情報保護學會論文誌
第 21 卷 第 5 號, 2011. 10

지능형 전력망 도입과 사이버보안 전략

이 상 근†
한국산업기술진흥원

A Study on Smart Grid and Cyber Security Strategy

Sang-Keun Lee†
Korea Institute for Advancement of Technology

요 약

지능형 전력망은 전력기술에 정보통신 기술을 접목하여 친환경, 고효율, 고신뢰의 지능화된 차세대 전력시스템이다. 이는 종래의 전력 네트워크와는 달리 수용가 및 전력 생산자와 전력망 운영 주체 사이의 양방향 정보 교환을 통해 보다 안정적이고 효율적으로 전력을 공급하도록 한다. 또한 재생 에너지원을 전력계통 운영에 포함시킴으로써 환경 문제에도 도움을 준다. 하지만 지능형 전력망은 양방향 서비스, 중·소규모 에너지원의 증가, 다량의 센서 및 제어기기의 설치 등으로 많은 사이버 보안 위협을 지닌다. 이러한 사이버 위협은 한 번의 실수로 큰 피해를 입게 되는 국가 전력망에 있어서 치명적인 문제가 된다. 따라서 이러한 사이버 보안 위협을 해소하기 위해 지능형 전력망의 사이버보안 전략을 수립하고, 이를 개발 단계에서부터 실제 도입단계에 이르는 전 과정에서 적용해야 한다. 본 논문에서는 지능형 전력망의 사이버 보안 위협을 분석하고 이를 해소할 수 있는 지능형 전력망에 필요한 사이버 보안전략을 제안한다. 사이버 보안전략을 지능형 전력망에 적용함으로써 안전하고 신뢰성 있는 지능형 전력망 구축의 초석이 될 것으로 기대된다.

ABSTRACT

Smart Grids are intelligent next generating Electric Power System (EPS) that provide environment-friendliness, high-efficiency, and high-trustworthiness by integrating information and communication technology with electric power technology. Smart grids help to supply power more efficiently and safely than past systems by bilaterally exchanging information between the user and power producer. In addition, it alleviates environmental problems by using renewable energy resources. However, smart grids have many cyber security risks because of the bilateral service, the increase of small and medium-sized energy resources, and the installation of multi-sensors or control devices. These cyber risks can cause critical problems within a national grid through even small errors. Therefore, in order to reduce these risks, it is necessary to establish a cyber security strategy and apply it from the developmental stage to the implementation stage. This thesis analyzes and recommends security strategy in order to resolve the security risks. By applying cyber security strategy to a smart grid, it will provide a stepping-stone to creating a safe and dependable smart grid.

Keywords: Smart Grids, Cyber Security

접수일(2011년 3월 24일), 게재확정일(2011년 6월 15일)
† 주저자, sky1960@kiat.or.kr

I. 서 론

최근 전 세계적으로 녹색 성장 및 미래 성장 동력의 핵심으로 지능형 전력망을 선정하고, 기술 선점 및 자국의 에너지 안보를 위해 급속히 사업화가 진행되고 있다. 특히 우리나라, 미국, 유럽, 일본 등지에서는 정부주도로 신속한 움직임을 보이고 있다.

지능형 전력망은 기존 전력망 운영 기술과 센서·통신·네트워크·자동제어 등의 정보통신 기술을 전력망에 도입함으로서 에너지를 절약하고, 비용을 줄이며, 신뢰도를 높여 보다 안정적인 전력 공급을 위한 새로운 형태의 전력망이다[1]. 지능형 전력망은 원자력, 수력 및 화력 발전소 등에서 생산된 전력이 송전망 및 배전망을 거쳐 소비자에게 전달되는 과정(grid)을 보다 똑똑하게 만들자는 것으로, 신재생 에너지의 이용 비율을 높여 지구 환경 문제 극복에 일조한다. 그리고 자동화된 송·배전을 통해 보다 안정적으로 고품질의 전기를 사용자에게 공급하며, 실시간 과금 체계를 통해 사용자에게 요금 절약 효과를 제공할 수 있고, 사용자의 요구를 반영하여 사용자에게 더 많은 이익 창출 기회를 제공한다. 또한 국가적으로 산업 활성화, 수출증대, 직업 창출을 통해 경기 부양 및 국가 성장에 새로운 원동력이 될 수 있는 분야다[2].

이렇듯 우리에게 유용한 지능형 전력망이지만, 정상적으로 운용되지 않을 경우에는 국가 전반에 걸쳐 큰 피해를 유발할 수 있다. 지능형 전력망의 정지 및 작동 불능 등으로 인해 전국은 정전 사태에 빠질 수 있고, 이러한 현상이 지속될 경우 심각한 국가 혼란이 초래될 수 있다. 정보기술이 전력망과 융합되면서 전력망이 외부 통신망과 연결되고, 이로 인해서 더욱 다양한 사이버 공격에 노출되어 상기와 같은 사이버 위협이 현실로 나타날 수 있다.

특히 지능형 전력망을 구축하기 위해서는 최종 사용자의 기기, 송·배전 선로 상의 센서, 발전 및 변전 설비에 설치된 센서 등으로부터 필요한 정보를 획득해 상황을 자율적으로 판단하고, 판단된 결과에 따라 스스로 필요한 조치를 내려야 하는데[3], 이 과정에서 잘못된 장치 및 센서에 의해서 수집된 악성 정보가 지능형 전력망 자체의 작동 불능, 불법적인 사용 등으로 이어질 수 있고, 더 나아가 지능형 전력망 내부에 고장을 유발하거나 제어 불능 상태로 만들어 큰 사고로 이어질 수도 있다. 더불어 사용자의 전력 사용 정보를 수집하는 원격자동검침시스템(AMI: Advanced Metering Infrastructure 또는 AMR: Automatic Meter Reading) 환경은 지능형 전력망의 핵심 운영 시스템 및 관리 시스템과 연계될 수 있어[4], 공격자에게는 좋은 침투 경로가 될 수 있다.

간단한 정보 시스템 및 웹 서버 등에 대한 사이버 공격의 피해는 개인 및 사업자에게 국한되지만, 지능형 전력망에 대한 공격과 그로 인한 피해는 국가 안보에 대한 위협만이 아니라 산업 및 일반 시민생활 전체에 재앙적 수준의 피해를 야기할 수 있는 중대한 문제이다. 실제 미국 에너지부에서도 지능형 전력망이 지녀야할 특징 중 하나로 사이버 공격에 견딜 수 있는 능력을 제시했다[5]. 우리나라도 (가칭) '스마트그리드 촉진법안'에 사이버보안위협에 대응하기 위한 법적 조항을 신설하였지만[6], 지능형 전력망을 구현함에 있어 향후 발생 가능한 다양한 보안 취약점을 면밀히 분석하고, 이에 대한 확실한 보안 대책을 세우는 일은 매우 중요한 과제 중의 하나다.

본 논문은 지능형 전력망이 사이버 공격으로부터 안전하게 운영되기 위한 구성 요소들의 보안 요구 사항을 도출하고, 보안 요구사항을 만족하기 위한 사이버보안 요소 기술을 정의하였다. 또한 안전한 지능형 전력망을 구축하기 위하여 사이버 보안 요소 기술 개발을 포함한 사이버 보안 전략을 제안하였으며, 제안한 전략을 통해 향후 지능형 전력망 설계, 도입 및 운영에 있어서 사이버 보안 위협을 예방하고 대응하는 초석이 될 것으로 기대된다.

본 논문은 다음과 같이 구성된다. 2장에서는 지능형 전력망에 대한 소개와 현재 진행 중인 기술동향, 추진 정책 등에 대해서 기술한다. 이후 3장에서는 기존 전력망의 침해사고를 분석하여 지능형 전력망에서 발생 가능한 사이버침해 위협 요소들을 분석하고, 이를 해소하기 위한 사이버 보안 전략을 제안한다. 끝으로 4장에서 본 논문의 결론을 맺는다.

