https://doi.org/10.21289/KSIC.2020.23.2.333 KSIC

프레임워크 기반 스마트시티 사이버 보안 메트릭스

Framework Based Smart City Cyber Security Matrix

김성민[1], 정혜선[2], 이용우[3*]

Sung-Min Kim[1], Hae-Sun Jung[2], Yong-Woo Lee[3*]

〈Abstract〉

In this paper, we introduce a smart city-cyber-security-grid-matrix methodology, as a result of research on overall cyber security of smart cities. The identified cyber security risks that threaten smart cities and smart-city-cyber-security-threat list are presented. The smart-city-cyber-security-requirements necessary to secure the smart city cyber security with the developed smart city-cyber-security-grid-matrix are given in this paper. We show how the developed smart city-cyber-security-grid-matrix methodology can be applied to real world. For it, we interlocked the developed smart city-cyber-security-grid-matrix methodology with the cyber-security-framework of the National Institute of Standards and Technology, and developed a framework-based smart city-cyber-security-grid-matrix. Using it, it is easy and comfortable to check the level of cyber security of the target smart ciy at a glace, and the construction and operation of the smart city security system is systematized.

Keywords : Smart-City, Smart-City-Cyber-Security, Framework, Smart-City-Cyber-Security-Grid-Matrix

1 정회원, 1저자, 서울시립대학교 전자전기컴퓨터공학과 박사과정, E-mail: kimseam1@uos.ac.kr

2 정회원, 2저자, 서울시립대학교 전자전기컴퓨터공학과 연구교수, E-mail: banyasun@uos.ac.kr

3* 정회원, 교신저자, 서울시립대학교 전자전기컴퓨터공학과 교수, E-mail: ywlee@uos.ac.kr

1 Ph.D. in Electronics, Electrical and Computer Engineering at University of Seoul, E-mail: kimseam1@uos.ac.kr

2 Professor of Electronic, Electrical and Computer Engineering at University of Seoul, E-mail: banyasun@uos.ac.kr

3* Professor of Electronic, Electrical and Computer Engineering at University of Seoul, E-mail: ywlee@uos.ac.kr

1. 서 론

스마트시티는 정보통신기술(ICT)을 기반으로 하는 미래도시 유형의 하나이다. 따라서, 사이버 보안이 매우 중요한 요소이다. 이전에는 상상하기 어려웠던 사이버 보안 위협들이 속속 등장하고 있다. 본 논문의 기반이 되는 선행 연구에서 저자들과 저자들이 소속한 연구그룹에서는 이 위협들과 해결책들을 지난 10년간 모두 추적해왔다. 이 노력의 결과로서, 본 논문에서 우리는 스마트시티에서의 사이버 보안에 대한 방법론으로서, 개발한 스마트시티-사이버-보안-그리드-메트릭스 방법론을 본 논문에서 제시하고, 개발한 스마트시티-사이버-보안-그리드 메트릭스 방법론을 미국의 국가표준 기술연구소(NIST)에서 개발한 프레임워크 방법론에 적용하여 유용성과 편이성 등의 장점을 검증한다. 이를 위하여, 스마트시티 사이버 보안 요구 사항들을 제시한다. 본 논문에서 설명되는 스마트시티-사이버-보안-그리드 메트릭스 방법론과 이를 적용한 프레임워크 기반 스마트시티 사이버 보안 메트릭스를 이용하면 구축하고자 하는 스마트시티 사이버 보안 시스템의 전체 수준을 한 눈에 쉽게 확인해 가면서, 스마트시티 보안 시스템의 구축과 운영을 체계화할 수 있다.

본 논문의 연구진은, 전국의 백여 개가 넘은 유시티 건설에 참여하였으며, 서울시 디지털 미티어 시티에 참여하였다. 2005년도에 스마트시티에 관한 대규모 연구를 시작하였으며, 지금까지 이어오고 있다. 연구결과들은 유럽연합의 스마트시티 프로젝트와 여러 국가들에 전파되었다. 본 논문은 이 연구들에 의한 산출물이다.

