https://doi.org/10.33778/kcsa.2021.21.1.107

안전한 스마트월드를 위한 사이버 테러위협 제거 방안 연구

한 충 희*, 한 창 희**

요 약

최근 스마트 시티, 스마트 홈, 스마트 교통, 스마트 케어 등 스마트 월드를 지향하는 대규모의 연구와 노력이 계속되고 있다. 이러한 스마트 월드가 보편화 될수록 인터넷과의 연결성 확대와 사이버 테러위협의 확대는 필연적일 것이다. 이러한 사이버 테러위협의 확대는 엄청난 재난안전사고로 연결될 가능성을 점점 높이고 있다. 이에 본 논문에서는 다양한 형태로 확대되는 스마트 월드에 대해 살펴보고 스마트 월드들이 가지고 있는 보안 위협 요인을 도출한다. 또한, 스마트 월드의 구축시 해외로부터의 접근이 필요하지 않는다면 해외로부터의 테러위협을 봉쇄하는 방안을 제안한다. 이를 통해 안전한 스마트월드의 구축과 운영을 위한 사이버 테러위협 제거방안을 제시하고자 한다.

Cyber Terror Threat Elimination Method Study for Safe Smart World

Han Choong-Hee*, Han ChangHee**

ABSTRACT

Recently, large-scale research and efforts aimed at the smart world such as smart city, smart home, smart transportation, and smart care are continuing. As these smart worlds become more common, the expansion of connectivity with the Internet and the threat of cyber terrorism will be inevitable. Increasing the threat of cyber terrorism is increasing the likelihood of a massive disaster and safety accident. Therefore, in this paper, we examine smart worlds that are expanded in various forms and derive the security threat factors that smart worlds have. In addition, it is proposed to block the threat of terrorism from abroad if access from abroad is not required when constructing a smart world. Through this, we intend to present a method to eliminate cyber terror threats for the establishment and operation of a safe smart world.

Key words : Smart world security, Smart city, Smart home, ESC Model

접수일(2021년 02월 01일), 게재확정일(2021년 03월 29일)

* 전력거래소 안전보안실/정보보안팀(주저자)

** 육군사관학교 교수부/AI연구센터(교신저자)

1. 서 론

"스마트 월드"는 인간에게 지능적으로 반응하도록 정보 통신 기술을 사용하여 감지하고 도시 운영을 위한 핵심 시스템의 주요 정보를 분석하고 통합한다. Smart World에는 스마트 시티, 스마트 산업, 스마트 환경 및 스마트 그리드와 같은 다양한 분야가 포함된다[1]. 스마트 월드는 여러 가지 형태를 가지고 있는데, 가령, 스마트 시티, 스마트 홈, 스마트 농업 등과 같이 전통적인 생활방식을 바꾸고 있으며, 결국에는 사이버, 물리적, 사회적, 그리고 생각의 공간들까지 확대될 것이다[2]. Smartness는 널리 쓰이고 있지만, 다르게 정의되어 있다. 개념, 사회경제환경과 엄격히 연관돼 있다[3].

현대 사회는 급속도로 성장하는 정보통신기술(ICT)의 발달과 인터넷의 확산으로 산업분야별 경계가 허물어 졌으며 새로운 변화를 촉발하는 4차 산업혁명이 도래하게 되었다. 4차 산업혁명의 중요기술로 거론되는 IoT(Internet of Things)의 발달은 고도화된 기술혁신을 가져왔으며, 다양한 분야에 적용되며 일상생활을 변화시키고 있다[4].

정부는 2018년 4월 기계설비법을 제정 공포하면서 미래 도시에 있어 기계설비 기술의 첨단화와 기계설비 산업의 고도화를 위한 국가의 역할을 표명하기도 하였다. 또한 IoT 기술과 빅데이터, 클라우드 기술 등의 지능정보 기술을 접목시켜 스마트 도시를 효과적으로 관리하고, 발생 가능한 도시문제들에 선제적으로 대비할 수 있도록 하고 있다[5].

