韓國IT서비스學會誌
第15卷 第4號
2016年 12月, pp.63-72

Journal of Information Technology Services
https://doi.org/10.9716/KITS.2016.15.4.063

주요기반시설 서비스의 안정적 운영을 위한 보안 프레임워크 설계에 관한 연구

이수연* · 유지연** · 임종인***

A Study on the Security Framework Design for Stable Operation of Critical Infrastructure Service

Suyeon Lee* · Jiyeon Yoo** · Jongin Lim***

■ Abstract ■

Critical infrastructure has been operating in a closed environment with a completely separate information system and in the private area. However, with the current ICT environment changes due to convergence and open platforms it has increased the threats and risks to critical infrastructure. The importance of cyber security is increasing in the infrastructure control system, such as the outbreak of Ukraine blackout in 2015 by a malicious code called 'black energy'.

This thesis aims to recognize the importance and necessity of protecting the critical infrastructure service, designing a security framework reflecting environmental and characteristic changes, and analyzing the management system suitable for a security framework. We also propose a theoretical basis for constructing a new security framework by comparing and analyzing seven international security management system standards, such as NIST 800-82 and IEC 62443-2-1, which are used in the control system.

As a result, the environment surrounding critical infrastructure changes with the characteristics of connectivity, openness, and finality was studied, and as a response to this, many scholars and institutions present critical infrastructure security frameworks as cycle enhancement type structures, risk management structures, and management domain expansion structures. In response, the security framework encompassing these structures, CISF (Critical Infrastructure Security Framework), was designed. Additionally, through the security related international standard and criterion analysis, as a newly designed security standard suitable for CISF, IEC 62443-2-1 is reviewed and suggestions are made.

Keyword : CISF(Critical Infrastructure Security Framework), Critical Infrastructure, IEC(International Electrotechnical Commission) 62443-2-1, Security Framework

Submitted : October 11, 2016 1st Revision : November 18, 2016 Accepted : November 21, 2016

* 고려대학교 정보보호대학원 박사과정, 주저자
** 상명대학교 일반대학원 지식보안경영학과 조교수
*** 고려대학교 정보보호대학원 교수, 교신저자

1. 서 론

과거 주요기반시설은 각 설비별 독자적인 운영체제와 응용 프로그램을 사용하는 등 정보시스템 및 민간 영역과 완전히 분리된 폐쇄적인 환경에서 운영되었다. 그러나 최근 주요기반시설 서비스가 ICT 융합 및 개방형 플랫폼을 채택하고 모바일 환경 연동이 증가하는 등 주요기반시설을 둘러싼 환경이 변화하고 있다(Im, 2011).

이처럼 주요기반시설 서비스와 이를 관리하는 제어시스템이 민간영역의 IT서비스와 연결되고, 개방성을 보유하게 됨으로써 서비스 운영 간소화 및 관련 비용 절감이라는 효과성이 높아진 반면 관리 및 유지 활동은 통상적인 방법으로 이루어짐에 따라 새로운 보안 위협이 증가하고 있다.

우리나라의 경우 지난해 한수원, 올해 코레일, 서울메트로 등 국가기반시설을 대상으로 해킹이 증가하였는데 이러한 사고의 내용을 살펴본 결과 인터넷에서 무료로 다운받을 수 있는 간단한 악성코드를 통한 공격이었다. 또한 해킹 사실을 몇 개월이 지난 후 다른 기관의 통지로 인해 뒤늦게 인지하였고, 심지어 코레일은 보안부서의 PC가 해킹 당해 중요 자료가 유출되기도 하였다(Lee, 2016).

위와 같은 위협이 증가하고 있는 상황에서 주요국은 주요기반시설 보안 강화에 큰 노력을 기울이고 있으며 관련 연구 및 제도·정책이 체계적으로 수립되고 있다. 그러나 국내의 경우 주요기반시설 보호를 위한 정책 및 제도는 주요정보통신기반시설 보호에 관한 거버넌스 체계 및 관리 프로세스 중심으로 추진되고 있으며 관련 연구 및 정책 분석 또한 제도 및 기술에 한정되어있다. 또한 제어시스템의 중요성 및 활용성이 확대됨에 따라 새로운 위험이 증가하고 있음에도 단순히 침해행위에 대한 대비 및 대응에만 치중하는 등 지속적으로 순환하는 과정으로써의 위험관리 프로세스는 구축되어있지 않은 상황이다.

