Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.2, Apr. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.2.241

기반시설 사이버보안 프레임워크 도출방안

권 성 문,[1†] 이 석 철,[1] 장 지 웅,[2] 손 태 식[3‡]
[1]아주대학교 컴퓨터공학과, [2]전력거래소, [3]아주대학교 사이버보안학과

Cyber Security Framework for Critical Infrastructure

Sungmoon Kwon,[1†] Seokcheol Lee,[1] Jiwoong Jang,[2] Taeshik Shon[3‡]
[1]Department of Computer Engineering, Ajou University
[2]Korea Power Exchange
[3]Department of Cyber Security, Ajou University

요 약

폐쇄적으로 운영되던 과거의 기반시설과 달리 현재의 기반시설 네트워크는 IoT 기기와 외부 망과의 연계를 통한 효율적인 관리 시스템을 도입하고 있다. 이를 통해 과거의 기반시설 네트워크에 비해 생산성과 관리의 효율은 증대 될 수 있으나 외부 망과의 연계 접점이 생김에 따라 S/W 취약점과 이를 악용한 사이버 보안 이슈가 발생할 수 있으며 이에 대응하기 위한 사이버보안 가이드라인은 필수적이다. 그러나 각 기관에서 적합한 사이버보안 가이드라인을 개발하는 것이 용이하지 않아 정부 기관에서 작성한 사이버보안 점검 리스트를 활용하고 있으며 이는 각 기반시설 네트워크의 특징을 충분히 반영하지 못하는 한계가 있다. 따라서 본 연구에서는 기반시설 네트워크의 특징을 반영한 사이버 보안 가이드라인을 개발을 위해 NIST CSF[2], DoE C2M2[3] 등 주요 국가의 사이버보안 가이드라인 관련 표준과 기반시설 네트워크를 분석하고 이를 통해 기반시설 네트워크 사이버보안 가이드라인 개발 방안을 도출하고 검증방안을 제시하였다.

ABSTRACT

Contrary to past critical infrastructure network, current critical infrastructure network is adopting IoT devices and efficient management system using the external networks. Using this system, productivity and management efficiency could be enhanced compared to past critical infrastructure network. But cybersecurity issue could be occurred at external network connection, so cybersecurity guideline is necessary. However, critical infrastructure organizations tend to use the cybersecurity guideline issued by government because it is hard to develop cybersecurity guideline on their own. But the government's cybersecurity guideline isn't suitable for the critical infrastructure network because it doesn't include critical infrastructure's specific characteristics. Therefor, we suggested the development method of cybersecurity guideline for the critical infrastructure network based on analysing cybersecurity guideline standards and critical infrastructure networks.

Keywords: Cybersecurity Guideline, Cybersecurity Framework, Critical Infrastructure

I. 서 론

과거의 기반시설 네트워크는 외부 망과 분리되어 운용됨으로써 그 자체로 보안을 보장받을 수 있었다. 그러나 현재의 기반시설 네트워크는 효율적인 관리를 위해 외부 망과의 연계 및 IoT를 산업제어시스템에 도입한 IIoT(Industrial Internet of Things)를 사용하고 있어 산업제어시스템 네트워크 또한 외부의 사이버 공격의 대상이 되고 있다. 특히 미국 ICS-CERT의 2015년 보고서[1]에 따르면 산업제어시스템 환경에서 사이버 공격에 의한 보안 사고는 총 295건으로, Fig.1.과 같이 2010년 40건 대비 7

Received(12. 26. 2016), Modified(03. 10. 2017), Accepted(03. 16. 2017)
† 주저자, minter@ajou.ac.kr
‡ 교신저자, tsshon@ajou.ac.kr(Corresponding author)

배 넘게 증가하였으며 매년 증가하는 추세이다. 따라서 기반시설 네트워크를 대상으로 한 사이버 공격에 대응하고 보안을 강화하기 위해 기반시설 네트워크의 특성을 반영한 사이버 보안 가이드라인은 중요한 보안 요소이다. 이를 개발하기 위해 사용 될 수 있는 대표적인 표준 및 가이드라인으로 미국 NIST(National Institute of Standards and Technology)의 Framework for Improving Critical Infrastructure Cybersecurity[2], DoE(Department of Energy)의 Cybersecurity Capability Maturity Model(C2M2)[3] 등이 있으나 문서의 많은 부분이 각 기관의 특징에 맞게 재해석하여 작성 및 활용해야 하는 점 때문에 각 기관이 스스로 가이드라인을 개발하는 것은 용이하지 않다. 따라서 많은 기반시설 기관에서는 정부 기관에서 배포한 사이버 보안 가이드라인을 기관에 맞게 일부 수정하여 사용하고 있으나, 이는 기존 레거시 장비 및 신규 IIoT를 사용하는 특수한 환경인 기반시설 네트워크의 특징을 충분히 반영하고 있지 않은 한계점을 지니고 있다. 이러한 문제점을 해결하기 위해 본 연구에서는 기반시설 네트워크의 특성 및 IIoT의 특성을 반영한 사이버 보안 가이드라인의 개발을 위해 사이버 보안 가이드라인 관련 표준과 기반시설 네트워크를 분석하고 이를 통해 기반시설 네트워크 사이버보안 가이드라인 개발 방안을 제시한다.

