Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.5, Oct. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.5.1089

미국 공급망 보안 관리 체계 분석*

손 효 현,† 김 광 준, 이 만 희‡
한남대학교

Analysis of U.S. Supply Chain Security Management System*

Hyo-hyun Son,† Kwang-jun Kim, Man-hee Lee‡
Hannam University

요 약

정보통신기술의 비약적인 발전을 통하여 스마트 제조 시대가 도래하고 있다. 이에 따라 많은 기업은 제조공정의 효율적인 업무를 위해 다양한 하드웨어 및 소프트웨어를 활용하기 시작하였다. 이때 사용되는 하드웨어 및 소프트웨어들은 제조·유통 과정을 거쳐 공급되는데, 이러한 공급 과정에서 각종 보안 위협에 노출되고 있다. 최근 공급망 공격 사례가 증가함에 따라 국외에서는 공급망 관리 체계를 정립하여 공급망 위험을 관리하고 있다. 이에 반해 국내는 일부 분야에 대한 공급망 위험 관리 연구가 진행되었다. 본 논문에서는 공급망 공격 사례를 통하여 공급망 위험 관리의 필요성을 강조하고, 국외 공급망 관리 체계의 동향을 분석하여 국내의 공급망 보안전략 방안의 필요성을 설명한다.

ABSTRACT

An era of smart manufacturing is coming through the rapid development of information and communication technology. As a result, many companies have begun to utilize a variety of hardware and software for the efficient business of the manufacturing process. At this time, the hardware and software used are supplied through manufacturing and distribution processes. These supply processes are exposed to a variety of security threats. As the recent cases of supply chain attacks have increased, foreign countries are establishing supply chain management systems and managing supply chain risks. In Korea, on the other hand, there was research on supply chain risk management in some fields. In this paper, we emphasizes the necessity of supply chain risk management through supply chain attack cases. In addition, we analyze trends of foreign supply chain management system and explains the necessity of domestic supply chain security strategy.

Keywords: Supply Chain Risk Management, Supply Chain Evaluation and Verification, Supply Chain Attack, SCRM

I. 서 론

정보화시대가 도래함에 따라 IT는 우리의 일상생활 속에서 매우 밀접한 관계로 활용되고 있다. 정보통신기술의 급속한 성장은 IT 환경의 급격한 변화를 초래하였고, 이에 따라 각종 제조업체는 업무 효율성 증진을 위해 제조과정에 IT 기술을 접목한 스마트 제조화를 추진하고 있다[1]. 이 과정에서 기업들은 제품 설계 및 공정 등 다양한 형태의 업무 시스템과 IT 인프라 구성을 위해 많은 하드웨어 또는 소프트웨어를 구성하여 사용하고 있다. 이때 사용되는 하드웨어 및 소프트웨어는 제조·유통의 과정을 거쳐 기업에 공급되게 되는데, 이러한 공급 과정에서 해킹 및 각종 보안 위협에 노출되어 있어 점차 공급망 보안의 중요성이 강조되고 있다.

여기서 공급망이란 일반적으로 제품 혹은 서비스를 공급자로부터 소비자에게 전달되는 과정 중 사람,

Received(04. 18. 2019), Modified(1st: 07. 16. 2019, 2nd: 08. 12. 2019), Accepted(08. 13. 2019)
* 본 논문은 2019년도 한남대학교 학술연구조성비 지원에 의하여 연구되었음.
† 주저자, sonhyohyun.kr@gmail.com
‡ 교신저자, manheelee@hnu.kr(Corresponding author)

정부, 자원, 조직 등에 대한 전반적인 시스템을 의미한다[2]. 이러한 공급망에 침투하여 사용자에게 전달되는 소프트웨어나 하드웨어를 변조하는 형태의 공격을 공급망 공격이라 일컫는다. 최근 발생한 MeDoc 업데이트 서버 해킹, 넷사랑 프로그램 변조 등은 공급망 공격의 위험성을 잘 보여주고 있다[2].

이를 방지 및 대응하기 위해 미국은 NIST(National Institute of Standards and Technology) IR 7622[3], NIST SP 800-161[4] 등의 지침을 마련하여 공급망 위험 관리를 시행하고 있다. 그러나 현재 국내는 공급망 공격에 있어 관련 지침 및 법률 일부는 존재하나[5][6], 규제상 제재 수위가 낮고 사전 대응에 대한 법적 근거가 되기 어려우므로 사실상 공급망 보안에 대한 국가적 지침이 없는 실정이다.