II. 지능형 전력망

2.1 개요

지능형 전력망은 전력망에 정보통신 기술을 접목한 새로운 형태의 전력 운영시스템이다. 기존의 전력 공급시스템은 발전소에서 가정에 이르기까지 일방향으로 구성되었지만, 지능형 전력망은 전력 공급을 위해서 전력 공급시스템과 사용자가 양방향으로 의사소통하는 시스템이다[7]. 공급자는 실시간으로 전력 사용정보를 제공하여 사용자의 의사에 따라 전력 사용 시간

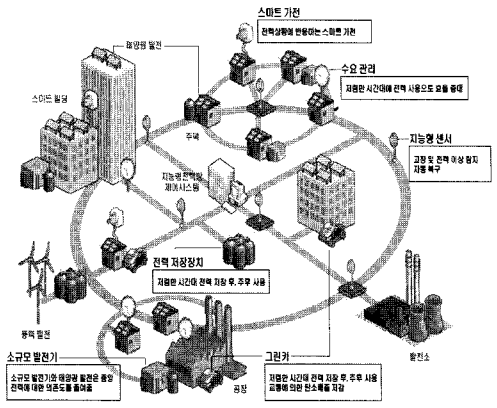
과 양을 제어할 수 있게 한다. 즉, 각 가정의 개별 전자제품의 전력 소모량과 이로 인한 탄소배출량 등을 사용자가 직접 확인할 수 있게 된다.

지능형 전력망 환경에서는 각 가정과 건물이 실시간으로 에너지 사용량을 확인할 수 있어 언제 사용량이 폭증하며 어느 시간 때에 사용량이 줄어드는 지를 확인할 수 있다. 또한 태양광 패널·연료전지·배터리 시스템 등 분산된 에너지 공급원을 활용해 전력 사용 피크 때를 대비해 미리 에너지를 확보할 수 있으며 연료전지 및 소형 발전기 등을 상황에 따라 자동적으로 가동할 수 있도록 해준다. 이를 위해서 수요가 폭증할 때 가동되는 에너지 집약 설비의 가동을 차단하거나 늦추는 등의 수요 절감기술을 활용하기도 한다[8].

지능형 전력망 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[9], 전기 자동차에 충전된 전력을 수요 피크 시 사용하거나 전력망에 되파는 'V2G(Vehicle-to-Grid)' 기술 등이 이러한 생각을 가능하게 한다[10].

〔그림 1〕은 지능형 전력망의 개념도를 나타내는 것으로 스마트 가전, 스마트 빌딩, 스마트 주택, 수요 관리, 지능형 센서, 전력 저장장치 등의 구성요소가 양방향 통신을 통해 지능형 전력망의 개념을 구체화한다. 즉 공급자 중심의 전력망이 소비자 중심으로, 중앙 집중적 발전이 분산 발전 통합제어로, 수동 복구 감시가 자가 자동 복구로, 제한적인 가격 신호를 가지던 시장에서 수요를 지원하는 시장으로 변화되는 것을 보여준다[11].

〔표 1〕은 지능형 전력망과 현행 전력망의 주요 특



〔그림 1〕 지능형 전력망 개념도

〔표 1〕 기존 전력망과 지능형 전력망 비교

항목	기존 전력망	지능형 전력망
통신	단방향	양방향(Interactive)
전력공급원	중앙전원(발전소), 소수 대규모	분산전원(발전소,태양광, 풍력 등), 다수 소규모
고장진단	불가능	자가 진단
고장복구	수동 복구	반자동 복구 및 자가 복구
설비점검	수동	원격
가격정보	제한적 (한달에 1회 총액만)	실시간으로 모든 정보 열람
소비자 전력 구매 선택	제한적	다양

출처 : 고동수, "녹색성장 구현을 위한 지능형 전력망 도입", 산업연구원 Issue Paper 2009-244

징을 비교한 표이다. 현행 전력망이 단방향 통신, 중앙전원, 제한적 가격 정보 제공 및 전력 구매의 선택이 제한된데 반해 지능형 전력망은 양방향 전원 제공, 자가 공장진단 및 자가복구, 원격 설비 점검, 실시간 정보 제공 등을 특징으로 한다.

2.2 도입배경

지능형 전력망은 다양한 목적에 의해 연구 개발이 시도되어 왔다. 지능형 전력망은 유럽, 미국, 한국 등 8개국에서 연구 개발을 추진 중이다.

유럽의 경우 신재생 에너지 자원을 활용한 전력원이 발달하면서 이를 최대한 활용하기 위한 계통운영 시스템이 필요하게 되었고 이를 위해 지능형 전력망을 연구하기 시작하였다[12]. 유럽의 지능형 전력망 전략에서 주목할 만 것은 기존의 전력에 정보통신 기술을 활용하는 수준을 넘어서, 에너지 라이프 사이클 전 단계에 걸쳐서 정보통신 기술을 확산시키는 방향으로 에너지 부문에서의 정보통신 활용범위를 확대하고 있다는 점이다. 즉 '스마트 에너지 네트워크' 과제에 기존의 지능형 전력망뿐 아니라 가스망(gas networks)의 지능형 시스템 구축을 포함하고 있다.

미국은 다양한 중소규모 정전 사태에 대응하기 위해서 노후한 설비의 최신화 및 디지털화를 피하기 위해서 지능형 전력망 연구를 수행하기 시작하였다[13]. 특히 미국의 전력산업은 대단히 보수적·폐쇄적 특성을 가지고 있어, 과거 30여 년간 전력설비에 대한 저조한 투자로 인해 전력망의 비효율성이 커지고 전력공급 신뢰도가 하락하는 등 엄청난 손실을 보고 있었다. 그리

고 여러 가지 규제 및 환경 이슈로 인하여 대규모의 발전, 송·변전 및 배전 설비의 투자 및 건설이 현실적으로 불가능하였고, 2003년 발생한 북동부 대규모 정전사고로 인해 지능형 전력망 연구에 더욱 박차를 가하게 되었다[14].

우리나라는 에너지·환경 문제와 그린산업 육성과제를 해결하기 위한 수단으로서, 또한 향후 새롭게 열리고 있는 지능형 전력망 세계시장을 선점할 수 있는 대표산업으로 육성하기 위하여 2010년 1월 '스마트그리드 국가 로드맵'을 확정하였다. 동 계획에 따르면 '스마트그리드 구축을 통한 저탄소 녹색성장 기반 조성'을 비전으로 설정하고, 시범도시·광역시도 등 '先거점구축, 後확산전략'에 따라 2030년까지 국가단위의 스마트그리드 구축완료를 목표로 설정하고, 이를 위해 지능형 전력망, 소비자, 수송, 신재생, 서비스 등 5대 분야에 대한 단계별 기술개발 및 비즈니스 모델을 제시하였다[15]

2.3 기술동향

현재 미국에서는 에너지부의 지원하에 EPRI (Electric Power Research Institute)에서 연구중인 인텔리 그리드[16]와 GridWise™ Alliance에서 개발 중인 그리드 와이즈[17] 등이 지능형 전력망의 주요 연구가 되고 있다.

EPRI의 인텔리 그리드에는 전체 지능형 전력망을 구성하기 위한 아키텍처 개발, 분산전원기술, 지능형 배전기술, 고속 계통 시뮬레이션 및 모델링 기술, 사용자 지원환경 등에 대한 연구 개발이 포함되어 있다. 또한 이산화탄소 포집 및 저장기술, 하이브리드 기술 개발 등의 연구가 진행되고 있다. 전력발전, 전송에서부터 환경, 안전, 건강 문제 등을 포함한 전력에너지와 환경기술 전 영역을 다루고 있다.

GridWise™는 에너지부의 배전분야 부서에 의해 설립 되었으며, 여러 전력 회사의 대표자들로 이루어진 GridWise Alliance로 구성되어 있다. 정기적으로 회의 및 성과 보고를 통해 기술 교류를 꾀하고 있으며, 인터넷을 통해 GridWise 전자 신문 및 보고서 등을 공개하고 있다. 사업자 및 일반 시민들도 이런 정보에 쉽게 접할 수 있다.

또한 미국의 엑셀에너지는 콜로라도주 볼더시를 지능형 전력망 도시로 만드는 프로젝트를 추진하여, 현재 볼더시에는 AMI를 비롯해, 사용자가 전력 소비 정보를 확인할 수 있는 웹포탈, 가정에서 태양광을 통해 발전된 전기를 사용하거나 다시 되파는 환경 등을 제공하고 있다[18].

대학에서도 지능형전력망 관련 연구가 활발히 진행중이다. UC Berkeley의 CITRIS[19]는 에너지 효율, 수송, 지진 안전, 교육, 헬스케어, 그리고 환경 등의 연구를 실용화시키기 위해 노력하고 있으며, 특히 전력 수요응답 제어에 대한 연구를 수행하고 있다. University of Illinois at Urbana Champaign[20]에서는 분산전원을 실제로 구현할 때 직면할 수 있는 문제점 중 하나인 계통연결문제의 해결방안과 새로운 분산전원 기술에 대해 연구하고 있다.