따라서 본 논문에서는 주요기반시설 서비스의 중요성 및 보호의 필요성을 인식하고 환경 및 특성 변화를 반영한 프레임워크를 설계하고 프레임워크에 적합한 보안 표준을 분석하는 것을 목표로 한다.

2. 주요기반시설 보호의 정의 및 관리 체계의 소개

2.1 주요기반시설의 정의

주요기반시설(Critical Infrastructure)은 국가에 필수적인 시스템 및 물리적 또는 가상의 형태의 서비스를 의미한다(Alcaraz and Zeadally, 2015). 국가 별로 주요기반시설의 정의 및 해당 시설은 상이하나 국가적 상징성, 에너지 및 통신 네트워크 등 인프라에 대한 의존성, 다른 인프라와의 상호연결성과 같은 세 가지 요소를 통해 주요기반시설을 개념화할 수 있다(Bahşi and Maennel, 2015). 사회는 수자원, 웹 서비스, 버스 서비스와 같은 필수 서비스를 제공하는 국가 인프라(CI)에 점점 더 의존하고 있으며 조직 및 CI사이의 상호연결이 증가하고 있다. 이러한 상황 속에서 주요기반시설 서비스의 중단은 국가적 안보, 경제, 공공의 보건 또는 안전에 심각한 영향을 미칠 수 있다(Alcaraz and Zeadally, 2015).

2.2 주요기반시설을 둘러싼 환경의 변화 및 보호의 필요성

주요기반시설을 둘러싼 환경이 개방적 환경으로 변화하고 있으며 이들 시설 내 IT 환경이 Shadow IT 등을 통해 새로운 위험요소가 등장하고 있는 것으로 분석되고 있다(Yoo and Jeong, 2016). 이로 인하여 주요기반시설에 대한 새로운 보안 위협이 지속적으로 증가하며 발생하고 있다. 대표적인 사례들을 살펴보면 <Table 1>과 같다.

ICT 융합 및 개방형 플랫폼 채택으로 인한 주요기반시설의 복잡성과 연결성, 데이터 보유량의 증가로 취약점이 증가하고 있는데 반해 규제표준

〈Table 1〉 Cyber Accident Case Summary

Year	Hacking Accident	The details
2009	US Power Net Cyber Spy Penetration	Power interruption in US power grid by malware distributed by Chinese and Russian agents
2010	Iran Nuclear Facilities Attack	The raid on Iran's nuclear facilities by infiltrating malicious codes, and by 2010, the raid was carried out by about 1,000 centrifuges that had been physically destroyed by the state of the country, which led to the development of cyber weapons for the first time in the country.(Stuxnet)
2014	German steel company control system attack	A report from a German steel company reported that the damage caused by the damage caused by cyber attacks resulted in a failure to operate the plant, causing a lot of damage to the blast system, preventing the blast from being disrupted by the blast.
2014	Japan monju nuclear power plant malicious code infection	A case in point is the malware infection in the PC used by the monju Nuclear Power Plant in Japan. Malicious codes were manufactured to collect information from the central government and major enterprises in Japan, and were updated using updated server servers in Japan to provide services in Japan.
2014	Korea Hydro & Nuclear Power Hacking Accident	It was attacked by a hacker known as "Anti-nuclear group" or "Who am I" on December 9, 2014. Using KHNP employee's e-mail address sent to KHNP employees to induce malicious code infection
2015	Ukrainian Power Network Hacking Accident	An incident occurred at the Ukrainian beullerereugo Power Station, which resulted in the interruption of a jeollyeok power supply, which resulted in a malicious code containing malicious codes, malware, and malicious codes inserted through e-mail.
2016	German nuclear power plant infection	On April 24, 2016, a malicious code was found in the IT network of the Fuel Treatment System in the IT of the Fuel Treatment System in Germany. The Atomic Power Plant Operational Seal(assumed) is responsible for preventing the nuclear power plant from leaking to the nuclear power plant, preventing malicious codes from being connected to the network, and by an error detected by an infected USB usage system(assumed by an infected USB usage).