본 논문은 구성은 다음과 같다. 2장에서, 본 논문과 관련된 연구들을 살펴본다. 3장에서, 어떠한 스마트시티를 연구의 대상으로 삼는지를 정의한다. 4장에서, 스마트시티-사이버보안-그리드-메트릭스 방법론과 이를 적용한 프레임워크 기반 스마트시티 사이버 보안 메트릭스를 설명하고 검증한다. 5장에서, 결론을 내린다.

2. 관련연구

저명한 국제표준화 기구인 세계표준기구(ISO)와 세계전자기술위원회 (IEC)는 사이버 보안을 위한 표준들을 제정해오고 있다. 표준제정이 진행 중인 ISO/IEC 27100, ISO/IEC 27101, ISO/IEC 27102 표준과 이미 제정된 ISO/IEC 27103 표준은 사이버 보안 프레임워크 표준을 활용하여 체계적으로 사이버 보안을 관리하기 위한 방법을 담고 있다[1][2][3]. 세계표준기구나 세계전자기술위원회는 스마트시티에서의 전체적인 사이버 보안에 대한 표준을 아직 발간하고 있지 않다. 대한민국 국가보안기술연구소는 ISO/IEC 15408 국제표준의 정보보호시스템 공통평가기준을 기준으로 ISO/IEC 18045 국제표준의 정보보호시스템 공통평가방법론에 기반을 두어 정보보호제품 평가와 인증을 7단계의 평가보증등급으로 구분하여 수행하고 있다. 이 선행연구들은 본 논문의 토대가 되었다.

미국 인터넷보안센터(CIS)는 미국 표준기술연구소(NIST)와 함께 사실상의 미국 사이버 보안 표준에 관한 내용들을 발표해오고 있다[4]. 본 논문은 이 제안들을 포괄한다. 유럽연합사이버보안기구는 사이버 보안에 대한 연구결과들을 발간하고 있다. 이들 내용들은 본 연구에 기반이 된다[5][6]. 유럽연합사이버보안기구는 스마트시티 공공교통과 스마트 병원에 대한 사이버 보안 연구 보고서를 출간하였다[7][8].

본 논문은 한국인터넷진흥원(KISA)의 국가정보보호백서들을 포괄한다[9]. 한국정보보호산업협회(KISIA)는 국내 정보보호산업 및 실태조사[10]와

스마트시티의 세부 분야 중에서 스마트 의료, 스마트교통, 스마트공장, 스마트안전/재난/환경, 스마트 에너지 분야와, 스마트시티에 필수적인 IoT에 관한 보안 가이드를 제공하고 있다[11]. 2019년 4월 3일에 청와대 국가안보실에서는 국가사이버안보전략을 발표하였다. 이들은 본 논문의 연구에 기반 자료로 활용되었다. 참고문헌 [12]와 [13]은 스마트시티에서의 보안시스템을 다루고 있는데, 이들 외에 스마트시티의 총체적인 보안에 대한 연구는 찾아 보기 어렵다.

3. 스마트시티

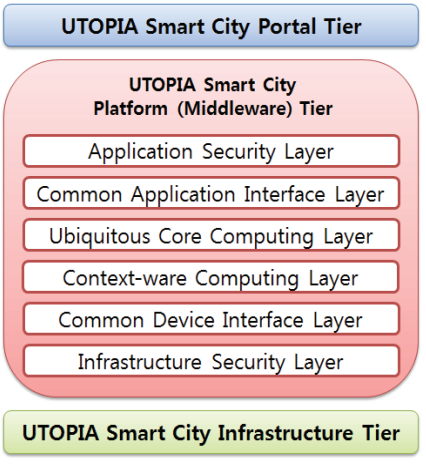

Fig. 1. UTOPIA Architecture

대한민국은 스마트시티를 2017년에 제정된 법률에서 “도시의 경쟁력과 삶의 질의 향상을 위하여 건설·정보통신기술 등을 융·복합하여 건설된 도시 기반 시설을 바탕으로 다양한 도시 서비스를 제공하는 지속 가능한 도시를 말한다[14].”라고 정의한다. 스마트시티 이전에, 대한민국은, 유시티(U-City: Ubiquitous City)라는 이름으로 선구자적으로 미래도시를 탐구했었다. 대한민국의 유비쿼터스 도시의 건설 등에 관한 법률은 “도시민의 삶의 질과 도시의 경쟁력 향상을 위하여 도시공간에 유시티 기술을 구현함으로써 언제 어디서나 유시티 서비스를 제공하는 도시[15]”라고 유시티를 정의하고 있다.