논문의 구성은 2장에서 사이버 보안 가이드라인 활용한 사례를 분석하고, 3장에서는 관련 사이버 보안 가이드라인과 보안요구사항 문서를 분석하며, 이러한 분석을 바탕으로 4장에서는 기반시설 네트워크를 위한 사이버보안가이드라인 개발 방안을 설명하며 5장에서 가이드라인 검증 방안을 제시하며 6장에서 결론을 맺는다.

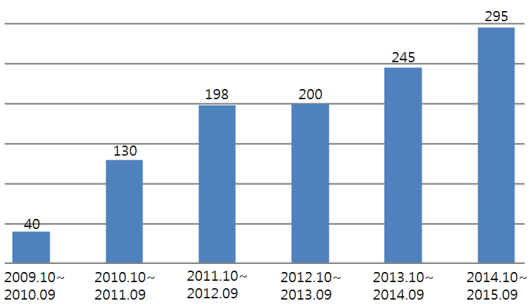

Fig. 1. Cyber Incidents on Industrial Control System - US ICS-CERT

II. 관련연구

미국 정부에서는 사이버보안 프레임워크를 사이버 보안성 향상을 위한 수단으로 인지하고 있으며, NIST CSF [2]가 사실상의 표준으로 인식되어 여러 단체 및 기관에서 활용하고 있다. 2015년 12월 Dell社에서 진행한 조사에 따르면 미국 정부기관 80%가 NIST CSF [2]를 사용하고 있으며, 이중 70%는 이로 인해 실질적으로 보안성이 증가되었다고 평가하였다. 그리고 미국 DoE C2M2[3]의 경우 미국 에너지와 관련된 조직에서 기본적으로 적용하고 있으며, NIST [2]문서와의 상호 운용성을 위해 문서의 일부를 개정 한 바 있다. 이러한 사이버 보안 가이드라인을 기관에서 활용한 것을 주제로 2015년부터 NIST와 DoE의 주관으로 워크숍과 교육이 활발히 이루어지고 있으며 최근에는 2016년 4월에 NIST에서 주관하는 워크숍이 열린 바 있다. 본 연구진 또한 2015년 10월에 DoE가 지원하여 미국 Dallas에서 EnergySec이 주최한 "Cybersecurity Frameworks: Theory and Applications" 워크숍을 참여한 바 있으며, 이 워크숍에서 분석한 가이드라인 개발 주요 예시로 전력계통 보안 가이드라인 개발 예시가 있다. 이 예시에서 활용한 가이드라인 및 표준은 NIST CSF[2], DoE C2M2[3]와 전력계통신뢰도 보안 표준인 NERC CIP(The North American Electric Reliability Corporation Critical Infrastructure Protection)[4]로 프레임워크의 기본 골자로 NIST CSF[2]의 Framework를 사용하여 DoE C2M2[3]와 상호 운용성을 보장하였으며, 주요 평가 항목과 스코어링 기법을 위해 DoE C2M2[3]를 이용하여 정량적 평가를 통한 보안 준수사항 평가 및 보안 개선 우선순위를 도출하였다. 세부 평가 항목을 위해서는 NERC CIP[4]와 DoE C2M2[3] 항목을 매핑한 보안요구사항을 평가 기준으로 활용하여 최종적으로 전력계통 보안을 체계적으로 평가 할 수 있는 보안 가이드라인을 제시하였다. 따라서 NIST CSF[2]의 부족한 세부 내용과 평가 방식을 DoE C2M2[3]의 평가 항목과 스코어링 기법을 활용하고, 세부 평가 항목은 기관 환경에 맞는 보안 요구사항을 사용하는 방법이다. 사이버 보안 가이드라인을 개발하기 위한 방안은 유용하나 세부적으

로는 특정 환경 및 목적을 위해서는 가이드라인에서 일부 불필요한 항목을 포함하며 특수성을 가진 세부 평가 항목은 기관에서 스스로 작성해야 하기 때문에 기반시설 네트워크의 특수성을 반영한 가이드라인의 개발의 연구가 필요하다.

III. 주요 가이드라인 및 표준 분석

본 장에서는 기반시설 네트워크 사이버보안 가이드라인 개발을 위해 활용한 주요 사이버보안 가이드라인 및 표준과 기반시설 네트워크의 IIoT 보안 요구사항을 분석한다. 크게 가이드라인의 큰 틀로 NIST CSF[2]를, 주요 평가 항목으로 DoE C2M2[3]를, 세부 평가 항목으로 여러 보안 요구사항 문서들을 분석한다.

3.1 Cybersecurity Framework - NIST

NIST CSF[2]문서는 발생 가능한 사이버보안 위협을 중심으로 이를 정의하고, 현재의 보안 상황을 점검하여 우선시 되는 보안 개선 요소를 파악 및 체계화하는데 초점을 맞추고 있다. 이를 위해 프레임워크는 크게 Core, Implementation Tier, Profile로 구성되어 있으며, Core는 보안 상황을 점검하기 위한 활동들을 정의하며 크게 Identify, Protect, Detect, Respond, Recover 5항목으로 분류하여 각 분류 항목 마다 세부 항목 및 참고 할 수 있는 문서를 제시하고 있다. Fig. 2.는 Core의 Identify의 세부 항목인 Asset Management 분류의 세부 분류와 참고 문서항목을 표준에서 캡처한 그림이다. 따라서 각 세부 항목에 대해 작성하는 것은 가이드라인

