국외 공급망 보안 사례

2020년 7월 16일

방지호 박사

(정보보안센터장, jhbang@ktc.re.kr)

한국기계전기전자시험연구원

1. 공급망 (Supply Chain) 보안(Security) 이란?

공급망(공급사슬)

- 물품의 생산에서 소비까지 전달 그리고 회수의 제반 활동이 일어나는 환경상에 존재하는 제조, 도매, 유통, 소매, 고객 등의 각 구성원들의 연결망

  [출처] TTAK.KO-06.0337 RFID 기반 공급망공통 플랫폼의 응용 서비스 인터페이스

- 원재료의 조달에서부터 완제품의 최종 소비에 이르기까지 재화와 서비스 및 정보의 흐름이 이루어지는 연결망

  [출처] 국립국어원

공급체계보안

- 제품과 서비스를 만들어 소비자에게 전달하는 과정에서 자료 유출 등 보안상의 문제점이 발생하지 않도록 보장하는 보안 정책과 기술

  [출처] TTA 정보통신용어사전, https://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=057121-1

1. 공급망 (Supply Chain) 보안(Security) 이란?

정부, WTO에 '日 수출규제' 안건 상정... "세계무역 교란"

정부가 8~9일(현지시각) 스위스 제네바에서 열리는 세계무역기구(WTO) 상품무역이사회에 일본의 반도체·디스플레이 소재 수출 규제를 추가 의제로 긴급 상정하고 규제 철회를 요청했다. 아울러 일본 측 조치는 글로벌 공급망을 크게 교란해 한국 기업 뿐만 아니라 세계 무역에도 부정적 효과를 미칠 수 있다고 주장했다. 또 지난달 28~29일 일본 오사카에서 열린 G20 정상회의에서 "자유롭고 공정하며, 비차별적이고 투명하며, 예측가능하고 안정적인" 무역환경의 중요성을 주장한지 불과 이틀만에 이에 정면으로 반하는 조치를 발표했다고 했다.

[출처] 2019.7.10, 조선비즈, https://biz.chosun.com/site/data/html_dir/2019/07/09/2019070902745.html

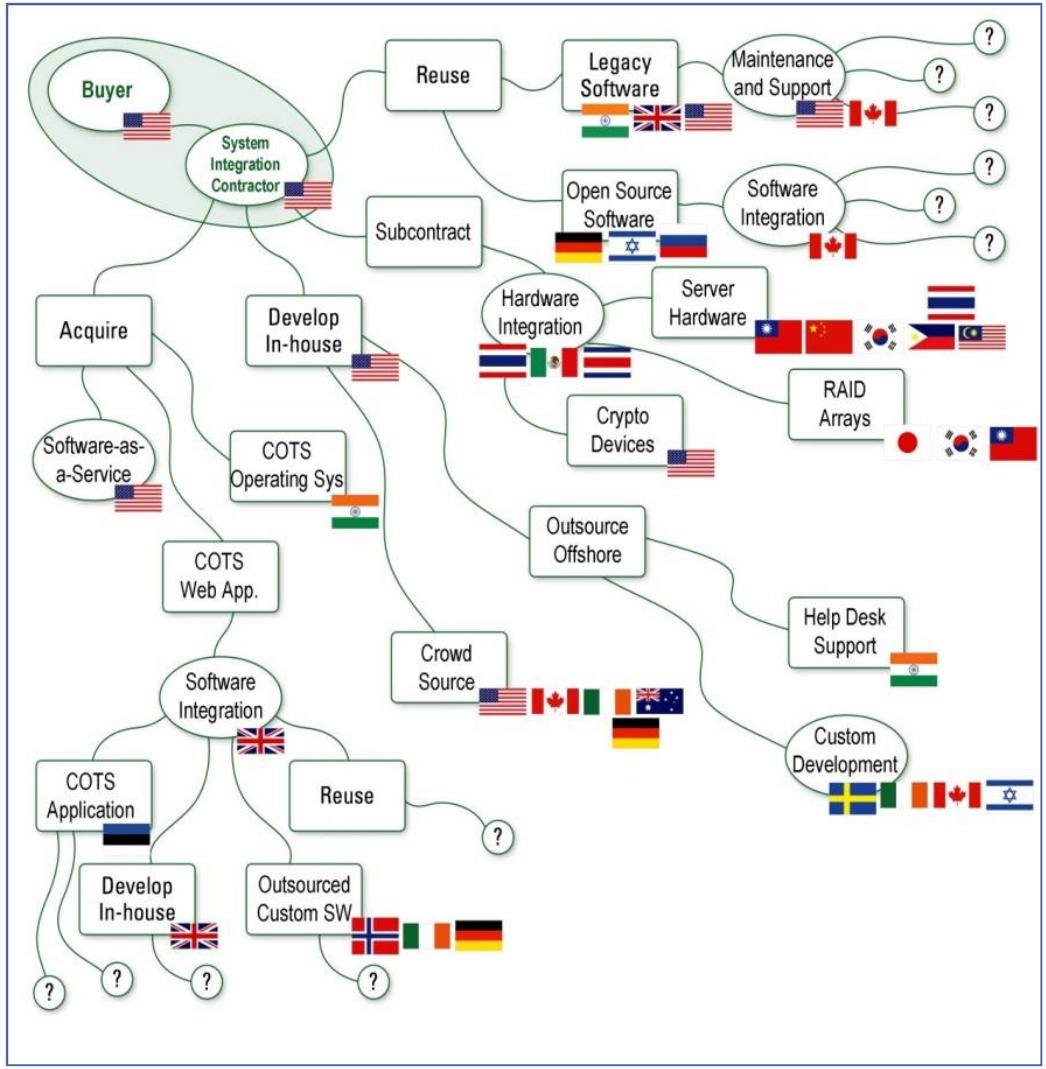
코로나19가 명분? "美, 글로벌 공급망에서 中 제거 위해 총력전"

중국을 글로벌 공급망에서 배제하려는 노골적인 움직임은 감지되고 있다. 대표적인 것이 바로 중국 통신장비업체인 화웨이에 대한 규제 강화다. 크라크 차관은 한국을 향해 화웨이 제품을 쓰지 말 것을 거듭 압박했다. 그는 "미국은 이미 동맹국을 대상으로 화웨이의 5세대(5G) 통신 장비를 사용하지 말 것을 요청했다"고 강조했다.

화웨이를 비롯해 미국과 중국의 갈등은 전방위적으로 퍼져가고 있다. 앞서 미국 상무부는 지난 15일 아예 화웨이가 미국 기술과 소프트웨어를 반도체 설계 및 제조에 활용할 수 없도록 제한하는 규제 강화 방안을 발표했다. 이 방안에 따르면, 120일 간의 유예기간이 지나면 미국의 반도체 설계 기술을 사용하는 외국기업들도 화웨이에 제품을 팔 수 없게 된다. 이에 대해 중국 상무부는 지난 17일 "중국은 모든 필요한 조치를 취해 중국 기업의 합법적인 권익을 단호하게 수호할 것"이라고 반발했다. 중국 관영 <환구시보>에 따르면 중국의 반격 조치로 애플, 퀄컴, 시스코 등 미 기업에 대한 중국 내 제한 및 조사, 보잉 항공기 구매 중단 등이 거론된다.