저자들의 연구그룹은 2005년에 Fig. 1과 같은 유토피아(UTOPIA) 스마트시티를 제안하였고 지금까지 발전시켜오고 있다. 이 패러다임은 현재 스마트시티의 주류가 되었다. 이 패러다임이 본 논문이 대상으로 하는 스마트시티이다. 이 패러다임에서는 스마트시티가 Fig.1에서처럼 세 개의 티어로 이루어져 있다[16].

스마트시티-포탈-티어는 사용자들이 다양한 스마트시티 서비스들을 온라인으로 이용할 수 있게 해준다. 스마트시티-플랫폼(미들웨어)-티어는 지능적인 다양한 융복합 솔루션을 제공하는 핵심 역할을 하며 클라우드 컴퓨팅을 포함한다. 스마트시티 플랫폼(미들웨어)을 사용하여 스마트시티를 하나의 시스템으로 유기적으로 관리하기 위하는 것이 현재 스마트시티 시스템의 대세이다. 모든 서비스를 통합하여 제공할 수 있게 해주는 역할을 통합 서버에 위치하는 통합 플랫폼이 한다. 강력한 통합 플랫폼 서비스를 제공하는 페러다임이 유토피아 패러다임이다. 도시의 데이터와 도시 인프라를 관리하므로 사이버 보안이 절대적으로 필요하다. 스마트시티-인프라스트럭처-티어는 스마트시티의 실제 각 구성요소들로 이루어져 있다. 스마트시티-인프라-스트럭쳐-티어는 다양한 정보통신기술을 융복합적으로 사용하여, 스마트시티 도시의 요소들을 유기적으로 연결하고 관리한다. 도시의 인프라스트럭쳐에 사물인터넷 기능을 적극적으로 사용하여 스마트시티-인프라스트럭쳐를 만들어 낸다. 사물인터넷를 사용함으로 인해, 보안은 더욱 중요해지고, 어려워졌다.

Table 1. Smart-City-Cyber-Security-Grid-Matrix

보안요소 \ 스마트시티 사이버보안 요구사항		멀웨어 공격	비인가 소프트웨어설치	사회공학적 공격	DDoS 공격	SPAM 공격	원격활동공격	데이터 유출	정보의 누설	개인정보 탈취	가짜인증서	패키지 비인가 조작	정보조작	감사도구의 악용	비인가 행위	거짓정보	목표된 공격	무차별 공격	송인 남용	정보 가로채기	워 드라이빙	방송자료 가로채기	메시지 재생 공격	네트워크 조작	세션 도용	출처미상정보사용
		SCR-01	SCR-02	SCR-03	SCR-04	SCR-05	SCR-06	SCR-07	SCR-08	SCR-09	SCR-10	SCR-11	SCR-12	SCR-13	SCR-14	SCR-15	SCR-16	SCR-17	SCR-18	SCR-19	SCR-20	SCR-21	SCR-22	SCR-23	SCR-24	SCR-25
1	PR.AC-1									0					0											
2	PR.AC-3						0																			
3	PR.AC-4							0	0	0			0	0										0		
4	PR.AC-5							0		0		0								0				0		
5	PR.AC-6									0	0															
6	PR.AC-7									0																
7	PR.DS-1							0	0																	
8	PR.DS-5							0	0																	
9	PR.DS-6	0	0								0															0
10	일회용비밀번호(OTP) 인증 제품									0																
11	공개키기반구조(PKI)를 제공하는 제품									△ (50%)																
12	통합접근관리(EAM)를 제공하는 제품									△ (50%)					△ (50%)											
13	통합계정관리(IM)를 제공하는 제품									△ (50%)					△ (50%)											
14	DDoS차단시스템				0		△ (70%)																	△ (30%)		
15	---																									
16	---																									

4. 사이버 보안 프레임워크 그리드 메트릭스

4장에서는 개발한 스마트시티-사이버-보안-그리드-메트릭스 방법론과 이를 미국의 표준 기술연구소(NIST)가 제시하는 사이버 보안 프레임워크와 결합한 프레임워크 기반의 스마트시티-사이버-보안-그리드-메트릭스 방법론을 제시한다. Table 1은 프레임워크 기반의 스마트시티-사이버-보안-그리드-메트릭스를 보여준다.

