https://doi.org/10.33778/kcsa.2020.20.4.125

국방 ICT 공급에 대한 보안 위협 대응 방안★

이 용 준*

요 약

정보통신기술 발전에 따라 국방분야에 ICT 제품의 공급이 증가하면서 잠재적 보안의 위협이 증가하고 있다. 국방 전력지원체계 및 무기체계의 정보시스템에 대한 공격을 통해 정보수집 및 파괴 등 무력화를 시도하는 경우 치명적 위협이 될 수 있다. 이에 국방분야에서 ICT 제품의 생산, 운용단계에서 유지보수 단계까지 고려한 공급망 전단계의 보안대책이 필요하다. 본 논문에서는 국방 ICT 공급망 생명주기 단계별 12개의 ICT 공급망 보안위협 대응을 위한 기술적, 관리적 방안을 제시하였다.

Defense ICT Supply Chain Security Threat Response Plan

Yong-Joon Lee*

ABSTRACT

The potential security threat is increasing as the supply of ICT products to the defense sector increases with the development of information and communication technology. Attempts to neutralize, such as intelligence gathering and destruction, through attacks on the defense power support system and the intelligence system of the weapons system could pose a fatal threat.Therefore, security measures of supply chain shear system that take into account ICT product production and operation stage to maintenance stage are needed in defense field. In the paper, technical and administrative measures for responding to 12 ICT supply chain security threats at each stage of the defense ICT supply chain life cycle were presented.

Key words : Defense ICT Supply Chain, Supply Chain Threat, Supply Chain Threat Response, ICT Threat, ICT Vulneravility

접수일(2020년 09월 30일), 수정일(1차: 2020년 10월 24일), 게재확정일(2020년 10월 27일)

★ 본 논문은 극동대학교 교내연구비 지원에 의하여 연구되었음.

* 극동대학교 사이버보안학과

1. 서 론

정보통신기술(ICT) 발전에 따라 ICT 제품의 공급이 증가하고 있으며 서버, PC, CCTV, 모바일 기기 등 ICT 제품과 IoT기기까지 공급망 과정에서 불법적인 기능이 삽입된 사례가 증가하고 있다. ICT 제조사는 생산의 효율성을 위해 다양한 부품의 조립과 생산 과정에서 정보통신기술과 융합하고 있다. 부품의 생산과정에서 모든 부품을 생산기업이 직접 제작하지 않기 때문에 유통과정은 복잡하다. 이러한 복잡성을 악용하여 ICT 공급망에 대한 보안 위협이 증가하고 있다[1]. 이러한 ICT 공급망 환경은 비용 절감만 고려하여 저가의 부품으로 제품을 생산에 사용하는 경우 제품에 결함이 발생하거나 불법적인 기능이 은닉될 수 있다[2]. 이러한 ICT 공급망에 대한 보안 위협에 대응하기 위해 해외에서는 ICT 공급망 보호를 위한 관리체계를 발표하고 있으며 국내에서도 ICT 공급망의 보안 위협에 대한 심각성에 대한 인식이 확산되고 있다[3].

2013년 미국 정보기관 국가안보국(NSA) 요원이었던 Edward Snowden의 폭로로 미국 정보기관이 시스코, 삼성 등 글로벌 IT기업의 부품 공급과정에 개입하여 ICT 제품에 숨겨진 도·감청부품, 백도어로 보안위협이 발생하였다[4]. 이로 인해 ICT 제품의 생산 및 개발, 도입, 운용, 폐기까지 공급망 전단계에 걸쳐 발생할 수 있는 ICT 공급망 공격(Supply Chain Attack)에 대한 대응방안이 강조되고 있다. 이에 미국은 자국의 안보를 위해 공급망 보안 전략과 관련한 연구를 추진 중에 있으며 2013년 오바마 행정부는 국방수권법을 통해 ICT 공급망 강화를 위한 법제도 근거를 마련하였다. 이와 함께 영국, 독일, 중국 등도 자국의 안보를 목적으로 해외 ICT 제품에 대한 공공분야 사용을 제한하거나 제품 검사를 강화하는 정책을 추진하고 있다.

이에 국내에서도 국방 분야에 다양한 ICT 제품이 도입되어 전력지원체계, 무기체계에서 운용되고 있기에 ICT 공급망 보안 위협에 대한 대응이 요구된다. 본 논문에서는 ICT 공급망에 대한 보안 위협에 대한 사례를 분석하고 국방 ICT 공급망 생명주기 단계별 12개 보안통제 항목을 제시하여 국방 ICT 공급망의 보안강화에 기여하고자 한다.

