평가와 모니터링
- 공급망 전체 생명주기의 계획

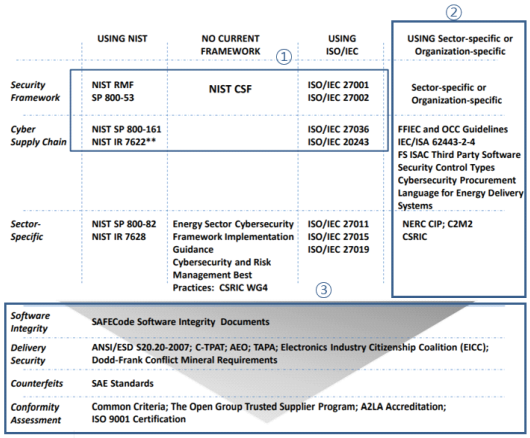

Fig. 14. Roadmap for Selecting Applicable Cyber Supply Chain Standards

또한, 다양한 표준과 우수한 사례 연구를 근거하여 핵심 권고사항을 만들었다.

- 조직 전체의 임원을 포함하도록 공급망 위험 협의회를 구성
- 공급망, 사이버보안, 제품 보안과 물리적 보안 기능에 대한 명확한 협업 역할, 구조와 프로세스 생성
- 정기적으로 위험 토론과 성과 측정 공유를 통해 C-SCRM에 대한 이사회 참여를 증대.
- 사이버 보안 고려사항을 시스템과 제품 생명주기에 통합
- 특정 공급업체 관계의 보안 측면에 대한 역할과 책임을 명확하게 정의
- 마스터 요구사항 목록 및 SLA를 사용하여 공급업체와 요구사항 설정
- 공급업체의 하위 공급업체에 보안 요구사항 전파
- 조직과 공급업체 조직의 주요 이해관계자 교육
- 보안을 염두에 두고 공급업체와 관계 종료
- 중요도 분석 프로세스 모델이나 BIA를 사용하여 공급업체 중요도 결정
- 공급업체의 생산 프로세스 가시성 설정
- 공급업체의 하위 공급업체가 데이터와 인프라에 접근할 수 있는지 파악
- 공급업체를 교육하여 사이버 보안 지침을 개선
- 취득자와 공급업체 조직 모두에서 같은 표준을 사용
- 취득자 평가 설문지를 사용하여 취득자의 사이버 보안 요구사항에 영향을 줌
- 사고 대응, 비즈니스 연속성, 재해 복구 계획과테스트에 주요 공급업체 포함
- 취약점 공개와 사고 공지를 위한 프로토콜 설정
- 사고 발생 시 외부 이해관계자와 소통을 위한 프로토콜 설정
- 학습한 결과 협업하고 결과를 기반으로 공동 계획을 업데이트.
- 타사 평가, 현장 방문 및 공식 인증을 사용하여 중요한 공급업체를 평가
- 공급된 제품 노후화 계획 수립

Table 1은 사이버 공급망 위험에 대한 대응의 지침과 다년간 NIST에서 연구하여 만든 핵심 권고사항을 매핑한 표이다. Table 2는 핵심 권고사항과 해외 공급망 보안기준을 서로 매핑한 표이다.

Table 1. Recommendations Mapped to Key Practices

	Integrate across the organization	Establish a formal program	Know and manage your critical suppliers	Understand your supply chain	Closely collaborate with your key suppliers	include key supplier in your resilience and improvement activity	Assess and monitor throughout supplier relationship	plan for the full lifecycle
Establish supply chain risk councils to include executives from across the organization	√	√						
Create explicit collaborative roles, structures, and processes for supply chain, cybersecurity, product security, and physical security functions	√	√						
Increase board involvement in C-SCRM through regular risk discussions and sharing of measures of performance	√	√						
Integrate cybersecurity considerations into the system and product life cycle	√							
Clearly define roles and responsibilities for security aspects of specific supplier relationships		√			√			
Use master requirements lists and SLAs to establish requirements with suppliers		√	√					
Propagate security requirements to suppliers' sub-suppliers		√	√		√			
Train key stakeholders in your organization and within the supplier's organization		√	√		√	√		
Terminate supplier relationships with security in mind	√	√	√	√				
Use the Criticality Analysis Process Model or BIA to determine supplier criticality			√					
Establish visibility into your suppliers' production processes			√	√	√			
Know if your data and infrastructure are accessible to suppliers' sub-suppliers			√	√	√			
Mentor and coach suppliers to improve their cybersecurity practices					√	√		
Require the use of the same standards within both acquirer and supplier organizations	√	√			√			
Use acquirer assessment questionnaires to influence acquirer's cybersecurity requirements		√	√		√	√		
Include key suppliers in incident response, business continuity, and disaster recovery 657 plans and tests	√	√	√	√	√	√		
Establish protocols for vulnerability disclosure and incident notification	√	√	√	√	√	√		