국내에서는 2005년부터 진행되어온 전력IT 10대 과제가 사실상 지능형전력망의 전초가 된다[21]. 이 10대 과제의 핵심 기술들은 실제 지능형전력망 환경에서 요구하는 지능화된 전력계통 운영 기술을 포함하고 있다. 그러나 분산 전원 기술 및 사용자와의 양방향 의사소통을 위한 환경, 사용자 요구 수용 및 대응 등에 대한 연구가 부족하다. 특히 전력 계통 운영 시스템의 사이버 공격에 대한 보안 기술 연구가 초보 단계에서 진행되고 있는 실정이다.

2.4 정부정책 및 추진전략

미국은 지능형 전력망에 대한 국가 차원의 종합 개발계획 수립 및 정책을 제시하고 있다. 언제 어디서나 풍부하고 저렴하면서도 깨끗하고 효율적이며 믿을 수 있는 전력을 누구든지 이용할 수 있는 환경을 실현하기 위해 2003년 Grid 2030[22]이라는 전력시스템에 대한 최초의 국가비전을 수립하였으며, 2004년 National Delivery Technology Roadmap을 통해 비전을 현실화하기 위한 기술 로드맵을 제시하였다. 2007년 Modern Grid 프로젝트[23]를 통해 Grid 2030의 비전을 9개 항목으로 구체화하였다. 2007년에는 에너지 안보법 (Energy Independence and Security Act of 2007, EISA 2007)을 제정하였다[24]. 이 법안은 지능형 전력망, 에너지 안보, 에너지 절약 등과 관계된 연구 개발 및 시장 적용을 유도하는 내용이다. 2009년에는 에너지부 표준화 사업을 통해 지능형 전력망 산업 전반의 표준을 작성하고 있다. 2009년 오바마 행정부는 지능형 전력망을 녹색뉴딜정책의 핵심정책으로 추진하고, 지능형 전력망에 33억 달러 이상 투자계획을 발표하였다.

유럽은 2005년에 유럽기술플랫폼 지능형 전력망[25]을 설립하여 2006년에서 2008년까지 지능형 전력

망의 비전 및 연구개발 전략을 수립하고 5개의 연구 부문에 19개의 세부과제를 선정하여 지능형 전력망 구축을 추진 중이다. 세부과제 내 "운영, 복구, 방어 계획을 위한 아키텍처와 도구"에는 지능형 전력망의 장애 및 외부 공격 대응 방안 연구가 포함되어 있다[26].

국내에서는 2009년 2월 대통령직속 녹색성장위원회 첫 회의에서 4대 실천과제의 하나로 국가단위의 '지능형 전력망' 구축 비전을 보고하였다. 2009년 3월 녹색성장위원회와 지식경제부가 주최하고, 한국전력이 주관하는 "지능형 전력망·그린카 세미나"를 개최하였으며, "지능형 전력망·그린카 실증단지 및 테마파크" 조성계획이 발표되었고, 2010년 1월 지능형 전력망 구축을 위한 상세 로드맵이 확정되었다[27].

국내의 지능형 전력망 추진전략은 기술개발, 로드맵 수립, 국제적 협력을 통해 2030년까지 세계 최초의 국가단위 스마트그리드 구축완료를 목표로 설정하고, 이를 위해 지능형 전력망, 소비자, 수송, 신재생, 서비스 등 5대 분야에 대한 단계별 기술개발 및 비즈니스 모델을 제시하였다. 특히 기업의 속도감 있는 비즈니스 모델 개발을 제도적으로 지원하기 위해 "스마트그리드 촉진법"에 대한 입법이 국회에 제출중에 있으며, 제주 실증단지에서 검증된 제품과 기술에 대해서는 국가표준으로 제정하고, 국내 보급사업에 우선적으로 지원할 계획이다. 또한 정책 및 기술개발 관련 의견교환을 통해 시행착오를 최소화하고 기술표준 협력을 통해 미국 수출시장 선점기회를 마련하기 위해 지능형 전력망 추진의 선두주자인 미국과의 전략적 협력을 추진한다. 이러한 계획에 따라 2011년 지능형 전력망 시범도시 지정, 2020년까지 소비자측 지능화 완료, 그리고 2030년에는 총 전력망에 대한 지능화 완료를 추진하고 있다[28].

III. 지능형 전력망에 대한 사이버보안전략

본 장에서는 현재의 전력망에 대한 사이버침해 사례를 검토하고, 이러한 사이버침해 사례가 지능형 전력망에 전개되지 않도록 하기 위한 사이버보안 전략을 제안한다.

3.1 전력망에 대한 사이버침해 사례

본 절에서는 전력망에 대한 사이버침해 사례에 대해서 소개한다.

2003년 1월, 미국 오하이오에 있는 Davis-Besse 원자력 발전소에서는 슬래머 웜이 거의 다섯 시간 동안 보안 모니터링 시스템을 작동 불능으로 만들었다[29][30].

2008년 5월 미국 회계감사원(GAO)에서 최대 전력회사인 TVA社의 발전소 제어시스템을 대상으로 시험한 모의해킹에서 인터넷에서 발전소에 침투하여 발전기 조작을 성공하였다[31].

IBM ISS의 연구원 스캇 런스포드가 원자력 발전소 침투 테스트를 하겠다고 제안하자, 원자력 발전소는 인터넷으로 발전소 주요시설을 접속할 수 없기 때문에 불가능할 것이라고 주장하였으나, 런스포드는 첫째날 네트워크를 침입했고, 일주일 만에 원자력 시설을 제어할 수 있는 수준까지 침투에 성공하였다. 런스포드가 공격한 취약 시스템은 지멘스, ABB, 록웰, 에머슨 등을 포함한 메이저 기업이 제작한 스카다 소프트웨어로 구동되는 시스템인 것으로 밝혀졌다[32].

2008년 3월, 미국 국토안보부가 아이다호 국립연구소와 제어시스템에 대한 사이버공격 실험에서 발전소 제어시스템을 해킹하여 발전기 가동 사이클을 변경함으로써 발전기파괴에 성공하였다. 그리고 같은 해 3월, 미국 조지아 해치 핵발전소에서 운영중인 시스템에 소프트웨어 업데이트 후 48시간 동안 발전소 가동이 중지되었다[33].

2008년 1월, 미국 CIA 수석분석가는 "Process Control Security Summit"에서 사이버 공격으로 여러 국가에서 정전 사태가 발생했다고 발표했으며, 인터넷을 통한 침입을 주원인으로 추정하였다[34].

2009년 4월 미국 정부공인 규제 기관은 전력회사들이 전력 시스템 사이버 공격 취약점의 정확한 분석에 실패했다고 결론 내렸다. 몇몇 보안전문가들은 러시아, 중국 등지에서 전력 시스템의 컴퓨터에 침입 시도가 있었음을 연방정부가 감지했다고 언급하였다[35].

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. 또한 CIA의 수석분석가는 최근 여러 나라에서 사이버공격에 의해 정전이 발생했다고 발표하였다[36].

2009년 3월 CNN등 주요 외신들에 따르면 미국 보안 컨설팅 업체인 IOActive社는 수년간 스마트 그리드 기기들에 대해 보안성을 점검한 결과 해커들이 간단한 해킹 기술로 네트워크에 접속, 전기 공급도 중

단할 수 있는 것을 확인하였다[37].

2009년 3월 FBI는 미국 텍사스 전력회사의 퇴직한 직원에 의해 컴퓨터 침입이 발생했다고 발표하였다. 컴퓨터 침입에 의해 회사 에너지 예측 시스템에 문제가 발생하였으며 26,000달러 이상의 손해를 입었다[38]. 해고된 직원은 Comanche Peak 핵발전소를 포함한 발전소 관리 시스템의 개발자였으며, 해고 당일 자신의 VPN 계정을 이용해 회사 시스템으로 들어가 내부 자료를 자신의 메일로 전송하고, 파일을 수정하거나 삭제했다. 삭제된 파일 중에는 전력 수요 예측에 입력으로 제공되어야 하는 데이터가 포함되어 있었으며, 이에 따라 2009년 3월 4일자 예측 자료를 생성할 수 없어 댈러스 전력 시장에 전기를 팔 수 없었다. 최근 독일 지멘스사의 산업자동화제어시스템을 공격 목표로 제작된 악성코드인 스턱스넷(Stuxnet)은 원자력, 전기, 철강, 반도체, 화학 등 중요 산업기반 시설의 제어시스템에 침투해 오작동을 발생시켜 시스템을 마비 시키고 있다. 제어시스템을 파괴하는 스턱스넷은 이란 부세르 원자력 핵발전소와 중국 1000여개 주요 산업시설을 비롯해 전세계 여러 국가에 감염을 확산시킨 것으로 보고되고 있다[39].