Table 1의 가로축의 값들은 스마트시티 사이버 보안 요구사항들로서 SCR로 시작하는 고유식별번호를 갖는다. 25개의 스마트시티 사이버 보안 요구사항들이 본 논문의 연구에서 도출되었는데, 각각의 요구사항들과 도출 근거와 이유를 4.1절에서 설명한다.

4.1 스마트시티 사이버 보안 요구사항

본 논문의 연구진은 스마트시티에 관한 지난 20년동안 축적된 선행연구결과들을 기반으로 하고, 전 세계의 사이버 보안에 관한 지금까지의 연구결과들을 반영하여, 스마트시티 보안 위협요소들을 선정하고 분류하였다[1]-[22].

분류는 7개 이상의 카테고리 분류로 진행되었으며, [카테고리 5]까지 소개하면 다음과 같다. [카테고리 1] 스마트시티의 사이버 보안에 직접적으로 위협을 가하는 요소, [카테고리 2] 물리적인 공격에 의한 위협요소, [카테고리 3] 재난에 의한 위협요소, [카테고리 4] 시스템과 기기들의 이상과 고장에 의한 위협, [카테고리 5] 정전 등과 같은 전기 공급 이상에 의한 위협 등으로 분류한다. 스마트시티 사이버 보안 요구사항들은 [카테고리 1] 위협요소들을 방어하도록 설정되었다.

SCR-01은 스마트시티가 멀웨어에 의한 공격들을 방어할 수 있어야 한다는 것을 요구한다. 웹-어플리케이션-공격에 쓰이는 멀웨어들,크립토재킹 공격에 쓰이는 멀웨어들, 랜섬웨어(Ransomware) 멀웨어들, 스파이웨어와 같은 기만하는 프로그램, 웜, 트로이-목마, 루트킷(Rootkit), 각종 모바일 멀웨어, 인가되지 않은 권한-상승-공격을 위한 멀웨어, 가짜-백신-프로그램, 익스플로잇-킷(Exploit kit), 기타 각종 바이러스 프로그램들이 대표적인 멀웨어들이다.

SCR-02는 스마트시티가 비인가-소프트웨어-설치에 의한 공격들을 방어할 수 있어야 한다는 것을 요구한다. 비인가 소프트웨어 설치 공격은 대부분이 웹-기반-공격이며 웹-기반-공격은 2018년에 2위를 기록했다[5]. 코드 주입에 의한 웹 기반 공격이 가장 많이 일어난다.

SCR-03은 스마트시티가 사회공학적-공격들을 방어할 수 있어야 한다는 것을 요구한다. 기술적인 방법이 아닌 사람들 간의 기본적인 신뢰를 기반으로 사람을 속여 비밀 정보를 획득하는 공격을 사회공학적-공격이라고 칭한다. 사회공학적-공격의 대표적인 경우가 2018년에 4위를 기록한 피싱(Phishing)과 스피어-피싱이다[5].