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	• CCS CSC 1 • COBIT 5 BAI09.01, BAI09.02 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	• CCS CSC 2 • COBIT 5 BAI09.01, BAI09.02, BAI09.05 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: Organizational communication and data flows are mapped	• CCS CSC 1 • COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.2.3.4 • ISO/IEC 27001:2013 A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	• COBIT 5 APO02.02 • ISO/IEC 27001:2013 A.11.2.6 • NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	• COBIT 5 APO03.03, APO03.04, BAI09.02 • ISA 62443-2-1:2009 4.2.3.6 • ISO/IEC 27001:2013 A.8.2.1 • NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	• COBIT 5 APO01.02, DSS06.03 • ISA 62443-2-1:2009 4.3.2.3.3 • ISO/IEC 27001:2013 A.6.1.1

Fig. 2. Core - Asset Management Category of Identify Function

에서 제시하고 있지 못하며, 큰 틀에서 보안 항목들만 제시하고 있다. Implementation Tier는 보안 수준에 따라 Partial, Risk Informed, Repeatable, Adaptive 4단계로 나누어 정의하며 Profile은 보안 요소로 선택한 Core 항목에 대해 Implementation Tier를 현재와 목표의 Profile을 작성하여 보안 개선을 위한 운선순위를 파악하는 과정이다. Implementation Tier 부분 또한 각 Core 항목 별로 기술 되어 있지 않고 범용적인 내용만을 포함하고 있기 때문에 NIST CSF[2]에서는 Core 항목을 통해 주요 사이버 보안 가이드라인의 항목을 파악하는 용도로 활용한다.

3.2 C2M2 - DoE

DoE C2M2[3]문서는 NIST CSF[2]의 Core의 와 유사한 10개의 주요 보안 항목인 Domain과 Implementation Tier와 유사한 MIL(Maturity Indicator Levels)에 대해 1,2,3단계로 기술하고 있다. 두 가이드라인의 가장 큰 차이점은 DoE C2M2[3]의 경우 Domain의 세부 보안 요소별 각 MIL 단계의 보안 요구사항을 명시한 것이다. Fig. 3.은 Risk Management Domain의 Manage Cybersecurity Risk Objective의 MIL에 따른 요구사항을 캡처한 것이다.

2. Manage Cybersecurity Risk		
MIL1	a.	Cybersecurity risks are identified
	b.	Identified risks are mitigated, accepted, tolerated, or transferred
MIL2	c.	Risk assessments are performed to identify risks in accordance with the risk management strategy
	d.	Identified risks are documented
	e.	Identified risks are analyzed to prioritize response activities in accordance with the risk management strategy
	f.	Identified risks are monitored in accordance with the risk management strategy
	g.	Risk analysis is informed by network (IT and/or OT) architecture
MIL3	h.	The risk management program defines and operates risk management policies and procedures that implement the risk management strategy
	i.	A current cybersecurity architecture is used to inform risk analysis
	j.	A risk register (a structured repository of identified risks) is used to support risk management activities

Fig. 3. Manage Cybersecurity Risk of Risk Management Domain

3.3 세부 보안 요구사항 문서 항목

세부 보안 요구사항을 작성하기 위해서는 일반 IT 보안 요구사항을 포함하여 기반시설 보안 요구사항 문서와 IIoT환경을 위한 보안 요구사항 등 다양한 보안 요구사항 문서가 활용 될 수 있다.

일반적인 IT 보안 요구사항을 위한 문서로는 CIS CSC(Center for Internet Security Critical Security Controls)[5], NISP SP 800-53[6], 한국인터넷진흥원의 IPv6 운영보안 안내서[7], 무

선랜 보안 안내서[8], 소프트웨어 보안약점 진단가이드[9], VoIP 보안권고해설서[10]가 있으며, 기반시설 환경의 보안 요구사항 문서로는 ANSSI(Agence nationale de la sécurité des systèmes d'information) Cybersecurity for ICS Detailed Measures[11], NIST SP 800-82[12]가 있다. 반면, IIoT의 경우 실증에 중점을 두고 있어 IIoT 특화 보안 요구사항이 아직 연구되지 않아 IoT 요구 사항인 OWASP IoT Top 10[13]에서 기반시설의 특성을 추가하여 사용할 수 있다. 이외 전력제어시스템의 경우 NERC[4]도 활용할 수 있으며 윈도우의 보안 설정 기준을 위해 USGCB[14](The United States Government Configuration Baseline) 또한 활용 할 수 있다.

IV. 기반시설 네트워크를 위한 사이버보안 가이드라인 개발 방안

본 장에서는 기반시설 네트워크를 위한 사이버보안 가이드라인 개발 방안을 설명하며, 가이드라인의 단계 도출 과정과 각 단계별 세부 항목 도출 과정을 설명한다.

4.1 가이드라인 단계 도출

우선 NIST CSF [2]의 Core 항목과 DoE C2M2 항목 중 네트워크 관점에서 필요한 항목만을 선별하였으며 이 항목들의 세부 내용과 기반시설 기관에서 요구하는 특징을 고려하여 가이드라인의 주요 단계를 도출하였다.