의 부족과 사고의 공개를 꺼리는 풍토, 충분하지 않은 사고 대비, 제한된 협업 및 정보공유가 주요기반시설에 대한 위험평가 및 보안의 태세와 투자가 충분하게 이뤄지지 않고 있다(Nanni, 2015).

3. 주요기반시설 보호를 위한 프레임워크 설계

주요기반시설을 둘러싼 환경이 연결성, 개방성, 목적성과 같은 새로운 특성을 가지게 되는 과정에서도 국내의 경우 이에 대응하는 조치를 취하지 못하고 있으며 단순히 침해행위에 대한 대비 및 대응 외에 지속적으로 순환하는 과정으로써의 위험관리 프로세스를 구축하고 있지 않다.

그러나 여러 국가에서는 주요기반시설별 관할 정부기관간의 유기적인 연계로 사이버위협 발생 시 관련 정보를 신속하게 전체 기반시설이 공유할 수 있는 시스템 구축과 사이버보안 강화를 위한 기본적인 보안 시스템 구축의 표준 프레임워크를 적극적으로 도입하고 있다.

따라서 본고에서는 여러 학자 및 기관이 제시했던 '주요기반시설 보안 프레임워크'의 정리 및 분석을 통해 주요기반시설 보호 및 기존 보안 관리체계의 개선을 위한 프레임워크를 새롭게 도입하고자 한다.

3.1 선행연구 정리

주요기반시설을 효과적으로 보호하기 위한 다양한 학자들의 보안 프레임워크에 대한 내용을 요약 및 정리하면 <Table 2>과 같다.

〈Table 2〉 Listing of Preceding Studies on Critical Infrastructure Security Framework

Reference	Requirements for framework	
Sodoma (2007)	This paper suggests the Microsoft model as having 7 stages to protect critical infrastructure. The 7 stages are composed of goal and role definition, identification of important functions and priorities, continuous evaluation and risk management, contingency plan establishment and training, public-private partnership establishment, establishment of security/flexibility for the work, technology/process update and innovation. In particular, the continuous evaluation and risk management stage emphasizes the cycle structure to enhance the risk management as it goes through processes such as risk evaluation, control identification and relaxation, control development, effectiveness measurement, etc.	Cycle enhancement type structure
Bahşi and Maennel (2015)	For the identification of critical information infrastructure(CII) service, 360° feedback framework according to 8 stages was suggested. The framework is composed of goal-setting and CII operator identification and standard setting, BIA and risk evaluation application, CII service identification, continuity plan report, cyber dependency identification and final list preparation. The framework is made through information sharing and cooperation among the decision maker, strategic operator and cooperating organizations of the country, and each stage also has the form of cycle structure to exchange feedback.	
Suter (2007)	To protect critical national infrastructure and services, a CIIP unit function model that can promote the cooperation among the existing bodies of interest was suggested. The function model is composed of 4 elements, which added a risk management cycle and crisis management such as prevention and early alarm, detection, response, etc. The CIIP unit requires different organizations, technologies, and analysis capabilities to carry out 4 tasks of the function model, and to save cost and manpower and to improve efficiency. It emphasizes the necessity of close cooperation with government organizations, an analysis(situation) center, and a specialized technology center such as CERT, etc.	Risk management structure
Jeimy et al. (2014)	The comprehensive framework responds to fast changes and new threats of the SCADA system was suggested. The framework is composed of 6 areas including management control, SCADA control, data and application program security, system assurance, monitoring and outsider control and 22 lower level sections. Such framework is asserted to be comprehensive, shall evolve according to the changing environment, shall satisfy the SCADA system's availability and general risk management and performance requirements, and shall have the characteristics of having compatibility with other standards.	Management domain expansion structure
Langner (2013)	For efficient and sustainable industry control system security, RIPE framework having the composition elements of the characteristics of the system entity, network architecture, composing elements, role and responsibility of manpower, development of the technology and capability of manpower, procedure guidelines, design and composition change, and system acquisition, etc. was suggested. Each area is in charge of process operation and physical facility control, and by integrating framework management domain and procedure in the control system operation, it emphasized the importance of cyber security with effective procedure and cost, and it tried to establish the responsibility for ICS security and safety.	