4차 산업혁명에서 사물인터넷을 언급하듯이 모든 세상이 연결된 사이버 세상이 되었다. 언제나 그렇듯 좋은 점이 있으면 반대적으로 나쁜 점도 존재하게 된다. 인터넷에 연결된 정보와 정보시스템을 선의의 목적으로 사용하는 것이 일반적이지만 나쁜 의도를 가진 사람들에게는 좋은 먹잇감이 된다. 또한 현대는 사이버전이다. 취약한 사이버보안 체계를 갖춘 도시는 기능이 쉽게 마비될 수 있다[6].

2. 선행 연구

2.1 스마트시티

스마트시티는 “도시의 경쟁력과 삶의 질의 향상을 위하여 건설·정보통신기술 등을 융·복합하여 건설된 도시기반시설을 바탕으로 다양한 도시서비스를 제공하는 지속 가능한 도시”로서 기존의 도시 인프라 고도화 차원의 단순 ICT 기술 접목이 아닌 교통, 헬스케어, 건설, 인프라, 에너지 등 도시를 유지시키는 영역의 다양한 기기와 서비스를 서로 연결하고 수집 분석된 데이터를 하나의 플랫폼과 같이 연동하여 운영되는 통합된 개념의 도시이다[7].

2.2 스마트홈

한국 스마트 홈 산업협회에 따르면 스마트홈은 “주거 환경에 IT를 융합하여 국민의 편익과 복지증진, 안전한 생활이 가능하도록 하는 인간 중심적인 스마트 라이프 환경”으로 정의되고 있다[8].스마트 홈은 기기가 수집한 데이터를 기반으로 상황을 인지하고, 이것을 분석하여 사용자 패턴에 맞게 데이터를 가공하여 개인 맞춤형 서비스를 제공한다[9].

스마트 홈 IoT 보안 위협은 IoT 플랫폼을 구성하는 Device, Connectivity, Platform 등의 계층에 따라 단말 및 센서 보안 기술, 통신 및 네트워크 보안 기술, 애플리케이션 등에서 발생할 수 있다. IoT 네트워크에서 근거리 통신에 사용되는 ZigBee의 경우 IEEE 802.15.4의 표준을 준수하며, 단말의 전력소모를 최소화 할 수 있다는 장점이 있다. 하지만, 통신할 수 있는 정보량이 한정되어 있고 높은 수준의 보안 기술을 적용하기 어렵다는 단점이 있다. ZigBee 통신을 위한 보안 기술로는 SSM(Standard Security Mode)과 HSM(High Security Mode) 두 가지 방식이 있으며, SSM은 낮은 수준의 보안을 제공하고, HSM은 높은 보안 수준을 요구하는 환경을 위하여 설계되었다. 이것은 장치 내부의 신뢰성은 보장되지만 외부와의 통신 과정에서의 보안 위협이 존재하기 때문에 별도 보안대책이 요구된다[10].

2.3 스마트교통

스마트 교통 시스템은 스마트 카를 다양한 개체와 연결하여 교통 효율 및 안전 향상, 환경 문제 개선, 사용자 편의 확대를 목표로 다양한 서비스를 제공한다.

스마트 교통 서비스는 크게 차량과 차량의 연결로 제공되는 V2V, 노변 기지국(RSU, Road Side Unit)과의 연결로 제공되는 V2I 백엔드서버와의 연결로 제공되는 V2N서비스가 있다. 스마트 카는 자동차에 인터넷과 모바일기기 등 IT기술이 융합된 형태로, 자동차가 주변과 실시간으로 통신하면서 다양한 서비스를 제공하는 '연결성을 강조한 자동차'를 의미한다. 차량 내부 네트워크 기술은 Controller Area Network(CAN), Local Interconnect Network (LIN), FlexRay, Media Oriented Systems Transport(MOST), 이더넷 등의 다양한 네트워크 시스템이 존재한다[11].