Identify Function은 대상을 식별하는 단계, Protect와 Detect Function은 식별된 대상의 보안을 점검하는 단계, Respond와 Recover Function은 보안 점검 결과를 피드백하여 보안을 향상시키는 단계로 볼 수 있다. 여기서 추가적으로 기반시설 네트워크의 신규 취약성을 식별하고 이를 분석하는 단계가 필요하다 판단하였으며 이를 추가하여 가이드라인을 크게 4단계로 도출하였다. 도출된 가이드라인의 단계는 가이드라인 적용 대상 범위를 설정하고 자산을 식별하는 Knowledge 단계, 식별된 자산에 대해 보안 점검을 수행하는 Capture 단계, 자산의 신규 취약점을 식별하고 분석하여 대응하는 Scheme 단계, 가이드라인을 검증하고 피드백을 수행하는 Fine-tune 단계로 구성하였으며 가이드라인 각 단계의 첫 글자를 따 K-CSF(Korea CyberSecurity Framework)로 칭한다.

그리고 Fig. 4.와 같이 NIST CSF [2], DoE C2M2 [3]의 각 항목 세부 내용을 참고하여 가이드라인 각 단계에서 참고하기 위한 항목을 선별하였다. Knowledge 단계에서 참고하기 위한 항목으로 NIST CSF [2] Identify Function의 Asset Management 항목과 DoE C2M2 [3] Asset,

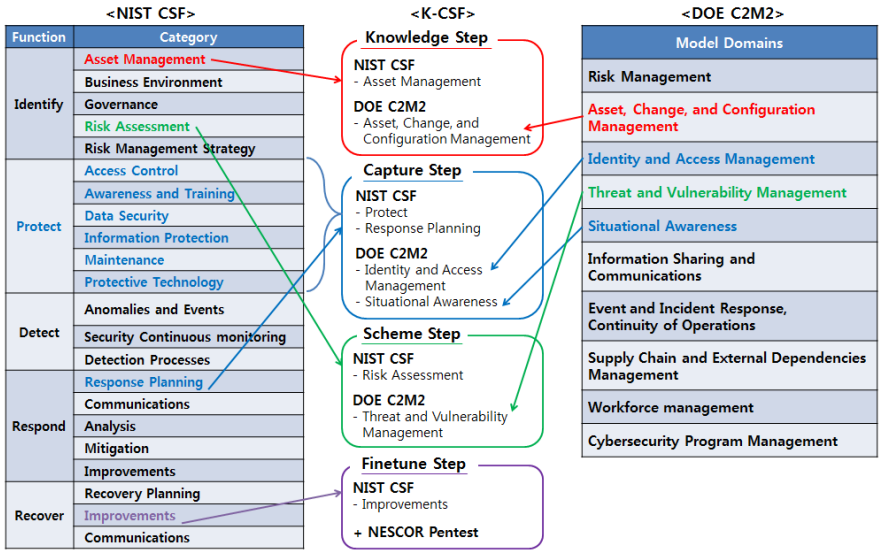

Fig. 4. Mapping Table of K-CSF, NIST-CSF and DoE C2M2

Change and Configuration Management 항목을, Capture 단계에서 참고하기 위한 항목으로 NIST CSF [2] Protect Function 전체 Category, Respond Function의 Response Planning 항목과 DoE C2M2 [3] Identity and Access Management, Situational Awareness 항목을, Scheme 단계에서 참고하기 위한 항목으로 NIST CSF [2] Identify Function의 Risk Assessment 항목과 DoE C2M2 [3] Threat and Vulnerability Management 항목을, Fine-tune 단계에서 참고하기 위한 항목으로 NIST CSF [2] Respond Function의 Improvements 항목을 선별하였다.

K-CSF의 전체 흐름도 및 주요 참고 항목은 Fig. 5.와 같으며 Knowledge 단계는 네트워크 Diagram, H/W 자산 목록, 시스템 목록, S/W 및 버전 목록, 정책과 절차문서, 네트워크 모니터링 정보, 무선 네트워크 정보, 시스템의 정보 흐름 Diagram, 시스템 관리자 및 사용자 정보를 수집하여 '대상 분석 보고서'를 작성하는 단계이다.

Capture 단계는 Knowledge 단계에서 산출된 대상 분석 보고서를 통해 식별된 네트워크/시스템/프로그램에 대하여 주요 보안 항목에 대한 점검을 수행하여 '보안 점검 보고서'를 작성하는 단계이다. 보안 점검 항목은 정적인 항목이 아닌 이후 단계에서 추가적으로 찾아지는 취약성을 계속 추가하게 되는 동적인 항목이다.

Scheme 단계는 자산의 정보를 키워드로 한 OSINT 정보를 수집하는 공개된 취약성 정보를 수집하는 단계이며 새로운 위협 및 취약성을 각 기관에 맞게 재해석하고 이에 대한 '위협 및 취약성 분석 보고서'를 작성 및 대응하며 추가적인 Capture 단계의 보안 점검 항목으로 추가한다.

Fine-tune 단계는 이전 단계까지의 점검 대상과 동일한 네트워크 범위를 대상으로 모의 침투 실험을 수행하여 가이드라인을 검증하고 피드백 하는 단계이며 보안 점검 항목 및 위협 분석 보고서의 식별된 취약점과 비교하여 모의 침투 실험 '검증 수행 보고서'를 작성하고 추가적으로 식별된 취약점을 Capture 단계의 보안 점검 항목으로 추가하여 피드백을 수행하는 단계이다.