선행연구를 정리한 결과 주요기반시설을 보호하기 위한 프레임워크는 각각 위험관리, 프로세스, 관리 도메인을 중심으로 구성되는 등 형태는 상이하나 공통적으로 주요기반시설의 필수 서비스 및 주요 의무와 책임 식별과 다양한 이해관계자간의 협력을 중요시하게 여기는 특성을 지니고 있으며 끊임없이 변화하는 환경 및 특성에 적응할 수 있는 유연한 프레임워크가 필요함을 주장하고 있다.

3.2 프레임워크의 구성

본 절에서는 새로운 프레임워크를 구성하기 이전에 각 프레임워크가 주요기반시설의 보호를 위해 접근하는 방식과 필요한 요구사항을 <Table 3>에 정리하였다.

〈Table 3〉 Critical Infrastructure Security Framework Requirements

Properties	Requirements	Reference
Cycle enhancement type structure	Technology and process update and innovation	Sodoma (2007)
	Public-private partnership establishment	
	Cycle structure	Sodoma (2007) Bahşi and Maennel(2015)
	Comprehensive framework	Bahşi and Maennel(2015)
	Information sharing	
Risk management structure	Promotion of cooperation among bodies of interest	Suter (2007)
	Flexibility and applicability	
	Cost efficiency	
	Identification of mandatory business, major duties, and responsibilities	
	Information and experience sharing	
	Domestic and international network	
	Non-technical protection	
	Cycle structure	
	Integration to overall crisis management structure	
	Periodical training	
Management domain expansion structure	Comprehensive framework	Jeimy et al. (2014)
	Flexibility and adaptability	
	System availability	
	Satisfying system's risk management and performance requirements	
	Efficiency, expandability, and sustainability	Langner (2013); Jeimy et al. (2014)
	Integrating framework to overall operation	Jeimy et al. (2014)

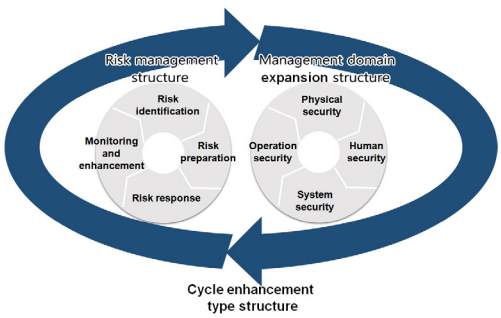
<Table 3>에 기술된 것과 같이 단계중심의 프레임워크는 주요기반시설의 보호 목표 및 역할 정의부터 변화하는 환경에 따른 적응 및 업데이트까지 각 보호 단계마다 공공-민간의 파트너십 및 정보공유를 강조하는 순환구조의 프레임워크를 지향하며 위험관리 중심의 프레임워크는 전체적인 위기관리 구조에 포함될 수 있는 절차·비용이 효율적인 프레임워크를 지향한다. 또한 국내 및 국제 네트워크를 활용한 정보·경험의 공유 및 협력체계, 변화하는 위협 환경에 대응할 수 있는 적응성과 유연성을 갖춘 순환구조를 지닐 것을 강조한다.

마지막으로 관리 도메인 중심의 프레임워크는 효율성, 확장성 및 지속가능성에 초점을 맞추어 전체적인 운영체계 및 시스템에 통합될 수 있는 포괄적인 프레임워크를 주장한다.

이처럼 각 프레임워크가 주요기반시설 보호를 위해 중점을 두는 특성은 다르지만 프레임워크 구성 요구사항은 유사함을 알 수 있다. 또한 주요기반시설의 기본 특성 및 환경의 변화를 잘 반영하면서도 효과적으로 보호하기 위해서는 다차원적이고 각 프레임워크 영역이 상호작용하는 순환 구조를 지녀야 함을 알 수 있다(Jeimy et al., 2014).