2.4 스마트헬스케어

스마트 헬스케어란 헬스케어와 인공지능(AI), 빅데이터, 사물인터넷, 클라우드, 나노 등의 기술들이 융합된 새로운 개념이다[12]. 스마트의료 시스템 환경은 의료기관 외부에서 정보가 수집되어 의료기관 내부로 전달 처리되는 영역과 의료기관 내부에서 정보가 수집되어 처리되는 영역, 각종 의료정보가 타 의료기관이나 외부기관(건강보험공단 등)으로 전송 처리되는 영역으로 구분할 수 있다. 의료기관 내부 영역에서는 전용 네트워크를 통해서 의료기기에서 전송된 정보를 가공하는 인터페이스 서버를 경유해서 의료정보 DB에 저장 관리되고, EMR/EHR과 같은 의료정보시스템을 이용해서 의료진이 진단 치료하게 된다. 의료기관 외부 영역에서는 환자 보호자의 개인건강기기나 웨어러블 의료기기로부터 유무선 네트워크를 통해서 게이트웨이로 정보가 모여서 전송되고, 의료기관 내부 영역으로 전달된다. 의료기관과 타 의료기관 및 외부기관과의 연계 영역에서는 환자의 보험가입여부 파악과 의약품 안전사용, 중복투약방지 등의 정보들이 인터넷망을 통해서 기관 간 연동되어 수시로 송수신되고 있다[13].

2.5 해외로부터의 사이버 테러위협

2014년 12월에 발생한 한국수력원자력 사이버테러 사건의 IP를 분석하였는데 북한 해커조직의 IP 대역과 중국 IP 대역들이 12자리 중 9자리까지 일치하였다고 분석하였다. 북한 IP 주소 25개, 북한 체신성 산하 통신회사인 KPTC에 할당된 IP주소 5개가 접속한 흔적이 발견되었다고 설명하고 있다[14].

중국의 사이버전 인력이 약 10만명에 이르며 북한의 사이버전 인력을 약 7,700여명으로 추정하였다. 또한 중국으로부터 유입되는 사이버 위협의 일정 부분들이 북한 사이버전 기지로부터 발생되고 있다고 주장하였다[15].

시만텍사의 자료를 이용하여 2007년의 국가별 보안위협 발원지 현황을 분석하였는데 보안 위협의 발원지 1위 국가는 미국 중국의 순이었다[16].

2.6 ESC 보안관제 모델

ESC 모델은 웹기반 정보시스템들에 대한 해외 사이버 테러위협 차단 순위 결정 의사결정 방법론이다. ESC모델은 Asset Identification 단계, Blocking Prioritization 단계, Enhanced Security Operation 단계로 이루어진다.

첫 번째 Asset Identification 단계는 자산 식별단계이다. 좀더 자세히 설명하자면, HTTP, HTTPS, SMTP 등 외부와 연계하여 서비스를 제공하는 공인 IP를 가진 정보시스템들을 식별하는 단계이다.

두 번째 단계인 Blocking Prioritization은 6개의 요인에 대해 0점에서 2점까지 각 요인에 대한 영향도를 부여하는 단계로 BID(Blocking Impact Degree)가 0~12까지 결정되며 BID가 낮은 정보시스템부터 우선적으로 차단 순위를 결정한다. BID 결정을 위한 6가지 요인은 Foreign Relation, Real Login, Blocking Complexity, Stop Tolerance, Outer Relation, Stop Impact로 구성된다. Foreign Relation(해외 연관도, FR)은 얼마나 해외와 연관되어 있느냐를 검토하는 요인으로 차단 순위를 결정하는데 가장 중요한 고려 요인이다. Real Login(실제 접속도, RL)은 해외 연관성이 있다고 판단되는 정보시스템에 대하여 해외의 정상 사용자들로부터의 실제 접속 빈도에 대한 검토 요인이다. Blocking Complexity(차단 복잡도, BC)는 정보시스템으로 유입되는 출발지 IP를 국내 IP대역과 회사 IP대역으로만 최적화할 경우에 예외처리 요청을 얼마나 많이 해주어야 하는지를 검토하는 요인이다. Stop

Tolerance(중단 허용도, ST)는 정보시스템의 중단 허용 시간의 범위를 통해 중요도를 검토하는 요인이다. Outer Relation(외부연계도, OR)은 해당 정보시스템이 외부와 얼마나 연계되어 있는지를 검토하는 요인이다. Stop Impact(중지 파급도, SI)은 정보시스템의 중지 시 피해 예상규모가 얼마나 예상되는지를 검토하는 요인이다.

