특집 05

스마트그리드 사이버 보안 동향

목 차

서정택 · 이철원
(ETRI 부설연구소)

1. 서 론

최근 지구온난화에 의한 기후변화가 세계적인 화제가 되고 있으며, CO_2 가스가 지구온난화의 주요 요인으로 지목되면서 세계 각국은 CO_2 가스 배출의 감축을 위해 신재생 에너지원과 전기차의 도입을 통해 화석연료 사용을 줄이는 등 다양한 노력을 시도하고 있다. 이러한 노력이 성공하기 위해서는 제어가 어려운 신재생 에너지원을 활용할 수 있도록 하며, 전기사용의 효율성을 증가시키고, 전기차 활용을 위한 인프라를 제공할 수 있는 새로운 형태의 지능화된 전력망이 필요하다. 이 새로운 형태의 전력망을 스마트그리드라 부르며, 최근 세계 주요 선진국을 위주로 스마트그리드 구축을 위한 노력이 가속화되고 있다[1].

이렇듯 우리에게 유용한 스마트그리드지만, 정상적으로 운용되지 않을 경우에는 국가 전반에 걸쳐 큰 피해를 유발할 수 있다. 기본적으로 전력망의 정지 및 작동 불능 등으로 인해 전국이 정전 사태에 빠질 수 있고, 이러한 현상이 지속될 경우 국가가 혼란에 빠질 수 있다. 미국 사이버 영향분석 기관(Cyber Consequence Unit)의 수장인 스콧 보그는 미국 전력망의 1/3이 3개월간 정전된다면 카트리나와 같은 대형 허리케인 40~50개에 달하는 피해를 입게 될 것이라고 밝힌바 있다. (그림 1)은 스콧 보그가 발표한 전력망 침해사고로 인한 정전 시 발생할 수 있는 피해에 대한 시나리오를 그림으로 나타낸 것이다.

더욱이 현재의 전력망과 달리 스마트그리드 환경에서는 정보기술이 전력망과 융합되면서 폐쇄망으로 운영하던 전력망이 다양한 정보 시스템과 통신망을 통해서 연결되며, 이러한 연결통로를 통해 사이버 스파이 등 외부 공격자들이 전력망을 장악할 수 있고, 긴급 상황 시 전력망을 공격하여 국가 기반을 무력화 시킬 수 있다.

간단한 정보 시스템 및 웹 서버 등에 대한 사이버 공격의 피해는 개인 및 사업자에게 국한되지만, 스마트그리드에 대한 사이버 공격과 그로 인한 피해는 국가 안보에 위협을 줄 수 있는 중대한 문제이므로 반드시 해결되어야 한다. 실제 미국 에너지부에서도 스마트그리드가 가져야할 특징 중 하나로 사이버 공격에도 견딜 수 있는 능력을 제시했다[2].

(그림 1) 전력망 침해사고로 인한 정전 피해 시나리오

본 논문에서는 전력망 및 스마트그리드에 대한 다양한 사이버 공격 사례를 살펴봄으로써 위험에 처한 스마트그리드 현실을 짚어보고, 국내외에서 진행 중인 스마트그리드 사이버 보안 동향을 살펴봄으로써, 안전한 스마트그리드 개발 및 구축을 위한 초석으로 삼고자 한다.

2. 스마트그리드(지능형 전력망)