한편, 분야별 공급망 공격에 대한 연구가 일부 진행된 바가 있다. 김동원과 한근희(2015)는 국내 자동차 분야에서 공급망 보안 연구를 수행하였고[7][8], 임수민(2016)은 원자력발전에서의 공급망 위험 관리 연구를 수행하였다[9]. 하지만 그 외 분야의 공급망 위험 관리에 대한 연구는 매우 미흡한 현황이다. 이와 더불어 공급망 보안 분야에서 가장 앞서있는 미국의 공급망 관리 체계 조차 국내에 제대로 소개되지 않고 있는 실정이다. 따라서 본 논문은 미국의 공급망 보안 관리 체계를 분석함으로써 국내 공급망 보안 연구 및 체계 구축의 필요성을 설명한다.

본 논문은 다음과 같이 구성된다. 2장에서는 공급망 공격과 관련하여 사이버 위협 동향을 분석하며, 국내에서 진행되었던 자동차와 원전 분야의 공급망 위험 관리 연구 사례를 살펴본다. 3장에서는 국내외로 이슈가 되었던 공급망 공격 사례를 소개하며, 4장에서는 국내의 공급망 관리 체계 및 국외 주요 선진국 중 하나인 미국의 공급망 관리 체계에 대하여 기술한다. 5장에서는 앞서 소개한 공급망 사례를 국내 및 미국의 공급망 관리 체계에 적용함에 따라 국내의 공급망 관리 체제가 미비함을 설명한다. 마지막으로 6장에서는 국내의 공급망 보안전략 방안의 필요성을 제안하며 결론을 맺는다.

II. 관련 연구

2.1 사이버 위협 동향 분석

최근 한국인터넷진흥원에서 발행한 사이버 위협 동향 보고서에 따르면 소프트웨어 개발 프레임워크에 보안취약점이 발견되는 등 공급망 공격의 발생 가능성이 꾸준히 높아지고 있음을 강조하였다[2]. 또한, 이 보고서는 국내·외 공급망 공격 사례를 소개하며, 이를 위한 대응방안을 소프트웨어 공급업체 및 사용기관 입장에서 기술하였다. 추가적으로 2019년 1월에 발행된 보고서에는 2019년 7대 사이버 공격 전망 중 하나로 소프트웨어 공급망 대상 사이버 공격이 증가할 것으로 전망하였다[10].

또한, Symantec의 최근 ISTR(Internet Security Threat Report)에도 소프트웨어 공급망 공격이 급증하고 있음을 소개하며, 공격자가 취약점을 찾아내는 것이 어려워지자 공급망을 통해 우회하는 공격이 증가하고 있다고 보고하였다[11]. 이후 2019년에 발행된 ISTR에는 공급망 공격에 대한 위험성을 다시 한번 서술하고 있으며, 2018년 공급망 공격이 전해 대비 78% 증가하였음을 강조했다[12]. 이렇듯 공급망 공격은 국내외에 중요한 보안 문제로써 대두되고 있다.

2.2 자동차 공급망 위험 관리

자동차의 안전한 공급망 보증을 위한 방안 연구를 통하여 한근희(2015)는 자동차 공급망 위험 관리(A-SCRM, Automotive-Supply Chain Risk Management) 프로세스를 제안하였다[7][8]. 이 프로세스는 '기준 정의 단계', '평가단계', '실행단계', '모니터링 단계'로 구분하여 공급망의 안전성을 보증한다.

해당 논문은 자동차 보안문제가 대두됨에 따라, 자동차 소프트웨어와 공급망에서의 보안성에 대한 보증방안이 필요함을 강조한다. 그를 위해 미국 NIST SP 800-161 문서에 기반한 효율적인 국내 자동차 공급망 위험 관리 방안을 제시하였다.

2.3 원전 디지털자산 공급망 위험 관리

임수민(2016)은 공급망을 통한 사이버보안 위험 사례와 원자력발전소 디지털 자산 공급망 위험 관리를 위한 미국의 지침을 소개하고, 원자력발전소에 대한 사이버 위험에 대응할 수 있는 실질적인 공급망의 보안 강화 필요성을 주장하였다[9].

또한, 원자력발전소의 공급망 관련 대책을 다루는 문서인 RG 5.71, RG 1.152, NIST SP 800.53

Rev. 4, IAEA TECDOC 966과 1169를 소개하였다[13][14][15][16][17]. 해당 문서들은 모두 미국에서 발행된 지침 및 규제들이다. 현재 국내의 공급망 관리 체계가 미비함에 따라 이러한 지침 및 규제 방안을 적극적으로 활용하여 국내에 적합한 공급망 위험 관리 지침의 정립이 필요함을 강조하였다.