[출처] 2020.5.22, 프레시안, https://www.pressian.com/pages/articles/2020052208484129779?utm_source=naver&utm_medium=search

1. 공급망 (Supply Chain) 보안(Security) 이란?



IT and Communications products are assembled, built, and transported by multiple vendors around the world.

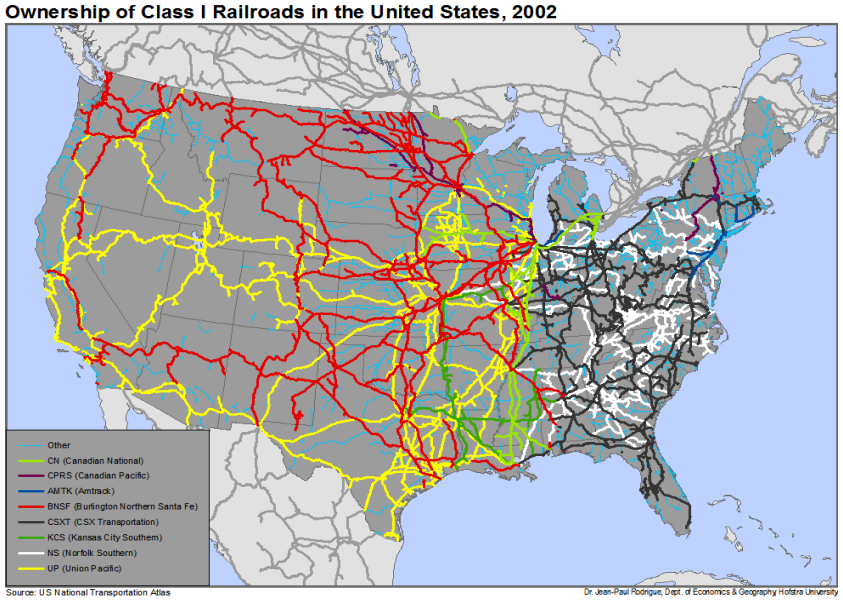
Software contributions include reusable libraries, custom code, commercial products, open source

[출처] Do You Have The Right Practices In Your Cyber Supply Chain Tool Box?, SEDC Conference, 2014.4월

1. 공급망 (Supply Chain) 보안(Security) 이란?

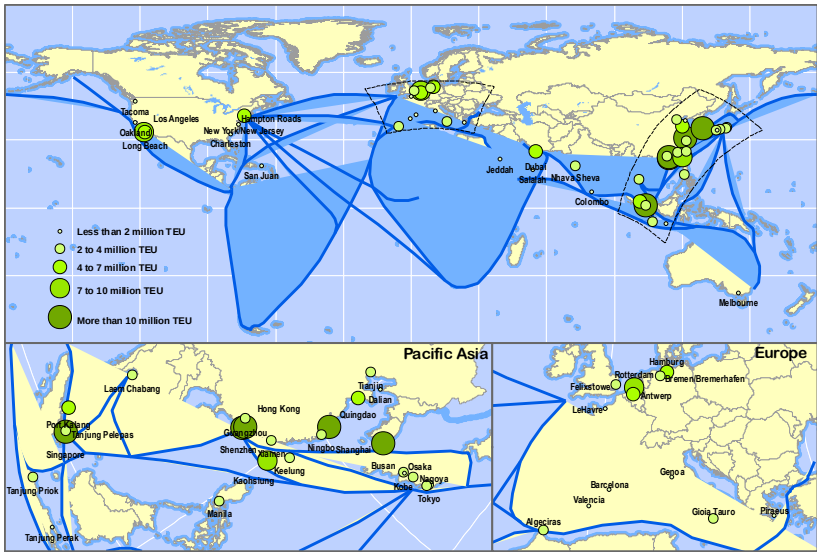
Supply Chain SECURITY

- Nodes of storage & throughput
- Lines of transport (& communication)



Supply Chain RESILIENCE

- Multi-sources
- Multi-nodes
- Multi-routes



Product INTEGRITY

- How do we improve **our trust & confidence in HW, SW & Services** we source from a global supply chain?

[출처] Do You Have The Right Practices In Your Cyber Supply Chain Tool Box?, SEDC Conference, 2014.4월

1. 공급망 (Supply Chain) 보안(Security) 이란?

화웨이, 5G 장비 국제 보안표준 최고 등급 획득…"세계 최초"

화웨이가 5G 기지국 장비에 대해 국제 보안 표준 최고 등급 인증을 받았다고 5일 밝혔다. 화웨이가 받은 인증은 국제 보안 CC(Common Criteria) EAL4+다. 5G 기지국 장비로 [redacted] 화웨이가 처음이다. 이번 인증 획득은 화웨이에 대한 보안성 논란을 불식시[redacted]결로 풀이 된다.

한편, 화웨이는 지난 5월 강도를 높인 미국 정부[redacted]세 조달 길이 막혔다. 이에 대해 화웨이는 "미국 기술과 공급망에 대한 [redacted]을 떨어트리고 결국 미국의 이익을 해칠 것"이라며 반발하고 있다.

화웨이, 5G 장비 CC인증 획득에도 백도어 논란 여전…왜?

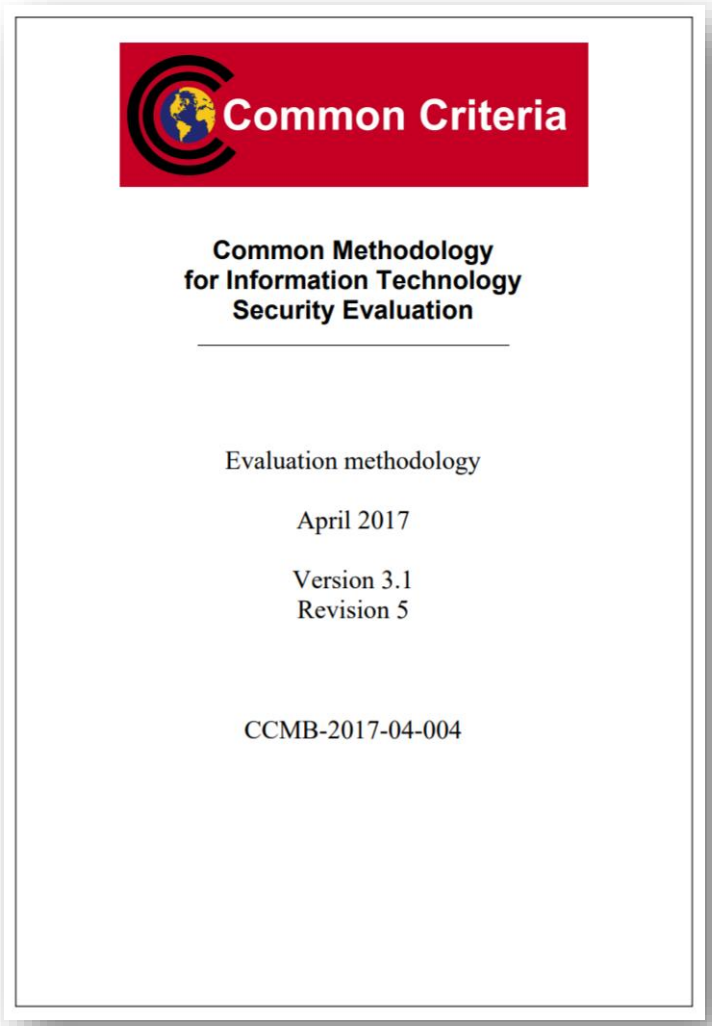
[출처] 2020.6.5, 블로터,
http://www.bloter.net/archives/387942
http://www.digitaltoday.co.kr/news/articleView.html?idxno=238729