Establish protocols for communications with external stakeholders during incidents	√	√	√	√	√	√		
Collaborate on lessons learned and update joint plans based on lessons learned	√	√	√	√	√	√		
Use third-party assessments, site visits, and formal certification to assess critical suppliers		√	√	√	√		√	
Have plans in place for supplied product obsolescence		√	√	√				√

Table 2. Recommendations to Key Government Framework

	NIST SP 800-161	NIST IR 7622	2015 Case study	2019 Case study	CSF	ISO/ IEC 27002	ISO/ IEC 27036	ISO/ IEC 20243
Establish supply chain risk councils to include executives from across the organization	√		√	√	√			
Create explicit collaborative roles, structures, and processes for supply chain, cybersecurity, product security, and physical security functions			√	√				√
Increase board involvement in C-SCRM through regular risk discussions and sharing of measures of performance			√	√				
Integrate cybersecurity considerations into the system and product lifecycle	√	√	√	√	√	√	√	√
Clearly define roles and responsibilities for security aspects of specific supplier relationships	√		√	√		√	√	√
Use master requirements lists and SLAs to establish requirements with suppliers	√		√	√		√	√	√
Propagate security requirements to suppliers' sub-suppliers	√	√	√	√	√	√	√	√
Train key stakeholders in your organization and within the supplier's organization	√	√	√	√	√	√	√	√
Terminate supplier relationships with security in mind	√	√				√	√	√
Use the Criticality Analysis Process Model or BIA to determine supplier criticality	√			√	√		√	
Establish visibility into your suppliers' production processes		√	√	√			√	√
Know if your data and infrastructure are accessible to suppliers' sub-suppliers	√			√		√	√	√
Mentor and coach suppliers to improve their cybersecurity practices	√		√	√	√			√
Require the use of the same standards within both acquirer and supplier				√				

organizations								
Use acquirer assessment questionnaires to influence acquirer's cybersecurity requirements				√				
Include key suppliers in incident response, business continuity, and disaster recovery 657 plans and tests	√		√	√	√	√	√	
Establish protocols for vulnerability disclosure and incident notification	√		√	√	√	√	√	√
Establish protocols for communications with external stakeholders during incidents	√		√	√	√	√	√	
Collaborate on lessons learned and update joint plans based on lessons learned	√		√	√	√	√	√	√
Use third-party assessments, site visits, and formal certification to assess critical suppliers	√		√	√	√	√	√	√
Have plans in place for supplied product obsolescence	√	√				√	√	√

VII. 국내에 적합한 ICT 공급망 보안 관리 항목

본 절에서는 앞에서 분석한 ICT 공급망 보안 요구사항, 인증 지침, 정책 등을 참고하여 국내에 적합한 ICT 공급망 보안을 위한 관리 항목을 제시하고자 한다. 또한, 분석한 미국의 SP800-161과 국제표준 ISO/IEC 27036-3에 소개되어있는 항목과 매핑을 해보았다.

국내 환경을 고려한 ICT 공급망 보안관리 항목은 크게 개발, 공급·유지보수, 관리로 구분되고 세부 점검항목은 22개로 이루어져 있다. NIST SP800-161 문서의 통제항목은 ICT 제품 및 서비스의 개발, 공급·유지보수, 관리를 전반적으로 관리하는 부분은 잘 되었지만, 사업계획 수립·이행 시에 공급망 보안예산 통제항목과 업체를 선정하고 계약 시에 보안점검을 요구하는 통제항목이 없는 단점이 있다. 국제표준 ISO/IEC 27036-3 문서에서는 개략적인 공급망 보안정책 수립에 대한 통제항목만 존재하여, 공급망 보안 이해관계자와 예산에 대한 자세한 요구사항과 지침은 존재하지 않는 단점이 있다.