4.2 Knowledge 단계 세부 항목 도출

Knowledge 단계 개발 개요도로 세부 항목 도출 과정은 크게 3단계로 나뉜다. 첫 번째 단계로, NIST [2]의 Knowledge 단계 관련 항목인 Identify- Asset Management의 참고문서 및 DoE [3]의 Asset, Change and Configuration Management Domain과 과학기술부의 위기대응 실무매뉴얼[15]의 정보자산통제 및 주요 국내 참고문서들을 분석하였다. 이를 통해 물리적 기기와 시스템 목록화, S/W 플랫폼 및 프로그램 목록화, 자원의 분류 및 우선순위 작성, 통신 연결 및 데이트 흐름 목록화, 외부 정보 시스템 목록화 항목을 도출하였다. 두 번째 단계로 도출된 5 항목에

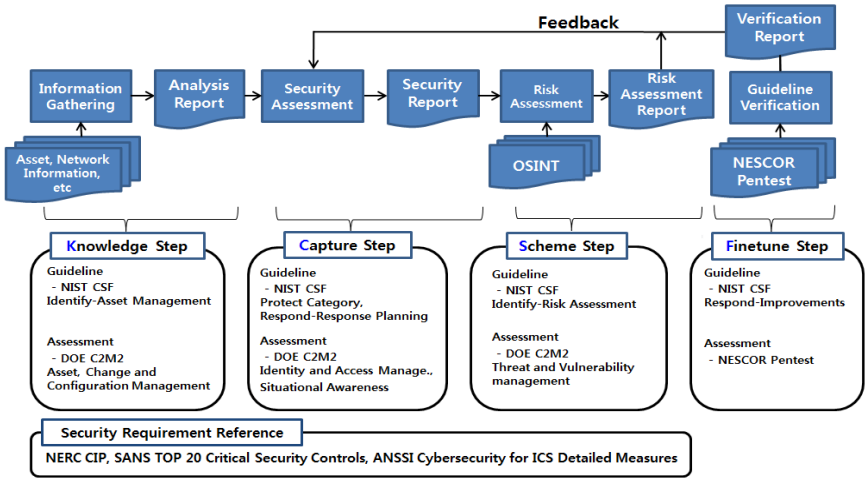

Fig. 5. Flow Chart of K-CSF and Major References

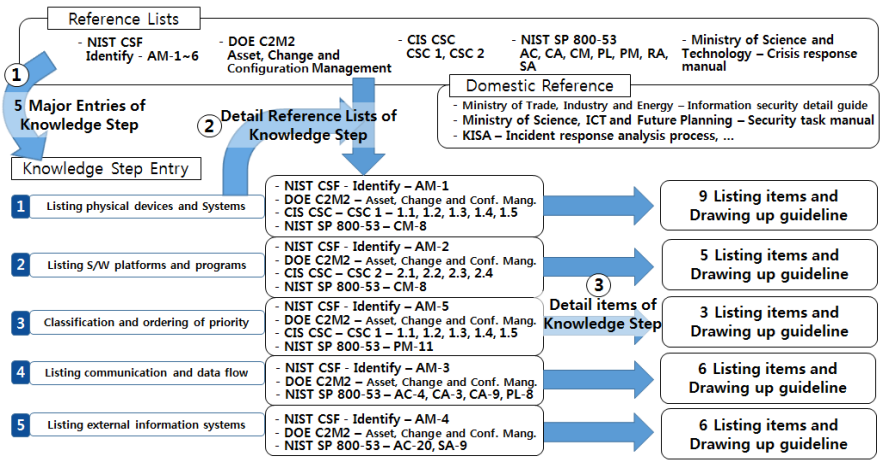

Fig. 6. Flow Chart of Knowledge Step Development

대해 각 항목에 해당하는 참고문서들을 분석하여 이 중 실제 기반시설 네트워크 관점에서 가이드라인 반영할 참고 항목들을 도출하였다. 마지막 단계에서는 도출한 참고 항목들을 통해 Knowledge 5항목의 각 세부 가이드라인을 작성하였으며 Fig. 6.은 이를 나타낸 것이다.

4.3 Capture 단계 세부 항목 도출

Fig. 7.은 Capture 단계 개발 개요도로 세부 항목 도출 과정은 크게 3단계로 나뉜다. 첫 번째 단계로 NIST [2]의 Capture 단계 관련 항목인 Protect의 참고문서 및 DoE [3]의 Identify and Access Managa Situational Awareness Domain과 관련 보안 가이드라인 참고문서[5-14]를 분석하였다. 이를 통해 기반시설 네트워크의 주요 보안 항목 10항목을 도출하였으며, 항목은 Access Control, Account Management, Information Flow, Configuration, Wireless Access Control, Physical Access Control, S/W Integrity, Remote Access Control, Continuous Monitoring and Logging,