Network and Network-Related Devices and Systems – 209 Certified Products

Product	Vendor	Product Certificate	Date Certificate Issued	Certificate Validity Expiration Date	Compliance	Scheme
Huawei 5900 Series 5G gNodeB Software V100R015C00SPC108 Certification Report Security Target	Huawei Technologies Co. Ltd.	CCRA Certificate	2020-06-05	2025-06-05	EAL4+ ALC_FLR.1	ES

[출처] https://www.commoncriteriaportal.org/products/

2. Common Criteria



[출처] https://www.commoncriteriaportal.org

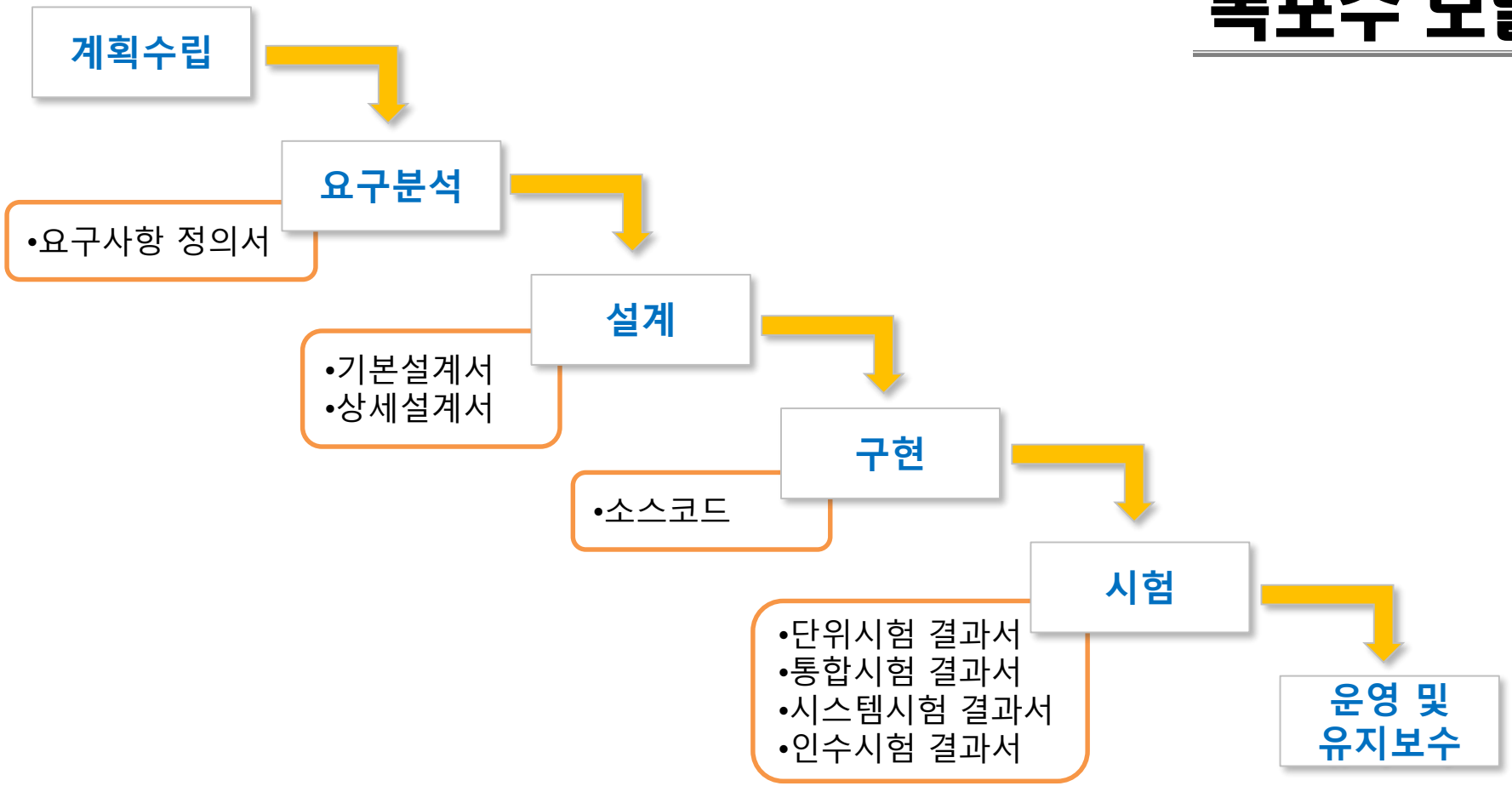
보증 클래스	보증 패밀리	평가보증등급에 따른 보증 컴포넌트						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
개발	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
설명서	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
생명주기 지원	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
보안목표 명세서 평가	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
시험	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
취약성 평가	AVA_VAN	1	2	2	3	4	5	5