따라서 본 논문에서는 위험관리, 관리 도메인을 모두 고려하면서도 각 영역 스스로 뿐만 아니라 전체 구조가 상호작용하는 순환구조를 지니는 프레임워크를 설계하고자 한다.

아래의 <Figure 1>은 새롭게 설계한 프레임워크 구조를 나타낸 그림이다.



〈Figure 1〉 Critical Infrastructure Security Framework

3.2.1 순환 개선형 구조

프로세스는 직접적으로 드러나지는 않지만 전체적인 프레임워크의 각 단계가 P-D-C-A(plan-do-check-act) 및 단계적으로 진행되는 구조를 의미한다. 그래서 이러한 단계는 프레임워크 내 가장 상위 항목으로 설정한다. 계획, 수립, 실현, 운영, 모니터링, 검토, 유지보수, 그리고 지속적 개선 모델로서 이러한 구조는 국제표준에서 효과성 향상 및 지속적 개선 모델로서 활용되고 있다.

Plan은 요구, 요구사항, 범위 등의 조직환경 및 전략목표 수립, 이해관계자와 지속적 통제 항목에 관련된 요구사항을 통제하는 단계이고 Do는 요구사항에 중점을 두어 접근하는 방법을 결정하고 관리하는 절차를 개발하는 단계이며 Check는 수행도 측정에 필요한 요구사항을 요약하고 피드백하는 단계이다. Act는 부적합을 식별하도 시정조치를 수행하는 단계이다.

3.2.2 위험관리 구조

위험관리 구조 중심의 프레임워크는 <Table 3>에서 알 수 있듯이 다른 두 개의 프레임워크 구성요구사항을 포함할 수 있는 가장 폭 넓은 구성을 지니고 있다. 또한 위험관리 자체가 위험 식별, 위험 대비, 위험 대응, 모니터링 순서의 순환구조로 구성되어 있기 때문에 프레임워크 내 주요 항목으로 설정한다.

위험 식별은 주요기반시설 내 자산 및 서비스를 식별한 후 기술·물리·인적 측면에서 발생가능한 위험을 식별하는 것을 의미한다.

위험 대비 항목에는 발생가능 한 위험을 대비하기 위해 조직이 미리 구축해 놓을 수 있는 보안정책, 조직 및 자산 관리 등이 포함되며 위험 대응은 위험에 대응하기 위한 여러 관리 요소의 집합으로 관리 도메인에 해당하는 물리적, 기술적, 인적, 관리적 보안 등으로 구성된다. 모니터링 및 개선 프로세스에는 위험평가 및 대응 모니터링 수행을 통해 도출된 결과를 다시 위험 식별 프로세스에 재 적용시킴으로써 위험관리 방법을 점차 발전시켜 나가는 순환 형태를 가지며 지속가능성이라는 속성을 가진 하위 항목으로 구성된다.

위험관리의 가장 큰 특징은 주요기반시설 서비스의 중단에 대한 복원력 강화를 위해 식별 및 대비와 같이 예방적 측면을 강조하는 포괄적인 형태를 지닌다는 것과 기술적 및 비 기술적인 정보 및 경험을 공유하는 협력체계가 필요하다는 것이다(Maennel, 2016).

3.2.3 관리 도메인 확장 구조

관리 도메인 확장 구조는 위험관리 프로세스의 하위 항목으로 물리적, 기술적, 인적, 관리적 보안으로 나눌 수 있으며 그 세부 항목으로 물리적·운영·시스템·인적보안 및 접근 통제 등으로 구성된다.

각 관리 도메인은 주요기반시설 시스템 및 서비스에 대한 가용성, 포괄적이고 변화하는 위협 환경에 맞게 진화할 수 있는 유연성 및 적응성, 적용 가능한 다른 표준과의 호환성 및 확장성을 가져야 하며 각 구성항목은 상호작용을 통해 복합적으로 작용하기도 한다(Jeimy et al., 2014).