위에서 언급한 단점들을 보완한 국내 ICT 공급망 보안을 관리하기 위한 항목을 아래 표에서 제시한다.

Table 3. Propose ICT supply chain security management items suitable for domestic

Division	Large category	Medium Category	NIST SP 800-161	ISO 27036-3
Development	Design and development security	System design	SA-3	6.4.3
		System implementation	SA-8	6.4.5
		System integration and testing	SA-11	6.4.3
		Security check	SA-12	6.4.3 & 6.4.6
	Environmental security	Access control	PE-6	6.3.5
		IT infrastructure security	AC & CM	6.2.2
		Source code management	CM-10	6.3.5
Supply and maintenance	Release, packaging and delivery security	Release	IR-6 & SC-4 & SI-2 & AC-22	6.4.7
		Packaging	SA-12	6.4.7
		Delivery	AC-18 & AC-21 & AU-10 & IA-5	6.4.7
	Installation and maintenance	Carry-in/out control	PE-3	6.3.5
		Installation and distribution control	CM-8	6.4.7
		Task management	MP-6 & PE-3	6.4.3

		Maintenance contract and cooperation	AC-21 & PL-2	6.4.10
		Update version and pattern	CM-5 & AU-12	6.3.5
		Support lifecycle management	IA-4 & SA-3	6.4.10
		Equipment and parts replacement	SA-18	6.4.10
	Disposal	Carry-in/out control	PE-3	6.4.11
		Data deletion and destruction	SA-19 & MP-6	6.4.11
Management	Supply chain security risk management	Risk analysis and evaluation	RA-3	6.3.4
		Vulnerability diagnosis	SA-15	6.3.4
	Establishment of supply chain security management base	Supply chain security policy establishment	PL-1 & PV-1	6.1.1
		Supply Chain Security Organization	PV-3	N/A
		Supply Chain Security Budget	N/A	N/A
	Business plan establishment and implementation	Define supply chain security requirements	PS-1 & SA-9	6.1.1
		Define supply chain security requirements	SA-12	6.4.6
	Selecting a company and signing a contract	Establish a self-security inspection plan	N/A	N/A
		Product and Service Selection	PV	6.2.3 & 6.3.2
		Security Requirements Compliance Agreement	PV	6.1.1
		Termination and Expiration of Contract	IR-4	6.4.11
	Business management	Training and Security Inspection	AT-1	6.2.4 & 6.4.6
		Contract compliance management	SA-12	6.4.6
		Inspection	SA-12	6.4.6 & 6.4.8
		Supply chain security verification	SA-12	6.4.6 & 6.4.8
	Consignment/Service	Outsourcing security	SA-9	6.3.2

VIII. 결 론

최근, 미국, EU 등의 국가들에서는 ICT 공급망 공격에 대응하기 위해 공급망 보안을 위한 새로운 보안기준 개발 및 프레임워크를 구축하고 안전한 제품·서비스 도입을 위한 시험·인증방법 및 절차마련을 검토하고 있으며 향후, 법제화 움직임도 있는 상황이다. 이에 따라 국내에서도 국가 차원에서 기업과 조직 시스템의 공급망 위험관리를 어떻게 수립해야 하는지 정책 방향 수립이 필요한 시점이다.

우선, 전 세계적으로 공급망 보안 관리을 위한 정책마련 및 이를 수행할 수 있는 조직 체계를 구성하여 급증하는 공급망 위협에 대응할 필요가 있다. 이는 ICT 공급망의 특성상 다양하고 복잡한 프로세스가 존재하며 통제범위를 벗어나는 조직 간의 보안체계 구축이 필요하므로 취약점 진단이나 모의 해킹과 같은 IT 보안 위주의 대책으로는 한계가 있다. 따라서 공급망 프로세스와 조직 관점에서의 위험요인들을 추가로 식별하고 이에 대응할 수 있는 보안대책이 필요하기 때문이다.