2. ICT 공급망 보안 위협

ICT(Information Communication Technolgy)는 정보기술(Information Technology)과 통신기술(Communication Technology)의 합성어로 컴퓨터, 미디어, 영상기기 등과 같은 정보기기를 운영하는데 필요한 H/W, S/W 기술과 이러한 기술을 이용하여 정보를 수집, 생산, 가공, 저장, 통신, 활용하는 기술로 정의한다. ICT 공급망(Supply Chain)에 대한 정의는 부품이 제품이나 서비스로 생산되는 과정과 제조된 제품 및 서비스가 고객에게 공급되는 과정에서 공급 산업내에 상호 연결된 공급체계라고 한다. 또는 공급자, 제조, 운송 및 보관, 유통 및 판매, 소비자의 연쇄구조라고 정의한다.

2.1 최근 ICT 공급망 위협 사례

최근 ICT 제품이나 서비스가 공급자로부터 사용자에게 제공되기까지 조직, 인원, 자원 등 ICT 공급망을 대상으로 사이버 위협이 증가하고 있다. 다수의 S/W 개발기업의 업무 시스템을 해킹하여 소스코드를 변경하여 정보수집 목적의 불법 소스코드를 은닉시키거나 S/W 배포를 위한 배포서버에 침투하여 업데이터 파일을 변조하는 방식의 ICT 공급망에 대한 공격이 증가하고 있다[5]. 중국 ICT기업인 레노버, 화웨이, ZTE에서 생산하는 전자제품에 숨겨진 불법 백도어 프로그램에 의한 정보 유출의 위협으로 인해 미국, 영국 정부는

중국 ICT기업이 제조한 전자제품의 국가기관 사용을 제한하였다[6].

이로 인해 미국 국방부는 2017년 사이버보안 강화를 위해 중국 드론 부품 제조기업 DJI의 부품, 소프트웨어의 사용을 전면 제한하였다[7]. 미국 방산기업 록히드마틴은 ICT 공급망 강화를 위해 부품 공급업체에 대한 가이드라인을 발표하였다[8]. ICT 공급망에 대한 보안 위협은 설계, 생산 단계에서 부터 치밀하게 계획된 불법적인 부품을 은닉하는 보안 위협이 발생하고 있어 공격 발생시 파급력이 위력적이다. 부품을 위조하는 공격은 불법적인 칩을 정식 부품으로 위조하는 방식으로 발생하였다. 2018년 중국은 스파이칩을 통해 미국 중앙정보국(CIA)과 기업의 기밀을 유출하였다. 중국 정보기관은 스파이칩을 제작하여 서버 회로기판에 숨기는 방식으로 미국 국방부, 아마존, 애플 등에 제품을 공급하였다[9].

2.2 국내·외 ICT 공급망 위협 대응 동향

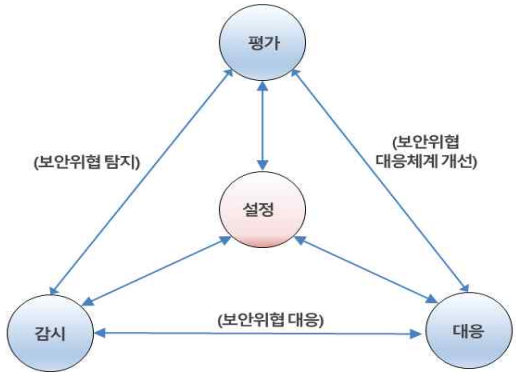
미국 오바마 행정부는 9·11 테러 이후 ICT 공급망 강화를 위해 공급망 안보전략을 발표하였다. 미국 국가표준기술연구소(NIST)는 정보통신기술(ICT) 공급망 위험을 식별, 평가하여 위험을 감소시키기 위해 국가기관 및 정보시스템을 대상으로 하는 ICT 공급망 위험관리 실무 가이드를 발표하였다. 2018년 미국 국토안보부는 민간기업으로 부터 ICT 공급망 위험에 대응하기 위해 정보통신기술 공급망 TF를 출범하였다.

영국은 ICT 기술 발전으로 인해 증가하는 사이버 위협에 대응하기 위해 2011년 사이버안보 전략을 수립하였다. 이는 사이버공격으로 인한 복원력 강화와 사이버상의 권익보호를 위해 국가와 산업체가 협력을 하고 있다. 2013년 ICT 공급망을 대상으로 하는 사이버 위협에 대응하기 위해 사이버 보안 표준에 기반한 위험 기반의 접근방법, 사이버 보안위협 정보 공유를 강화하고 있다[10].