III. 공급망 공격 사례

본 절에서는 공급망 공격 사례들을 통하여 공급망 공격의 위험성에 대해 소개한다.

3.1 MeDoc 업데이트 서버 해킹 사례

MeDoc은 우크라이나에서 회계 관리 소프트웨어를 개발하는 회사로서, 우크라이나는 모든 정부 기관에 대해 이 소프트웨어의 사용을 의무화하고 있다[2]. 2017년 6월에 발생한 이 사건에서 공격자는 MeDoc의 업데이트 서버를 해킹하여, 업데이트 요청 시 정상 업데이트가 아닌 Petya 랜섬웨어를 배포하도록 변조하였다 (Fig. 1)[18]. MeDoc은 우크라이나의 90%의 기업에서 사용되었던 만큼 피해도 매우 컸으며, FedEx등 국제적 기업에도 피해를 입혀 총 10조원의 손실이 있었던 것으로 알려진다[19].

불특정 다수를 목표로 하여 광범위하게 확산되는 일반적인 랜섬웨어와 달리, 본 공격에서는 Petya 랜섬웨어를 특정 국가의 기업에 공급되어 운영 중인 세무회계 소프트웨어의 업데이트 서버를 대상으로 한 것이 특징이다. 본 사례는 소프트웨어 공급망 과정 중 배포 단계를 침투한 공급망 공격이다. 결국, 이 소프트웨어를 공급받아 이용하는 우크라이나 내의 모든 기업과 정부 기관은 공급망 배포 단계의 업데이트 서버 공격에 완전 무방비 상태였다고 할 수 있다.

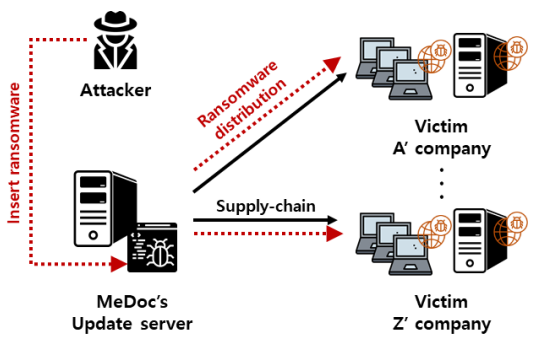


Fig. 1. MeDoc Supply-chain Attack Process

3.2 넷사랑 서버 관리 프로그램 변조 사례

넷사랑 프로그램은 넷사랑컴퓨터에서 제작하고 배포하는 네트워크 관리 소프트웨어이다[20]. 주요 제품은 Xlpd, Xmanager, Xshell, Xftp 이며, 서버 및 애플리케이션의 원격관리가 주 기능이다.

2017년 8월에 발생한 이 사건에서, 해커는 넷사랑 제품의 패키지 과정을 공격하였다. Fig. 2와 같이, 공격자는 빌드 서버에 침입하여, 배포 패키지 빌드에 사용되는 정상 파일 대신에 Shadowpad 악성코드가 삽입된 파일로 교체하였다[21]. 이후 감염된 패키지는 파일 공유 서버를 거쳐 업데이트 서버에 업로드되어 넷사랑 제품 사용자들에게 배포되었다. 넷사랑 프로그램을 이용하던 사용자 측에서 의심스러운 DNS 접속 행위가 탐지됨에 따라 이 공격 사실이 밝혀졌다[2].

감염된 사용자들의 PC는 프로그램을 업데이트 함과 동시에 설치된 Shadowpad 악성코드를 통하여 PC에 저장되어있는 사용자 정보를 C&C 서버로 전송하였다. 특히, 이 공격은 피해자의 PC에 백도어를 삽입하여 공격자는 언제든지 정상 인증 과정 없이 사용자의 시스템에 접근 가능했으므로 그 위험성이 매우 큰 공격이라고 할 수 있다.

본 사례는 소프트웨어 공급망 과정 중 제작 단계를 침투한 공급망 공격이다. 결국, 이 소프트웨어를 공급받아 사용하는 많은 기업들은 개인자료 유출 및 무단접근 공격에 무방비 상태였다고 할 수 있다.