ALC_LCD.1 개발자가 정의한 생명주기 모델

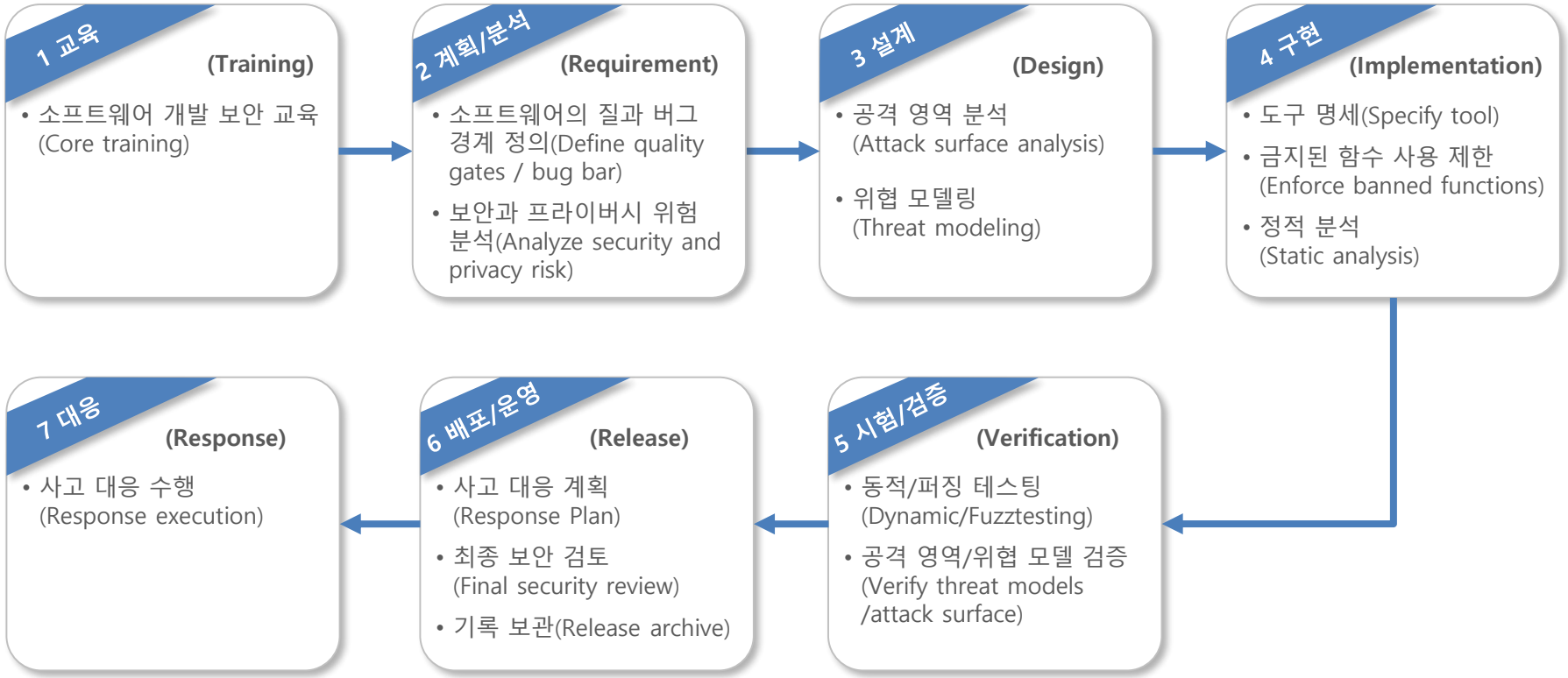
- ALC_LCD.1.1D 개발자는 TOE의 개발과 유지에 사용되는 생명주기 모델을 수립해야 한다.
- ALC_LCD.1.2D 개발자는 생명주기 정의 문서를 제공해야 한다.
- ALC_LCD.1.1C 생명주기 정의 문서는 TOE의 개발과 유지에 사용되는 모델을 서술해야 한다.
- ALC_LCD.1.2C 생명주기 모델은 TOE의 개발과 유지에 필요한 통제를 제공해야 한다.

2. Common Criteria

폭포수 모델



MS SDL(Secure Develop Lifecycle)



ALC_TAT.1 잘 정의된 개발 도구

- ALC_TAT.1.1D 개발자는 TOE에 사용된 각 개발 도구를 식별한 문서를 제공해야 한다.
- ALC_TAT.1.2D 개발자는 각 개발 도구에 대해 구현-종속적인 선택사항을 문서화하여 제공해야 한다.
- ALC_TAT.1.1C **구현에 사용된 각 개발 도구는 잘 정의된 것**이어야 한다.
- ALC_TAT.1.2C 각 개발 도구 문서는 **구현에 사용된 모든 규정과 지시어** 뿐만 아니라 모든 **명령문의 의미를 모호하지 않게 정의**해야 한다.
- ALC_TAT.1.3C 각 개발 도구 문서는 **모든 구현-종속적인 선택사항의 의미를 모호하지 않게 정의**해야 한다.

2. Common Criteria

ALC_TAT.1 잘 정의된 개발 도구

- ALC_TAT.1.1D 개발자는 TOE에 사용된 각 개발 도구를 식별한 문서를 제공해야 한다.
- ALC_TAT.1.2D 개발자는 각 개발 도구에 대해 구현-종속적인 선택사항을 문서화하여 제공해야 한다.
- ALC_TAT.1.1C **구현에 사용된 각 개발 도구는 잘 정의된 것**이어야 한다.
- ALC_TAT.1.2C 각 개발 도구 문서는 **구현에 사용된 모든 규정과 지시어** 뿐만 아니라 모든 **명령문의 의미를 모호하지 않게 정의**해야 한다.
- ALC_TAT.1.3C 각 개발 도구 문서는 **모든 구현-종속적인 선택사항의 의미를 모호하지 않게 정의**해야 한다.

ALC_DVS.1 보안대책의 식별

- ALC_DVS.1.1D 개발자는 개발보안 문서를 작성하여 제공해야 한다.
- ALC_DVS.1.1C 개발보안 문서는 **개발환경 내**에서 TOE 설계 및 구현 과정의 **비밀성과 무결성을 보호하기 위하여 필요한 모든 물리적, 절차적, 인적및 기타 보안대책**을 서술해야 한다.

2. Common Criteria

ALC_CMC.4 생산지원, 수용절차 및 자동화

- ALC_CMC.4.1D 개발자는 TOE 및 그에 대한 참조를 제공해야 한다.
- ALC_CMC.4.2D 개발자는 형상관리 문서를 제공해야 한다.
- ALC_CMC.4.3D 개발자는 형상관리 시스템을 사용해야 한다.
- ALC_CMC.4.1C TOE는 유일한 참조를 위한 레이블을 붙여야 한다.
- ALC_CMC.4.2C 형상관리 문서는 형상항목을 유일하게 식별하는 데 사용된 방법을 서술해야 한다.
- ALC_CMC.4.3C 형상관리 시스템은 **모든 형상항목을 유일하게 식별**해야 한다.
- ALC_CMC.4.4C 형상관리 시스템은 **형상항목에 인가된 변경만을 허용하는 자동화된 수단**을 제공해야 한다.
- ALC_CMC.4.5C 형상관리 시스템은 **자동화된 수단을 이용하여 TOE의 생산을 지원**해야 한다.
- ALC_CMC.4.7C 형상관리 계획은 형상관리 시스템이 TOE 개발에 사용되는 방법을 서술해야 한다.
- ALC_CMC.4.8C 형상관리 계획은 **변경되거나 새로 생성된 형상항목을 TOE의 일부로 수용하는데 사용된 절차**를 서술해야 한다.
- ALC_CMC.4.9C 증거는 모든 형상항목이 형상관리 시스템 하에 유지되고 있음을 입증해야 한다.
- ALC_CMC.4.10C 증거는 형상관리 시스템이 형상관리 계획에 따라 운영되고 있음을 입증해야 한다.

ALC_DEL.1 배포 절차

- ALC_DEL.1.1D 개발자는 소비자에게 TOE나 TOE 일부를 배포하는 절차를 문서화하여 제공해야 한다.
- ALC_DEL.1.2D 개발자는 **배포 절차**를 사용해야 한다.
- ALC_DEL.1.1C 배포 문서는 TOE를 소비자에게 **배포할 때 보안을 유지**하기 위해 필요한 모든 절차를 서술해야 한다.