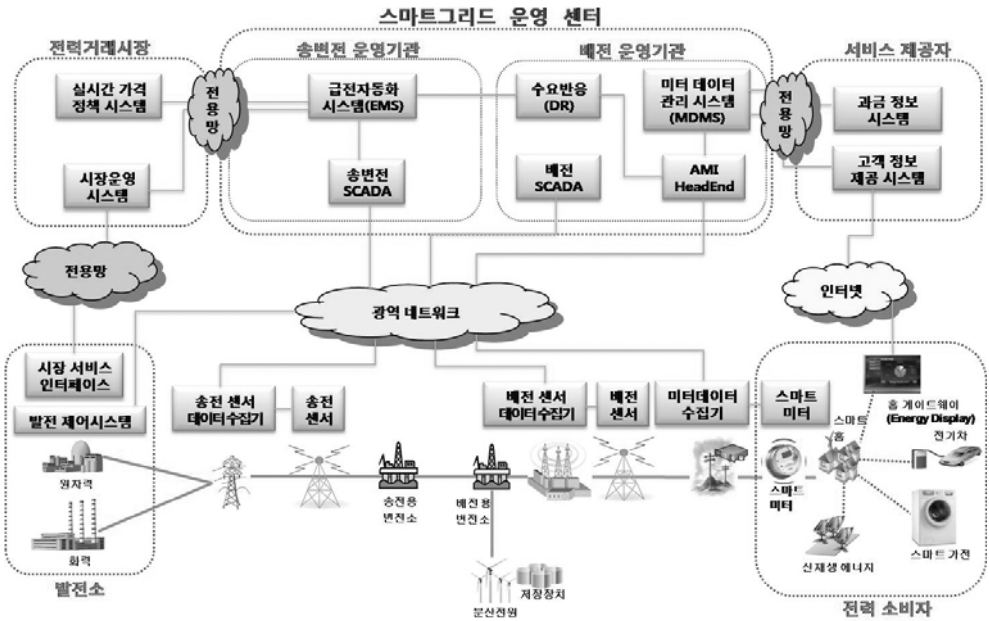
스마트그리드는 전력망에 정보통신 기술을 접목한 새로운 형태의 전력 공급시스템이다[3]. (그림 2)에 나타난 바와 같이 기존의 전력 공급 시스템이 발전소에서 가정에 이르기까지 일방향으로 이루어져 있었는데 비해, 스마트그리드는 전력 공급을 위해서 전력 공급시스템과 사용자가 양방향으로 의사소통하는 시스템이다[4]. 사용자의 전력 사용 데이터가 실시간으로 공급자에게 전달되며, 이를 가공해 생성한 다양한 정보와 실시간으로 변하는 전력 가격 정보가 사용자에게 제공된다. 이러한 정보를 바탕으로 사용자는 자신의 의사에 따라 전력 사용 시간과 양을 제어할 수 있게 된다.

(그림 3)은 미국표준기술원(NIST: National Institute of Standards and Technology)에서 발표한 스마트그리드 운영 모델을 보다 간소화한 것이다[5]. 모델에서와 같이 스마트그리드 환경

(그림 2) 스마트그리드 개념도

에서는 많은 시스템이 복잡하게 얽혀 서로 협력하면서 전력을 안정적으로 공급하고, 깨끗한 전력을 공급하며, 사용자 참여를 유도하여 효율적으로 전력을 사용할 수 있도록 한다.

스마트그리드에서 이러한 일을 가능하게 하는 것은 새로운 형태의 인프라인 AMI(Advanced Metering Infrastructure)와 수요반응(DR: Demand Response) 시스템이다. AMI는 전력공급자와 소비자 사이의 소통을 가능하게 하는 새로운 형태의 통신 인프라다. 각 가정에 설치된 스마트 미터를 통해서 다양한 전력 사용 정보를 원격으로 수집하며, 중앙의 미터 데이터 관리시스템(MDMS: Meter Data Management System)은 수집된 데이터를 보관, 관리, 가공하며, 필요시 에너지관리시스템 및 수요반응 시스



(그림 3) 스마트그리드 시스템 구성도

템 등에게 정보를 제공한다. 수요반응 시스템은 에너지관리시스템 및 MDMS와 연계하여 현 상황의 전력수급현황에 따라 사용자의 전력사용을 제어하는 역할을 수행한다. AMI를 통해 소비자에게 전달되는 실시간 가격 정보 및 개인 전력사용 정보는 소비자가 자율적으로 전력 소비를 결정하는데 도움이 된다.

또한, 송전 및 배전 시스템은 각각 자동화되고 협업이 가능한 모니터링 및 제어시스템을 통해 기기 고장 및 사고를 조기 진단하고, 문제를 자체적으로 해결할 수 있게 된다. 그리고 불안정한 신재생 에너지원을 계통에 안정적으로 연계시켜 깨끗한 에너지를 사용할 수 있게 된다.

스마트그리드 환경은 기존에 단순히 전력 소비만을 하던 소비자가 자신의 상황에 따라 전기를 공급하는 소규모 공급자가 될 수도 있게 한다. 태양광 발전으로 축전된 전기를 공급할 수 있도록 하는 분산전원 기술, 전기 자동차에 충전된 전력을 수요량이 많아 전력이 부족한 상황에 사용하거나 전력 공급자에게 되파는 'V2G (Vehicle-to-Grid)' 기술 등을 통해 이와 같은 일이 가능해진다.