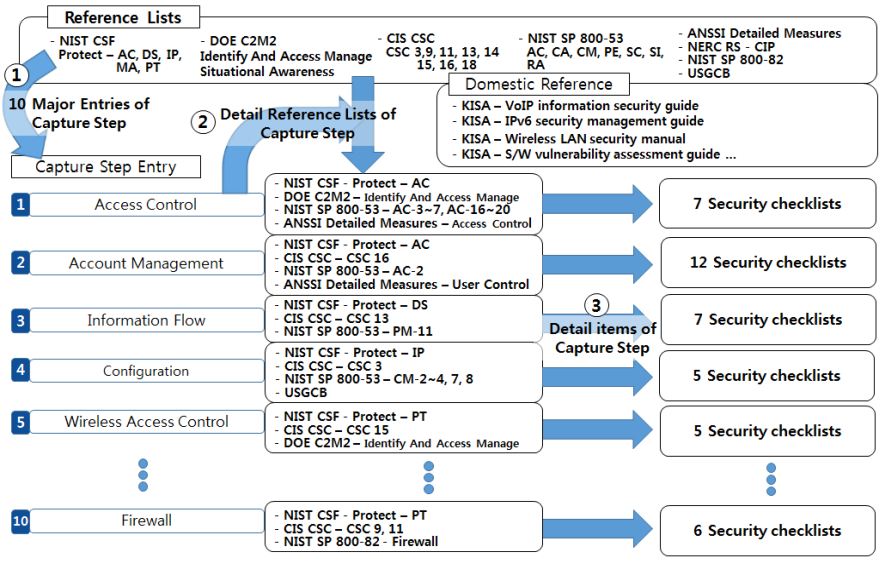

Fig. 7. Flow Chart of Capture Step Development

Firewall and Boundary Protection, S/W Development로 도출하였다. 두 번째 단계로 도출된 보안 항목에 대해 각 항목에 해당하는 참고문서들을 분석하여 기반시설 네트워크 관점에서 주요하게 판단되는 참고 항목들을 작성하였으며, 마지막 단계에서 이를 정리하여 각 보안 항목에 대한 세부 보안 점검 항목으로 가이드라인을 작성하였으며 총 71세부 항목이 작성되었다.

4.4 Scheme 단계 세부 항목 도출

Fig. 8.은 Scheme 단계 개발 개요도로 세부 항목 도출 과정은 크게 3단계로 나뉜다. 첫 번째 단계로 세부 항목 도출을 위해 NIST [2]의 Scheme 단계 관련 항목인 Identify-Risk Assessment의 참고문서 및 DoE [3]의 Threat and Vulnerability Management Domain을 분석하였다. 이를 통해 위협 및 취약성 수집, 위협 및 취약성 분석, 위협 및 취약성 대응방안 작성 단계를 도출하였다. 두 번째 단계로 도출된 Scheme 단계 항목에 대해 각 항목에 해당하는 참고 문서들을 분석하여 주요 참고 항목들을 작성하였으며 이를 기반 하여 마지막 단계에서 Scheme 단계의 세부 내용이 도출되었다. 위협 및 취약성 수집 단계에서는 주요 위협 및 취약점이 보고되는 ICS-CERT Alerts, ICS-CERT Vulnerability Notes, CVE Vulnerabilities, NVD(National Vulnerability Database) Checklist 및 제품의 제조사의 취약점 보고 사이트에서 정보 수집과 자산 정보를 이용하여 기본적인 Google 검색엔진을 포함한 Shodan, Censys, theHarvester, Pastebin을 활용한 공개된 정보 수집을 수행한다. 위협 및 취약성 분석 단계에서는 수집된 취약성 및 위협 정보에 대한 분석을 수행한다. 취약성의 경우 주로 취약한 시스템과 대응 방안에 대한 정보가 명확하고 추가적인 레퍼런스가 공개되어 분석과 활용이 수월할 수 있으나, 위협 정보의 경우 취약한 시스템에 대한 명확한 기술이 부족한 경우가 있어 이러한 경우 각 기관의 대상에 맞게 재해석을 통해 취약할 수 있는 시스템과 시스템이 침해 되었을 때에 대한 영향을 분석하여 대응방안을 도출하여야 한다. 이러한 분석에 기반하여 위협 및 취약성 대응방안 작성 단계에서 '위협 및 취약성 분석 보고서'를 작성한다. '위협 및 취약성 분석 보고서'의 작성 항목을 위해서는 CVE(Common Vulnerabilities and Exposures), Cisco Advisory, Symantec Alert를 분석하여 9항목을 도출하였다.

4.5 Fine-tune 단계 세부 항목 도출

Fine-tune 단계는 모의 침투 실험을 수행하여 가이드라인을 검증하며 피드백을 수행한다. 모의 침투 실험 절차를 위해 NESCOR(National Electric Sector Cybersecurity Organization Resource)의 전력제어시스템을 대상으로 한 모의 침투 실험 절차인 Guide to Penetration Testing for Electric Utilities[16], Guide to Vulnerability Assessment for Electric Utility Operations Systems[17]를 참고하여 모의 침투 실험 절차 및 임베디드 장비, 네트워크 통