세 번째 단계인 Enhanced Security Operation은 출발지가 any로 되어 있는 방화벽 정책을 국내 IP대역과 회사의 인터넷 IP대역으로 수정하여 해외로부터의 사이버 테러위협을 원천 차단하는 단계이다. ESC 보안관제는 해외 사이버 공격자들에게 노출되는 웹기반 정보시스템들의 숫자를 줄여서 효율적인 보안관제를 할 수 있게 해준다[17].

3. 해외 사이버 테러위협 제거사례 분석

2019년 4월부터 2020년 3월까지 HTTP서비스를 제공하는 28개 웹기반 정보시스템 중 26개 정보시스템들을 대상으로 ESC모델을 적용하여 해외 IP대역 봉쇄작업을 진행하였다. 해외 IP대역 봉쇄 결과 크게 여섯 가지의 사이버 테러위협 제거 성과가 나타났다.

첫째, 사이버 침해사고 발생위험도가 대폭 감소하였다. 해외 IP대역을 봉쇄한 26개 정보시스템들에 대한 사이버 테러위협 이벤트 발생이 전혀 발생하지 않게 되어 사이버 침해사고 발생 위험도가 92.9% 감소하였다.

둘째, 단순 정보수집 이벤트를 제외한 고위험도의 사이버 테러위협 이벤트들이 대폭 감소하였다. 2018년에는 고위험도 사이버 위협이 79.4% 수준이었다. 그러나 2020년 3월 해외 IP대역 제한작업을 완료한 이후에는 29.9% 수준으로 감소하여 2018년 대비 고위험도의 사이버 위협 점유비율이 약 50% 감소하였다.

셋째, 사이버 테러위협 이벤트 유입량이 대폭 감소하였다. 2020년 4~6월 1일 평균 사이버 위협 이벤트량은 2,290건/일로서, 2018년 평균 1일 평균 이벤트량 5,502건/일 대비 58.4%가 감소하였다.

넷째, 악성 IP 발생량이 2018년 대비 약 40% 감소하였다. IPS에서 탐지하는 사이버 테러위협 이벤트 중 2회 이상의 이벤트 또는 고위험도의 이벤트를 악성 IP로 분류하고 보안장비에 블랙리스트로 등록한다. 악성 IP 발생량의 감소는 악성 IP 탐지와 등록에 소요되는 시간을 감소시켜 효율적인 보안관제를 가능하게 해주는 것으로 분석된다.

다섯째, 사이버 테러위협 탐지대응시간이 대폭 감소하였다. 사이버 테러위협의 탐지 대응의 핵심은 사이버 테러위협을 발생시키는 악성 IP를 블랙리스트로 보안장비에 등록하는 활동이라고 할 수 있다. 2018년에 16.79시간 소요되던 대응시간에서 약 6.8시간의 대응시간이 감소하였다.

여섯째, ESC 보안관제 모델 적용으로 사이버 위협에 대한 책임추적성이 강화되었다. 해외 IP 사용에 대한 예외처리시 각각의 해외IP에 대한 접속신청을 별도로 받아 보안조치를 시행하므로써 누가 어디로부터 접속하는지에 대한 책임추적성이 강화되어 사고조사 환경을 크게 개선하였다.