본 프레임워크에서는 주요기반시설의 효율성 및 지속 가능성을 위해 한쪽 영역에만 치우치지 않고 전체적인 측면에서 모든 관리 도메인이 적절하게 포함되어야 함을 강조한다.

3.3 프레임워크의 특징

본 프레임워크는 위험관리 과정의 순환뿐만 아니라 관리 도메인 및 프로세스까지 전체적인 구성요소가 서로 피드백을 통해 주요기반시설의 보안 수준의 향상을 목표로 하는 순환 구조를 띈다.

또한 ISO27019 및 NERC CIP 등의 특정 산업 대상의 가이드라인의 비교·분석에도 적용이 가능하다.

따라서 본 논문에서는 프레임워크를 활용하여 주요기반시설 보호와 관련한 여러 표준을 재정리하고 및 비교·분석을 통해 가장 효과적인 보호에 알맞은 표준을 도출하고자 한다.

4. 주요기반시설 보호를 위한 국제 표준 및 기준 비교 분석

ISO와 같은 국제기관 및 국가 산하 조직에서는 주요기반시설의 서비스 및 시스템 보호를 위해 다양한 표준 및 지침을 수립하고 있다. 이러한 표준 및 지침은 다양한 주요기반시설의 요구사항 및 중요자산 및 관리 현황에 맞게 변경하여 활용되거나 국가적 차원의 관리 및 인증체계로 발전하여 좀 더 강력한 보안을 위해 사용되고 있다.

따라서 본 장에서는 기존의 주요기반시설 보호와 관련된 여러 표준 중 주요기반시설을 둘러싼 환경 및 특성 변화를 잘 반영하고 발생가능 한 위험의 식별 및 대응, 서비스 중단 상황에서의 복원력(회복탄력성) 강화에 가장 적절한 표준을 도출하고 이를 주요기반시설의 보안을 위한 관리체계로 발전 및 개선하기 위해 비교·분석을 수행하고자 한다.

〈Table 4〉 Comparison of Security Management Standard

Process	Category		ISO 27001	NIST 800-53	NIST 800-82	IEC 62443-2-1	ISO 27019	NERC CIP 002-009
Cycle structure			–	–	–	◉	–	–
Risk identification	Asset identification and management		◉	◉	◉	◉	◉	◉
	Risk identification and evaluation		◉	◉	◉	◉	–	○
Risk preparation	Security policy		◉	◉	◉	◉	◉	◉
	Security organization		◉	○	○	◉	◉	–
	Education and training		◉	◉	◉	◉	○	○
	External requirements		○	–	–	○	◉	–
Risk response	Human security	Insider security	◉	◉	◉	◉	◉	○
		Outsider security	◉	○	○	–	◉	–
	System security	Development security	◉	◉	◉	○	◉	–
		Composition management	–	◉	◉	◉	○	○
		System evaluation and certification	–	◉	◉	○	–	–
		Password control	◉	○	○	○	◉	○
	Operation security	Operation procedure and change management	◉	○	○	○	◉	○
		System and service operation	◉	◉	◉	◉	○	◉
		Electronic trade and information transmission	◉	–	–	–	◉	–
		Entity security	◉	◉	◉	–	◉	–
		Log management and monitoring*	◉	–	–	○	◉	◉
	Physical security		◉	◉	◉	◉	◉	◉
	Access control and network partition		○	◉	◉	◉	◉	○
	Threat detection and removal		–	○	○	–	○	–
	Accident management and response		◉	◉	◉	◉	◉	◉
Monitoring and enhancement	Business continuity management		◉	◉	◉	◉	◉	◉
	Internal audit**		○	◉	◉	◉	–	–
	Post management**		◉		–	◉	–	○

* 정보시스템, 응용 프로그램, 보안시스템, 네트워크 장비 등에 대한 로그 관리 및 모니터링에 해당.