ALC_FLR.1 기본적인 결함교정

- ALC_FLR.1.1D 개발자는 TOE 개발자를 위한 결함교정 절차를 문서화하여 제공해야 한다.
- ALC_FLR.1.1C 결함교정 절차 문서는 TOE의 **각 배포본에서 보고된 모든 보안 결함을 추적하는 데 사용되는 절차를** 서술해야 한다.
- ALC_FLR.1.2C 결함교정 절차는 **결함에 대한 교정사항의 발견 상태** 뿐 아니라 **각 보안 결함의 특성과 영향에 대한 설명이 제공**되도록 요구해야 한다.
- ALC_FLR.1.3C 결함교정 절차는 **각각의 보안 결함에 대해 교정행동이 식별**될 것을 요구해야 한다.
- ALC_FLR.1.4C 결함교정 절차 문서는 **TOE 사용자에게 결함 정보, 교정사항, 교정행동 지침을 제공하는 데 사용되는 방법**을 서술해야 한다.

3. 미국 사이버 공급망 위험관리 정책

구분		주요 내용
공공부문(연방정부)	CNCI ('08)	▪ 글로벌 공급망 위험관리를 위한 **다방면의 접근방식 개발** (CNCI #11) – NIST IR 7622('12) ⇒ NIST SP800-161('15) (연방정부기관 SCRM 실무)
	EO-13556 ('10)	▪ 연방정부와 계약을 체결한 민간 등 공급자들이 처리하는 **CUI**(Controlled Unclassified Information)*에 대한 **정부차원에서의 보호 프로그램 실시** – NIST SP800-171 Rev.1('16) (민간 등 비연방기관에서 처리하는 CUI에 대한 보호 지침) * 비기밀등급(Unclassified Information) 정보 중에서 관련 법률, 규정, 정부 정책에 따라 **반드시 보호해야 하는 정보**를 말함
	OMB Circular A-130('16)	▪ 연방정부기관은 NIST SP800-161에 따라 **공급망 위험관리 계획 수립**
	EO-13833 ('18)	▪ 정부기관의 CIO에 **IT 투자와 조달에 관한 책임** 부여
	국가사이버 전략 ('18)	▪ 연방정부의 공급망 위험관리 향상 – 공급망 위험관리 프로세스, 공급망 위협정보 공유, **공급망 위험이 있는 벤더사 및 제품, 서비스 배제** 등
	EO-13873 ('19)	▪ 정보통신기술 및 서비스 공급망 확보 – **국가안보에 위협이 되는 특정 기업의 정보통신기술과 서비스에 대해 미국 정부 및 기업에서도 취득·설치·거래 및 사용 금지**

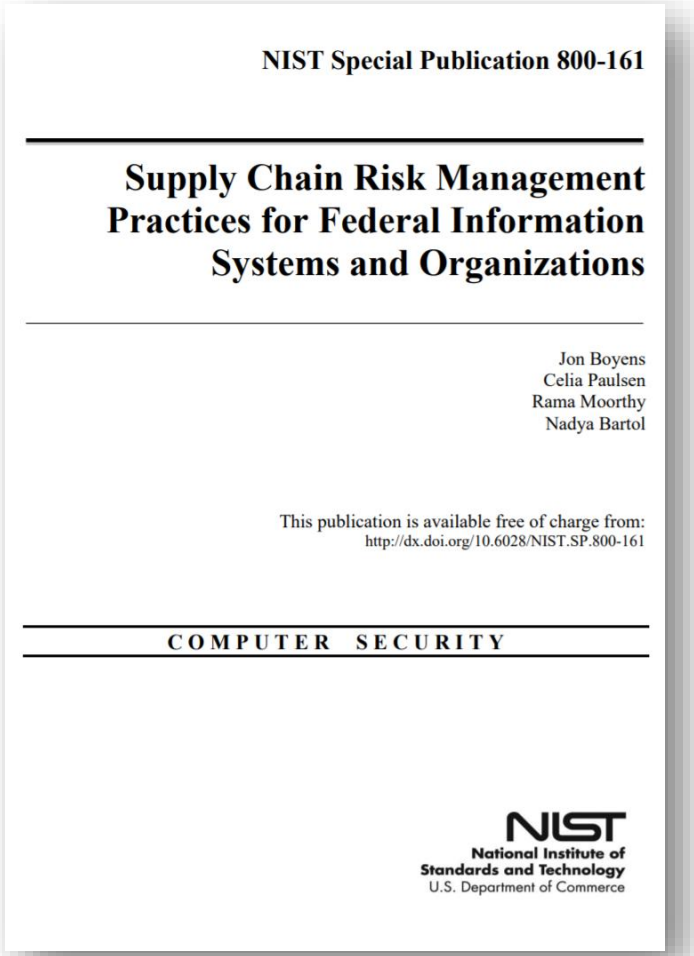
[출처] 주요국 사이버 공급망 위협 관리 정책 동향 및 시사점, 2019년 Vol.12 KISA Report

3. 미국 사이버 공급망 위험관리 정책

구분		주요 내용
민간 부문	S/W	▪ SAFECode for S/W Supply Chain Integrity Papers
	IT/OT	▪ **OTTP**(Open Trusted Technology Provider) ▪ **ISO/IEC 27036** (공급자와의 관계에서의 보안요구사항) ▪ **IEC 62443-2-4** (산업자동화 및 제어시스템 서비스 제공자에 대한 보안요구사항)
	전력	▪ NERC CIP-013-1 공급망 위험관리 ▪ APPA(American Public Power Association) & NRECA(National Rural Electric Cooperative Association) 공급망 위험관리 시 고려사항 및 모범사례
민관 협력	주요기반시설	▪ NIST **Cybersecurity Framework**(NIST CSF) Ver.1.1 – ID.SC(공급망 위험관리): 조직의 우선순위, 제약사항, 위험허용도 등을 고려하여 공급망 위험을 식별 및 평가, 관리하는 프로세스를 마련
	ICT	▪ CISA 산하 ICT SCRM Task Force – 정부와 산업계 간의 양방향 공급망 위험정보 공유를 위한 공통된 위험관리 프레임워크 개발 – ICT 공급 및 제품, 서비스의 위협을 식별·평가하기 위한 프로세스와 기준 수립 – 적격 입찰자 및 제조업체 목록을 작성하기 위한 업계와 평가 기준 수립 – OEM 또는 공인된 판매업자로부터 ICT 구매 장려, 위·변조된 ICT 조달을 방지하기 위한 정책 권고안 작성