SCR-04는 스마트시티가 각종 분산서비스-거부(DDoS) 공격들을 방어할 수 있어야 한다는 것을 요구한다. 이 공격은 2018년에 5위를 기록했다[5]. SCR-05는 스마트시티가 원하지 않는 E-mail 수신 공격들을 방어할 수 있어야 한다는 것을 요구한다. 대표적인 경우가 스팸(Spam) 공격이다. 2018년에 6위를 기록했다[5]. SCR-06은 스마트시티가 봇넷(Botnets) 등을 통한 원격활동 공격들을 방어할 수 있어야 한다는 것을 요구한다. SCR-07은 스마트시티가 데이터 유출 사고를 방지할 수 있어야 한다는 것을 요구한다. 데이터-유출-사고는 기밀 정보의 의도적 또는 비의도적 유출 사고를 말하며, 기밀-정보-유출-사고라고도 하며, 2018년에 8위로 기록되었다[5]. SCR-08은 스마트시티가 정보의 누설 사고를 방지할 수 있어야 한다는 것을 요구한다. 정보-누설-사고는 관리자가 의도하지는 않았지만, 정보가 외부로 누설되는 것을 말한다. 2018년에 11위를 기록했다[5]. SCR-09는 스마트시티가 개인 정보 탈취를 통한 신원-도용-공격들을 방어할 수 있어야 한다는 것을 요구한다. 개인 정보 탈취하여 신원 도용을 하려는 공격은 2018년에 12위를 기록했다[5]. SCR-10은 스마트시티가 가짜 인증서를 생성하여 사용하는 공격들을 방어할 수 있어야 한다는 것을 요구한다. SCR-11은 스마트시티가 하드웨어와 소프트웨어의 인가를 받지 않은 조작에 의한 공격들을 방어할 수 있어야 한다는 것을 요구한다.

SCR-12는 스마트시티가 정보를 조작하여 공격하는 행위들을 방어할 수 있어야 한다는 것을 요구한다. 라우팅 테이블 조작, DNS 조작과 같은 정보의 조작에 의한 공격을 방어할 수 있어야 한다. SCR-13은 스마트시티가 감사 도구의 악용과 남용에 의한 공격들을 방어할 수 있어야 한다는 것을 요구한다. SCR-14는 스마트시티가 소프트웨어의 비인가 사용과 같은 비인가 행위에 의한 공격들을 방어할 수 있어야 한다는 것을 요구한다. SCR-15는 스마트시티가 거짓 정보에 의한 공격들

을 방어할 수 있어야 한다는 것을 요구한다. SCR-16은 스마트시티가 목표된 공격들을 방어할 수 있어야 한다는 것을 요구한다. APT(Advanced Persistent Threat) 등을 사용한 공격을 목표된 공격이라고 호칭한다. SCR-17은 스마트시티가 무차별 공격들을 방어할 수 있어야 한다는 것을 요구한다. 키-전수조사라고도 호칭되는 무차별 공격은 나날이 그 수법이 향상되고 있다.

SCR-18은 스마트시티가 승인 남용에 의한 공격들을 방어할 수 있어야 한다는 것을 요구한다. 남발된 승인을 통해 액세스하여 공격하는 것을 승인 남용에 의한 공격이라고 한다. SCR-19는 스마트시티가 정보의 가로채기 공격들을 방어할 수 있어야 한다는 것을 요구한다. 특정한 사람이나 기관에 대한 정보를 수집하려는 의도를 가진 스파이웨어 또는 기만하는 프로그램에 의한 공격을 정보의 가로채기라고 칭한다. 특정한 사람이나 기관에 대한 정보를 수집하려는 의도를 가진 사이버 스파이 공격은 2018년에 15위를 기록하였다[5]. SCR-20은 스마트시티가 워-드라이빙 공격들을 방어할 수 있어야 한다는 것을 요구한다. 워-드라이빙(War driving)은 정보를 가로채 가는 공격과 유사한 공격 행위로서, 무선 네트워크를 이용한 해킹 수법의 하나이다. SCR-21은 스마트시티가 방출자료-가로채기-공격들을 방어할 수 있어야 한다는 것을 요구한다. 정보를 갖는 시그널을 방사하는 것을 자료-방출이라고 호칭한다. 방출 자료 가로채기는 사물인터넷을 사용하는 스마트시티에게 큰 위협이 되고 있다.