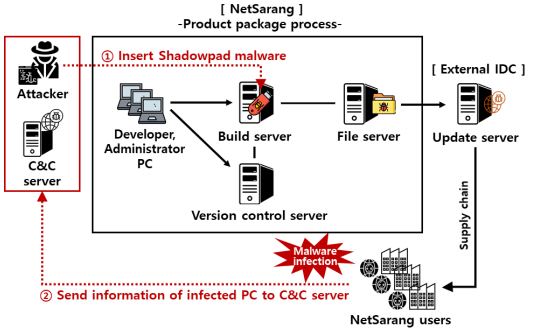


Fig. 2. NetSarang Supply-chain Attack Process

3.3 스마트공장 공급망 공격 사례

스마트제조의 발달로 인하여 스마트공장이 형성됨에 따라 모든 제조·생산 과정은 초 연결성인 특징을 가지고 있다. 스마트공장내에서 발생하는 공급망 공격은 통합적인 시스템을 이용하여 제조·생산을 목적으로 하는 스마트공장에 특징에 따라, 일반적인 환경에서 발생하는 공급망 사례들과 달리 정상적인 생산활동이 이루어질 수 있도록 가용성이 우선적으로 확보되어야 한다. 최근 5년동안 발생한 제조업 주요 보안사고는 다음과 같다(Table.1)[22].

공격 대상 및 공격 방식은 이전에 소개한 공급망 공격 사례와 같이 공급망 과정에 침투하여 공격 대상을 무력화하고 시스템을 제어하였다. 본 공격의 결과, 제품의 제조 및 생산 과정에 차질이 발생하거나 시스템 사용이 불가능해졌음을 볼 수 있다. 그에 따라 한 과정이 공격을 당하더라도 전체적인 제조·생산 과정이 중단되는 결과가 발생한다. 이는 일반적인 공급망 공격 사례보다 그 피해가 더욱 클 것으로 전문가들은 판단하며, 그에 따라 공급망 공격의 사전대응 및 공급망 보안 관리가 필요함을 강조한다[22].

IV. 국내 및 미국의 공급망 관리 체계

본 절에서는 국내에서 시행중인 공급망 침해 사고 발생 시 적용 가능한 법률을 소개한다. 또한, 미국의 공급망 관리 체계의 지침서인 IR 7622와 SP 800-161 문서에 대해 기술한다.

4.1 국내 관련 법률

국내 공급망 공격에 적용 가능한 법률은 조달청 지침 및 정보통신망법에 의거하여 규정하고 있다. 먼저 조달청지침 제527호 「네트워크 장비 구축·운영 사업 추가특수조건」의 제4조(계약상대자 정보보안 준수 의무)는 보안요구사항 관리 및 네트워크의 비정상적 접근을 규제하고 있으며, 백도어에 대하여 명시적으로 언급한다[5]. 이때 백도어는 정상적인 인증 과정을 거치지 않고 컴퓨터 및 시스템에 접근 가능하게 하는 공격으로, 소프트웨어 공급망 공격 방법 중 하나이다.

본 지침에서 네트워크 장비 구축 또는 네트워크 장비 운영사업의 계약상대자는 국가정보원의 국가 정보보안 기본지침 및 수요기관 보안업무규정 및 세부지침 등을 준수해야한다. 또한, 세부 보안요구사항을 충족하기 위하여 조치를 취해야 하며, 기능상 보안 취약점 등의 결점을 발견할 경우 개선해야함을 명시한다. 네트워크 장비 내에 백도어 등이 설치 및 운영되지 않도록 주기적인 점검을 진행 할 것을 경고하고 있으며, 보안대책 마련을 권장한다. 마지막으로 결점을 발견할 경우 수요기관에 즉시 신고해야 하며 신속한 조치를 진행해야 한다고 명시한다. 만약 이에 위반할 경우 제5조에 의거, 관계 법령에 따라 입찰참가자격 제한 처분 및 계약 해제 또는 해지 할 수 있다.

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서는 정보통신망침입죄를 규정하고 있으며, 제48조(정보통신망 침해행위 등의 금지)에는 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하여서는 안됨을 명시한다. 또한, 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·변경·위조하거나 악성프로그램을 전달 또는 유포해서는 아니 된다[6]. 이를 위반한 자는 제72조(벌칙)에 의해 3년 이하의 징역 또는 3천만원 이하의 벌금에 처하며, 미수범은 처벌만 진행한다.

이렇듯 IT 제품 공급망 제조 및 배포 과정에 있어 악의적인 목적을 가지고 공격을 시도하였어도, 해당

Table 1. Manufacturing Security Accident Case

Year of occurrence	Country of occurrence	Attack target	Attack method	Result
2014	Germany	Control system	Hacking	Block control system functions Loss of control
2017	Japan	Production information PC / Server	Ransomware	Semiconductor production discontinued
2017	Saudi Arabia	Emergency safety device	Malware	Block gas leak attempts
2018	Taiwan	Production information PC	Ransomware	Semiconductor production discontinued

사항에 대한 법률적 제재는 관련 권한 박탈 및 벌금에 그치는 매우 미비한 실정이다. 또한, 사전 대응에 대한 법적 근거로써 어려운 한계점이 존재한다.