4. 안전한 스마트월드 구현방안

4.1 IoT 기기 운영서버 해외 접근 제한

스마트 월드 구축시 해외로부터의 접근을 제한하는 것이 반드시 필요하다. 스마트 월드를 구성하는 다양한 IoT 기기들은 최신 통신 기술들을 통해 국내 ISP 업체를 거쳐 PC, 테블릿, 스마트폰 등을 사용하는 운영서버와 인터넷 통신을 하며, 이와 동시에 국내외에 위치하는 IoT 제조회사의 IoT 관리서버와 SW 업그레이드, 유지보수 등의 다양한 이유로 인터넷 통신을 하게 되는데 사이버 위협의 95%는 해외로부터 유입되고 있기 때문이다.

해외로부터의 접근을 제한하는 가장 좋은 방법은 스마트 월드를 연결하는 역할을 하는 ISP 사업자로 하여금 제도적으로 해외 IP대역을 제한하게 하는 것이다. ISP 사업자는 스마트시티 등 수많은 스마트 월드에 대한 인터넷 연결시 해외 IP대역을 제한하는 방화벽 정책 설정 작업을 시행하여야 한다. 인터넷진흥원에서 제공하는 국내 IP대역은 총 2,000개 정도로서 방화벽에서 출발지 IP대역을 국내 IP대역으로 제한하는 작업을 수행할 수 있을 것이다.

IoT기기 제조사가 국내에 있다면 해외 IP대역을 제한한다고 하더라도 큰 문제가 발생하지 않을 것으

로 판단된다. 그러나 IoT기기 제조사가 IoT 관리서버를 해외에 위치하고 있다면 해외로부터의 인터넷 통신이 발생할 것이기에 이러한 경우에 대한 예외처리가 반드시 필요할 것이다. ISP사업자는 국내 스마트월드 사용자 또는 운영자로부터 인터넷 통신 연결신청을 받을 때 IoT기기 제조사의 운영서버의 해외 IP를 예외처리 신청 받아서 해당 해외 IP를 허용해주도록 해야 한다.

인터넷 연계서비스의 목적과 서비스 대상이 개별적으로 다르게 설정되어 일괄적으로 해외 IP대역을 제한하는 것이 어려운 경우에는 각 스마트월드 네트워크별로 공인 IP를 가진 스마트월드 운영서버들에 대하여 해외 IP대역을 차단하는 방법을 고려해야 한다.

IP기반의 사이버 공격들은 ID, 비밀번호, 지문인식, 공인인증 방식으로는 막을 수 없는 실정이다. 또한 사이버 공격에 대해서 조사하거나 처벌하려고 하더라도 해외로부터 다수의 사이버 공격이 들어오고 있는 상황에서는 악의적 행위에 대한 조사와 처벌을 하려면 매우 어렵고 복잡한 과정을 거쳐야 한다.

스마트 월드의 구축시 해외로부터의 접근을 제한하는 것은 사이버 공격에 대한 책임 추적성 확보를 위해 필수적이다. 해외의 사이버 공격자들이 국내 IP로 우회하여 유입되는 경우와 해외 IP로 바로 유입되는 경우는 사이버 침해사고 조사를 수행하는데 큰 변화를 줄 수 있을 것이다. 해외를 제한함으로써 사이버 공격자들을 추적하고 조사할 수 있는 발판이 마련될 수 있는 것이다. 우리나라 정보시스템들의 대규모 연계가 이루어지는 스마트 월드에 대한 사이버 공격시 철저한 조사와 처벌이 반드시 필요하다. 사이버 공격자들의 공격의지를 감소시키기 위해서는 사이버 공격을 하면 반드시 조사되고 처벌된다는 것을 사이버공격자들에게 명확하게 인식시키는 것이 중요하다.

4.2 스마트월드 보안관제센터 구축

스마트 월드 구축시 사이버 위협 탐지 대응을 위한 스마트 월드 보안관제센터를 구축 하는 것이 반드시 필요하다. 각 지자체들이 경쟁적으로 구축하는 스마트시티 사례를 살펴보면 보안관제센터의 구축은 간과되고 있는 실정이다. 대부분의 스마트시티 관제센터는 다양한 설비에 대한 장애여부를 모니터링하는 장애관제 기능에 그치고 있다. 여기에 보안관제센터 기능도 추가 구축되어야 할 것이다.