이에 한국에서는 ICT 제품 생산부터 유통, 유지보수, 폐기에 이르는 전단계에서 강화된 보안 위험관리 대책을 수립해야 한다는 요구가 지속적으로 제기됐다. 2014년 사물인터넷(IoT) 제품과 서비스 공급 전단계에 걸쳐 보안 내재화를 추진하고 위험요소를 관리할 수 있도록 제도를 추진하였다[11]. 2019년 주요 정보통신 기반시설의 보안환경을 개선하기 위해 공급망 보안 점검체계를 도입하였다. 국가 사이버안보 기본계획에는 6개 전략과제를 뒷받침하기 위해 국가 기관별 실행계획을 18개 중점과제, 100개 세부과제로 종합하여 2022년까지 단계적으로 추진한다. 특히 주요 기반시설에 공급되는 주요 ICT 제품의 공급망 보안 관리체계를 구축하고, 관련 기관의 이행점검을 위한 제도적 기반을 마련하고 있다. 이를 위해 미국 공급망 관리체계(NIST SP 800-161)를 바탕으로 한국형 ICT 공급망 보안관리체계를 개발 중에 있다[12].

2.3 ICT 공급망 위험 관리

위험관리는 조직이 보유하고 있는 자산과 자산에 대한 보안 위협과 취약점을 분석하여 위험을 평가하여 보안대책을 수립하는 환류체계로 정의한다.



(그림 1) 위험관리 프로세스

(그림 1)과 같이, 위험설정, 위험평가, 식별된

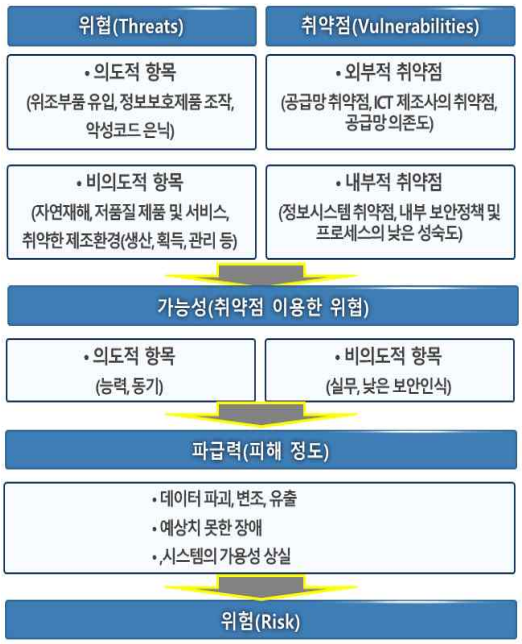
위험 대응, 위험 대응 활동에 대한 지속적 개선을 통해 전사적 의사소통, 피드백으로 ICT 공급망 위험을 감시하여 전술적 단계로 부터 전략적 단계까지 위험을 경감시키는 전반적 대응 활동을 수행한다[13].

ICT 공급망 위험을 증가시키는 요인으로 공급망의 글로벌화, 경쟁 강화로 인해 ICT 제조기업 증가, 생산의 외주화가 중요한 요인으로 분석되고 있다. ICT 공급망의 위험관리는 개별적 대응보다는 공급망을 구성하는 다양한 요소의 상호관계에 대한 종합적 위험 관리가 필요하다. ICT 공급망 위협을 식별하기 위한 원칙으로 1개의 주요한 사건이 발생하기 전에 29개의 작은 사건이 사전에 발생하고 300개의 사전 징후가 존재한다는 하인리히(Heinrich) 법칙이 중요하다. ICT 공급망에 대한 모든 위협을 식별하기 위해 MECE (Mutually Exclusive, Collectively Exhaustive) 방법을 통해 식별된 ICT 공급망 위험은 상호 배타적으로 보안 위협을 누락없이 모두 식별되어야 한다[14].

ICT 공급망 위험은 ICT 공급망에서 발생할 수 있는 잠재적인 위협(Threat)과 취약점(Vulnerability)으로 정의할 수 있다. 미국 NIST는 ICT 공급망 위험요소를 위조 제품, 불법 생산 및 변조, 도용, 악성 S/W, H/W(위치 추적장치, 스파이 칩) 삽입과 영세한 제조 등 ICT 공급망의 취약점을 악용한 위협으로 명시하고 있다.