국내의 전력망에 대한 사이버침해 사례는 현재까지 공개된 내용은 없지만, 지식경제부 사이버안전센터의 내부 자료[40]에 따르면 2009년 2,933건과 2010년 4,270건의 사이버공격이 탐지 되었다. 사이버공격 시도는 2009년에는 전력부문에 2010년에는 전력부문과 무역, 산업 및 R&D 부분에 집중 되었다. 그 외에도 2009년 7월과 2011년 3월에 국내에서 발생한 조직적인 DDoS 공격시도는 정부 및 공공기관 그리고 주요 산업시설 통신망 운영에 대한 경각심을 주고 있다. 따라서 국내의 전력망이 인터넷과 물리적으로 분리되어 운영된다고 하나 관련 기관간의 정보교환 및 사업상 필요성으로 인하여 인터넷과 연결된 구간이 있을 가능성이 있고, 그로 인한 사이버침해 발생 가능성이 있으므로 미리 대비해야 한다.

이상에서 제시한 전력망과 지능형 전력망 구성요소에 대한 사고사례의 시사점을 분석하면 다음과 같이 요약할 수 있다.

첫째, 전력망은 폐쇄망으로 운영된다는 일반 상식과는 다르게, 전력망이 인터넷과 연결되어 인터넷을 통한 웜·바이러스의 감염, 해커의 침입이 가능하였다. 이는 전 세계 어느 곳에서나 인터넷을 통해 전력망을 공격할 수 있음을 시사한다.

둘째, 전력망의 주요 제어시스템에서 사용하는 소프트웨어 문제로 인해 운영이 중지되었다. 이러한 사례는 제어시스템의 소프트웨어가 해커에 의한 공격으로 문제를 유발할 수 있으며, 이로 인한 전력망 운영이 중지될 수 있음을 시사한다.

셋째, 지능형 전력망의 필드 기기들에 대한 사이버 보안이 개발 단계부터 고려되지 않아, 해커에 의해 쉽게 공격을 받을 수 있다.

넷째, 퇴사한 직원 및 내부 직원에 대한 보안관리 미흡으로 인하여 문제가 발생할 수 있으며, 이에 대한 대책이 필요하다.

다섯째, 해커의 공격 대상이 국가 혼란을 유도할 수 있고 파급력이 큰 전력망 등의 제어시스템으로 이동하고 있다. 따라서 향후 지능형 전력망이 구축되면 공격 경로의 증가로 인해 해커의 공격 대상 일 순위가 될 것으로 추정된다.

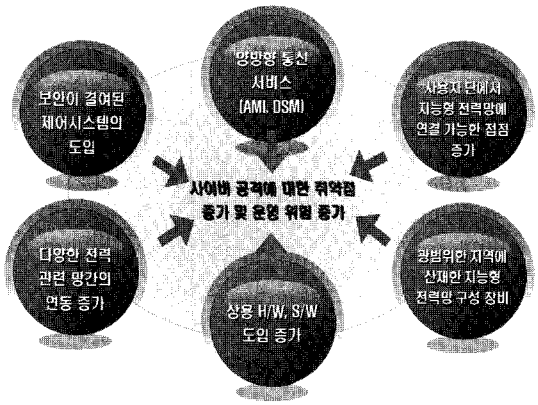
3.2 지능형 전력망 보안 고려사항

3.2.1 지능형 전력망의 사이버 보안 위협 발생 요인

기존 전력망이 대규모 발전소로부터 생산되는 중앙전원으로부터 전력 수요자까지 일방향의 전력 전달체계로 구성된 반면, 지능형 전력망은 사용자단에 연결되는 다수의 장비와 이들 장비와 운영기관의 양방향 통신 서비스, 분산 전원 공급자의 증가 등의 특성으로 인해 사이버 공격이 증가할 것으로 예상된다. 특히 지능형 전력망의 기반 통신망으로 논의되고 있는 FTTH, HFC 등의 유선 통신과 WiFi, WiMAX, 3G, TDMA, CDMA, VSAT 등의 무선통신은 개방형 네트워크 형태를 취하고 있다. 이로 인해 웜이나 바이러스에 의한 해킹이나 서비스거부 공격등과 같은 사이버 공격 위협이 현저하게 높아질 것으로 예상된다. 기존 전력망에서는 기본적으로 폐쇄망을 사용하였기 때문에 보안에 크게 문제가 되지 않았지만, 지능형 전력망에서는 개방된 네트워크의 사용으로 인하여 위협요인 전달경로가 다양화됨에 따라 보안 취약성이 보안이슈로 제기되고 있다[41].

지능형 전력망의 사이버 보안 위협의 발생 원인은 [그림 2]와 같은 요인들에 의해서 기존 전력망보다 증가할 것으로 예상된다.

첫째, 지능형 전력망에서는 최종 단말 장치와 내부 운영 시스템 사이의 양방향 정보 교환이 필요하다. 지능형 전력망은 다양한 정보 수집과 요구 사항 수집을 통해 적절한 전력 수급 및 계통 운영을 자동화하며,



〔그림 2〕 지능형 전력망 보안 취약점 발생 요인

또한 필요에 따라 지능형 전력망 운영 시스템에서 최종 단말 장치로 제어 명령 및 정보 제공을 해야 할 필요가 있다.

이를 통해서 효과적으로 지능형 검침 장치(AMI : Automated Meter Infrastructure), 주문 관리(DSM : Demand-Side Management), 송/배전 관리 등의 시스템을 운영할 수 있다. 그러나 사용자 단에 설치된 기기들도 운영 시스템과 양방향 통신을 수행하기 때문에 스마트 미터와 같은 사용자 단 기기를 탈취함으로써 지능형 전력망의 운영 시스템 및 제어시스템에 접속하여 사이버 공격이 가능하다.

둘째, 지능형 전력망에서는 사용자 단에서 전력망에 접속할 수 있는 접점의 수가 증가하게 된다. 즉 지능형 전력망을 효과적으로 사용하기 위해 모든 가정에서 접속하는 스마트 가전, 각 가정의 전력 사용량 측정 등을 수행하는 스마트 미터, 스마트 미터로부터 정보를 수집하는 지능형 검침 장치 등 사용자 단에서 지능형 전력망으로 접속되는 장치의 수가 증가한다. 이러한 지능형 전력망에 접속하는 장치의 수가 증가할수록 공격자에게는 공격 경로의 수가 증가하는 것이며, 이를 통해서 사이버 공격이 증가할 수 있다.

셋째, 광범위한 지역에 산재한 지능형 전력망 구성 장비에 의해 사이버 공격이 증가할 수 있다. 앞에서 설명한 바와 같이 지능형 전력망을 구성하는 구성요소는 각 가정에서부터 설치되고, 송전 및 배전망에도 관련 정보의 수집을 위한 다양한 센서가 설치된다. 이와 같이 광범위한 지역에 설치된 장치들에 대한 엄격한 보안관리가 요구된다. 광범위한 지역에 산재된 장치들에 대한 보안관리가 미흡할 경우 공격자에 의해 사이버 공격의 경로로 활용될 수 있다.

넷째, 지능형 전력망에서는 이미 개발되어 있는 상용 하드웨어 및 소프트웨어 기술을 지능형 전력망 환경에 적합하게 수정하여 사용하는 경우가 증가할 것이다. 지능형 전력망은 기존 전력망 기술과 정보통신 기술의 융합을 통해서 개발되므로 기존에 개발된 상용 정보통신 기술이 많이 도입될 것으로 예측된다. 특히 통신 기술 및 소프트웨어 기술 등이 이에 해당한다. 하지만 이는 상용 정보통신 기술에 현존하는 다양한 사이버 보안 위협이 곧 지능형 전력망에서의 사이버 보안 위협으로 이어질 수 있음을 의미한다. 이는 상용 소프트웨어 및 통신 기술의 취약점을 알고 있는 공격자는 동일한 기술을 이용하여 지능형 전력망을 공격할 수 있음을 의미한다.