이로써 스마트그리드는 단방향의 전력공급 및 제한적인 전력망 관리 수준에 머물러있던 현재의 전력망을 보다 자율적이며 능동적으로 문제를 해결하며, 소비자의 능동적인 참여를 유도하여 전력소비를 효율화하는 지능화된 전력망으로 변화시킨다.

3. 스마트그리드 사이버 침해 위협

3.1 전력망 사이버 침해 사례

앞서 밝힌 바와 같이 스마트그리드가 우리에게 주는 이로움은 매우 다양하다. 하지만 다양한 소비자 장치와 연계되고, 분산 전원과 연결되는 등 현재 전력망 보다 더 열린 네트워크를 구성하게 되기 때문에, 스마트그리드는 사이버 공격에 보다 더 취약하다. 실제 세계 각국에서는 전력망

에 대한 다양한 공격 사례가 다음과 같이 보고되고 있다.

2003년 1월, 미국 오하이오에 있는 데이비스-베시 원자력 발전소에서는 슬래머 웜이 거의 다섯 시간 동안 보안 모니터링 시스템을 작동 불능으로 만들었고, 이로 인해 발전기가 작동을 멈추었다[6][7].

2007년 8월, IBM ISS社의 연구원 스캇 런스포드는 인터넷과 분리되어 있다고 알려진 원자력 발전소에 인터넷을 통해 침입하였다. 그는 지멘스, ABB, 록웰, 에머슨 등을 포함한 메이저 기업이 제작한 제어시스템 소프트웨어로 구동되는 시스템의 취약점을 이용해 침입한 것으로 밝혀졌다[6].

2008년 1월, 미국 CIA 수석분석가 톰 도나휴는 "Process Control Security Summit"에서 사이버 공격으로 여러 국가에서 정전 사태가 발생했다고 발표했으며, 인터넷을 통한 침입을 주요원인으로 추정하였다[11].

2008년 3월, 미국 조지아 해치 핵발전소에서 운영 중인 시스템에 소프트웨어 업데이트 후 48시간 동안 발전소 가동이 중지되었다[10].

2008년 3월, 미국 국토안보부가 아이다호 국립연구소와 제어시스템에 대한 사이버공격 실험에서 발전소 제어시스템을 해킹하여 발전기 가동 사이클을 변경함으로써 발전기 파괴에 성공했다[9].

2008년 5월 미국 회계감사원(GAO: Government Accountability Office)에서 최대 전력회사인 TVA社의 발전소 제어시스템을 대상으로 시험한 모의해킹에서 인터넷에서 발전소 제어시스템 침투에 성공하였다[8].

2009년 3월 CNN등 주요 외신들에 따르면 미국 보안 컨설팅 업체인 IOActive社는 수년간 스마트그리드 기기들에 대해 보안성을 점검한 결과 해커들이 간단한 해킹 기술로 네트워크에 접속, 전기 공급도 중단할 수 있는 것을 확인하였다[13].

2009년 3월 FBI는 미국 텍사스 전력회사에 해고직원에 의한 컴퓨터 침입이 발생했다고 발표했다. 해고직원은 회사 시스템에 침입해 내부 자료를 자신의 메일로 전송하고, 파일을 수정하거나 삭제했다. 삭제된 파일 중에는 전력 수요 예측에 필요한 데이터가 있었으며, 이에 따라 예측 데이터 생성 실패로 인해 사고 다음 날 댈러스 전력 시장에 전기를 판매할 수 없었으며, 이로 인해 26,000달러 이상의 손해를 입었다[14].

2009년 4월 사이버 스파이가 미국 전력 시스템에 침투하여 시스템을 파괴할 수 있는 악성프로그램을 설치한 것이 발각되었다고 국가안보담당 공무원이 밝혔다. 스파이는 중국, 러시아 등의 출신으로 미국 전력 시스템을 돌아다니며 조작하는 것이 목표였다[12].

2009년 7월 세계 최대의 해킹 컨퍼런스인 BlackHat USA 2009에서 IOActive社의 마이크 데이비스는 스마트 미터에서 동작하는 웜을 시연하였고, 파급효과를 시뮬레이션 했다. 그 결과 24시간 만에 15,000~20,000 가구의 스마트 미터가 감염되었다[15]. 스마트 미터에는 원격지에서 전기 공급을 중단시킬 수 있는 기능이 있으므로, 전파된 웜이 일시에 동작하면 지역적인 정전 사태가 발생할 수도 있다. 더욱이 미터 데이터를 가장한 악성코드가 존재한다면, AMI 운영시스템으로 악성코드를 전파시켜 스마트그리드 운영시스템과 제어시스템 까지도 위험에 빠지게 할 수 있다.