또한, 최근에 빈번히 발생하는 SW 업데이트 서버를 통한 정상 SW를 위·변조에 의해 발생하는 공급망 보안사고를 사전에 차단하기 위해서는, 신뢰할 수 있는 제품목록을 만들어 보안성이 인증된 제품, 기술과 서비스를 이용하는 환경 마련이 필요하다. 이를 통해, CPS/IoT 각 산업 활동에서 Security By Design에 근거해서 구성요소 전체의 보안성 확보와 더불어, ICT 공급망 보안을 통한 전체 사이버 환경에서의 안전성을 보증할 필요가 있다.

본 연구에서는 미국, EU와 국제표준의 ICT 공급망 보안 요구사항, 인증 지침 기준을 설명하고 비교분석하여 국내에 적합한 공급망 보안 요구사항을 도

출하는 방향성을 제시하였다. 하지만, ICT 공급망 생명주기 내의 참여업체와 방식의 다양화, 보안사고 시 책임성 등을 고려하였을 때, 모든 공급망 보안의 요구사항을 충족할 수 없는 한계가 존재한다. 따라서, 글로벌 공급망 위험관리 체계를 면밀히 분석해, 국제적으로 통용되는 제도마련이 필요하다.

이를 위해 5가지 중요 추진과제를 제안하고자 한다.

첫 번째는 정부의 공급망 보안정책 수립을 위한 거버넌스 체계 구축이 시급하다. 모든 것이 연결되는 IoT와 CPS 환경에서 의료, 교통, 스마트시티 등 전 산업에서 공급망 보안정책 수립이 가장 중요하다.

두 번째는 산업별 공급망 보안 기준(가이드라인) 개발이 필요이다. 이를 위해 공급망 보안 국제표준인 ISO/IEC 27036, ISO/IEC 20243등을 준용한 기준(가이드라인) 개발과 더불어, 산업별(스마트 팩토리, 스마트 헬스케어, 스마트 시티, 자율주행 자동차 등)로 적용하기 위한 단계별 기준 마련이 필요하다. 특히, 산업별 주요정보통신기반시설에 공급되는 ICT 장비의 공급망 보안을 위한 관리체계를 구축하고 관계기관의 이행점검을 위한 제도 기반 마련이 필요하다.

세 번째는 공공분야의 공급망 보안 조달체계가 필요하다. 기존의 ICT제품, 서비스의 보안 조달체계(보안성 검토제도 등)에 공급망보안 요구사항을 요구해야 하며, 글로벌 정책 움직임에 맞춰, 기존 관련 보안인증(CC, ISMS)활용 및, 자체 인증, 제3자 인증 등의 인증체계 마련이 필요하다.

네 번째는 공급망 보안의 생태계 구축방안이 필요하다. 오픈소스를 비롯한 안전한 SW, IoT 장치에 대한 구성품 품목관리(신뢰목록 관리 등)를 위한 기술, 제도적 해결방안을 마련해야 하고, 취약점이 발견된 품목에 대한 패치와 신뢰목록 제외 등의 공급망 취약점 대응체계 마련이 필요하다.

다섯 번째는 SW, 기기에 대한 안전성 시험, 검사 기술확보가 필요하다. SW에 대한 검증기술과 HW의 비정상적인 트로이잔 등을 탐지하기 위한 기술개발이 무엇보다 필요하다.

향후 본 논문에서 소개한 ICT 공급망 보안의 미국, 유럽, 국제표준에서 요구하는 보안 요구사항을 심층 분석해, SW공급망 보안관리를 위한 SW품목관리(SBOM, Software Bill of Materials) 방법에 대해 연구할 예정이며, 공급망 장비에 하드웨어 보안과 신뢰성 검증기술에 관한 연구를 진행하여 하드웨어 트로이를 탐지하는 방안을 연구할 예정이다.