NIST는 사이버보안(800)과 관련된 SP(Special Publication)를 발표하고 있다. ICT 공급망 보안 위협이 발생하는 경우 회복탄력성(Resiliency)에 대한 방법을 제시하고 있다. 회복탄력성은 2013년 미국 국방부 국방과학위원회 TF가 회복탄력성을 갖춘 시스템과 첨단 사이버 위협(Resilent Military Systems and the Advanced Cyber Threat) 보고서에서 발표하였으며 자연적/인공적이든 비의도/의도적이든 어떠한 장애에도 불구하고 수용 가능한 방식으로 운용할 수 있는 능력이라고 정의하였다.

(그림 2)에 보듯이, NIST SP 800-161에서 ICT 공급망 위협과 취약점이 위협에 미치는 잠재적 영향을 도식화하여 보여주고 있다.



(그림 2) ICT 공급망 위험

2.4 ICT 공급망 위험의 특징

ICT 공급망 위험은 ICT 제품을 생산하여 공급하는 제조사로부터 제품을 사용하는 국가기관, 기업, 개인 등 모두가 잠재된 보안 위험에 의한 피해 대상이 될 수 있다. 본 연구에서는 NIST SP 800-161(Supply Chain Risk Management Practices for Federal Information Systems and Organizations)을 기준으로 특징을 분석하였다[15].

공격자는 정치적, 군사적, 경제적, 기술적 스파이 활동, 금전의 부정 취득 목적이 높다. ICT 공급망 위험의 대상은 국가기관, 국방 관련 기관 및 방산기업, 국가 기간망 시스템(공공시설, 통신,

교통, 발전 등), 금융기관, ICT기업을 대상으로 발생한다. 국방 관련하여 전력지원체계, 무기체계의 정보시스템에 대한 공격이 발생하는 경우 정보수집 및 파괴 등 무력화로 치명적 보안 위협이 될 수 있다. 다음은 최근의 ICT 공급망 위험의 특징이다.

- 글로벌 기업(델, 시스코, 화웨이, 삼성 등) 공급망을 이용한 통해 침투 시도
- 공격 대상과 목적에 따라 다양한 공격도구(H/W, S/W)와 침투기법 사용
- ICT 공급망 보안위협에 대한 내부 보안시스템의 탐지를 회피하고 침투한 시스템을 장기간 활용하기 위한 은밀성
- 정보기관, 해킹조직 등 재원과 전문인원을 보유한 조직화
- 피해 발생여부, 원인, 의도, 공격자에 대한 식별의 어려움

2.5 ICT 공급망 생명주기 단계별 보안위협

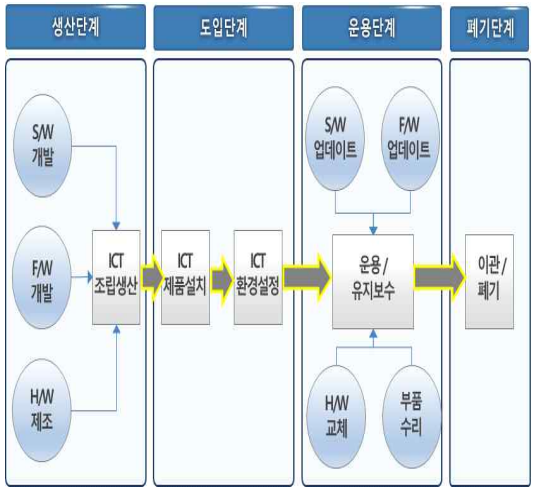
<표 1>에서는, ICT 제품의 수명주기(Life-Cycle)와 ICT 공급망의 연속적인 상호관계를 생산, 도입, 운용, 폐기 4단계로 구분하고 각 단계에서 발생할 수 있는 잠재적 보안 위협을 분석하였다.

<표 1> ICT 공급망 단계별 보안위협

단계	생산	도입	운용	폐기
위험요소	• 위조부품 사용 • 불법부품 은닉 • 잠재된 취약점 • 악성코드 은닉	• 부실한 제품 검수 • 제품위조/변경 • 제품정보 변조 • 악성코드/부품 삽입	• 재생/위조 부품사용 • 악성코드/부품교체 • 외주인원 통제소홀 • 보안 취약점 미조치	• 내용연수 초과 사용 • 임의 재사용 • 잔존 정보 유출

3. 국방 ICT 공급망 위협 대응방안

(그림 3)과 같이 국방 ICT 공급망에 대한 보안 위험 관점에서 현재 국방정보시스템의 도입단계에 중점하는 대책을 제시하고 있어 소요제기에서부터 제품의 생산단계, 운용, 유지보수 단계까지 고려한 ICT 공급망 전단계의 보안대책이 필요하다.