SCR-22는 스마트시티가 메시지-재생-공격들을 방어할 수 있어야 한다는 것을 요구한다. 유효한 데이터 전송을 가로채어서, 악의적으로 또는 사기적으로 데이터 전송을 반복하거나 데이터 전송을 지연시키는 공격을 메시지 재생 공격이라고 한다. SCR-23은 스마트시티가 네트워크 조작에 의한 공격들을 방어할 수 있어야 한다는 것을 요구한다. 네트워크 정찰을 통하여 네트워크를 조사하여 보안 취약점을 알아내어서, 네트워크를 조작하거나, 네트워크 트래픽 조작해서 필요한 정보를 모아가는 공격 행위이다[23]. SCR-24는 스마트시티가 세션-도용-공격들을 방어할 수 있어야 한다는 것을 요구한다. 세션 도용은 데이터 패킷을 가로채어서 세션 쿠키를 훔침으로써 사용자 세션을 가로채려는 공격을 말한다. SCR-25는 스마트시티가 신뢰할 수 없는 출처의 정보 사용과 출처 미상 정보 사용에 의한 공격들을 방어할 수 있어야 한다는 것을 요구한다. 스마트시티에서, 신뢰할 수 없는 기기나 정보를 사용하여서, 스마트 홈 등의 스마트시티에 접근한 후, 기기들을 가동하는 공격이 자주 발생한다. 이상과 같은 25개의 사이버 보안 위협 요소들이 Table 1의 가로축 항목이다.

4.2 프레임워크 기반 보안

미국 표준기술연구소 사이버 보안 프레임워크는 2014년에 버전(Version) 1.0이, 2018년 4월 16일에 버전 1.1이 공개되었다. 프레임워크는 프레임워크 코어, 프레임워크 구현 계층, 프레임워크 프로필이라는 3개의 주요 요소를 제공한다.

프레임워크 코어는, 기능, 카테고리, 서브 카테고리, 참조문헌으로 명칭 되는 4개의 요소로 이루어져 있다. 이 중 “기능” 요소는 인지, 보호, 탐지, 대응, 복구로 명칭 되는 5개의 카테고리로 다시 세분되며, 이들 5개의 카테고리는 다시 108개의 서브 카테고리로 세분된다. 프레임워크 구현 계층은 부분적 적용티어, 위험 정보 활용 티어, 반복 티어, 적용 티어를 거쳐서 구축하고자 하는 기관에 맞게 다듬을 수 있게 해준다. 프레임워크 프로파일 요소에서, 사이버 보안을 구축하는 기관에 맞게 프레임워크 코어 요소에서 선택한 요구 사항

을 기반으로 프레임워크 프로파일이 도출된다[4].

미국 표준 기술연구소의 프레임워크는 방법론만을 제시하므로, 각 기관에서는 프레임워크 방법론을 사용하여, 각 기관 자신만의 구체적인 실현 방안을 만들어야 한다. 각 기관이 만든 구체적인 보안 방안을 Table 1의 세로 항목에 채워 넣음으로써, Table 1과 같은 스마트시티-사이버-보안-그리드-메트릭스를 얻을 수 있다.

4.3 메트릭스 검증

미국 표준기술연구소의 프레임워크 방법론은, 현재의 사이버보안 상태와 목표 수준을 정하면, 연속적이고 반복적인 피드백 작업으로 개선하여서, 정한 목표 수준까지 얼마나 달성하였는지를 평가하는 방식으로 진행된다[4]. Table 1은 결정된 목표 수준까지 얼마나 달성하였는지를 일목요연하게 평가할 수 있게 해 주기 때문에, 프레임워크 방법론에 큰 도움이 된다. 본 논문의 연구진은 프레임워크 방법론을 스마트시티에 적용하여, Table 1을 얻었다. 세로 항목에서 처음 9개 항목은, 프레임워크의 108개의 소항목에 속하는, 보호(Protect) 항목의 세부 항목들 중에서 일부에 대하여 작성되었다.

이들을 설명하면 다음과 같다. 1) PR.AC-1은 아이디(ID)와 인증의 발급, 관리, 검증, 철회 등을 관리하는 보호를 구현한 경우를 말한다. 2) PR.AC-3은 원격 액세스 관리 보호를 구현한 경우이다. 3) PR.AC-4는 액세스 승인, 인증 관리에서 최소 권한의 원칙과 임무 분리 원칙을 구현한 경우이다. 4) PR.AC-5는 네트워크 무결성을 보호하는 경우이다. 5) PR.AC-6은 아이디를 모든 활동에서 검증하는 경우이다. 6) PR.AC-7은 사용자, 디바이스, 기타 전산자원을 매 트랜잭션마다 인증 관리하는 경우이다. 7) PR.DS-1은 대기 중인 데이터를 보호하는 경우이다. 8) PR.DS-5는 데이터 누출에 대한 보호를 구현한 경우이다. 9) PR.DS-6은 무결성 검사 메커니즘을 사용하여 소프트웨어, 펌웨어, 정보의 무결성을 검증하는 경우이다.