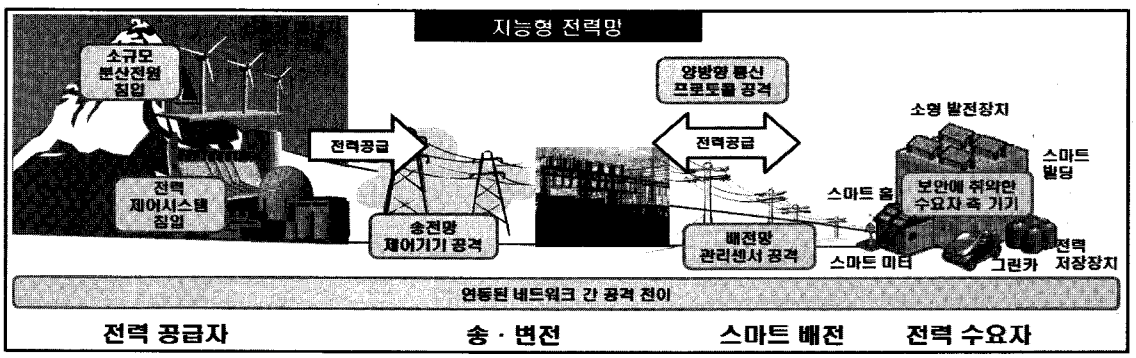
다섯째, 지능형 전력망에 참가하는 다양한 전력 관련 네트워크인 급전자동화시스템, 발전 제어시스템, 내부업무망, 원격자동검침망 등의 다양한 망간의 자료 교환을 위하여 네트워크간 연동이 증가한다. 이러한 네트워크 간 연동의 증가는 하나의 네트워크가 공격자에게 공격을 당하면 다른 네트워크로 공격이 전이될 수 있으며, 이를 통해 전체 지능형 전력망에 영향을 미칠 수 있다.

여섯째, 지능형 전력망 역시 정보기술이 융합된 전력망의 일종이며 제어 시스템의 관리 하에 운영된다. 기존에 사용하고 있는 대부분의 제어시스템은 사이버 보안에 대한 고려가 부족하거나 고려 없이 개발되어서, 이로 인해 다양한 보안 취약점을 내재하고 있어 보안 위협이 크다. 지속적으로 보고되고 있는 전 세계 다양한 제어시스템 해킹 관련 사례 발표[42], 보안 기술 연구[43][44][45], 취약점 보고[46] 등이 이를 뒷받침한다. 즉 기존 제어시스템이 가진 취약점을 이용한 사이버 공격이 가능하며 공격자의 관심이 파급 효과가 큰 영역으로 이동됨에 따라 지능형 전력망은 매우 중요한 공격 대상이 될 것으로 예상된다.

3.2.2 지능형 전력망 보안 위협

지능형 전력망의 보안 위협을 발생하는 요인들을 기준으로 지능형 전력망에서 발생 가능한 보안 위협을 설명한다. 〔그림 3〕은 지능형 전력망의 보안 위협 및 경로를 표시한 것이다.

지능형 전력망의 첫 번째 보안 위협은 보안 기능을 제공하지 않는 사용자 단의 취약한 전력 수요자측 기기로서 스마트 미터, 원격 검침 장치 등이 있다. 3.1절의 사고 사례에서도 설명한 바와 같이 보안 기능이 없는 스마트 미터는 공격자들이 간단한 해킹 기술로

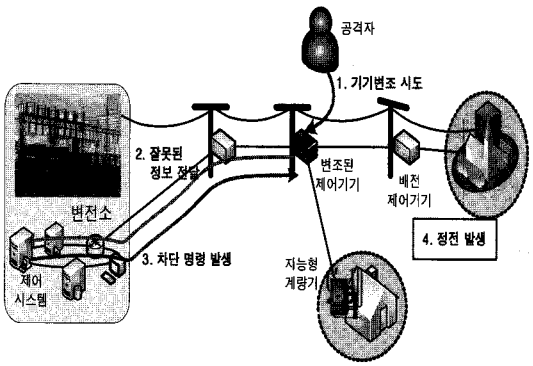


〔그림 3〕 지능형 전력망 보안 위협

네트워크에 접속 해 전기 공급도 중단할 수 있었다. 지능형 전력망이 본격 구축되면 각 사용자 단에 설치되는 각종 기기는 지능형 전력망 공격의 제일 목표가 될 것이다. 따라서 수요자측에 설치되는 기기를 보호할 수 있는 보안 기술을 지능형 전력망 기술개발 및 도입 초기부터 고려해야 한다.

두 번째 보안 위협은 스마트 배전을 위해 배전 구간에 설치되는 배전망 관리 센서이다. 배전망 관리 센서들은 배전 상태 정보를 수집하고, 수집된 정보를 배전 담당 시스템으로 전송하여 배전을 지능적으로 수행할 수 있도록 한다. 이러한 배전망 관리 센서를 공격자가 장악하여 악의적인 정보를 지속적으로 전송함으로써 특정 지역의 정전 사태를 유발할 수 있다.

예를 들어 〔그림 4〕와 같이 공격자가 배전 선로에 설치된 여러 센서를 자신이 만든 잘못된 정보를 보내는 센서로 교체하고, 해당 선로에 문제가 생겼음을 인지할 수 있는 정보를 지속적으로 제어시스템에 보고할 경우, 실제 상황과는 관계없이 제어 시스템은 해당 선로의 전원 공급을 차단하는 명령을 내리게 된다. 이로 인해 주변 지역은 전원 공급이 차단되어 정전 사태를 겪게 되고, 이는 큰 손실로 연결된다.



〔그림 4〕 배전 제어기기 해킹을 통한 전력망 오작동

세 번째 보안 위협은 대형 발전소 및 중소형 신재생에너지 발전소 등에서 생산된 전력을 전달하는 송전 선로를 제어하는 제어기기이다. 지능형 전력망에서는 송전 상태 감시를 위한 센서를 송전 선로상의 송전탑 및 송전선로에서 지속적으로 수집하여 이를 토대로 지능적으로 전력망을 운영하게 된다. 두 번째 보안 위협과 동일한 방식으로 송전 제어기기 및 센서를 장악하여 악의적인 정보를 지속적으로 전송함으로써 전력 수급에 불균형을 초래할 수 있다.

네 번째 보안 위협은 지능형 전력망에 사용되는 양방향 통신 프로토콜이다. 지능형 전력망은 다양한 역할을 담당하는 시스템들이 상호작용하며 사용자에게 효율적이고 안정적인 전력공급을 담당한다. 이를 위해서는 다양한 시스템들 사이에 상호작용을 돕거나 제어 기능을 수행할 수 있도록 하는 통신 프로토콜이 필요하다. 현재의 전력망은 이러한 상호 정보 교환 및 제어 명령 전달을 위해서 〔표 2〕와 같은 프로토콜들을 사용하고 있다[47][48][49]. 지능형 전력망 역시 다양한 역할을 담당하는 시스템들이 상호운용성 보장 및 서비스 운용을 위해서 이와 같은 프로토콜을 사용할 것이다. 특히 DNP와 ICCP는 현재의 전력망 환경에서 널리 고려되고 있는 프로토콜이다.

〔표 2〕에서 보는 바와 같이 각 프로토콜들은 현재 보안성이 전혀 고려되고 있지 않다. 전력망 제어 시스템이 일반 네트워크와 분리되어 있어 안전하다는 생각 때문이다. 하지만 지능형 전력망 환경이 되면 사용자 정보 및 소규모 분산 전원 등과 정보 교환을 해야 하므로 통신 연계점이 생기게 마련이고, 이 경우 보안에 취약한 현재 프로토콜들은 공격자의 침투 경로로 사용될 수 있다.

〔표 2〕 제어 시스템에서 사용하는 제어 메시지 교환 프로토콜

프로토콜	설명	전력망 내 사용범위	관련 표준	보안성
DNP (Distributed Network Protocol)	제어장치와 제어센터 사이의 메시지 상호 전달을 위한 프로토콜로 마스터-슬레이브 개념으로 동작	말단 제어기기와 제어시스템 간 정보 교환 및 제어 메시지 전달 예. EMS ↔ RTU	IEC 60870-5	보안기능 없음
ICCP (Inter-Control Center Communications Protocol)	제어센터 간 통신을 위한 응용계층 프로토콜로 서버-클라이언트 개념으로 동작	제어시스템과 변전소 사이의 정보 교환 예. EMS ↔ RCC	IEC 60870-6	보안기능 없음
Modbus	단일 마스터가 여러 개의 하위 클라이언트들을 제어하며, 전형적인 마스터/슬레이브 형태의 폴링(polling)방식 프로토콜	다양한 시설 제어분야에 활용	산업표준	보안기능 없음

보안 기능이 없는 프로토콜을 사용할 경우 공격자가 메시지를 중간에 가로채서 정보를 획득할 수 있고, 가로챈 메시지를 재사용해 잘못된 제어 명령을 내릴 수도 있다. 또한 메시지에 대한 인증 기능을 수행하지 않을 경우 제어 센터의 서버로 가장하여 모든 말단 제어기기들을 공격자 마음대로 제어할 수 있다.