4.2 NIST IR 7622

2012년 10월 미국 NIST에서 발행한 NIST IR 7622 문서는 연방 정보보안 관리법(FISMA, Federal Information Security Modernization Act)과 공법(P.L., Public Law) 107-347에 의거 법적 책임을 증진하기 위해 개발되었다[3]. 본 문서는 연방 기관이 ICT 공급망 위험 관리를 위하여 ICT 제품 및 서비스를 도입할 경우 고려해야 할 사항들을 명시하며, 공급망 위험 관리에 대한 전체적인 배경 지식을 제공하는 것을 목표로 한다.

본 문서는 ICT 공급망 위험 관리 문제 해결을 위해, 여러 분야의 공급망 관리 사례를 제시하였으며, 시스템 및 소프트웨어 엔지니어링, 정보보안, 소프트웨어 보증, 공급망 및 물류, 취득 등에서의 공급망 관리 사례를 포함하였다.

4.3 NIST SP 800-161

2015년 4월에 공개된 NIST SP 800-161은 ICT 공급망 위험을 식별, 평가 및 완화하기 위한 지침을 제공한다[4]. 본 문서는 FISMA의 법정 책임에 따라 개발되었으며, FIPS 199, NIST SP 800-30 Rev.1, NIST SP 800-37 Rev.1, NIST SP 800-39, NIST SP 800-53 Rev.4 문서들을 기반으로 제작되었고, NIST IR 7622 문서는 본 문서의 제작 배경연구로 참조되었다[23][24][25][26][15][3].

ICT 공급망 위험 관리는 기관에서 관리하는 하드웨어 및 소프트웨어를 포함한 모든 ICT 제품과 서비스의 생명주기 전반을 대상으로 한다. 이때, 관리 대상의 생명주기는 연구개발, 설계, 제조 및 운영 단계부터 처분, 폐기까지의 모든 활동을 포함한다. 이에 따라 NIST는 본 문서에서 공급망 과정 내 제품 무단 생산, 변조, 도난, 악성 소프트웨어 및 하드웨어 삽입, ICT 공급망의 제조 및 개발 관행 부실 등을 공급망 위험 요소로 지정하였다.

또한, 이 문서는 다양한 분야에서 기존의 표준화된 관행을 기반으로 하여 ICT 공급망 위험 관리를

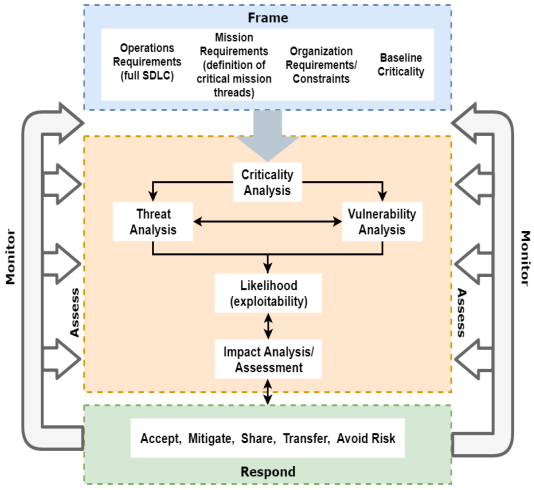


Fig. 3. ICT SCRM Risk Management

수행하도록 하였다. 그에 따라 진보된 ICT 공급망 위험 관리에 초점을 맞추기보다 기존의 관행 수준을 고려하여 ICT 공급망 위험 관리(SCRM)를 진행하고 있으며, 관련 지침들을 기반으로 하여 Fig.3과 같은 위험 관리 프로세스를 제안하였다.

먼저 기관들은 ICT 공급망 위험 관리를 위하여 운영·임무·기관 요구사항 및 중요도에 따라 위험 기반 의사 결정을 해야 한다. 이를 통해 프레임을 구축한 후 위험도를 평가한다. 이 과정에서 중요성과 위협, 취약점, 악용 가능성, 영향력에 따라 위험도를 판별한다. 위험을 파악한 후, 프로세스에 따라 대응 방안을 세우고, 이에 따라 위험 사항에 대한 조치를 완료한다. 이와 함께 위험 관리의 각 과정을 지속적으로 모니터링하여, 위험 관리 프로세스를 개선할 수 있도록 한다.