(그림 3) 국방 ICT 공급망 생명주기

3.1 생산단계(4개 보안통제 항목)

생산단계는 국방기관의 소요제기에 대해 제조기업의 제품 설계 및 개발이 이루어지는 단계로 신뢰할 수 있는 공급기업을 선정하고 제품의 검사를 통해 위·변조 제품의 도입과 불법적 기능이 은닉되는 것을 최소화하기 위해 4개의 보안통제 항목을 제시하였다.

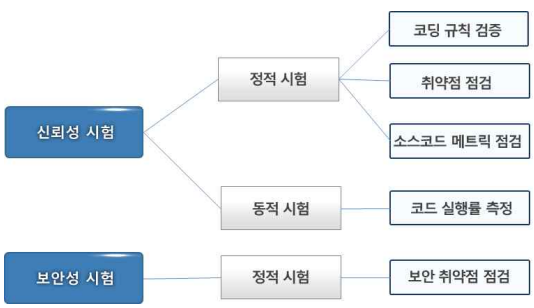
① ICT 제품 위·변조 검사

주요 ICT 부품에 대해 생산기업의 자체검사 또는 제3의 기관 검사를 통해 제품의 안전성과 신뢰도를 보장하기 위해 위·변조 검사를 수행한다. 검사방법은 KS-Q-ISO 2859-1 의 표준 샘플링

검사를 기반으로 육안검사, 가열용매검사, X-Ray 검사, 납땜성분검사 등을 한다. 위조부품의 검사 과정은 개별 부품을 확인하는 것은 불가능하기 때문에 비파괴 검사(Nondestructive Testing)를 통해 부품을 해체하지 않고 검사를 한다. 비파괴 검사는 재마킹, 재도색, 비정상적인 샌딩의 흔적 여부를 확인하기 위해 부품 표면을 육안 식별을 한다. 육안 식별에서 부품의 이상이 확인되면 부품의 코팅을 제거하여 마킹 제거된 흔적을 검증할 수 있는 솔벤트 검사(Solvent Rub Test)를 진행한다. 형광 엑스레이(X-ray Fluorescence) 검사를 통해 부품 크기 및 패턴으로 제조상 차이를 식별할 수 있으며, SAM(Scanning Acoustic Microscopy) 방법으로 초음파를 이용하여 회로 형상의 균열과 박리를 확인할 수 있으며, 전기적 시험으로 부품의 스펙과 데이터 시트를 검증하는 방법 등이 있다. 이러한 방법은 부품의 표면 상태를 훼손하지 않고 검사를 할 수 있는 비파괴 검사 방법으로 제품의 원상태 유지와 검사 시간을 단축할 수 있다.

② 소프트웨어 보안 취약점 진단

국방정보시스템의 소프트웨어 용역 개발시 개발단계에서 소요기관은 행정기관 및 공공기관 정보시스템 구축 운영 지침과 공공정보화 사업 유형별 제안요청서 가이드라인을 기초하여 소스코드 보안 취약점 제거 등을 의무화하였다.



(그림 4) SW 보약점 진단 항목

국방부는 2013년 신뢰성 시험을 실시하면서 SW 보안성 검증이 제기되어 국방전력발전업무 훈령에 반영, 방사청에서 SW 보안성 검증을 수행하고 있으며 (그림 4)와 같이 SW 용역 개발에 대한 다양한 취약점 점검 항목을 검사한다.

③ ICT 공급망 보안·품질관리 인증제도

국방 정보화사업에서 ICT공급망에 대한 보안 및 품질관리 관련한 국제인증을 획득하도록 유도하는 방안이 필요하다. ICT 공급망 보안 및 품질관리와 관련한 공급망보안경영(ISO 2800), 품질경영체계(ISO 9001) 등 국제인증을 획득한 공급기업에 적격심사, 제안서 평가시에 가산점을 부여한다. 지속적으로 ICT 공급망 보안·품질관리를 인증한 공급업체가 정보화사업에 참여할 수 있도록 강화해야 한다.

④ 보안사고·취약점 공유 강화

미국의 국방수권법과 같이 공급업체가 보안사고가 발생하거나 공급한 제품에 보안 취약점이 발견된 경우 소요기관에 고지하도록 의무화하고 관련한 협력기업에 공유를 강화해야 한다. 소요기관은 공급기업의 보안사고 고지를 의무화 하여 보안사고가 발생한 경우 사고전파 및 제품의 취약점 제거를 통해 ICT 공급망으로 인한 보안위협을 최소화한다.