더 나아가 공격에 대한 보호 메커니즘이 존재하지 않으므로 공격자는 말단 제어기기를 가장해 악성 코드를 전송하는 방법을 통해 손쉽게 서버에 침투하여 관리자 권한을 획득할 수 있고, 이는 곧 전체 제어 네트워크를 공격자가 원하는 대로 제어 할 수 있음을 의미한다. 또한 메시지 인증 및 세션 관리를 수행하지 않음으로 인해 공격자에 의한 메시지 플러딩(flooding) 방식의 분산 서비스 거부 공격(Distributed Denial-of-Service attack, DDoS)도 위협의 대상이 된다.

다섯째 보안 위협은 지능형 전력망이 수용하는 전력 생산 주체의 하나인 소규모 분산전원이다. 소규모 분산전원 역시 지능형 전력망에서 전력 생산의 주체로서 역할을 수행하므로 지능형 전력망과 연계되어 운영된다. 현재 원자력 발전, 화력 발전 등의 대형 발전주체들에 대한 제어시스템은 그 중요성과 소수인 관계로 국가적인 관리가 잘 되고 있다. 그러나 소규모 분산전원이 도입되면 많은 수의 분산 전원에 대한 보안 관리가 쉽지 않을 것으로 예상된다. 그러나 이들 소규모 분산 전원 역시 지능형 전력망에 접속되므로, 공격자들이 보안 관리가 미흡한 소규모 분산 전원을 공격한 후 지능형 전력망의 다른 시스템으로 공격을 쉽게 전이할 수 있을 것으로 예상된다.

여섯째 보안 위협은 기존 전력제어시스템이다. 기존 전력제어시스템은 초기 개발단계에서 사이버 보안에 대한 고려 없이 개발 되어 운용되고 있으며, 개발된 시스템의 운용기간이 일반 정보통신 시스템에 비해 상대적으로 길기 때문에 진화하는 사이버 보안에 적절히 대처하기 어렵다. 취약한 전력 제어시스템을 공격할 경우, 공격자는 지능형 전력망에 대한 대부분의 제어권을 확보할 수 있으며 이는 지능형 전력망의 최대 위협이다. 예를 들어 급전소 및 급전분소의 전력 공급 상태를 제어 프로토콜을 변조하여 제어함으로써 특정 지역에 정전사태를 유발하거나, 전국적인 정전 사태를 유발할 수 있다.

기존 전력 제어시스템은 제어시스템과 내부업무망을 연동하여 자료를 송수신하고 있다. 이러한 연동구간은 침입차단시스템과 같은 보안제품을 사용한다고 하더라도 차단 정책 설정 등의 오류 발생 등으로 인해 침입이 발생할 수 있으므로 세심한 관리가 요구된다.

또한 앞에서 설명한바와 같이 제어용 통신 프로토콜에 보안기능이 제공되지 않아서 공격자가 통신 내용을 스니핑하거나 유출할 수 있는 취약점이 있으며, 명령 변조를 통해 악의적인 행위를 수행할 수 있다. 또한 전력망 소프트웨어 자체의 버퍼오버플로우 취약점 등을 공격할 수 있다.

특히 소프트웨어 자체의 취약점은 상용 정보통신 기술을 도입함에 따라 공격자가 별도의 분석 없이 기존 상용 정보통신 시스템에서의 취약점 공격방법을 그대로 활용할 수 있다. 관리적 취약점의 하나로서 전직 직원이나 내부자에 의한 보안 침해 위협도 상존하고 있으며, 이러한 예는 3.1 절에서 설명한 바 있다.

일곱째 보안위협은 지능형 전력망은 다양한 전력 생산 주체, 전력 공급 주체, 전력 소비 주체 사이의 다양한 네트워크가 상호 연동되어 운영되므로, 특정 네트워크로의 침입이 성공한 경우 다른 네트워크 및 중

요한 제어 네트워크로의 침입 전이가 용이할 수 있다. 예를 들어 스마트미터를 장악한 공격자는 스마트미터가 접속하여 정보를 송수신하는 원격자동검침 네트워크내의 시스템을 공격하고, 원격자동검침 네트워크에서 전력 공급을 조절하는 제어시스템이 있는 네트워크로 공격을 전이해 갈 수 있다. 지능형 전력망의 설계 시 침입 전이를 차단하고 보안성을 향상시킬 수 있는 방안을 고려해야 한다.

3.3 지능형 전력망과 사이버보안 전략

지능형 전력망에는 3.2절에서 기술한바와 같이 양방향 통신 서비스, 광범위하게 산재된 단말장치 및 구성 장비, 다양한 전력망간의 연동 증가 등의 원인으로 인하여 현존 전력망보다 더 많은 사이버 보안 위협을 포함하고 있다. 현 전력망에서도 3.1에서 기술한 것과 같은 다양한 침해사고가 발생하고 있으나, 지능형 전력망이 구축되면 이러한 사이버 침해사고는 더욱 증가될 것으로 예상된다. 이러한 지능형 전력망에 대한 사이버 침해사고에 대응하기 위해서는 사이버보안 전략을 수립하여 사업 초기부터 적용함으로써 안전한 지능형 전력망을 확보할 수 있을 것이다.

본 절에서는 지능형 전력망의 사이버 보안 위협을 해소하여 안전하고 신뢰성 있는 지능형 전력망 구축을 위한 사이버보안 전략을 법·제도적 측면, 기술개발 측면과 국제적 협력 측면에 대해 살펴보고자 한다.

3.3.1 법·제도적 측면

지능형 전력망에 대한 사이버 보안 위협을 예방하고 대응하기 위하여 공청회 및 입법예고를 거쳐 내용이 일부 수정된 '스마트그리드 촉진법안'이 2010년 10월 국회에 제출되었다. 스마트그리드 촉진법 조항에는 비록 처벌적 조항으로 충분하지는 않지만 지능형 전력망 정보의 보호 장치가 마련되었다. 법안에는 누구든지 지능형 전력망 정보 중 개인을 식별할 수 있는 정보를 그 개인의 동의 없이 수집하거나 처리할 수 없도록 하고, 지능형 전력망 사업에게는 정보의 안정성과 신뢰성을 보장하기 위한 기술적·관리적 조치를 하도록 의무를 부과하며, 누구든지 정당한 접근권한 없이 지능형 전력망에 침입하거나 정당한 사유없이 지능형 전력망 정보를 조작·파괴·은닉 또는 유출하는 행위등을 금지함으로써 지능형 전력망 사업의 초기 단계부터 사이버 보안을 고려하고 있다.

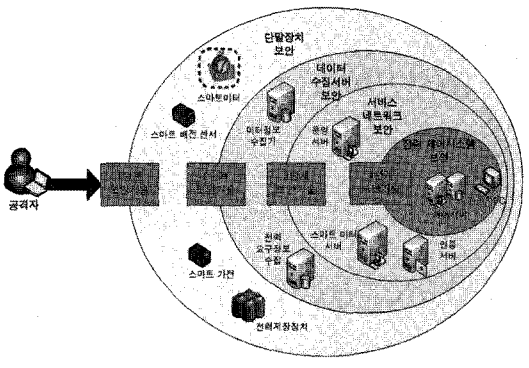
지능형 전력망 기기 등에 대한 인증을 위해서는 안정성 및 상호 운영성을 확보하기 위해 지능형 전력망 기기 및 제품, 서비스 등에 관하여 인증을 할 수 있는 제도적 장치를 마련하고 있다. 즉 인증제도를 통해 기기 및 소프트웨어의 사이버 보안 취약점을 분석하여 사전 조치함으로써 공격자에 의한 지능형 전력망의 사이버 침입을 예방하도록 하고 있다.

지능형 전력망 표준수립과 관련해서는 사이버 보안을 중요요소로 고려하여야 한다. 표준 수립은 향후 국내 지능형 전력망 관련 제품의 국외 수출과 관련되어 있으며, 특히 사이버보안이 고려되지 않은 지능형 전력망 관련 제품은 국외 수출이 어려울 것으로 판단된다. 따라서 향후 국내 지능형 전력망 기본계획 및 시행계획의 수립·시행에 사이버 보안 분야를 우선적으로 고려하여 보안기술이 개발될 수 있도록 해야 한다.

특히 전력 관련 망간의 연동으로 인한 침입 전이를 예방하고 안전한 운영을 위하여 지능형 전력망간의 안전한 연동 가이드라인과 지능형 전력망에 운영되는 모든 시스템을 안전하게 운영할 수 있는 보안 기준인 보안 가이드라인을 개발하여 제시함으로써 지능형 전력망의 보안성을 향상 시킬 수 있도록 해야 한다[50].