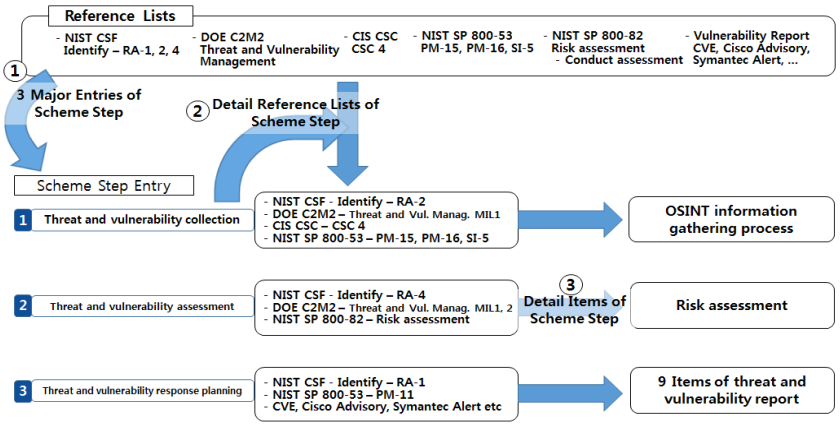

Fig. 8. Flow Chart of Scheme Step Development

신, 운영체제, 응용 프로그램에 따른 모의 침투 실험 기법을 도출하였다. 모의 침투 실험 절차는 주요 사항들에 대해 결정하는 Assessment Team Synchronization 단계, 대상 네트워크 및 시스템에 대한 정보를 수집하는 Information Gathering 단계, 실험 대상 기기를 확정하고 실험을 위해 필요한 유저 및 계정 정보를 파악하는 Enumeration 단계, 취약성 스캐닝 도구를 점검 및 스캐닝을 실시하는 Exploration 단계, 식별된 취약성을 문서화하는 Identification and Documentation 단계, 작성된 취약성 문서의 우선순위를 부여하고 추가적인 테스트를 수행할지 결정하는 Escalation and Repetition 단계로 구성되어 있다. 장비 유형 별 모의 침투 실험 기법에는 각 유형 별 요구되는 테스트 장비, 기법을 정리하였으며 Fig. 9.는 NESCOR 모의 침투 절차이다.

이러한 방법론과 구성을 통해 산업제어시스템 네트워크를 위한 사이버보안 가이드라인, K-CSF를 개발하였으며 이는 Knowledge 단계의 5단계, 29 목록화 항목, Capture 단계의 10점검 항목과 세부 점검 항목의 71개의 점검 항목, Scheme 단계의 세부 3단계와 취약성 분석 보고서 9항목, Fine-tune 단계의 모의 침투 실험 절차 6단계와 4가지 유형의 대상에 대한 모의 침투 실험 기법 55항목으로 구성하였다.

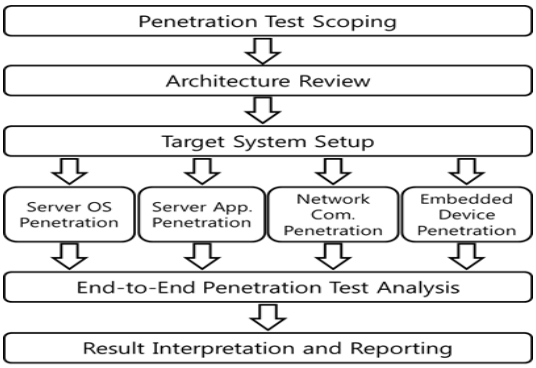

Fig. 9. NESCOR Penetration Testing Process

V. 가이드라인 검증 방안

가이드라인은 실제 기반시설 네트워크 망 구성정보를 수집하고 이에 기반 하여 가이드라인을 적용해야 한다. 그러나 실제 주요 기반시설 정보를 활용하여 검증 예시를 작성 하는 것은 기반시설 네트워크의 주요 정보를 노출 할 수 있어 불가능하다. 따라서 본 장에서는 이러한 점을 고려하여 개발된 기반시설 네트워크 가이드라인을 검증하기 위한 방안을 제시한다.

Knowledge 단계의 검증을 수행하기 위해 대상 네트워크를 설정하고 대상 네트워크에 대한 다양한 정보를 수집하여 29항목에 대한 목록화를 수행하여 대상 분석 보고서를 작성한다. 이때 수집되어 활용될 수 있는 항목으로는 네트워크 Diagram, H/W 자산 목록, 시스템 목록, S/W 및 버전 목록, 정책과 절차문서, 네트워크 모니터링 정보, 무선 네트워크 정보, 시스템의 정보흐름 Diagram, 시스템 관리자 및 사용자 정보 등이 있다. 작성된 대상 분석 보고서은 다음 단계에서 활용할 뿐만 아니라 허가된 장비 및 S/W 여부, 허가된 통신 여부, 상위 보안 데이터의 하위 보안기기로의 전송과 같은 비정상적인 데이터 흐름 등에 대한 보안 점검에 활용한다.

Capture 단계의 검증을 수행하기 위해 Knowledge 단계에서 작성한 대상 분석 보고서를 활용하여 각 기기 및 S/W, 네트워크에 대해 해당하는 Capture 보안 점검 항목을 통해 보안 점검을 수행하며 보안 점검 보고서를 작성한다.

Scheme 단계의 검증을 수행하기 위해 Knowledge 단계에서 작성한 대상 분석 보고서를 참고하여 S/W 이름 및 버전 등 자산의 주요 정보를 통해 공개된 위협 및 취약성을 수집한다. 수집된 위협 및 취약성은 기관에 맞게 재해석되어야 하며 이를 통해 위협 및 취약성 보고서를 작성하여 Capture 단계의 보안 점검 항목에 추가한다.

Fine-tune 단계의 검증을 수행하기 위해서는 대상 네트워크에 대해 식별된 취약점을 모의 침투 실험하여 가이드라인의 올바른 수행을 통한 보안 강화를 검증하며 추가적인 취약점을 식별하여 피드백을 수행한다.