제도적으로 스마트월드 보안관제센터를 신설하여 스마트월드에 대한 사이버 위협을 모니터링하고 대응하는 역할을 수행해야 한다. 스마트월드 보안관제센터에서 국내외 IoT 제조회사간의 통신시 해외 IP대역을 제한하고 국외 IoT 제조사의 공인 IP들을 예외처리해주는 방식을 검토할 수 있을 것이다. 이를 위해서는 국외 IoT 제조사들이 국내에서 IoT 제품을 판매하고자 하는 경우에는 국내 스마트월드 보안관제센터에 반드시 자신들의 운영서버의 공인 IP를 통보하도록 하는 절차를 만들어야 할 것이다. 접수된 해외 IP에 대해서는 사이버안보 담당 부처에 의한 신뢰성 검증이 반드시 필요하다.

4.3 IoT 기기 보안 강화

스마트 월드의 구축시 공인IP를 최소화하고 기기 자체의 보안성을 강화하는 것이 반드시 필요하다. 사물인터넷(Internet of Things, IoT)은 인위적인 개입 없이 센싱, 네트워킹, 정보처리 등 지능적 관계를 형성하는 사물들의 거대한 연결망이라고 할 수 있다. 이를 위한 통신기술은 기존의 센서 기술을 기반으로 근거리 통신기술 NFC, RFID, ZigBee, 블루투스, Wifi 등의 다양한 통신기술들이 사용되어 IoT 운영서버로 데이터를 전송하게 될 것이다. IoT기기들과의 통신을 위해 IP를 부여하게 되는데 공인 IP 대신 사설 IP를 부여하여 상호간의 통신을 하도록 할 필요가 있다. 공인 IP를 부여하는 경우 외부에 노출되어 사이버 공격 위험이 커질 수 있다.

IoT기기 자체가 비인가자에 의해 악의적으로 탈취되지 않도록 패스워드 기반 인증, MAC 주소 기반 인증, 경량 암호 기반 인증 등 사물인터넷 환경에 적합한 단말기기 인증이 강화되어야 한다. 낮은 컴퓨팅 능력, 저전력 사용 등의 특성을 고려하여 암호 강도를 높여 비인가자의 데이터 탈취가 방지되도록 구성해야 한다. 이를 위해 통신에 참여하는 모든 기기들에게 상호인증을 수행하게 하여 IoT 기기 인증을 강화하는 것이 필요하다.

5. 결론

전체 사이버 테러위협의 95% 이상이 해외로부터 유입되고 있는 상황에서 해외 IP 대역의 접속 허용에 대한 심도 있는 논의가 필요한 시점이다. 해외로부터의 접근을 제한하는 것은 사이버 공격에 대한 책임 추적성 확보를 위해 필수적이다. 따라서, 해외 IP대역에 대한 봉쇄가 반드시 필요하다. 이를 위해 각 정보시스템별로 ESC 모델을 적용하여 해외 IP대역을 봉쇄해야 하는 것이다.

해외를 제한함으로써 사이버 공격자들을 추적하고 조사할 수 있는 발판이 마련될 수 있는 것이다. 우리나라 정보시스템들의 대규모 연계가 이루어지는 스마트 월드에 대한 사이버 공격시 철저한 조사와 처벌이 반드시 필요하다. 사이버 공격자들의 공격의지를 감소시키기 위해서는 사이버 공격을 하면 반드시 조사되고 처벌된다는 것을 사이버공격자들에게 명확하게 인식시키는 것이 중요하다. 이러한 모든 활동들을 통해서 우리가 살아갈 스마트월드가 보다 더 안전하게 지켜질 것으로 판단된다.

참고문헌

[1] Guangjie Han, Haofei Guan, Zeren Zhou, Zhifan Li, “CTRA: A complex terrain region-avoidance charging algorithm in Smart World”, Journal of Network and Computer Applications, volume 151, pp. 1 ~ 10, Feb. 2020.