** 보안사고 및 이벤트, 인적 보안 등 한 영역에 한정된 것이 아니라 전체적인 거버넌스 측면에서의 내부감사 및 사후관리에 해당.

4.1 비교 대상 및 기준

본 논문에서는 국내에서 주요정보통신 기반시설의 주요 정보자산을 보호하기 위해 수립된 정보보호 관리절차와 과정을 지속적으로 관리 및 운영하기 위한 종합적인 체계인 ISO/IEC 27001과 NIST의 정보시스템 관리 가이드라인인 NIST 800-53(rv.4) 및 산업제어시스템 보호를 위한 가이드라인 NIST 800-82, ISO/IEC 27001을 보완하기 위해 기반시설의 특수성을 반영하여 작성된 표준인 IEC62443-2-1, 특수영역의 제어시스템 보호를 위한 표준인 ISO27019, NERC CIP까지 총 9개의 표준을 비교·분석하여 효과적인 관리체계로 도출해내고자 한다.

특히 비교 기준의 경우에는 가장 상위 항목에 해당하는 위기관리를 가장 대분류로 설정하고 위기관리 각 프로세스에 해당하는 물리적, 기술적, 관리적, 인적 측면의 인증 항목들을 재배치하여 구성하였다. 또한 프레임워크가 주요기반시설 보호의 각 영역별뿐만 아니라 전체적인 관점에서 서로 상호작용하여 발전시켜나가는 순환구조의 특징을 지고 있기 때문에 이를 대분류에 추가하여 기존 표준 중 순환구조를 강조하는 표준을 도출해내고자 하였다.

4.2 비교분석의 수행

비교 방법의 경우 앞 절의 비교 대상 및 기준을 이용하여 각 기준 별 비교를 수행하였으며 대분류 및 세부항목이 각 표준의 항목과 매우 유사할 경우에는 '◉' 표시를 항목의 이름 및 기능이 유사하나 구체적인 범위 및 방법에 차이가 있을 경우 '○'표시, 기능 및 범위가 서로 상이한 경우에는 '-' 표기를 수행하였다. 또한 음영을 통해 각 표준의 특징적인 항목을 따로 표시하였다.

앞선 <Table 4>는 제 3장에서 도출해낸 '주요기반시설 보호를 위한 프레임워크'를 기준으로 각 표준 항목을 비교하여 나타낸 표이다.

위의 비교를 수행한 결과 프레임워크에 가장 적합한 표준은 IEC62443-2-1임을 알 수 있었다. IEC62443-2-1 표준은 위험관리 중심의 순환구조를 지닌 표준으로써 각 관리 도메인별 세부항목이 골고루 포함되어 있으며 기반시설의 특성을 잘 반영한 표준이다. 또한 ISO27019, NERC CIP표준과 같이 특정영역에 초점이 맞춰져있지 않기 때문에 국내 주요기반시설의 서비스 및 시스템과 관리 현황에 맞게 변경하여 사용할 수 있는 유연한 '플랫폼'이라는 장점을 가지고 있다.

이상의 분석을 통해 주요기반시설 보호를 위한 프레임워크에 가장 적합한 표준으로 IEC62443-2-1을 도출해냈다. 이 표준 자체는 하나의 플랫폼으로써 각 주요기반시설에서 자발적으로 사용할 수 있으나 한편으로는 우리나라 상황에 적합한 관리체계로의 개선이 요구된다.

5. 결 론

본 연구에서는 주요정보통신기반시설의 제어시스템과 정보시스템과의 연결성(통합성)이 증가함에 따라 나타나는 보안 위협과 위험에 대응하여 요구되는 보안관리체계의 프레임워크를 제시하고자 추진되었다.

본 연구의 결과 분석과 시사점을 정리하면 다음과 같다.

주요정보통신기반시설의 제어시스템은 정보시스템 특성과는 달리, 종합 위협 변화 프로파일을 충족하도록 진화되어야 하며 제어시스템의 가용성 요구 사항을 충족시켜야 한다. 그리고 제어시스템의 일반적인 위험 관리 및 성능 요구 사항을 충족하며 적용 가능한 다른 표준과 규정을 충족 확장하여야 함을 확인하였다.