[출처] 주요국 사이버 공급망 위협 관리 정책 동향 및 시사점, 2019년 Vol.12 KISA Report

3-1. NIST SP 800-161



NIST Special Publication 800-161

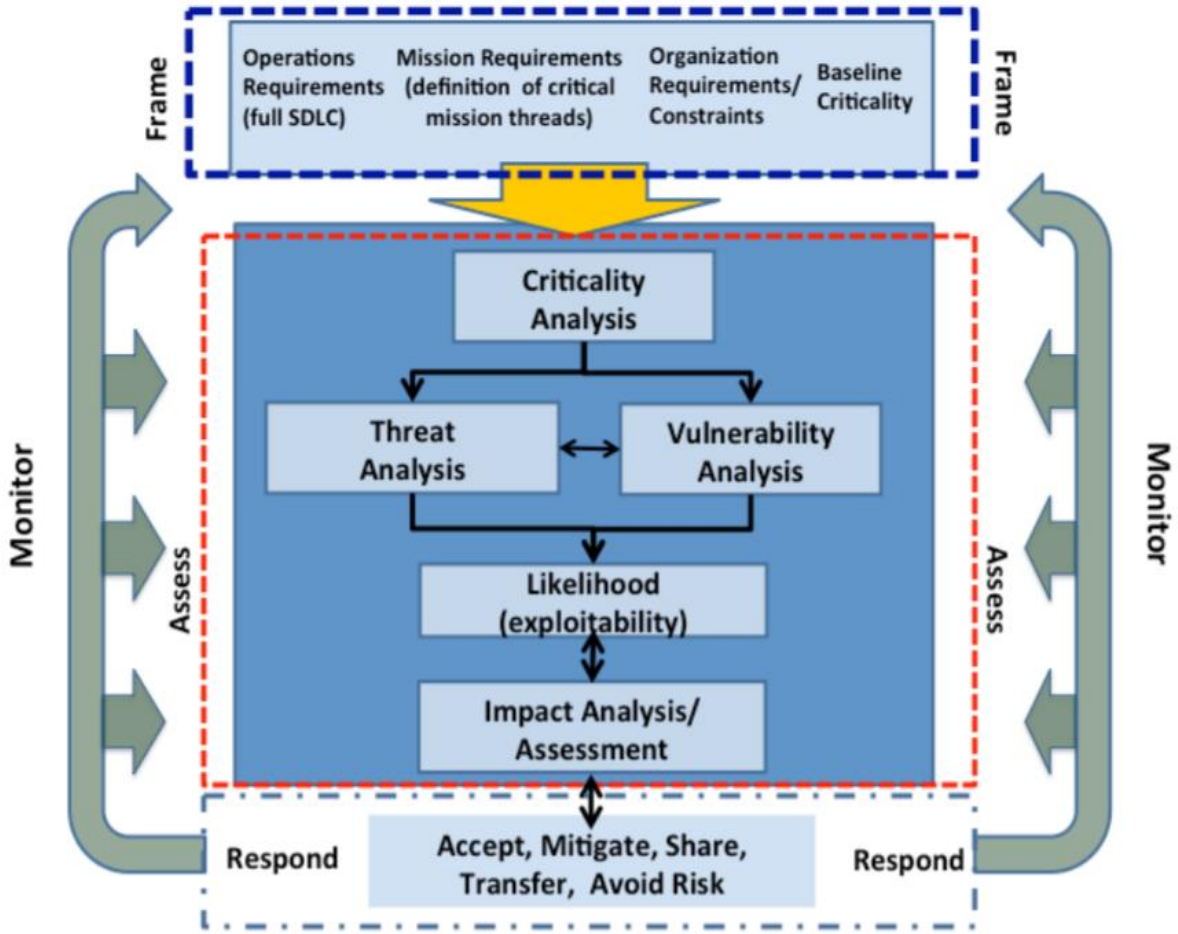
Supply Chain Risk Management Practices for Federal Information Systems and Organizations

Jon Boyens
Celia Paulsen
Rama Moorthy
Nadya Bartol

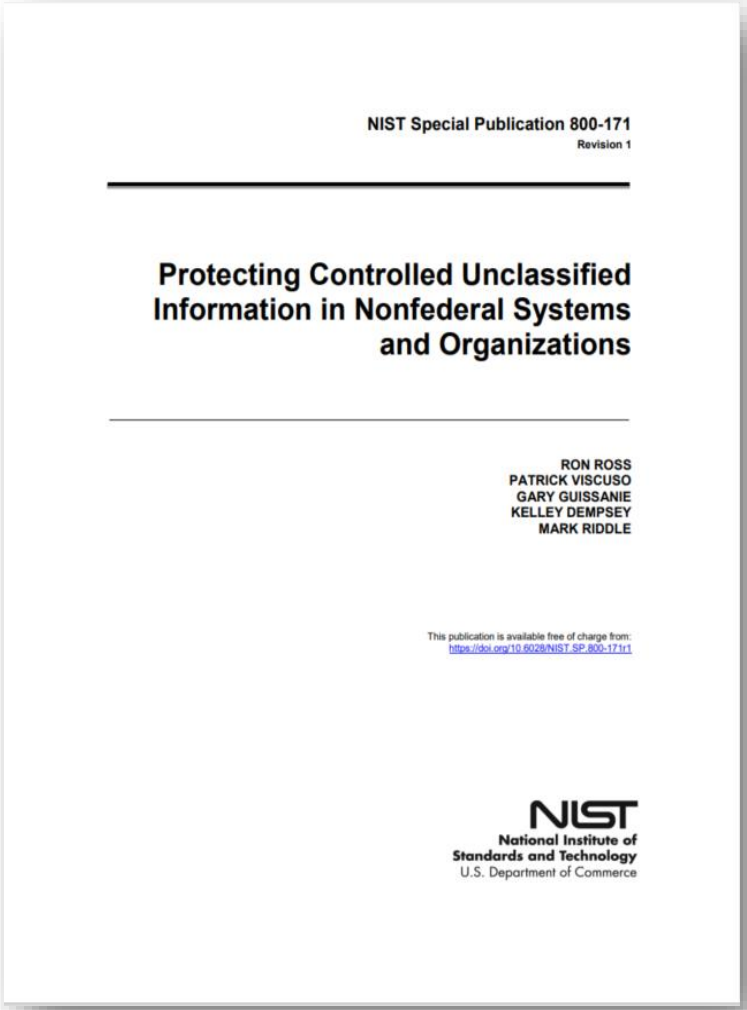
This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-161

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce



3-2. NIST SP 800-171


NIST Special Publication 800-171
Revision 1

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
PATRICK VISCUSO
GARY GUISSANIE
KELLEY DEMPSEY
MARK RIDDLE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r1