[2] J. Ma, L.T. Yang, B.O. Apduhan, R. Huang, L. Barolli, M. Takizawa, “Towards a smart world and ubiquitous intelligence: A walkthrough from smart things to smart hyperspaces and UbicKids”, International Journal of Pervasive Computing and Communications 1(1) pp. 53 ~ 68, 2005.

[3] Marcelo Masera, ettore F. BoMpard, “Smart (Electricity) Grids for Smart Cities: Assessing Roles and Societal Impacts Information Security”, IEEE, vol. 106, No. 4, April. 2018.

[4] Won Jong-Hyuk, “Effects of Perceived Values and Perceived Risks on Public IoT Services Use Recognition and Use Intention”, Doctor’s Thesis, Department of Educational Administration of Graduate School of Hansung University, pp. 1~187, Dec. 2018.

[5] Jin Sang-Ki, “Life Satisfaction Depending on Digital Utilization Divide within People with Disabilities”, The journal of Informatization Policy Vol. 26, No.3, pp.069-089, Sep. 2019.

[6] Lee Kyungwhan, “An Implementation of Cyber Security Governance System for IOT Enabled Smart City”, Journal of Korean Institute Of Industrial Engineers, pp. 4381-4405, Apr. 2019.

[7] Act on the promotion of smart city development and industry, Act No 16388(Oct. 24, 2019), Ministry of Land, Infrastructure and Transport.

[8] Park GwanSu, “A Study on the Direction of Cyber infringement Response in Smart Home Environment”, Master’s Thesis, Department of Information Technology Graduate School of Aju University, pp. 1-19, Feb. 2019.

[9] KM. Tsui (2012), “Demand Response Optimization for Smart Home Scheduling Under Real-Time Pricing”, IEEE Transactions on Smart Grid 2012.
[10] Yu Woo Young, “A Study on Access Control Policy Management between IoT Devices for Smart Home Security”, Doctor’s Thesis, Department of Security Convergence Graduate School of Chung-Ang University, pp. 1-115, Aug. 2018.
[11] KISA, Jeong Imyoung, “Analysis of Smart Transportation Security Vulnerability and Development for its Countermeasures”, Korea Internet Security Agency, pp. 1~278, Nov. 2017.
[12] NIFDSE, “Smart Healthcare Medical Device Technology & Standard Strategy Report”, National Institute of Food and Drug Safety Evaluation, pp. 1~84, Aug. 2018.
[13] IoT Security Alliance, “Cyber Security Guide for Smart Medical Service”, Korea Internet Security Agency, pp. 1~27, May. 2018.
[14] Lee HooGee, 'A Study on Estimation of Malicious IP Storage Cycle in Security Monitoring Base', Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology Vol.7, No.7, pp. 953-962, July, 2017.
[15] Shin Kyoungsoo, 'A study on cyber threats from North Korea and counterstrategies', ChoongNam National Univ. Doctor’s Thesis, pp. 103-239, Feb, 2018.
[16] Choi HaeGwon, 'Study on trend of DDoS threats and prevention for the Network Service Security Risk', JeonBuk Univ Master’s Thesis, Feb, 2008.
[17] Han Choong-Hee, “Enhanced Security Control model for critical infrastructures with the blocking prioritization process to cyber threats in power system”, International Journal of Critical Infrastructure Protection, Volume 26, 100312, Sept. 2019. (https://doi.org/10.1016/j.ijcip.2019.100312)

〔저자소개〕

한 충 희 (Han Choong-Hee)
1996년 2월 동국대 컴퓨터공학 학사
2002년 2월 동국대 정보보호학 석사
2019년 8월 전남대 정보보호학 박사
email : justicehan@kpx.or.kr

한 창 희 (Han ChangHee)
1990년 육군사관학교 물리 이학사
1994년 美 Syracuse 대학교 전산학 석사
2004년 美 Univ. of Southern California 전산학 박사
1994년~현재 육사 컴퓨터과학과 교수
email : chhan46@gmail.com