4.4 ICT Supply Chain Risk Management Task Force

2018년 7월 DHS(미국 국토안보부, U.S. Department of Homeland Security)는 국가적 공급망 위험 관리를 위한 태스크포스(ICT supply chain risk management task force)를 신설하였다[27]. 이 태스크포스는 미국 ICT 공급망에 대한 위험을 식별하고 관리하기 위한 권고안을 작성하기 위해 신설되었으며 정부 기관과 민간 기업이 공동으로 참여하고 있다(Table.2). 이는 미국 DHS National Protection and Programs

Table 2. List of Executive Committee Organizations on Task Force

Industry	Accenture	AT&T
	CenturyLink	Charter
	Cisco	Comcast
	CTIA	CyberRx
	Cybersecurity Coalition	Cyxtera
	FireEye	Intel
	ITI	IT-ISAC
	Microsoft	NAB
	NCTA	NTCA
	Palo Alto Networks	Samsung
	Sprint	Threat Sketch
	TIA	T-Mobile
	USTelecom	Verizon
Government	DHS (Department of Homeland Security)	DoD (Department of Defense)
	Department of Treasury	DOJ (Department of Justice)
	DOC (Department of Commerce)	GSA (General Services Administration)
	ODNI (Office of the Director of National Intelligence)	SSA (Social Security Administration)

Directorate's (NPPD) Cyber Supply Chain Risk Management (C-SCRM) 프로그램의 일부로써, 연방 정부기관을 위해 공급망 위험 관리 기능을 개발 및 배포한다.

또한, 태스크포스는 기존의 공급망 위험 관리 방안을 조사하여 목록화하는 것 이외에 다음과 같은 4가지의 주요 계획안을 발표하였다[28][29].

- 정부와 산업계 간 공급망 위험에 대한 정보의 양방향 공유를 위하여 공통된 위험 관리 프레임워크 개발
- ICT 공급, 제품 및 서비스의 위협 기반 평가를 위한 프로세스 및 평가 기준 정립
- 적격 입찰자 및 제조업체의 목록에 대한 시장 식별 및 평가 기준 정립
- 제품의 제조업체 또는 공인된 판매업체로부터 ICT 구매를 장려하기 위한 정책 권고안 작성

V. 국내 및 미국 공급망 관리 체계 적용

2장에서 소개한 공급망 공격 사례들을 미국의 공급망 위험 관리 프로세스에 적용하면 다음과 같다. MeDoc과 넷사랑 업체는 각 회사에서 제조하는 제품에 대한 보안요구사항 및 중요도에 따라 위험 기반 의사 결정을 진행한다. 이를 기반으로 프레임을 구축해야하며, 해당 프레임에서 발생 가능한 위험을 파악한다. 두 업체 모두 프로그램 개발 및 배포과정에 개발 시스템, 버전 관리 서버, 빌드 서버, 파일 서버, 업데이트 서버, 배포 과정 등 다양한 위험 요소가 존재한다. 그 중 관리자가 파일 위변조 사실을 파악하기 어려운 업데이트 서버와 빌드 서버의 침입 및 악성코드 유입이 가장 큰 위협으로 판단된다. 따라서 위험도에 따라 우선순위를 지정하여 관리해야 하며, 서버 진입 과정의 보안 절차를 강화하거나 원격 접속을 차단하는 등의 대응방안 및 위험 상황 발생 시 조치가 가능한 매뉴얼을 구축하여야 한다. 보안 담당자들은 해당 프로세스에 대한 지속적인 모니터링을 통하여 사전 방지 및 위험 발생 시 실시간 대응이 가능하도록 해야 한다.

스마트공장의 사고 사례의 경우 랜섬웨어 및 악성코드 감염으로 인하여 제어시스템과 각종 관리 PC들이 제 기능을 수행하지 못해 가용성을 확보하지 못하게 되었다. 따라서 스마트공장 또한 산업제어시스

템, 생산/제조시스템 등 각 제조과정 별로 공급망 위험 관리 프로세스를 구축하고 지속적인 모니터링을 수행하여 위험 상황 발생 시 조기 대응이 가능하도록 상시 대비한다면, 공급망 공격 노출의 위험성을 감소할 수 있을 것으로 기대한다.

반면 해당 사례를 국내의 법률에 적용시켜 보았을 때, 공격자는 MeDoc 및 넷사랑 서버 그리고 스마트공장의 제어시스템에 침입하여 정상적 인증과정을 거치지 않고 시스템에 접근하였으므로 조달청지침 제527호의 제4조를 위반한 것으로 보인다. 그에 따라 공급자는 제5조에 의거, 입찰참가자격 제한 처분 및 계약 해제가 이루어져야한다. 결국 공급자 또한 공격자로 인해 피해를 받은 입장임에도 불구하고 법적 해석에 따라 계약 해지가 가능한 상황이다.