세로 항목에서 그 다음 5개 항목은, 프레임워크 방법론을 적용해서 나온 보안방안에 의거하여, 일부를 실현한 것들이다. 이들을 설명하면 다음과 같다. 10) 일회용 비밀번호(OTP) 인증 제품을 사용한 경우, 11) 공개키 기반구조 (PKI)를 제공하는 제품을 사용한 경우, 12) 통합접근관리(EAM)를 제공하는 제품을 사용한 경우, 13) 통합계정관리(IM)를 제공하는 제품을 사용한 경우, 14) DDoS 차단시스템을 사용한 경우이다.

Table 1의 스마트시티 사이버 보안 그리드 메트릭스에서 동그라미의 의미는 세로 항목에 표시된 보안 기능을 구현하였을 때, 가로 항목에 표시된 스마트시티-사이버-보안-요구-사항을 만족하는가에 대한 점검을 했을때, 만족한다는 의미이다. 동그라미 대신에, 퍼센트 값으로 표시할 수 있는데, 이럴 경우, 훨씬 상세한 스마트시티-사이버-보안-그리드-메트릭스가 된다.

Table 1의 프레임워크 연동 스마트시티-사이버-보안-그리드-메트릭스를 사용하면, 스마트시티에서 구현되는 사이버 보안의 정도를 매 점검 순간마다 일목요연하게 확인할 수 있다. 따라서, 프레임워크 작업을 진행할 때, 스마트시티-사이버-보안-그리드-메트릭스를 활용하여 스마트시티 시스템의 사이버 보안의 정도를 원하는 시점에서 점검할 수 있다. 따라서, 스마트시티의 사이버 보안 구축을 성공적으로 완수할 수 있는 가능성을 크게 향상시킨다. 각 스마트시티는 스마트시티의 사이버 보안 메트릭스를 사용하여 원하는 수준의 스마트시티 사이버 보안을 구현할 수 있게 계획을 수립하고 집행하고, 확인하고, 유지 보수를 할 수 있게 된다.

5. 결 론

스마트시티 사이버 보안에 대한 도구(Methodology)로 개발한 스마트시티-사이버-보안-그리드-메트릭스 방법론을 본 논문에서 제시하였다. 개발된 스마트시티-사이버-보안-그리드 메트릭스 방법론을 미국의 국가 표준 기술연구소(NIST)에서 개발한 프레임워크 방법론에 적용하여 유용성과 편이성 등의 장점을 검증하였다. 이 과정에서, 스마트시티 사이버 보안을 확보하기 위한 스마트시티 사이버 보안 요구 사항들이 설명되었다.

본 논문에서 설명되는 스마트시티-사이버-보안-그리드 메트릭스 방법론과 이를 적용한 프레임워크 기반 스마트시티 사이버 보안 메트릭스를 이용하면, 구축하고자 하는 스마트시티 사이버 보안의 전체 수준을 한 눈에 쉽게 확인해 가면서, 스마트시티 보안의 구축과 운영을 체계화할 수 있음을 검증하였다. 본 논문에서 소개한 스마트시티 사이버 보안 메트릭스를 사용하여, 원하는 수준의 스마트시티 사이버 보안을 구현할 수 있게 계획을 수립하고 집행하고, 확인하고, 유지 보수를 할 수 있음을 설명하고 검증하였다.