3.2 도입단계(3개 보안통제 항목)

도입단계에서는 생산기업의 품질검사의 수행 여부와 불법 SW 및 위조 부품이 사용되었지는 정보시스템 도입전에 검사하고 신규 도입된 ICT 제품과 상호연동 되는 운용 시스템에서 발생할 수 있는 보안 위협을 예방하기 위해 3개의 보안통제 항목을 제시하였다.

⑤ ICT 제품 도·감청장치 탐지

ICT 제품 내부에 은닉될 수 있는 도·감청장치 또는 불법 부품을 탐지해야 한다. 도·감청 검사 방법으로 제품에 대한 외부 침입의 접점을 점검하는 방식이 있는데 물리적 인터페이스 포트의 취약점이 있는지 점검하는 인터페이스 노출 점검 방법과 비파괴 검사의 방법이 있다. 외부 침입 접점에 대한 부품을 탐지하는 경우 인터페이스 역분석을 실시한다. 인터페이스 역분석으로 제품 납땜을 제거하여 검사 소켓을 장착하고 역어셈블리를 통해 데이터를 분석한다. 부품 내부에 칩을 삽입하여 디버깅을 통해 분석하는 방법도 있다.

위조된 회로칩을 탐지하는 방법으로는 동적 탐지와 정적 탐지 방법이 있다. 동적 탐지는 불법 기능이 삽입된 회로가 많은 전력을 소비하는 특성을 검출하거나 불법 기능이 전력에 미치는 영향을 증폭하는 인버터를 통해 탐지할 수 있다. 위조 부품이 삽입되면 원래 회로의 기능을 지연시키는 특징을 탐지하는 방법으로 최근에는 탐지 커버리지를 높이는 GA(Genetic Algorithm)와 복잡한 트리거 조건을 탐지하는 SAT(boolean SATisfiability)를 이용하여 자동화된 검출 패턴을 생성하여 검사할 수 있다. 정적 탐지 방법은 구현 단계에서 하드웨어가 침해되지 않도록 보안 우선순위를 설정하도록 개발된 HDL(Hardware Description Language) 언어의 코드에 대한 단위 시험 및 통합시험을 시행하여 위험을 사전에 알려주는 방법과 FPGA(Field Programmable Gate Array)로 합성된 후에 기존의 불법 기능에 대한 검출 패턴을 비교하여 탐지하는 비트 스트림 데이터를 검출하는 방법이 있다.

⑥ ICT 제품 보안 인증제도

국방정보시스템을 구성하는 ICT 제품의 신뢰성과 보안성 검증이 필요한 정보보호제품, 네트워크 장비 등을 대상으로 하는 CC(Common Criteria) 인증, 보안적합성 검증 제도를 통해 ICT 제품을 대상으로 안전성 검증된 장비를 도입한다. 시험기관으로는 국방과학연구소, 상호운용성센터 등을 활용할 수 있다.

⑦ ICT 제품 검수 절차

ICT 제품이 생산업체로부터 소요기관에 공급될 때 소요기관은 검수업무를 수행한다. 검수과정에서 ICT 공급망의 보안위협에 대응하기 위해 제품이 정상적인 제조과정과 품질인증을 거쳤는지 검수 절차가 강화되어야 한다. 공급업체의 제품의 품질검사 여부, 불법 S/W 및 위조 부품 사용여부를 도입과정에서 검증하여 잠재적 보안 위협을 예방할 수 있다. 소요기관에서 ICT 제품 검수할때 국립전파연구원의 제품 일련번호를 확인하여 샘플 검사를 수행할 수 있다. ICT 제품의 인증번호와 제품 일련번호 확인하여 검수를 강화할 수 있다. 검수 대상 ICT제품이 많아 전수검사가 어려울 경우 전체 제품수에서 표준 샘플링 검사를 통해 정상여부를 확인을 해야 한다.

3.3 운용단계(3개 보안통제 항목)

운영단계에서는 하드웨어, 소프트웨어, 펌웨어 등 운용중인 ICT 하드웨어와 소프트웨어 보안 패치 및 업데이트, 부품 교체 등으로 유지보수 과정에서 발생할 수 있는 보안위협을 예방하는 것을 목적으로 3개의 보안통제 항목을 제시하였다.

⑧ 비인가 ICT 장비 통제

일반적으로 위·변조가 어렵다고 알려진 USB 펌웨어를 악성코드로 감염을 시킬 수 있는 USB 보안위협이 발생하고 있다. USB 보안위협은 컨트롤러 펌웨어를 조작하여 키보드 자판 입력 정보 획득으로 파일 관리자 비밀번호 등 중요정보 회득, 인터넷에서 악성코드가 은닉된 웹사이트로 유도, USB 포트를 통해 주변장치에 대한 악성코드 감염을 시킬 수 있는 위협은 크지만 보안패치 또는 백신

검사를 통해 탐지가 어렵다. 이에 국방정보시스템에 불필요한 USB포트를 물리적 차단, 서버·컴퓨터 케이스 잠금장치 사용 및 봉인, 불필요한 USB 포트를 연결을 제거하여 비인가 ICT 장비가 무단 연결되는 것을 방지하여 국방정보시스템의 정보 유출에 대응해야 한다.