2009년 10월 미국 제어시스템 보안 학회에서 트레비스 굿스피드가 ZigBee 통신 기술 기반 스마트 미터의 회로에서 전류흐름을 읽어 데이터 및 암호키를 알아내는 해킹 기술에 대해 발표했다[16].

국내의 전력망에 대한 사이버침해 사례는 현재까지 공개된 내용은 없다. 그러나 국내의 전력망도 관련 기관간의 정보교환 및 사업상 필요성으로 인하여 인터넷과 연결된 구간이 있을 가능

성이 있고, 그로 인한 사이버침해 발생 가능성이 있으므로 미리 대비해야 한다.

3.2 스마트그리드 보안 위협

앞서 살펴본 다양한 전력망과 스마트그리드 구성요소에 대한 사고 사례를 분석하면, 침해사고의 발생요인을 다음과 같이 다섯 가지로 요약할 수 있다.

첫째, 전력망은 폐쇄망으로 운영된다고 알려진 바와 달리 전력망이 인터넷과 연결되어 인터넷을 통한 웜·바이러스의 감염, 해커의 침입이 가능하였다. 이는 전 세계 어느 곳에서나 인터넷을 통해 전력망을 공격할 수 있음을 시사한다. 이러한 현상은 스마트그리드 환경에서는 더욱 심각해진다. 스마트그리드 환경에서는 소비자 영역에 설치되는 스마트 미터, 송·배전망의 상태를 파악하기 위한 여러 센서 등 물리적 보안이 취약한 다양한 기기들이 설치되며, 이들은 공격자에게 가장 손쉬운 공격대상이 될 수 있다.

둘째, 전력망의 주요 제어시스템에서 사용하는 소프트웨어 문제로 인해 운영이 중지되었다. 스마트그리드 환경에서는 다양한 형태의 서비스가 존재하며, 이를 위해서 많은 소프트웨어들이 시스템에 설치되어야 한다. 따라서 각 소프트웨어의 안전성에 문제가 있거나 보안 취약점이 존재할 경우, 공격자는 이를 이용하는 공격 기법을 통해 운영시스템을 공격하거나, 악성코드를 제작·유포하여 스마트그리드 네트워크를 위험에 빠뜨릴 수 있다.

셋째, 스마트그리드 단말기기에 대한 사이버 보안이 고려되지 않아, 해커에 의해 쉽게 공격을 받을 수 있다. 스마트 미터는 각 가정이나 건물의 외벽에 설치되는 경우가 종종 있으며, 기기 자체에 대한 물리적 보안이 매우 취약하여 공격자가 쉽게 무단으로 접근하여 조작할 수 있다. 특히, 스마트 미터는 운영센터에 위치할 미터데이터 관리시스템과 통신하므로, 공격자가 스마트 미터를 무단으로 조작하여 운영센터 내 시스템으로 침입할 여지가 있다.

넷째, 퇴사한 직원 및 내부 직원에 대한 보안관리 미흡으로 인하여 문제가 발생하였다. 퇴사한 직원에 대한 즉각적인 권한 해제 조치가 이루어지지 않아 이를 이용하거나, 개발단계에서 소프트웨어에 고의로 숨겨두는 취약점을 이용하여 퇴사 직원이 스마트그리드 시스템을 공격할 수 있다.

다섯째, 해커의 공격 대상이 국가 혼란을 유도할 수 있고 파급력이 큰 전력망 등의 제어시스템으로 이동하고 있다. 전력공급이 끊어질 경우 발생할 수 있는 혼란은 이미 서론에서 밝힌바 있다. 만약 전쟁 시에 이러한 혼란이 발생한다면, 전쟁의 승패는 매우 쉽게 판가름이 날 것이다. 따라서 테러단체, 해커 등의 관심이 기존 일반 정보시스템에서 기반시설을 위한 정보시스템으로 옮겨가고 있다.

이러한 사실들을 종합해볼 때, 사이버 보안이 잘 이루어지지 않은 스마트그리드 시스템을 전 국민이 이용한다면, 국민에게 편익을 제공하기 위한 스마트그리드 시스템이 오히려 국가 위기 상황을 초래하게 될 수도 있다. 따라서 스마트그리드의 사이버 보안성을 강화하기 위한 노력이 조속히 시행되어야 한다.