3.3.2 기술 개발 측면

지능형 전력망의 사이버 보안을 위한 기술 개발은 가정 등의 말단에 설치되는 단말장치에서 전력을 제어하는 전력 제어시스템까지를 단계별로 구분하여, 각 단계별 위협에 대응할 수 있는 기술 개발을 추진해야 한다. [그림 5]는 지능형 전력망의 단말장치에서 제어시스템까지를 4단계로 구분하여 지능형 전력망의 추진 전략에 맞추어 각 구간에 적합한 보안 기술 개발을 추진하도록 한다.



[그림 5] 지능형 전력망 Defense-in-Depth 보호체계

스마트 미터, 스마트 배전 센서, 스마트 가전, 전력 저장 장치 등으로 구성된 단말장치를 보호하기 위한 1단계 보안기술로는 초경량, 저비용, 다기능의 보안 모듈을 개발하여 인증, 침입차단, 안전한 통신 프로토콜 서비스를 제공하여 공격자가 스마트 기기에 대한 탈취 및 임의 조작을 방지하고, 네트워크 상의 정보 획득을 방지하도록 한다.

미터정보 수집기, 전력 요구정보 수집기 등의 데이터 수집 서버에 대한 보호를 위한 2단계 보안기술은 안전한 지능형 전력망 통신 프로토콜로서 단말장치 및 서비스 네트워크와 데이터 수집 서버간의 안전한 통신 환경을 제공한다. 통신 프로토콜은 지능형 전력망에 최적화된 기밀성, 무결성, 인증기능을 제공함으로써 공격자가 통신 내용의 열람, 과금 정보의 조작, 불법 기기의 통신 접속을 방지하도록 한다.

사용자가 접속하여 정보를 확인할 수 있는 운영서버와 스마트 미터 서버가 있는 지능형 전력망 서비스 네트워크에 대한 보호를 위한 3단계 보안 기술은 인증 및 접근제어 기술이다. 지능형 전력망 장비의 경우 다양하고 광범위한 지역에 분산되어 있어 공격자가 장비를 임의로 네트워크에 설치하고 이를 통해 지능형 전력망으로 접근이 가능하므로, 불법적인 장비의 서비스 네트워크 접근을 방지하고 내부자로부터의 사이버 공격에 대응하기 위한 키관리, 인증 체계, 접근제어 체계를 구축 및 운용하는 기술을 개발해야 한다.

전력 제어시스템이 운영되는 제어망을 보호하기 위한 4단계 보안 기술은 지능형 전력망 서비스 네트워크 보안관제 기술, 일방향 자료 전달 기술, 이상징후 감시 및 제어네트워크 관제 기술, 통신 보호 기술이 요구된다. 지능형 전력망 서비스 네트워크 및 제어 네트워크에 대한 이상징후 감시 및 관제 기술 개발을 통해 지능형 전력망에서 발생하고 있는 사이버 위협 현황을 분석하고 조기에 조치하도록 한다. 또한 제어망과 서비스 망간 안전한 자료 교환을 위한 일방향 자료 전달 기술이 필요하며, 네트워크 구간 사이에서의 소통되는 정보의 무결성, 기밀성, 인증 기능을 제공하여 비인가 장치를 통한 사이버 공격에 대응할 수 있어야 한다.

또한 모든 단계에서 적용 가능한 보안 기술로는 지능형 전력망을 구성할 수 있는 테스트베드를 구축하여, 지능형 전력망에 적용되는 기기 및 소프트웨어에 대한 취약성을 분석하는 기술 개발이 필요하다. 이는 개발된 기기나 소프트웨어의 취약점이 공격자의 침투 경로로 활용되기 때문에 이를 사전에 조치함으로써 공격자의 침투 경로를 제거할 수 있다.

3.3.3 국제 협력적 측면

국내 지능형 전력망의 비전은 세계 최초의 국가단위의 지능형 전력망 구축으로서 이를 통해 지능형 전력망 세계시장을 선점하여 반도체, 조선에 이은 우리나라의 대표산업으로 성장시키고자 하고 있다. 이를 위해서는 지능형 전력망 기술의 선두주자인 미국과 유럽 그리고 지능형 전력망을 개발하는 국가들과 국제적 협력을 통해 국제 표준화를 주도해야 한다.

미국은 2003년 북동부 대정전 이후 전력시스템을 최신화하기 위해 많은 투자를 하고 있으며, 국립표준기술원(NIST, National Institute of Standards and Technology)을 통해 지능형 전력망 상호 운영성 및 보안을 위한 표준개발을 주도하고 있다. NIST에서는 지능형 전력망 전반에 걸친 사이버 보안 강화를 위해 사이버보안 워킹그룹(CSWG, Cyber Security Working Group)을 상시적으로 운영하면서, 보안 기술 표준화에 많은 노력을 경주하고 있다.

유럽연합도 2009년 '유럽연합 명령 441'에 의거해 유럽의 표준화 단체가 지능형 전력망 표준 개발 프로젝트인 OPENmeter을 발표하였다. 발표된 내용에는 보안 위협으로 인가되지 않은 자의 정보접근 및 수정, 권한을 획득한 해커에 의하여 전기, 수도, 가스 등의 차단, 스마트 미터와 미터 데이터 수집기 및 관리 시스템 등에 대한 DDoS공격 등을 정의하고 구체적 보안기술개발 및 표준화 방안 등을 제시하였다[51].

국내에서도 안전하고 성공적인 지능형 전력망 기술 개발 및 표준화를 위해 실행 로드맵을 제시하여 추진하고 있지만, 한 국가가 단독으로 수행하기에는 많은 어려움이 예상된다. 따라서 지능형 전력망 보안 기술 및 표준개발을 주도하는 미국과 유럽 국가들과 기술제휴 와 협력을 적극 추진하고, 국내 전문가 지식 네트워크의 활성화를 통해 사이버 보안에 대한 기술 개발 및 정책 역량을 높여 나가야 한다.

IV. 결 론

본 논문에서는 현재 국가 신성장 동력 사업이자, 향후 환경 문제 해결에 큰 역할을 할 지능형 전력망의 보안 위협을 다 방면에서 분석하고, 이를 해결하기 위한 보안 요소 기술들을 정의하였으며, 지능형 전력망에 사이버 보안을 강화하기 위한 사이버보안 정책 및 전략을 고찰함으로써 다양한 사이버 공격으로부터 안전한 지능형 전력망 구현을 돕고자 하였다. 특히 지능

형 전력망의 성공을 위해서는 법과 제도의 정비, 필요 기술에 대한 개발 그리고 관련 기술의 표준화을 위한 국제 협력이 중요하다는 것을 살펴볼 수 있었다.

전력과 정보통신이 융합된 지능형 전력망에서 보안 전략이 강조되는 이유는 공격자가 네트워크, 제어 시스템 등을 사이버 공격으로 손쉽게 장악할 수 있으며, 이러한 우려가 현실화 될 경우 국가시설에 대한 단순한 해킹 공격이 아닌 국가안보 전체에 큰 위협을 끼치게 되는 사이버 전쟁으로 발전될 수 있다. 전력망이 주요 사이버 공격목표가 될 수 있는 이유는, 상대적으로 손쉬운 해킹 공격으로 한 국가에 전쟁, 대형지진, 쓰나미에 준하는 피해를 야기 시킬 수 있고, 세계 언론과 대중 매체의 집중보도로 국가 신인도를 하락시킬 수 있으며, 그리고 추측이 불가능한 엄청난 경제적 손실을 야기 시킬 수 있기 때문이다.

미국 사이버 영향분석 기관의 수장이며 경제학자인 스콧 보그는 미국 전력망의 1/3이 3개월 정전된다면 카트리나와 같은 대형 허리케인 40~50개가 동시에 강타한 것과 같은 피해를 입게될 것이라고 밝힌바 있다. 따라서 이러한 재앙 수준의 피해를 예방하기 위해서는 지능형 전력망 구축에 있어 보안 정책 및 기술은 반드시 함께 구현되어야 한다.

지능형 전력망은 향후 기술적 측면에서 많은 발전이 이루어질 것으로 예상되기 때문에 사이버침해 기술 발전에 선제적으로 대응할 수 있는 보안기술 개발 및 정책수립은 매우 중요하다고 할 수 있다. 본 논문은 지능형 전력망 보안 연구의 초석을 다지는 계기가 될 것이며, 나아가 이를 통해 안전한 지능형 전력망 환경이 구현된다면 향후 한국형 지능형 전력망 기술은 세계 경쟁에서 우위를 점하게 될 것이다.

참고문헌

[1] U.S. Department of Energy, "The Smart Grid: An Introduction," *DoE Report*, pp.10-12, Apr. 2009

[2] U.S. Department of Energy, "Grid 2030: A National Vision for Electricity's Second 100 Years," *DoE Report*, pp.17, Jul. 2003.