⑨ ICT 제품 교체 절차

정보시스템을 최초 도입할때는 검수와 CC 인증, 보안적합성 검증 제도화를 통해 보안을 강화하지만 운용단계에서 시스템 유지보수를 위해 교체되는 하드웨어 제품과 부품에 대해서는 도입단계와 비교하여 검수가 소홀한 경우가 있다. 하드웨어 제품 장애 또는 기능개선을 위해 도입된 제품에 대해서도 도입단계와 동일한 수준으로 검사를 강화해야 한다. 시스템 관리자는 장애 발생으로 제품이나 부품을 교체하는 경우 제품에 대한 인증번호와 일련번호를 검증하고 제조사 정품 공급 여부를 검수해야 한다. 유지보수기업은 제품 교체시 시스템 관리자에게 사전 승인을 반드시 받아야 하며 도입된 제품과 동일한 제품과 버전으로 교체해야 한다.

⑩ S/W 업데이트 절차

2011년 농협 전상망 장애, 2013년 주요 언론사 및 금융기관을 대상으로 발생한 3·20 사이버 공격은 내부 시스템의 S/W 업데이트 서버를 해킹하여 악성코드를 은닉시켜 발생한 대표적 보안사례였다. 다수의 정보시스템에 설치되어 있는 운영체제, 어플리케이션 등 소프트웨어 보안 취약점과 기능을 개선하기 위해 정기적, 수시로 소프트웨어 패치와 업데이트를 수행해야 한다. 이 과정에서 시스템 관리자 또는 운영자는 S/W 업데이트 서버 또는 유지보수 인원 반입한 프로그램이 보안조치 없이 S/W 패치나 업데이트할 경우 심각한 보안 위협이 발생할 수 있다. 국방정보시스템의 H/W, S/W 등의 업데이트, 부품 교체 등 유지보수 과정에서 발생하는 보안위협을 예방해야 한다. 정보시스템에 탑재된 S/W, 펌웨어의 보안패치와 업데이트를 위해 반입되는 프로그램의 무결성을 검증해야 한다. 소요기관은 IT 외주인력 보안통제 안내서, S/W 업데이트 체계 보안 가이드라인을 기초하여 시스템 관리자는 제품에 대한 보안패치나 업데이트 수행할 때 필요한 프로그램과 저장매체에 무결성 검증을 수행한다. 유지보수 기업은 제품의 보안패치 및 업데이트 작업내용을 시스템 관리자에게 사전에 승인을 받아야 하며 작업일지에 상세기록을 남겨야 한다.

3.4 폐기단계(2개 보안통제 항목)

ICT공급망에서 폐기 단계는 일반적으로 시스템 도입이나 개발이 완료된 이후 관련 사업자료나 컴퓨터에 남아 있는 저장자료의 외부 유출을 차단하기 위한 절차와 외주 인원에 대한 보안통제로 2개 보안통제 항목을 제시하였다.

⑪ 국방정보시스템 이관 절차

국방정보시스템의 이관할 경우에 추가로 보안절차가 필요하다. 서버, 스토리지, 네트워크, 백업장비 등 국방정보시스템 전체 또는 일부를 다른 용도로 이관할 경우가 있다. 국방정보시스템을 이관할 때는 외부 인원에 의해 시스템의 저장자료, 펌웨어에 저장된 IP주소, 계정정보 등 ICT 환경설정에 대한 기본정보가 유출될 수 있다. 추가적으로 국방정보시스템이 타용도로 이관되거나 재활용되는 경우 추가적인 정보유출 또는 악성코드가 은닉되는 것에 대비해야 한다. 저장매체 폐기 절차를 준수하면서 ICT 제품의 펌웨어에 남아있는 암호기능 및 보안 환경설정 정보를 완전 삭제 또는 초기화해야 한다.