4. 국내·외 스마트그리드 사이버 보안 동향

지금까지 전력망에 대한 침해 사례를 살펴보고, 침해 사례 분석을 통해 스마트그리드 환경에서 발생할 수 있는 사이버 보안 위협에 대해서 알아보았다. 현재 스마트그리드 구축을 서두르고 있는 미국과 유럽에서는 스마트그리드에 대한 보안 위협을 직시하고 이를 해소하기위해서 다양한 노력을 경주하고 있다. 본 장에서는 국내·외의 스마트그리드 사이버 보안 동향을 살펴보도록 한다.

4.1 국외 스마트그리드 사이버 보안 동향

미국은 정부차원에서 스마트그리드에 대한 사이버 보안에 대해 큰 관심을 보이고 있다. 미국은 지난 2007년 제정된 에너지 독립 및 안보법(Energy Independence and Security Act of 2007)에서 스마트그리드 추진에 대한 법률을 제시하였는데, 이 법안에서는 사이버 공격에 대한 대응 능력을 스마트그리드의 주요 기능 중 하나로 명시하였다. 또, 2009년 4월 미국 상·하원 국토안보위원회는 전력인프라보호법(Critical Electric Infrastructure Protection Act)을 발의하여 전력인프라 사이버 침해에 대한 대응 체계를 제시하였다. 이 법안에서는 연방에너지규제위원회(FERC)에 전력 인프라의 사이버보안 관련 긴급 명령 및 제재 권한을 부여하고, 사이버 보안 위협에 대응하기 위한 임시 표준을 정립하도록 요구하였으며, 국토안보부(DHS)에 연방 소유의 중요 전력인프라가 외부로부터 침입되었는지를 알아내기 위한 조사 권한을 부여하였다.

또한 미국 의회는 NIST를 통해서 스마트그리드의 모든 시스템이 상호운용될 수 있도록 표준을 제시하도록 하였으며, 이에 대한 결과물로 NIST에서는 스마트그리드 상호운용성을 위한 표준 로드맵 1차 버전을 2009년 9월 발표하였다[17]. 이 문서는 스마트그리드의 성공을 위해 우선적으로 고려해야 할 표준 목록을 제시하고 있으며, 〈표 1〉에서 보는 바와 같이 제시된 표준 중 8개의 표준이 사이버 보안과 관련되어 있다. 또, NIST에서는 스마트그리드 상호운용성 보장을 위한 업무를 수행하기 위해서 스마트그리드 전문가 그룹인 SGIP(The Smart Grid Interoperability Panel)을 운영하고 있으며, SGIP 내에 스마트그리드 전 영역에 걸친 사이버 보안 문제를 고려하기 위해 사이버 보안 워킹그룹(CSWG: Cyber Security Working Group)을 별도로 운영하고 있다. SGIP-CSWG는 2009년 9월 스마트그리드에 대한 사이버 보안 요구사항을 정립하기 위한 스마트그리드 사이버 보안 전략 및 요구사항에 대한 보고서의 1차 초안을 발

〈표 1〉 NIST가 선정한 스마트그리드 관련 표준 중 사이버 보안 관련 표준 목록

표준명	적용 영역
Security Profile for AMI	MDMS로부터 스마트 미터와 HAN 사이의 인터페이스까지에 이르는 AMI 전 영역에 대한 보안 가이드라인 및 통제사항 제시
Catalog of Control System Security : Recommendation for Standards Developers	물리적 공격 및 사이버 공격의 위협으로부터 제어시스템을 보호하여, 제어시스템의 보안성을 향상시키기 위해, 다양한 기관으로부터 추천받은 보안관행을 집대성하여 제시
DHS Cyber Security Procurement Language for Control System	제어시스템 및 제어서비스를 위한 사이버보안 기술의 조달과정을 위한 가이드라인
IEC 62351 Parts 1~8	전력 시스템 제어 과정에서의 정보보안
IEEE 1686-2007	IED, PLC, RTU 등의 제어장치에 대한 보안 권고사항
NERC CIP 002~009	대규모 전력 설비에 대한 사이버보안 강화 권고사항
NIST Special Publication 800-53	연방 정보시스템 보안강화를 위한 종합적인 보안통제사항
NIST Special Publication 800-82	안전한 산업 제어시스템 구축을 위한 보안 가이드라인

표하고 검토하였으며, 검토 의견을 수렴한 2차 초안을 2010년 2월 발표했다[18].