또한, 정보통신망침입죄의 경우 정당한 사유 없이 프로그램을 변경·위조하여 악성프로그램을 전달 및 유포함에 따라 제48조를 위반하게 된다. 그에 따라 공격자는 제72조에 의거하여 벌금 또는 징역에 처하게 되나, 이는 공격자를 검거하였을 시 처벌 가능해 보이는 법칙으로 법적 효력에 미비함이 보인다.

이렇듯 국내 공급망 관리 현황의 부족한 점을 보완하여 사전 대응이 가능한 공급망 관리 체제를 정립할 필요성이 있다. 이에 따라 미국의 공급망 위험 관리 프로세스를 기반으로 하여, 국내의 공급망 보안 위험 관리 프레임워크를 개발한다면 보다 보안성이 제고된 제품이 공급 및 수요 가능할 것으로 기대된다.

VI. 결 론

스마트 제조가 고도화 될수록 다양한 IT 제품 및 서비스가 빠르게 공급망에 포함될 것으로 예상된다. 이때, 제조 및 유통을 거쳐 기업에 공급되기까지 다양한 업체를 통해 형성된 유기적인 공급망은 해킹 및 각종 보안 위협에 노출되어 있어, 스마트 제조에서 공급망 보안의 중요성은 더욱 강조될 것으로 판단된다.

최근, 공급망 공격은 안전한 보안 인프라가 구축된 네트워크망에 직접 침투하기보다, 상대적으로 보안이 미흡한 제조·납품 업체를 공격하여 우회 침투하기 시작했다. 이에 따라 본 논문에서는 그간 알려진 다양한 공급망 공격 중, 업데이트 서버를 해킹하여 사용자들에게 랜섬웨어를 배포한 MeDoc 공급망 공격 사례와 제품 패키지 과정에 침입하여 제품에 백도어를 삽입한 넷사랑 공급망 공격 사례, 그리고 스마트공장의 제조업에서 발생한 보안사고 사례를 소개함으로써 공급망 공격의 위험성을 강조하였다.

이를 방지하기 위하여 국외에서는 공급망 관리 체계를 정립하여 시행하고 있다. 본 논문에서는 미국의 공급망 위험 관리 노력을 소개하였다. 미국은 NIST IR 7622와 NIST SP 800-161 지침을 통하여 ICT 공급망 위험 관리의 배경지식을 소개하고 위험 관리 프로세스를 제안하였다. 또한, 태스크포스를 신설함으로써 보다 체계적인 공급망 위험 관리 방안 도출을 위해 노력하고 있다. 이에 반해 국내는 공급망과 관련된 법률과 규제는 존재하지만, 사전 대응방안이 미흡함에 따라 구체적인 공급망 관리 체계 및 검증 프로세스가 필요한 시점이다.

향후 연구로는 미국 외 다양한 국가들에서 시행중인 공급망 위험 관리 체계를 분석하여 국내 환경에 적합한 공급망 위험 관리 및 검증체계 수립을 위한 연구를 진행할 예정이다. 추가로 국내 정부 기관의 IT 제품 도입 과정에 있어 CC 평가·인증과 더불어 공급망 안전에 대한 사전 검증 기술 및 관리 체계에 대한 연구를 수행할 예정이다.

References

[1] Keun-Hee Han, “Smart Factory based convergence security issue and solution,” KISA REPORT, vol. 08, pp. 53-61, Aug. 2018.

[2] KISA, “Cyber-treat Trends Report,” Jul. 2018.

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

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

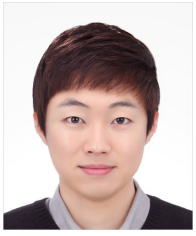
[5] National Law Information Center, “Additional Special Conditions for Network Equipment-Building and