References

[1] KISA, “Cyber Threat Trend Report”, Jul. 2018

[2] Hyo-hyeon Son, Kwang-jun Kim and Man-hee Lee, “US supply chain security management system analysis.”, Journal of the Korea Institute of Information Security & Cryptology, 29(5), pp. 1089-1097, Oct. 2019

[3] Eung-kyu Lee and Jung-duk Kim, “A Case Study on ICT Supply Chain Attacks.”, The Journal of Information Technology and Architecture, 16(4), pp. 383-396, Dec, 2019

[4] MITRE, “Supply Chain Attack Framework and Attack Patterns”, Dec. 2013

[5] Office of the Under Secretary of Defense for Acquisition & Sustainment, “Supply Chain Attack Pattern : Framework and Catalog”, 2014

[6] MITRE, ‘Supply Chain Attacks and Resiliency Mitigations.“, Oct. 2017

[7] National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity. version 1.0” , Feb. 2014

[8] National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity. version 1.1” , Apr. 2018

[9] National Institute of Standards and Technology,“ Supply Chain Risk Management Practices for Federal Information Systems and Organizations” Special Publication 800-161, Apr. 2015

[10] National Institute of Standards and Technology, “Notional Supply Chain Risk Management Practices for Federal Information Systems” IR 7622, Oct. 2012

[11] National Institute of Standards and Technology, “Managing Information Security Risk Organization, Mission,

and Information System View" Special Publication 800-39, Mar. 2011
〔12〕 National Institute of Standards and Technology, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" Special Publication 800-171 revision 2, Feb. 2020
〔13〕 National Institute of Standards and Technology, "Minimum Security Requirements for Federal Information and Information Systems" Federal Information Processing Standards Publication 200, Mar. 2006
〔14〕 National Institute of Standards and Technology, "Security and Privacy Controls for Federal Information Systems and Organizations" Special Publication 800-53, Apr. 2013
〔15〕 National Institute of Standards and Technology, "Assessing Security Requirements for Controlled Unclassified Information" Special Publication 800-171A, Jun. 2018
〔16〕 European Cyber Security Organisation, "Overview of existing Cybersecurity standards and certification schemes v2", Dec. 2017
〔17〕 International Standard, – Information security for supplier relationships – Part 1: Overview and concepts", ISO/IEC 27036-1, Apr. 2014
〔18〕 International Standard, – Information security for supplier relationships – Part 2: Requirements", ISO/IEC 27036-2, Aug. 2014
〔19〕 International Standard, – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security", ISO/IEC 27036-3, Nov. 2013
〔20〕 International Standard, – Information security for supplier relationships – Part 4: Guidelines for security of cloud services", ISO/IEC 27036-4, Oct. 2016
〔21〕 International Standard, "Information technology – (O-TTPS) – Mitigating maliciously tainted and counterfeit products – Part 1: Requirements and recommendations", ISO/IEC 20243-1, Feb. 2018
〔22〕 International Standard, "Information technology – Mitigating maliciously tainted and counterfeit products – Part 2: Assessment procedures for the O-TTPS and ISO/IEC 20243-1:2018", ISO/IEC 20243-2, Jan. 2018
〔23〕 Office of the Under Secretary of Defens e for Acquisition & Sustainment, "DFA RS 252.204-7012 Defense Industrial Ba se Compliance Information", Nov. 2011
〔24〕 European Cyber Security Organisation, "European Cyber Security Certification A Meta-Scheme Approach v1.0", Dec. 2017
〔25〕 National Institute of Standards and Technology, "Workshop Brief on Cyber SCRM Standards Mapping"
〔26〕 National Institute of Standards and Technology, "National Institute of Standards and Technology, "Workshop Brief on Cyber SCRM Standards Mapping(Draft)" , IR 8276, Feb. 2020
〔27〕 https://www.ncsc.gov.uk/collection/supply-chain-security/principles-supply-chain-security
〔28〕 UK Cabinet Office, "Supplier Assurance Framework: Good Practice Guide", May.2018

〈저 자 소 개〉

민 성 현 (Seong-Hyun Min) 학생회원
2020년 2월: 강원대학교 컴퓨터공학과 졸업
2020년 3월~현재: 강원대학교 컴퓨터과학과 석사과정
〈관심분야〉 공급망 보안, 하드웨어 트로이 탐지, 개인정보보호&Mydata 활용

손 경 호 (Kyung-Ho Son) 종신회원
2015년 8월: 성균관대학교 컴퓨터공학과 박사졸업
2001년 1월~2018년 8월: 한국인터넷진흥원 팀장/단장/센터장
2018년 9월~현재: 강원대학교 교수
〈관심분야〉 IoT/CPS보안, 보안성 시험·인증, 개인정보 비식별& Mydata 활용