미국 에너지부의 지원을 받아 스마트그리드 시범사업을 진행하기 위해서는 반드시 각 기술에 대한 사이버 보안 대책을 수립하고 이를 검증할 수 있는 방안을 제시하도록 되어 있다[19]. 이에 따라 현재 모든 스마트그리드 구축을 위한 프로젝트들이 사이버 보안 대책을 수립하기 위해 노력하고 있다.

유럽에서도 스마트그리드 유럽기술플랫폼(SmartGrids : European Technology Platform) 프로젝트에서 2006년부터 2008년까지 스마트그리드 비전 및 향후 연구개발 전략을 수립했다. 이 연구에서는 5개 연구부분에 19개 세부과제를 선정하였으며, 세부과제 중 하나로 "운영·복구, 방어 계획을 위한 아키텍처와 도구"를 선택하였다. 이 과제는 스마트그리드의 장애 및 외부 공격 대응 방안에 대한 연구와 송·배전 시스템의 사이버 보안 및 복구 능력 향상을 위한 방법론을 연구하는 것을 목표로 하고 있다.

또한, EU의 주도로 진행하고 있는 OpenMeter 프로젝트에서는 2009년 7월 보안요구사항을 포함하는 스마트 미터링 명세서를 발표했다. 이는 스마트그리드를 구성하는 중요 인프라인 AMI의 핵심 구성요소인 스마트 미터와 통신 인프라에 대한 보안 요구사항을 제시하고 있다.

4.2 국내 스마트그리드 사이버 보안 동향

현재 국내에서도 스마트그리드에 대한 보안 고려가 차츰 진행되고 있다. 우선 2010년 공표될 스마트 그리드 활성화를 위한 특별법에 사이버 보안과 관련된 내용을 포함시킬 예정이다. 이 법률에서는 전력망 보안체계의 수립과 국가 안보를 위한 보안관제체계의 확립을 종용하고, 기기 및 인프라의 보안관리 체계를 수립하여 보다 안전하게 스마트그리드를 관리하고자 한다.

지난 2010년 1월 지식경제부에의해 발표된 스마트그리드 국가로드맵에서는 스마트그리드 구축을 위한 5개 사업 영역[1]에 대한 실행 로드맵을 제시하고 있다. 각 사업영역에 대한 로드맵들은 모두 사이버 보안을 강화하기 위한 실행계획 로드맵이 포함되어 있다. 로드맵의 주요 내용으로는 스마트그리드의 안전한 구축을 위한 보안 가이드라인을 마련하고, 국가단위의 스마트그리드에 적합한 보안 체계를 마련하도록 하고 있으며, 스마트그리드 보안성 유지를 위한 보안 인증제도를 운영하도록 하고 있다.

또한 현재 진행 중인 제주 스마트그리드 실증단지에서도 스마트그리드의 사이버 보안 문제 해결을 위한 노력을 기울이고 있다. 제주 스마트그리드 실증단지는 국내 스마트그리드 기술을 시험·평가하기 위해 제주도 내 구좌읍을 대상으로 구축되는 시범사업 단지다. 다양한 스마트그리드 시스템이 설치되고 실제 전력계통과 연계되어 운영될 예정이어서 사이버 보안 문제 해결이 필수적이다. 또한 향후 한국형 스마트그리드 모델이 이 사업에서 결정될 가능성이 높으므로, 구축 초기에 사이버 보안에 대한 고려가 반드시 이루어져야 한다. 현재 사업에 참여하는 각 사업자들이 개별적으로 사이버 보안 대책을 마련하고 있으며, 사업을 주도하는 스마트그리드 사업단에서는 국가보안기술연구소를 통해 보안센터를 운영한다. 보안센터에서는 실증단지 보안 가이드라인을 작성하고, 각 시스템 및 기기의 취약점 분석을 수행하며, 사이버 모의 훈련을 수행하는 등 다양한 실증단지 사이버 보안성 강화 업무를 추진한다.

5. 결 론

스마트그리드는 양방향 통신, 정보기술 등을 이용하는 차세대 전력인프라로, 기후변화 개선,

1) 스마트그리드 5개 사업영역에는 지능형 전력망, 지능형 소비자, 지능형 운송, 지능형 신재생, 지능형 서비스 등이 속한다.