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

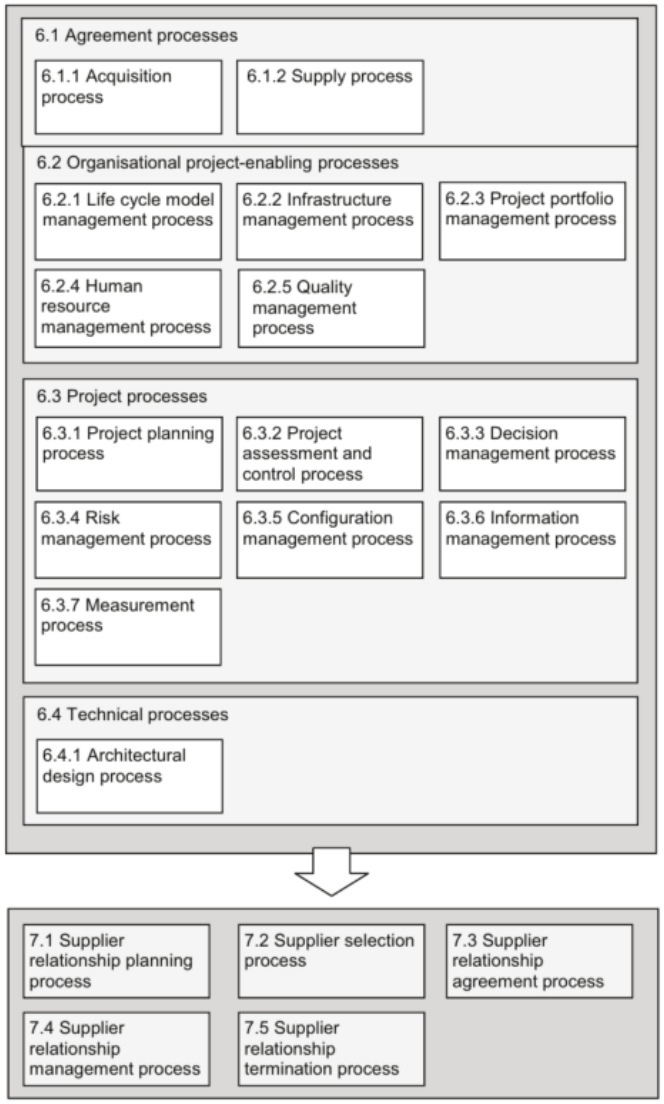
· 비 연방 시스템 및 조직에서 **분류되지 않은 제어된 정보보호**

· 이 문서의 목적은 CUI(Controlled Unclassified Information)가 비 연방 시스템 및 조직에 상주 할 때 CUI의 기밀성을 보호하기 위해 권장되는 보안 요구사항을 연방 기관에 제공

- 비 연방 조직이 연방 기관을 대신하여 정보를 수집하거나 기관을 대신하여 시스템을 사용하거나 운영하지 않는 경우

- 규정 또는 정부차원의 정책에 의해 규정된 CUI의 기밀성을 보호하기위한 특정 보호 요구사항이 없는 경우

3-3. ISO/IEC 27036-2



공급업체 관계 관리의 정보보안 요구사항

6.1 계약 과정
6.1.1 획득 과정
6.1.2 공급 과정

6.2 조직 프로젝트 가능 과정
6.2.1 수명주기 모델 관리 과정
6.2.2 인프라 관리 과정
6.2.3 프로젝트 포트폴리오 관리 과정
6.2.4 인적 자원 관리 과정
6.2.5 품질 관리 과정

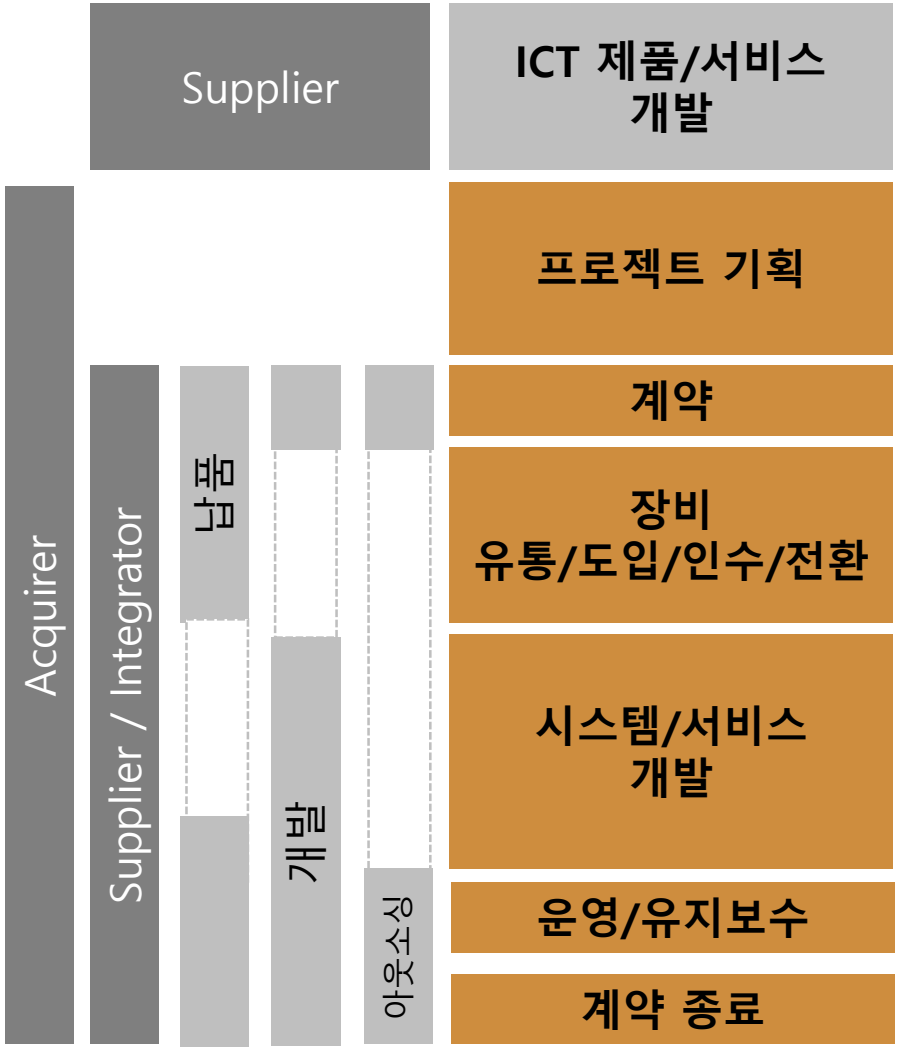
6.3 프로젝트 과정
6.3.1 프로젝트 계획 과정
6.3.2 프로젝트 평가 및 관리 과정
6.3.3 의사 결정 관리 과정
6.3.4 위험 관리 과정
6.3.5 구성 관리 과정
6.3.6 정보 관리 과정
6.3.7 측정 과정

6.4 기술 과정
6.4.1 구조적 설계 과정

단일 공급업체 적용 정보보안 요구사항

7.1 공급 업체 관계 계획 과정
7.2 공급 업체 선정 과정
7.3 공급 업체 관계 계약 과정
7.4 공급 업체 관계 관리 과정
7.5 공급 업체 관계 종료 과정