감사의 글

본 연구에 기여한 박종원 박사, 윤철상 연구원, 스마트시티 사업단, 서울그리드센터, 유비쿼터스 그리드(클라우드) 연구실의 연구원들에게 감사한다. 이 논문은 2019년도 서울시립대학교 학술연구비에 의하여 지원되었음

참고문헌

[1] ISO/IEC TS 27100 — Information technology — Security techniques — Cybersecurity — Overview and concepts, https://www.iso27001security.com/html/27100.html. (Accessed: March 01, 2020)

[2] ISO/IEC TS 27101 — Information Security, Cybersecurity and Privacy Protection — Cybersecurity framework development guidelines, https://www.iso27001security.com/html/27101.html. (Accessed: March 01, 2020)

[3] ISO/IEC TR 27103:2018 — Information technology — Security techniques — Cybersecurity and ISO and IEC standards, https://www.iso27001security.com/html/27103.html. (Accessed: March 01, 2020)

[4] “Framework for Improving Critical Infrastructure Cybersecurity”, National Institute of Standards and Technology, (2018).

[5] “ENISA Threat Landscape Report 2018”, European Union Agency For Network And Information Security, pp. 24-115, (2019).

[6] “ENISA Threat Taxonomy”, European Union Agency For Network And Information Security, (2016).

[7] “Cyber security for Smart Cities - An architecture model for public transport”, European Union Agency For Network And Information Security, (2015).

[8] “Smart Hospitals - Security and Resilience for Smart Health Service and Infrastructures”, European Union Agency For Network And Information Security, (2016).

[9] 2019 National Information Protection White Paper, Available From: https://www.kisa.or.kr/public/library/etc_View.jsp?regno=0012001&searchType=&searchKeyword=&pageIndex=1. (Accessed: March 01, 2020)

[10] “Survey for Information Security Industry in Korea : Year 2019”, Korea Information Security Industry Association, (2019).

[11] Smart Medical, https://www.kisa.or.kr/public/laws/laws3.jsp. (Accessed: March 01, 2020)
[12] E. D, Hwang, and Y. W. Lee, "User Authentication of a Smart City Management System", Journal of the Korea Convergence Society, vol. 10, no. 1, pp. 53-59, (2019).
[13] E. D, Hwang, and Y. W. Lee, "Smart City Security Management in Three Tier Smart City Management System", Journal of the Korea Convergence Society, vol. 10, no. 1, pp. 25-33, (2019).
[14] Korean Ministry of Land, Infrastructure and Transport, Act on Smart City Creation and Industry Promotion, etc, This Decree enter into force on Sept. 22, 2017. Law No.14718.
[15] Korean Ministry of Land, Transport and Maritime Affairs(Ministry of land, transport and maritime affairs), Korea, ACT ON THE CONSTRUCTION, ETC. OF UBUQUITOUS CITIES, amended by Act No. 9705, May 22, (2009).
[16] H. S. Jung, C. S. Jeong, Y. W. LEE and P. D. Hong, "An Intelligent Ubiquitous Middleware for U-city: SmartUM", Journal of Information Science and Engineering, vol. 25, no. 2, pp. 375-388, (2009).
[17] Threat Classification Taxonomy Cross Reference View, http://projects.webappsec.org/w/page/13246977/Threat%20Classification%20Views. (Accessed: March 01, 2020)
[18] Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies, https://s2erc.georgetown.edu/sites/s2erc/files/CyberISE%20Taxonomy.pdf. (Accessed: July 01, 2016)
[19] Two taxonomies of deception for attacks on information systems, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.457.5398&rep=rep1&type=pdf. (Accessed: March 01, 2020)
[20] CIF Taxonomy Assesment v1", https://code.google.com/p/collective-intelligence-framework/wiki/TaxonomyAssessment_v1. (Accessed: July 01, 2016)
[21] HP Tipping Point Event Taxonomy V 2.2, http://h10032.www1.hp.com/ctg/Manual/c03964615. (Accessed: July 01, 2016)
[22] A Taxonomy of Operational Cyber Security Risks, http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=9395. (Accessed: March 01, 2020)
[23] H. H. Kim, et al., "Development of CAN network intrusion detection algorithm to prevent external hacking", The Korean Society of Industry Convergence, vol. 20, no. 2, pp. 177-186 (2017).

(접수: 2020.03.01. 수정: 2020.03.29. 게재확정: 2020.04.02.)