에너지 효율성 향상, 신산업 발전 등에 도움을 줄 수 있다. 하지만 스마트그리드가 사이버 공격을 통해 침해를 당하면 작게는 국지적 정전, 크게는 국가 차원의 정전으로 이어질 수 있어 큰 피해가 예상된다. 실제 전력망에 대한 공격 시도는 지속적으로 증가하고 있어 차후 사이버 戰에서는 스마트그리드가 제 1 공격목표가 될 것이다.

이에 미국, 유럽 등의 스마트그리드를 추진하는 국가들은 모두 사이버 보안 강화에 큰 노력을 쏟고 있다. 국내에서도 스마트그리드의 사이버 보안 강화를 고려하고는 있지만, 그 노력의 상대적 크기가 매우 작은 상황이다. 따라서 국내 스마트그리드의 안전을 위해 스마트그리드 보안 강화 노력에 박차를 가해야 하겠다.

참고문헌

[1] F. Sissine, "Energy Independence and Security Act of 2007: A Summary of Major Provisions", CRS Report for Congress, Dec. 2007.

[2] NETL, "A Vision for the Modern Grid", The NETL Modern Grid Initiative, National Energy Technology Laboratory, Mar. 2007.

[3] Office of Electricity Delivery and Energy Reliability, "The Smart Grid: An Introduction", U.S. Department of Energy, 2008.

[4] E.W. Gunther, A. Snyder, G. Gilchrist, D. R. Highfill, "Smart Grid Standards Assessment and Recommendations for Adoption and Development", Technical Report, EnerNex Corporation, Feb. 2009.

[5] U.S. National Institute of Standards and Technology, "NIST Smart Grid Framework 1.0 document", NIST, 2009.

[6] http://www.forbes.com/2007/08/22/scada-hackers-infrastructuretech-security-cx__ag__0822hack.html

[7] Government Accountability Office, "Critical infrastructure protection: Challenges and efforts to secure control systems", GAO-04-354, 2004.

[8] TVA Power Plants Vulnerable to Cyber Attacks, GAO Finds.

[9] http://edition.cnn.com/2007/US/09/27/power.at.risk/index.html

[10] http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html

[11] http://www.msnbc.msn.com/id/22734229/

[12] http://online.wsj.com/article/SB123914805204099085.html

[13] http://www.etnews.co.kr/news/detail.html?id=200903240003

[14] http://www.wired.com/threatlevel/2009/05/efh/

[15] Mike Davis, "Smart Grid Device Secuiry - Advantures in a New Medium", Blackhat USA 2009, July 2009.

[16] Travis Goodspeed, "AMI Hacking Demonstration", Control System Cyber Security Conference 2009, Oct. 2009.

[17] US NIST, "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0", NIST Special Publication 1108, Sept. 2009.

[18] US SGIP-Cyber Security Working Group,

"Smart Grid Cyber Security Strategy and Requirements", Draft NISTIR 7628, Feb. 2010.

[19] US Department of Energy, "Financial Assistance Funding Opportunity Announcement, DE-FOA-0000036", pp. 9~10, Jun. 2009.

저자약력

서 정 택

1999년 충주대학교 컴퓨터공학과(학사)
2001년 아주대학교 컴퓨터공학과(석사)
2007년 고려대학교 정보경영공학전문대학원 정보보호전공(박사)
2001년~현재 한국전자통신연구원 부설연구소 선임연구원 / 과제책임자
관심분야 : 스마트그리드 시스템 및 통신 보안, 제어시스템 보안, 제어시스템 통신 프로토콜 보안, 취약성 분석평가, DDoS 공격 탐지 및 대응
이 메 일 : seojt@ensec.re.kr

이 철 원

1987년 충남대학교 수학과(학사)
1989년 중앙대학교 전자계산학과(석사)
2009년 아주대학교 컴퓨터공학과(박사)
1989년~1994년 한국전자통신연구원 선임연구원
1994년~2000년 한국정보보호진흥원 선임연구원 / 과제책임자
2003년~2004년 Texas A&M University 방문연구원
2001년~현재 한국전자통신연구원 부설연구소 책임연구원 / 본부장
관심분야 : 사이버 안전, 정보보호시스템 평가, S/W 안전성 분석, 산업보안 등
이 메 일 : cheolee@ensec.re.kr