Operation Projects," Procurement Service Directive No.5538, Last modified Jun. 2018.
〔6〕 National Law Information Center, "ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND INFORMATION PROTECTION, ETC," Law No. 16021, Last modified Dec. 2018.
〔7〕 Dong-Won Kim, Keun-Hee Han, "Automotive-Software & Supply Chain Assurance," Review of KIISC, 25(1), pp. 39-46, Feb. 2015.
〔8〕 Dong-Won Kim, Keun-Hee Han, In-Seok Jeon, Jin-Yung Choi, "A Study on Supply Chain Risk Management of Automotive," Journal of The Korea Institute of Information Security & Cryptology, 25(4), pp. 793-805, Aug. 2015.
〔9〕 Soo-Min Lim, A-Ram Kim, Ick-Hyun Shin, "Trends of Cyber Security Regulation of Digital Asset Supply Chain of International Nuclear Power Plants," Review of KIISC, 26(1), pp. 54-60, Feb. 2016.
〔10〕 KISA, "Cyber-treat Trends Report," Jan. 2019.
〔11〕 Symantec, "Internet Security Threat Report," Mar. 2018.
〔12〕 Symantec, "Internet Security Threat Report," Feb. 2019.
〔13〕 Nuclear Regulatory Commission, "Cyber Security Programs for Nuclear Facilities," NRC Regulatory Guide 5.71, Jan. 2010.
〔14〕 Nuclear Regulatory Commission, "Criteria for use of computers in safety systems of nuclear power plants Rev 3," NRC Regulatory Guide 1.152, Jul. 2011.
〔15〕 National Institute of Standards and Technology, "Security and Privacy Controls for Federal Information Systems and Organizations," NIST SP 800.53, Feb. 2014.
〔16〕 International Atomic Energy Agency, "Procurement Engineering and Supply Chain Guidelines in Support of Operation and Maintenance of Nuclear Power Plants," IAEA-TECDOC-919, Dec. 1996.
〔17〕 International Atomic Energy Agency, "Managing Suspect and CounterFeit Items in the Nuclear Industry," IAEA-TECDOC-1169, Aug. 2000.
〔18〕 Wikipedia, "Petya malware" https://en.wikipedia.org/wiki/2017_cyberattacks_on_Ukraine, Oct. 2019.
〔19〕 Wired, "NotPetya" https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/, Oct. 2019.
〔20〕 NetSarang, "NetSarang" https://www.netsarang.com/ko/, Oct. 2019.
〔21〕 Kaspersky, "ShadowPad" https://www.kaspersky.com/about/press-releases/2017_shadowpad-how-attackers-hide-backdoor-in-software-used-by-hundreds-of-large-companies-around-the-world, Oct. 2019.
〔22〕 Kye-Geun Kim, "Smart Factory Security," 2019 KISA REPORT, vol. 05, pp. 27-35, Jun. 2019.
〔23〕 National Institute of Standards and Technology, "Standards for Security Categorization of Federal Information and Information Systems," FIPS 199, Feb. 2004.
〔24〕 National Institute of Standards and Technology, "Guide for Conducting Risk Assessments," NIST SP 800-30 Rev.1, Sep. 2012.
〔25〕 National Institute of Standards and Technology, "Guide for Applying the Risk Management Framework to

Federal Information Systems," NIST SP 800-37 Rev.1, Feb. 2010
〔26〕 National Institute of Standards and Technology, "Managing Information Security Risk," NIST SP 800-39, Mar. 2011.
〔27〕 U.S. Department of Homeland Security, "Supply Chain Risk Management" https://www.dhs.gov/, Feb. 2019.
〔28〕 U.S. Department of Homeland Security, "ICT SCRM Task Force" https://www.dhs.gov/cisa/information-and-communications-technology-ict-supply-chain-risk-management-scrm-task-force, Mar. 2019.
〔29〕 U.S. Department of Homeland Security, "ICT Supply Chain Risk Management Task Force," Nov. 2018.

〈저자소개〉

손 효 현 (Hyo-hyun Son) 학생회원
2019년 2월: 한남대학교 컴퓨터통신무인기술학과 학사
2018년 3월~현재: 한남대학교 컴퓨터공학과 학·석사연계과정
〈관심분야〉 정보보호, 정보보호정책, 소프트웨어 평가 및 검증, 보안적합성 검증



김 광 준 (Kwang-Jun Kim) 학생회원
2017년 2월: 한남대학교 컴퓨터공학과 학사
2019년 2월: 한남대학교 컴퓨터공학과 석사
2019년 3월~현재: 한남대학교 컴퓨터공학과 박사과정
〈관심분야〉 정보보호, 침입 탐지, 네트워크/시스템 보안

이 만 희 (Man-hee Lee) 종신회원
1995년 2월 경북대학교 컴퓨터공학과 공학사
1997년 2월 경북대학교 공학석사
2008년 8월 Texas A&M 대학교 컴퓨터공학과 공학박사
1997년~2003년 한국과학기술정보연구원 연구원
2008년~2009년 Cisco Systems, San Jose
2010년~2012년 국가보안기술연구소 선임연구원
2012년~현재 한남대학교 부교수
〈관심분야〉 네트워크/시스템/스마트폰 보안, 고성능 시스템, 컴퓨터교육