이에 주요정보통신기반시설의 제어시스템에 적용될 프레임워크는 위험관리 차원의(식별-대비-대응-모니터링/개선) 각 도메인별로(관리적, 물리적, 기술적, 인적) 프로세스적(PDCA : Plan-Do-Check-Act) 추진을 포함한 순환 개선형 구조의 프레임워

크를 제시한다.

본 연구는 학술적 관점에서 주요정보통신기반시설의 특성과 요구사항을 분석하고 관련 표준을 비교분석하여 새로운 프레임워크를 제시하였다는 점에서 의미가 있다. 실무적 관점에서는 현재 개선 논의가 제기되고 있는 주요정보통신기반시설 관리 및 인증체계에 대한 개선방안을 제시하였다는 점에서 정책의 기초자료로 활용이 높을 것으로 판단된다.

본 연구는 주요정보통신기반시설의 특수성으로 인한 실증 분석이 아쉬우며 향후에는 제시된 프레임워크를 반영한 관리체계를 마련하고 주요 정보통신 기반시설 보호대책으로의 타당성을 확보와 단계별・수준별 항목 중요성 평가 연구가 필요하다.

References

Alcaraz, C. and S. Zeadally, “Critical Infrastructure Protection : Requirements and Challenges for the 21st Century”, *In International Journal of Critical, Infrastructure Protection(IJCIP),* Vol.8, 2015, 53-66.

Bahşi, H. and O.M. Maennel, “A Conceptual Nationwide Cyber Situational Awareness Framework for Critical Infrastructures”, *Secure IT Systems*, Vol. 9417, 2015, 3-10.

Im, K.H., “Control System Security Vulnerabilities and Countermeasures”, Korea University, 2011.

(임길환, “제어시스템 보안취약점현황 및 개선방안 연구”, 고려대학교 석사학위논문, 2011.)

Jeimy, J., M. Cano, and Ph.D, CFE, “The Information Security Function : Current and Emerging Pressures From Information Insecurity”, *ISACA Journal,* Vol.6, 2014.

Langner, R., “The RIPE Framework : A Process-Driven Approach towards Effective and Sustainable Industrial Control System Security”, *Langner Communications GmbH*, 2013.

Lee, H.J., “The Study on Security Enhancement of National Control System for Critical Infrastructure : Focusing on Comparison about Policy of Major Countries and Domestice”, Sangmyung University, 2016.

(이현주, “국가기반 강화를 위한 제어시스템 보안 대응 연구 : 주요국과 한국의 정책 비교중심으로”, 상명대학교 석사학위논문, 2016)

Nanni, G., “Security Posture for Critical Information Infrastructure Protection(CIIP)”, *RSAC Conference,* 2015.

Sodoma, P., “Resiliency Rules : 7 Steps for Critical Infrastructure Protection”, Microsoft, 2007.

Suter, M., “A Generic National Framework For Critical Information Infrastructure Protection(CIIP)”, *Center for Security Studies,* ITU, 2007.

Yoo, J.Y. and N.Y. Jeong, “A Study on the New Management System Considering Shadow IT”, *Journal of Information Technology Services,* Vol.15. No.3, 2016, 33-50.

(유지연, 정남영, “Shadow IT를 고려한 새로운 관리체계 도입에 관한 연구”, *IT서비스학회*, 제15권, 제3호, 2016, 33-50.)

About the Authors

No Image

Suyeon Lee (llsyeon33@gmail.com)

Researcher Suyeon Lee is currently a PhD student at Korea University Graduate School of Information Security. She submitted various research papers in the field of cyber security control and information security management system. Also, Her interests are in the policy of cyber security and network forensics.

Jiyeon Yoo (yooo@smu.ac.kr)

Jiyeon Yoo is currently a Professor of Sangmyung University. She received her Ph.D. in Information Management Engineering from Korea University. Her current research interests include Information Strategy, IT Management System, and Cyber Security etc.

Jongin Lim (jilim@korea.ac.kr)

Professor Jongin Lim is currently a Professor of Graduate School of Information Security at Korea University. He served as a special advisor to the security advisor in 2015~2016. Also, He published many papers on cryptography and cyber security. Currently, he is working as the head of Cyber Defense Research Center, Graduate School of Information Security, Korea University.