3-4. ISO/IEC 27036-3



ICT 제품/서비스 개발	• 상용S/W (COTS, Commercial Off the Shelf) 개발 • H/W, 펌웨어 개발 • 품질 및 보안성 보증(Assurance)
프로젝트 기획	• ICT 제품 및 서비스 도입 준비 및 계획 수립 • 프로젝트 위험 평가 및 공급자 선정기준 마련
계약	• 공급자 선정 및 계약 체결
장비 유통/도입/인수/전환	• ICT 제품 유통, 납품 이력관리 • ICT 제품 검수, 구매, 설치
시스템/서비스 개발	• 시스템/서비스 개발 요구사항 분석 • 보안을 고려한 설계 및 요구사항 검증(Verification) • 시스템 구현 및 통합 • 취약점 진단 및 테스트(Validation)
운영/유지보수	• S/W 업데이트, H/W부품 교환 등 이벤트 관리
계약 종료	• 시스템 폐기, 비밀유지 협약 등

[출처] 공급망(Supply-Chain) 보안체계 수립방안, 강원대 손경호 교수(2020.2월)

3-5. O-TTPS (ISO/IEC 20243-1, 20243-2)

공급망 위협 기술

	Taint			Counterfeit		
	Upstream	Provider	Downstream	Upstream	Provider	Downstream
멀웨어	☑	☑	☑			
악성코드	☑	☑	☑			
승인되지 않은 부분	☑	☑	☑	☑		
승인되지 않은 형상			☑			
폐품/수준이하 부분				☑		
승인되지 않은 제품				☑		☑

[출처] O-TTPS Standaridization for Product Integrity and Supply Chain Security, SSCA 2018 Fall

3-5. O-TTPS (ISO/IEC 20243-1, 20243-2)

Technology Development (기술개발)

제품 개발/엔지니어링 요구사항

- 소프트웨어/펌웨어/하드웨어 설계 프로세스
- 개발/엔지니어링 프로세스 및 실행
- 형상관리
- 품질/시험 관리
- 제품 지속 관리

시큐어 개발/엔지니어링 요구사항

- 위협 분석 및 경감
- 런타임 보호 기법
- 취약성 분석 및 대응
- 제품 패치 및 교정
- 시큐어 엔지니어링 실행
- 위협 환경 변화의 영향을 모니터링 및 평가

Supply Chain (공급망)

공급망 요구사항

- 위험관리
- 물리적 보안
- 접근통제
- 종업원과 공급자 보안 및 사업파트너 보안
- 공급망 보안 교육
- 정보시스템 보안
- 신뢰된 기술 컴포넌트
- 오픈소스 처리
- 위조 경감
- 멀웨어 탐지

[출처] O-TTPS Standaridization for Product Integrity and Supply Chain Security, SSCA 2018 Fall

4. 호주 사이버보안 센터(ACSC)

[출처] https://www.cyber.gov.au

· 모든 조직은 사이버 공급망 위험 관리를 고려 해야 함.

· 효과적인 사이버 공급망 위험 관리는 가능한 한 수명주기 동안 시스템에 대한 제품 및 서비스의 안전한 공급을 보장함

· 사이버 공급망 위험 관리는 사이버 공급망 **식별**, 사이버 공급망 **위험 이해**, 공급업체와의 **사이버 보안 기대치 설정**, 공급 업체 **준수 감사**, 사이버 공급망 보안 관행의 **지속적인 모니터링 및 개선**을 통해 수행 할 수 있음.

5. ENISA, 공급망 무결성

· 이 문서의 주요 목표는 **공급망의 무결성과 관련된 위협, 위험 및 가능한 솔루션을 식별**하는 연구에 대해 보고

· 유능한 국가 기관 및 업계 대표들과의 리서치 및 인터뷰를 통해 이 연구는 모범 사례를 식별하고 기존의 한계를 고려하여 다양한 산업 분야에 대한 의견을 주제로 함.

· 최신 조사에는 **칩 제조업체, 공급업체, 운영자 등 공급망 내 모든 주요 업체로부터 경험**을 검토하고 여러 분야의 최종 사용자 조직을 검토하도록 하는 내용이 포함.

6. 일본 사이버 공급망 위험관리 정책

구분		주요 내용
공공 부문 (정부 기관)	▪ IT 제품 또는 서비스의 조달방침 및 절차에 관한 합의('18)	▪ 23개 정부기관은 정보시스템·기기·서비스 **조달 시의 발생 가능한 공급망 위험에 사전 대응** (IT 종합전략실 및 NISC에 검토·자문 요청)
민간 부문	▪ 제2차 사이버보안전략('18) ▪ 산업사이버보안 강화를 위한 이행계획(Action Plan)('18)	▪ **사이버-물리 보안대책 프레임워크(CPSF) 수립** 및 분야별 대응 구체화, 국제화 추진 (경제산업성) ▪ 공급망을 공유하는 ASEAN 국가의 **사이버보안 역량 강화 지원** (미국과 연계하여 공동 훈련 추진, 경제산업성) ▪ 사이버-물리 보안에 관한 **연구개발** 추진 (내각부, 총무성, 경제산업성) ▪ 정부기관 및 산·학 연계를 통해 공급망 위험에 대응하기 위한 **기술검증체계 방안 마련** (내각관방) ▪ 중소기업 사이버보안대책 촉진 (내각관방, 총무성, 경제산업성) – **중소기업 대상** 사이버보안대책 사례 등 **가이드라인 개발, 사이버보험 활용, 사고 발생 시 지원, 인센티브 제공** 등 보안투자 촉진

[출처] 주요국 사이버 공급망 위협 관리 정책 동향 및 시사점, 2019년 Vol.12 KISA Report

7. 국외 사이버 공급망 위험관리 주요 지침 및 가이드라인

구분	국제표준	국내	미국	일본	영국	호주
조직 사이버 보안	▪ ISO/IEC27001 ▪ ISO/IEC27002	▪ 정보보호 및 개인정보보호 관리체계 (ISMS-P) ▪ 주요정보통신 기반시설 취약점 분석·평가 기준	▪ NIST RMF[21] ▪ NIST SP 800-53 ▪ NIST CSF Ver1.1. (ID.SC)	▪ NISC 정부기관 정보보호 대책에 관한 공통규범 ▪ 경제산업성 사이버보안 경영가이드라인 V2.0 ▪ 경제산업성 CPSF (CPS.SC)	▪ NCSC Cyber Assessment Framework (Supply Chain)	▪ Cyber security guidelines (Outsourcing)
사이버 공급망 보안	▪ ISO/IEC 27036 ▪ ISO/IEC 20243 ▪ IEC 62443-2-4	▪ 클라우드 보안인증제 (클라우드 서비스제공자) ▪ IoT 보안인증 (IoT제품)	▪ NIST SP 800-161 ▪ NISTIR 8179 ▪ FedRAMP (클라우드 서비스제공자) ▪ NIST SP 800-171	▪ JASA[22] 공급망 정보보호 관리	▪ NCSC Supply Chain Security Guidance ▪ NCSC Cloud Security Principles	▪ Cyber Supply Chain Risk Management ▪ Cyber Supply Chain Risk Management Practitioner Guide

[출처] 주요국 사이버 공급망 위협 관리 정책 동향 및 시사점, 2019년 Vol.12 KISA Report

KTC는 고객과 함께

미래를 만들어 나가겠습니다.