⑫ 국방정보시스템 폐기 절차

국방정보시스템 내용연수 도래에 따른 폐기할 경우 저장장치, 펌웨어를 통한 시스템 정보 유출을 차단해야 한다. ICT 제품의 펌웨어 초기화 또는 펌웨어 업데이트를 통해 완전 초기화하거나 필요한 경우 물리적 파괴를 수행한다. 추가적으로 국방정보시스템의 정상적 폐기 후에도 폐기된 시스템의 정보(제품명, 버전, 일련번호 등)를 시스템 관리자가 일정기간 보유하여 추후 시스템 침해사고 발생 또는 취약점 발견하는 경우 관련 제품의 정상적 폐기 여부를 확인하고 사고분석을 위해 이력 추적이 가능하도록 보유해야 한다.

4. 결 론

본 논문은 정보통신기술 발전에 따라 ICT 제품의 공급이 빠르게 증가하면서 잠재적 보안 위협인 ICT 공급망에 대한 보안 위협에 대한 대책을 다음과 같이 제시하였다.

첫째 생산단계로부터 ICT 공급망의 보안 위협을 예방하기 위해 국방 정보화사업 소요단계에서 ICT 제품 위·변조 검사, 소프트웨어 보안 취약점 진단, ICT 공급망 보안·품질관리 인증제도, 보안사고 및 취약점 공유 강화가 필요하다.

둘째, 도입단계에서는 소요기관에 의한 ICT 제품 도·감청장치 탐지, ICT 제품 보안 인증제도, ICT 제품 검수 절차가 강화되어야 한다.

셋째, 운영단계에서는 비인가 ICT 장비 통제, ICT 제품 교체 절차, S/W 업데이트 절차에 대한 보안통제가 필요하다.

넷째, 폐기단계에서는 국방정보시스템 이관 절차, 국방정보시스템 폐기 절차 과정에서 제품의 내용연수 초과 사용으로 발생할 수 있는 보안사고를 예방하고 추후 ICT 제품 폐기 이력을 추적이 가능하도록 관리방안을 제시하였다.

본 논문에서는 ICT 공급망에 대한 보안 위협에 적극적으로 대응하기 위해 ICT 공급망 전단계에 대한 12개의 단계별 대응방안을 제시하였다.

참고문헌

[1] NRC, 10 CFR 73.54, “Protection of digital computer and communication systems and network”, November 2009,

[2] Department of commerce, “Defense industrial base assessment: Counterfeit electronics”, January 2010.

[3] NRC Regulatory Guide 5.71, “Cyber Security Programs for Nuclear Facilities”, January 2010.

[4] NRC Regulatory Guide 1.152, “Criteria for use of computers in safety systems of nuclear power plants Rev 3”, July 2011.

[5] “레노버-화웨이-ZTE 中백도어 논란”, KINE WS, 2015.02.25.

[6] “해킹의혹 중국산 PC, 영국 정보기관서 퇴출”, 연합뉴스, 2013.07.30.

[7] “미국, 中화웨이·70개 계열사 거래제한...안보침해 위협제기”, MK뉴스, 2019.05.16.

[8] 김태호, 박태형, “SW공급망 사슬 위험관리”, 월간 SW중심사회, pp.41-44. 2015.

[9] 국립외교원, “미국의 신 글로벌 공급망 안보 전략 검토”, 주요국제문제분석, 제 2012-13호, pp. 1-13, 2012.

[10] 배병환, “영국 사이버보안 전략 분석 및 시사점”, 주간기술동향, 제 1775호, pp. 1-14, 2014.

[11] 김종화, 임재성, “사이버 위협 대응을 위한 軍정보화자산관리시스템과 연계한 軍취약점 관리방안”. 융합보안논문지, 제18권, 제1호,pp.111-116, 2018.

[12] 이대성, 안영규, 김민수, “북한의 사이버전 위협에 대한 분석과 전망”. 융합보안논문지, 제16권, 제5호, pp.11-16, 2016.

[13] 김종화, 김용철, 김경민, 강정흥, “안전한 공급망 관리를 위한 국방사이버보호 파트너십 인증 방안 연구”. 융합보안논문지, 제19권,제3호, pp.101-107, 2019.

[14] 김권일, 김지원 “4차 산업혁명 기술 도입에 따른 하드웨어 공급망 위협과 대응 방안”. 한국산업보

안연구, 제10권, 제2호, pp.37-57, 2020.
[15] NIST SP 800-161 Supply Risk Management Practices for Federal Inforamtion System, NIST, April 2015.

〔저자소개〕

이 용 준 (Yong-joon Lee)
1999년 2월 강남대학교 전자계산학과 학사
2001년 2월 숭실대학교 컴퓨터학과 석사
2005년 2월 숭실대학교 컴퓨터학과 박사
현 재 극동대학교 사이버보안학과 조교수
email : 2020032@kdu.ac.kr