[3] K. Moslehi, A.B.R. Kumar, H.D. Chiang, M. Laufenberg, A. Bose, P. Hirsch, and L. Beard, "Control Approach for Self-Healing Power Systems: A Conceptual Overview," *Conference Proceeding*, Carnegie Mellon University, pp.1-3, Dec. 2004.

[4] S. Borenstein, M. Jaske, and A. Rosenfeld, "Dynamic Pricing, Advanced Metering, and Demand Response in Electricity Markets," *Report*, University of California Energy Institute, pp.39-41, Oct. 2002.

[5] National Energy Technology Laboratory(NETL) for the U.S Department of Energy, "A Vision for the Modern Grid," *NETL Report*, pp.5, Mar. 2007.

[6] 이창훈, "스마트그리드 촉진법에 관한 입법학적 고찰," 한국전기산업연구원(자체성과과제, 2010-02), pp.1-19, 2010년 12월

[7] E.W. Gunther, A. Snyder, G. Gilchrist, and D. R. Highfill, "Smart Grid Standards Assessment and Recommendations for Adoption and Development," *EnerNex Corporation Report*, pp.9-12, Feb. 2009

[8] 안기봉·한태환, "스마트그리드(지능형 전력망)와 스마트 세대분전반," 조명·전기설비 학회지 제23권 제4호, pp.2-4, 2009년 8월

[9] UK Department of Trad and Industry, "Meeting the Energy Challenge: A White Paper on Energy," *DTI Report*, pp.14-15, May 2007.

[10] J. Tomic and W. Kempton, "Using Fleets of Electric-drive Vehicles for Grid Support," *Journal of Power Sources*, Elsevier, Vol. 168, Iss. 2, pp.459-468, Jun. 2007.

[11] 박남제·안길준, "스마트 그리드에서의 프라이버시 보호," 정보보호학회지 20(3), pp.64-65, 2010년 6월

[12] [12] A. Battaglini, J. Lilliestam, C. Bals, and A. Haas, "The SuperSmart Grid," *Report*, European Climate Forum, pp.5-7, Jun. 2008.

[13] K.R. Nahingian, "The Smart Alternative: Securing and Strengthening Our Nation's Vulnerable Electric Grid," *Report*, The Reform Institute, pp.3-7, Jun. 2008

[14] Smart Grid: Fewer Blackouts, More Greenbacks For The Northwest http://www.electricnet.com/article.mvc/Smart-Grid-Fewer-Blactouts-More-Greenbacks-Fo-0001
[15] 지식경제부 보도자료, '스마트그리드 국가로드맵', 2010년 1월
[16] P. Haase, "IntelliGrid: A Smart Network of Power," *EPRI Journal*, pp.27-32, Fall 2005
[17] L.D. Kannberg, D.P. Chassin, J.G. DeSteese, S.G. Hauser, M.C. Kintner-Meyer, R.G. Pratt, L.A. Schienbein, and W.M. Warwick, "GridWise™: The Benefits of a Transformed Energy System," *Report*, Pacific Northwest National Laboratory, pp.11-23, Sep. 2003
[18] Xcel Energy Inc., "Xcel Energy Smart Grid," *White Paper*, pp.9-12, Feb. 2008.
[19] CITRIS(Center for Information Technology Research in Internet Society), http://www.citris-uc.org/
[20] Power and Energy Systems/Department of Electrical & Computer Engineering http://energy. ece.illinois.edu/
[21] 전력IT 사업단(한국스마트그리드사업단으로 개편), http://www.smartgrid.or.kr
[22] 한국에너지자원기술기획평가원, "Grid2030 vision", 보고서, pp.3-5, 2009년 4월 http://www.oe.energy.gov/smartgrid.htm
[23] National Energy Technology Laboratory(NETL) for the U.S Department of Energy, "The Modern Grid Strategy", *NTEL Report*, pp.2-5, Aug. 2009
[24] F. Sissine, "Energy Independence and Security Act of 2007: A Summary of Major Provisions," *CRS Report for Congress*, Dec. 2007.
[25] European Commission, "European Technology Platform SmartGrids: Vision and Strategy for Europe's Electricity Networks of the Future", *EU Report*, EUR 22040, pp.6-7, Apr. 2006
[26] European Commission, "European Technology Platform SmartGrids: Strategic Research Agenda for Europe's Electricity Networks of the Future", *EU Report*, EUR 22580, pp.29-71, Apr. 2007
[27] 녹색성장위원회, 녹색성장 국가전략 및 5개년계획, pp.21-26, 2009년 7월
[28] 최재덕·서정택·이철원, "제주 스마트그리드 실증단지 보안대책 현황," 정보보호학회지 20(5), pp.14-18, 2010년 10월
[29] http://www.forbes.com/2007/08/22/scada-hackers-inrastructure-tech-security-cx_ag_0822hack.html
[30] Critical infrastructure protection: Challenges and efforts to secure control systems(GAO-04-354). GAO(Government Accountability Office), *Report*, May 2004
[31] TVA Power Plants Vulnerable to Cyber Attacks, GAO Finds http://www.washingtonpost.com/wp-dyn/content/article/2008/05/20/AR2008052002354.html
[32] Mouse click could plunge city into darkness, experts say http://edition.cnn.com/2007/US/09/27/power.at.risk/index.html
[33] Cyber Incident Blamed for Nuclear Power Plant Shutdown http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html
[34] CIA: Hackers demanding cash disrupted power http://www.msnbc.msn.com/id/22734229/
[35] Electric Utilities May Be Vulnerable to Cyberattack http://www.washingtonpost.com/wp-dyn/content/article/2009/04/08/AR2009040803904.html?referrer=emailarticle
[36] Electricity Grid in U.S. Penetrated By Spies http://online.wsj.com/article/SB-123914805204099085.html
[37] http://www.etnews.co.kr/news/detail.html?id=200903240003
[38] http://www.wired.com/threatlevel/2009/05/efh/
[39] http://www.economi.co.kr/bbs/board.php?bo_table=NI001&wr_id=302

[40] 지식경제부 사이버안전센터, 연간 침해사고 탐지 현황 자료, 2011년 3월
[41] 이경복·독고지은·유지연·이숙연·임종인, "스마트 그리드에서의 소비자 참여와 보안 이슈," 정보보호학회지 19(4), pp.25-30, 2009년 8월
[42] M. Abrams and J. Weiss, "Malicious Control System Cyber Security Attack Case Study - Maroochy Water Services, Australia," *Report*, NIST Computer Security Division, pp.2-12, Aug. 2008.
[43] Juniper Networks Inc., "Architecture for Secure SCADA and Distributed Control System Networks," *White Paper*, pp.2-9, Feb. 2009.
[44] Y. Wang and B.T. Chu, "sSCADA: Securing SCADA Infrastructure Communications," *Cryptology ePrint Archive*, pp.1-12, Aug. 2004.
[45] R.J. Robles, M. Choi, E. Cho, S. Kim, G. Park, and S. Yeo, "Vulnerabilities in SCADA and Critical Infrastructure Systems," *International Journal of Future Generation Communication and Networking*, pp.99-104, Dec. 2008.
[46] US-CERT, "Control Systems Security Program - Vulnerability Notes," 2009, http://www.us-cert.gov/control_systems/csdocuments.html.
[47] DNP Users Group, "A DNP3 Protocol Primer", *Report*, pp.1-7, Mar. 2005.
[48] IEC TC57 WG7, "Telecontrol Equipment and Systems - Part 6-505: Telecontrol Protocols Compatible with ISO Standards and ITU-T Recommendations - TASE.2 User Guide," *IEC TR 60870-6-505*, Dec. 2006.
[49] Modbus IDA, "Modbus Application Protocol Specification V1.1b," *Report*, pp.3-12, Dec. 2006.
[50] [50] 이명훈·배시화·손성용, "전력IT기반 파워그리드 실증 보안 체계 설계," 한국해양정보통신학회 논문지 14(11), pp.2498-2504, 2010년 12월
[51] 이건희·서정택·이철원, "스마트그리드 사이버 보안 추진 현황," 정보보호학회지 20(5), pp.9-11, 2010년 10월

〈著者紹介〉

이 상 근 (Lee, Sang Keun) 종신회원
1991년 4월: 독일 베를린자유대학교 졸업
1996년 6월: 독일 베를린자유대학교 석사
2001년 2월: 독일 베를린자유대학교 박사
2004년 10월~2010년 2월: 지식경제부 정보화담당관
2010년 3월~현재: 한국산업기술진흥원 경영기획본부장
〈관심분야〉 사이버보안, 정보보호, 국제경영