VI. 결 론

본 논문에서는 산업제어시스템 네트워크를 위한 사이버 보안 가이드라인을 NIST CSF[2], DoE C2M2[3]와 여러 보안 요구사항 문서를 통해 개발하는 방안을 제시하고 이를 검증하기 위한 방안을 제시하였다. 가이드라인 K-CSF는 IIoT 환경을 고려하였으며 ICS 관련 공개된 취약성을 업데이트 하는 구조로 산업제어시스템 네트워크의 특성을 고려한 특

징을 가지고 있다. K-CSF는 총 4단계로 Knowledge 단계 5항목, Capture 단계 세부 10 보안 항목, Scheme 단계 3항목, Fine-tune 단계 6항목으로 구성되어 있으나 가이드라인은 정적으로 사용되는 체크리스트가 아닌, Capture 단계의 보안 점검 항목은 기본적인 보안 점검에 활용하며 Scheme 단계의 공개된 취약성 정보와 Fine-tune 단계의 모의 침투 실험을 통한 피드백으로 지속적으로 가이드라인을 개발해 나가는 구조이다.

본 연구는 기반시설 네트워크 사이버보안 관점에서 주요 항목만을 도출하여 조직의 운영과 정책적인 면을 포함한 방대한 범위의 사이버보안 가이드라인을 각 기관에서 독자적으로 개발 가능한 규모의 가이드라인으로 제시하였다. 또한 정부 기관의 정적인 사이버보안 가이드라인은 기반시설 네트워크의 특징을 반영하지 못하는 한계를 지닌 반면 본 연구에서는 각 기반시설 기관에서 기관의 특징을 반영하고 지속적으로 개발 가능한 가이드라인 개발방안을 제시 하여 기반시설 네트워크의 보안을 향상시킬 수 있는 방안으로 활용될 수 있을 것이다.

References

〔1〕 Industrial Control Systems Cyber Emergency Response Team, "NCCIC/ICS-CERT Year in Review FY 2015"

〔2〕 National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity", Feb. 2014

〔3〕 Jason D. Christopher, Foward Muneer, et al. "Cybersecurity Capability Maturity Model Facilitator Guide", The Department of Energy, Feb. 2014

〔4〕 North American Electric Reliability Corporation, "Reliability Standards for the Bulk Electric Systems of North America", Apr. 2015

〔5〕 Center for Internet Security, "The CIS Critical Security Controls for Effective Cyber Defense", Oct. 2015

〔6〕 Ronald S. Ross, Gary Stoneburner, et al. "Security and Privacy Control for Federal Information Systems and Organizations", National Institute of Standards and Technology, Apr. 2013

〔7〕 Yoojae Won, Dongmyung Shin, et al. "IPv6 security management guide", Korea Internet & Security Agency, Feb. 2010

〔8〕 Korea Internet & Security Agency, "Wireless security guide", Jan. 2010

〔9〕 Korea Internet & Security Agency, "Software vulnerability diagnosis guide", May 2012

〔10〕 Korea Internet & Security Agency, "VoIP security recommendation manual", Oct. 2012

〔11〕 Agence nationale de la sécurité des systèmes d'information, "Cybersecurity for Industrial Control System Detailed Measures", Jan. 2014

〔12〕 Keith Stouffer, Suzanne Lightman, et al. "Guide to Industrial Control Systems Security", National Institute of Standards and Technology, Jun. 2011

〔13〕 The Open Web Application Security Project, "OWASP Internet of Things Project", https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

〔14〕 National Institute of Standards and Technology, "The United States Government Configuration Baseline", https://usgcb.nist.gov/

〔15〕 Korea Ministry of Science and Technology, "Cyber security incident response executive manual"

〔16〕 Justin Searle, Galen Rasche, Andrew Wright and Scott Dinnage, "Guide to Penetration Testing for Electric Utilities" National Electric Sector Cybersecurity Organization Resource

〔17〕 Glen Chason, Scott Dinnage, et al. "Guide to Vulnerability Assessment for Electric Utility Operations Systems", National Electric Sector Cybersecurity Organization Resource, Jun. 2014

〈저자소개〉

권 성 문 (Sungmoon Kwon) 학생회원
2013년 2월: 아주대학교 정보컴퓨터공학부 공학사
2013년 3월~현재: 아주대학교 대학원 컴퓨터공학과 석박사통합과정
〈관심분야〉 스마트그리드 보안, 디지털 포렌식, 비정상행위 탐지

이 석 철 (Seokcheol Lee) 학생회원
2012년 2월: 아주대학교 정보 및 컴퓨터공학부 공학사
2012년 3월~현재: 아주대학교 컴퓨터공학과 석박사통합과정
〈관심분야〉 스마트그리드 보안, 디지털 포렌식, 네트워크 보안

장 지 웅 (Jiwoong Jang) 정회원
2003년 2월: 한양대학교 전자전기공학부 졸업
2007년 2월: 한양대학교 경제금융대학 석사
2009년 2월: 한양대학교 경제금융대학 박사수료
2013년 8월: 고려대학교 정보보호대학원 석사
2016년 9월~현재: 고려대학교 정보보호대학원 박사과정
2003년 8월~현재: 전력거래소 정보보안팀 차장
〈관심분야〉 제어시스템 보안, 보안경제학

손 태 식 (Taeshik Shon) 종신회원
2000년: 아주대학교 정보및컴퓨터공학부 졸업(학사)
2002년: 아주대학교 정보통신전문대학원 졸업(석사)
2005년: 고려대학교 정보보호대학원 졸업(박사)
2004년~2005년: University of Minnesota 방문연구원
2005년~2011년: 삼성전자 통신/DMC 연구소 책임연구원
2011년~현재: 아주대학교 정보통신대학 사이버보안학과 부교수
2017년~현재: Illinois Institute of Technology 방문교수
〈관심분야〉 산업제어시스템 보안, 비정상행위탐지, 디지털 포렌식